ВЕСТНИК

Воронежского института МВД России

№ 2 / 2026

Учредитель — Федеральное государственное казенное образовательное учреждение высшего образования «Воронежский институт Министерства внутренних дел Российской Федерации».

Журнал зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций. Реестровая запись 27.01.2022 серия ПИ № ФС77-82578.

Журнал входит в перечень изданий, рекомендованных ВАК при Минобрнауки России для опубликования результатов диссертаций на соискание ученой степени доктора и кандидата наук, по 10 научным специальностям: 2.2.13. Радиотехника, в том числе системы и устройства телевидения (технические науки); 2.2.14. Антенны, СВЧ-устройства и их технологии (технические науки); 2.2.15. Системы, сети и устройства телекоммуникаций (технические науки); 2.3.1. Системный анализ, управление и обработка информации (технические науки); 2.3.4. Управление в организационных системах (технические науки); 1.2.2. Математическое моделирование, численные методы и комплексы программ (технические науки); 2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки); 5.1.1. Теоретико-исторические правовые науки (юридические науки); 5.1.2. Публично-правовые науки (юридические науки); 5.1.4. Уголовно-правовые науки (юридические науки).

При полной или частичной перепечатке или воспроизведении любым способом ссылка на источник обязательна.

Редакционная коллегия

Председатель: **А. П. Нахимов**, начальник Воронежского института МВД России, кандидат философских наук;
Заместитель председателя: С. В. Родин, заместитель начальника Воронежского института МВД России по научной работе, кандидат технических наук, доцент;
В. В. Алексеев, профессор кафедры информационных систем и защиты информации Тамбовского государственного технического университета, доктор технических наук, профессор;
В. А. Ананич, профессор кафедры уголовно-исполнительного права и криминологии уголовно-исполнительного факультета Академии Министерства внутренних дел Республики Беларусь, доктор исторических наук, кандидат юридических наук, профессор;
В. В. Гриценко, профессор кафедры административного и административного процессуального права Воронежского государственного университета, доктор юридических наук, профессор;
Т. Д. Зражевская, профессор кафедры конституционного и муниципального права Воронежского государственного университета, доктор юридических наук, профессор;
А. В. Калач, начальник кафедры безопасности информации и защиты сведений, составляющих государственную тайну Воронежского института ФСИН России, доктор химических наук, профессор;
А. И. Климов, профессор кафедры инфокоммуникационных систем и технологий Воронежского института МВД России, доктор технических наук, профессор;
М. А. Кожевина, профессор кафедры теории и истории права и государства Омской академии МВД России, доктор юридических наук, профессор;
С. Я. Лебедев, заведующий кафедрой уголовного права и адвокатуры Российского государственного университета им. А. Н. Косыгина, доктор юридических наук, профессор;
В. А. Лелеков, профессор кафедры уголовно-исполнительного и уголовного права Воронежского института ФСИН России, доктор юридических наук, профессор;
С. П. Матвеев, профессор кафедры административного и административного процессуального права Воронежского государственного университета, доктор юридических наук, доцент;
В. В. Меньших, профессор кафедры математики и моделирования систем Воронежского института МВД России, доктор физико-математических наук, профессор;
В. А. Мещеряков, заведующий кафедрой судебной экспертизы и криминалистики Центрального филиала Российского государственного университета правосудия им. В.М. Лебедева (г. Воронеж), доктор юридических наук, профессор;
Т. В. Мещерякова, начальник кафедры автоматизированных информационных систем органов внутренних дел Воронежского института МВД России, доктор технических наук, профессор;
И. А. Насонова, профессор кафедры уголовного процесса Воронежского института МВД России, доктор юридических наук, профессор;
А. С. Овчинский, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий Московского университета МВД России им. В. Я. Кикотя, доктор технических наук, профессор;
А. Л. Осипенко, заместитель начальника Краснодарского университета МВД России по научной работе, доктор юридических наук, профессор;
А. В. Останков, заведующий кафедрой радиотехники Воронежского государственного технического университета, доктор технических наук, доцент;

К. К. Панько, профессор кафедры уголовного права Воронежского государственного университета, доктор юридических наук, доцент;
Ю. Г. Пастернак, профессор кафедры радиоэлектронных устройств и систем Воронежского государственного технического университета, доктор технических наук, профессор;
О. В. Пьянков, заместитель начальника кафедры инфокоммуникационных систем и технологий Воронежского института МВД России, доктор технических наук, профессор;
Н. В. Рябова, заведующий кафедрой радиотехники и связи Поволжского государственного технологического университета, доктор физико-математических наук, профессор;
Е. В. Сафронова, профессор кафедры конституционного и международного права юридического института Белгородского государственного национального исследовательского университета, доктор юридических наук, профессор;
А. Б. Сизоненко, профессор кафедры Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С. М. Штеменко Министерства обороны Российской Федерации, доктор технических наук, профессор;
Ю. В. Сорокина, профессор кафедры теории и истории государства и права Воронежского государственного университета, доктор юридических наук, профессор;
Ю. Н. Старилов, ректор Воронежского государственного университета, доктор юридических наук, профессор;
В. И. Сумин, профессор кафедры вычислительной техники и информационных систем Воронежского государственного лесотехнического университета им. Г. Ф. Морозова, доктор технических наук, профессор;
Н. М. Тихомиров, начальник научно-технического управления АО «Концерн «Созвездие», доктор технических наук, старший научный сотрудник;
А. Б. Токарев, профессор кафедры радиотехники Воронежского государственного технического университета, доктор технических наук, доцент;
З. С. Токубаев, профессор кафедры уголовного права и криминологии Карагандинской академии МВД Республики Казахстан имени Баримбека Бейсенова, доктор юридических наук, профессор;
В. В. Трухачев, профессор кафедры уголовного права Воронежского государственного университета, доктор юридических наук, профессор;
И. С. Федотов, судья Воронежского областного суда, доктор юридических наук, доцент;
Н. С. Хохлов, профессор кафедры инфокоммуникационных систем и технологий Воронежского института МВД России, доктор технических наук, профессор;
О. Н. Чопоров, проректор по цифровой трансформации Воронежского государственного медицинского университета им. Н. Н. Бурденко, доктор технических наук, профессор;
В. Б. Шабанов, заведующий кафедрой криминалистики Белорусского государственного университета, доктор юридических наук, профессор;
Н. А. Шишкин, заместитель Генерального прокурора Российской Федерации, кандидат юридических наук;
Ю. К. Язов, старший научный сотрудник Государственного научно-исследовательского испытательного института проблем технической защиты информации Федеральной службы по техническому и экспортному контролю, доктор технических наук, профессор

Редакция

С. В. Родин — главный редактор;
В. Ю. Калинская, Н. Ф. Палихова — редакторы;
С. М. Шапиро — верстка номера

Подписано в печать 25.06.2026
Выход в свет 30.06.2026
Формат 60x84 1/8
Усл. печ. л. 36,27
Гарнитура Таймс Новая
Печать офсетная
Бумага офсетная
Тираж 200 экз.
Цена свободная

Оформить подписку на журнал.
www.pressa-rf.ru/cat/1/edition/t45898/
Подписной индекс 45898
Адрес редакции, издателя, типографии:
394065, Воронеж,
проспект Патриотов, 53
Тел./факс (473) 264-92-00
E-mail: vestnik_vimvd@mail.ru
https://ВИ.МВД.РФ/Nauka/nauchnij-zhurnal-vestnik
ISSN 2071-3584
© Воронежский институт МВД России, 2026

VESTNIK

of Voronezh Institute of the Ministry of the Interior of Russia

№ 2 / 2026

The founder of the journal is Federal state-owned public educational institution "Voronezh Institute of the Ministry of the Interior of Russia".

The journal is registered with the Federal Service for Supervision of Communications, Information Technology and Mass Media. Registry entry 27.01.2022 PI series No. FS77-82578.

This peer-reviewed journal is included into the list of periodicals recommended by the Higher Attestation Commission of the Ministry of Science and Education of the Russian Federation for publishing doctoral and PhD research results on 10 scientific specialities: 2.2.13. Radiotechnics, Including Television Systems and Devices (Technical Sciences); 2.2.14. Antennas, Microwave Devices and Technologies (Technical Sciences); 2.2.15. Systems, Networks and Telecommunication Devices (Technical Sciences); 2.3.1. System Analysis, Information Control and Processing (Technical Sciences); 2.3.4. Management in Organizational Systems (Technical Sciences); 1.2.2. Mathematical Modeling, Numerical Methods and Programme Systems (Technical Sciences); 2.3.6. Methods and Systems of Data Protection, Information Security (Technical Sciences); 5.1.1. Theoretical and Historical Legal Sciences (Legal Sciences); 5.1.2. Public Law Sciences (Legal Sciences); 5.1.4. Criminal Law Sciences (Legal Sciences).

Citation of reference sources is obligatory in case of reprint or reproduction by any means.

Editorial board

***Editor-in-chief*: A. P. Nakhimov**, Head of Voronezh Institute of the Ministry of the Interior of Russia, PhD in Philosophy;
***Deputy Editor-in-chief*: S. V. Rodin,** Deputy Head of Voronezh Institute of the Ministry of the Interior of Russia for Scientific Work, Candidate of Technical Sciences, Associate Professor;
V. V. Alekseev, Professor of the Chair of Information Systems and Information Security of Tambov State Technical University, Doctor of Technical Sciences, Professor;
V. A. Ananich, Professor of the Chair of Penal Enforcement Law and Criminology of the Penal Enforcement Faculty of Academy of the Ministry of Internal Affairs of the Republic of Belarus, Doctor of Historical Sciences, Candidate of Legal Sciences, Professor;
V. V. Gritsenko, Professor of the Chair of Administrative and Administrative Procedural Law of Voronezh State University, Doctor of Law, Professor;
T. D. Zrazhevskaya, Professor of the Chair of Constitutional and Municipal Law of Voronezh State University, Doctor of Law, Professor;
A. V. Kalach, Head of the Chair of Information Security and Protection of Information Constituting a State Secret of Voronezh Institute of the Federal Penitentiary Service of Russia, Doctor of Chemical Sciences, Professor;
A. I. Klimov, Professor of the Chair of Infocommunication Systems and Technologies of Voronezh Institute of the Ministry of the Interior of Russia, Doctor of Technical Sciences, Professor;
M. A. Kozhevina, Professor of the Chair of Theory and History of Law and State of Omsk Academy of the Ministry of the Interior of Russia, Doctor of Law, Professor;
S. Ya. Lebedev, Chief of the Chair of Criminal Law and Advocacy of A. N. Kosygin Russian State University, Doctor of Law, Professor;
V. A. Lelekov, Professor of the Chair of Penitentiary and Criminal Law of Voronezh Institute of the Russian Federal Penitentiary Service, Doctor of Law, Professor;
S. P. Matveev, Professor of the Chair of Administrative and Administrative Procedural Law Voronezh State University, Doctor of Law, Associate Professor;
V. V. Menshikh, Professor of the Chair of Mathematics and Systems Modelling of Voronezh Institute of the Ministry of the Interior of Russia, Doctor of Physical and Mathematical Sciences, Professor;
V. A. Meshheryakov, Head of the Chair of Forensic Examination and Criminology of Central Branch of the Russian State University of Justice named after V. M. Lebedeva (Voronezh), Doctor of Law, Professor;
T. V. Meshheryakova, Head of the Chair of Automated Information Systems of Internal Affairs Bodies of the Voronezh Institute of the Ministry of the Interior of Russia, Doctor of Technical Sciences, Professor;
I. A. Nasonova, Professor of the Chair of Criminal Proceeding of Voronezh Institute of the Ministry of the Interior of Russia, Doctor of Law, Professor;
A. S. Ovchinskiy, Professor of Information Security Chair of the Academic Training Complex of Information Technologies of Moscow University of the Ministry of the Interior of Russia named after V. Ya. Kikot, Doctor of Technical Sciences, Professor;

A. L. Osipenko, Deputy Head of the Krasnodar University of the Ministry of Internal Affairs of Russia for scientific work, Doctor of Law, Professor;
A. V. Ostankov, Chief of the Chair of Radio Engineering of Voronezh State Technical University, Doctor of Technical Sciences, Associate Professor;
K. K. Panko, Professor of the Chair of Criminal Law of Voronezh State University, Doctor of Law, Associate Professor;
Yu. G. Pasternak, Professor of the Chair of Electronic Devices and Systems of Voronezh State Technical University, Doctor of Technical Sciences, Professor;
O. V. Pyankov, Deputy Head of the Chair of Infocommunication Systems and Technologies of Voronezh Institute of the Ministry of the Interior of Russia, Doctor of Technical Sciences, Professor;
N. V. Ryabova, Head of the Chair of Radio Engineering and Communication of Volga State University of Technology, Doctor of Physical and Mathematical Sciences, Professor;
E. V. Safronova, Professor of the Chair of Constitutional and International Law of Belgorod State National Research University Law Institute, Doctor of Law, Professor;
A. B. Sizonenko, Professor of the Chair of the Krasnodar Higher Military Orders of Zhukov and the October Revolution of the Red Banner School named after Army General S. M. Shtemenko Ministry of Defense of the Russian Federation, Doctor of Technical Sciences, Professor;
Yu. V. Sorokina, Professor of the Chair of Theory and History of State and Law of Voronezh State University, Doctor of Law, Professor;
Yu. N. Starilov, Rector of Voronezh State University, Doctor of Law, Professor;
V. I. Sumin, Professor of the Chair of Computer Science and Information Systems of Voronezh State Forest Engineering University named after G. F. Morozov, Doctor of Technical Sciences, Professor;
N. M. Tikhomirov, Head of Department of the Joint-stock Company «Concern «Sozvezdie», Doctor of Technical Sciences, Senior Scientific Employee;
A. B. Tokarev, Professor of the Chair of Radio Engineering of Voronezh State Technical University, Doctor of Technical Sciences, Associate Professor;
Z. S. Tokubaev, Professor of the Chair t of Criminal Law and Criminology of the Karaganda Academy Ministry of Internal Affairs of the Republic of Kazakhstan named after Barimbek Beisenov, Doctor of Law, Professor;
V. V. Trukhachev, Professor of the Chair of Criminal Law of Voronezh State University, Doctor of Law, Professor;
I. S. Fedotov, Judge of the Voronezh regional court, Doctor of Law, Associate Professor;
N. S. Khokhlov, Professor of the Chair of Infocommunication Systems and Technologies of Voronezh Institute of the Ministry of the Interior of Russia, Doctor of Technical Sciences, Professor;
O. N. Choporov, Vice-Rector for Digital Transformation of Voronezh State Medical University named after N. N. Burdenko, Doctor of Technical Sciences, Professor;
V. B. Shabanov, Chief of the Chair of Criminalistics of Belarusian State University, Doctor of Law, Professor;
N. A. Shishkin, Deputy Prosecutor General of the Russian Federation, PhD in Law;
Yu. K. Yazov, Senior Researcher of State Research and Testing Institute of Problems of Technical Protection of Information of the Federal Service for Technical and Export control, Doctor of Technical Sciences, Professor

***Editorial Staff*:**
S. V. Rodin — Chief Editor;
V. Yu. Kalinskaya, N. F. Palikhova — Editors;
S. M. Shapiro — Layout Designer

Passed for printing on June 25th, 2026
Data of edition June 30th, 2026
Format 60x84 1/8
Conventional printed sheets 36,27
Times New Font
Offset printing
Offset paper
Issue 200 copies
Uncontrolled price

Subscribe to the magazine.
www.pressa-rf.ru/cat/1/edition/t45898/
Subscription index 45898
Address of Editors Office, Publisher, Printing Office:
394065, Voronezh, Prospect Patriotov, 53.
Tel./fax (473) 264-92-00
E-mail: vestnik_vimvd@mail.ru
https://ВИ.МВД.РФ/Nauka/nauchnij-zhurnal-vestnik
ISSN 2071-3584
© Voronezh Institute of the Ministry of the Interior of Russia, 2026

СОДЕРЖАНИЕ

МВД РОССИИ: ПРОШЛОЕ, НАСТОЯЩЕЕ, БУДУЩЕЕ

Нахимов А. П., Кирнос А. В., Колесников В. А. Воронежская городская милиция в конце первого десятилетия советской власти: организация и функциональное состояние (по материалам инспекторских обследований в марте 1927 г.).....9

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Дровникова И. Г., Тужикова Т. Ю. Вербальная модель процесса реализации угроз безопасности информации в автоматизированных системах органов внутренних дел с использованием фейковых сайтов 21
Ланкин О. В., Застрожнов И. И., Попов А. Д. Моделирование процессов утечки и восстановления информации в системах защиты информации.....35
Лоскутова А. Е., Алейникова Н. А., Матвеев М. Г. Автоматизация мониторинга и управления качеством образовательного процесса..... 46
Меньших В. В., Никитенко А. Н. Численный метод и алгоритм максимизации полезности функционирования децентрализованных мультиагентных систем..... 60
Пьянков О. В., Казанцева Е. А. Разработка методики анализа и прогнозирования потребностей образовательных организаций МВД России в технических средствах обучения 71
Власенко А. В., Назаров А. К. Асимптотический анализ одной модели эпидемии в компьютерных сетях с быстроосциллирующими параметрами 81
Гудков М. А., Гапеев А. А., Мещеряков А. В., Герасименко Е. С. Интегративный подход к оценке качества образовательных программ 88
Зверева Д. Д. Динамические модели изменения пропускной способности транспортной сети при деградации и восстановлении каналов 99
Звягин Д. С., Пименова О. В. Особенности использования индикаторов поля и частотомеров при обеспечении безопасности конфиденциальной информации 108
Телков А. Ю., Жуков М. М., Полухин Д. И. Защищенный маршрутизатор с поддержкой L3 VPN и многофакторной аутентификации на базе Astra Linux SE в сценариях применения «сеть-сеть» и «сеть-пользователь» 116
Терентьев А. А., Пославская В. Я. Алгоритм расчета индекса эффективности экспертно-криминалистического центра органов внутренних дел 132

РАДИОТЕХНИКА И СВЯЗЬ

Радченко Ю. С., Овчинникова Т. М., Удалов В. П. Обработка сложных сигналов с неизвестным законом модуляции в антенной решетке на основе анализа собственных значений.....144
Антиликаторов А. Б., Алексеенко С. П., Чирков О. Н. Методика сравнительного анализа точности восстановления канала связи в OFDM системах на основе алгоритмов глубокого обучения.....154

ЮРИДИЧЕСКИЕ НАУКИ

Денисенко В. В. Цифровая трансформация публичного управления в сфере миграции: правовые проблемы и перспективы.....165
Насонов А. А. О перспективах развития уголовно-процессуального института согласия.....170

Насонова И. А. Принцип свободы оценки доказательств
и проблемы его правовой регламентации 174
Ахмедов У. Н. Особенности приобретения несовершеннолетними
уголовно-процессуального статуса, его изменение и динамика
в российском уголовном судопроизводстве.....178
Белоусова А. Н., Запорожцева Е. А. Особенности использования интернет-сервисов
размещения объявлений для вовлечения несовершеннолетних
в мошеннические действия.....185
Буданова Е. А., Шикалова Э. Р. Криминологический анализ
современного экстремизма: традиционные и цифровые формы проявления 191
Колесников Р. В., Юрьева Я. В. Публичные призывы к осуществлению
экстремистской деятельности с использованием СМИ
либо информационно-телекоммуникационных сетей, в том числе сети Интернет:
понятие, вопросы квалификации и судебная практика 198
Коник А. А. Административно-правовое регулирование и инновационные подходы
к применению беспилотных воздушных судов
в деятельности органов внутренних дел Российской Федерации 207
Можаева С. Ю., Полякова Н. В. О некоторых особенностях
проведения доследственных проверок по сообщениям о преступлениях,
предусмотренных статьей 314.1 Уголовного кодекса Российской Федерации 214
Новикова Е. П., Гетманова Л. А. Расстрелы в школе (скулшутинг):
история, причины, профилактика.....221
Пидусов Е. А. Факторы, способствующие совершению мошенничеств
с использованием средств телекоммуникации.....227
Пучнин А. В., Польшиков А. В., Демидова О. В. Комплексный подход
к ранней профилактике вовлечения несовершеннолетних
в диверсионную и террористическую деятельность 232
Пучнина М. Ю., Безуглая У. В. Криминологическая характеристика
современного терроризма: вооруженное насилие, скулшутинг, цифровая вербовка 240
Азарова И. В. Криминологический портрет лица, совершившего мошенничество
при получении выплат.....247
Волкодавова Г. Н. Институт руководителя в системе МВД России:
нравственный аспект профессиональной деятельности.....255
Кочкина М. С. Стелсинг как форма сексуализированного и репродуктивного насилия 262
Курашова М. М. Вопросы этико-правового регулирования
цифровой трансформации публичного управления.....268
Сенцов В. В. Уголовно-правовая характеристика фиктивной регистрации
и постановки на учет иностранных граждан и лиц без гражданства:
проблемы теории и практики 274
Сидорова Е. И. Следственная группа как оптимальная
организационная форма взаимодействия следователя с оперативными подразделениями
при расследовании преступлений.....280
Смагин П. Г. Цифровой рубль как инструмент противодействия
финансовым преступлениям: перспективы и ограничения.....286
Чачхиани М. Н. Систематизация деятельности в области превенции
незаконного оборота наркотических средств и психотропных веществ 292
Чунихина Е. И. Административная ответственность
в системе средств противодействия распространению информации,
посягающей на традиционные российские духовно-нравственные ценности.....299

Информация для авторов.....307

CONTENTS

RUSSIAN MINISTRY OF INTERIOR: PAST, PRESENT, FUTURE

Nakhimov A. P., Kirnos A. V., Kolesnikov V. A. Voronezh city police at the end of the first decade of soviet power: organization and functional status (based on inspection surveys in march 1927) 9

INFORMATICS, COMPUTER ENGINEERING AND AUTOMATIC

Drovnikova I. G., Tuzhikova T. Yu. Verbal model of the process of implementing information security threats in automated systems of internal affairs bodies using fake sites 21
Lankin O. V., Zastrozhnov I. I., Popov A. D. Modeling of information leakage and recovery processes in security systems 35
Loskutova A. E., Aleynikova N. A., Matveev M. G. Automation of monitoring and management of the educational process quality 46
Menshikh V. V., Nikitenko A. N. Numerical method and algorithm for maximizing the utility function of decentralized multi-agent systems 60
Pyankov O. V., Kazantseva E. A. Development of a methodology for analyzing and forecasting the needs of educational organizations of the ministry of internal affairs of Russia in technical training facilities 71
Vlasenko A. V., Nazarov A. K. Asymptotic analysis of a model of epidemics in computer networks with fast-oscillating parameters 81
Gudkov M. A., Gapeev A. A., Meshcheryakov A. V., Gerasimenko E. S. Integrative approach to assessing the quality of educational programs 88
Zvereva D. D. Dynamic models of transport network capacity change under channel degradation and recovery 99
Zvyagin D. S., Pimenova O. V. Features of using field indicators and frequency meters in implementing security of confidential information 108
Telkov A. Yu., Zhukov M. M., Polukhin D. I. Secure router with L3 VPN and multifactor authentication support based on Astra Linux SE for network-to-network and network-to-user application scenarios 116
Terentyev A. A., Poslavskaya V. Ya. Algorithm for calculating the efficiency index of the expert criminalistic center of the internal affairs bodies 132

RADIOENGINEERING AND COMMUNICATION

Radchenko Yu. S., Ovchinnikova T. M., Udalov V. P. Processing complex signals with unknown modulation law in an antenna array based on eigenvalue analysis 144
Antilikatorov A. B., Alekseenko S. P., Chirkov O. N. Method for comparative analysis of the accuracy of recovery of the communication channel in OFDM systems based on deep learning algorithms 154

LEGAL SCIENCES

Denisenko V. V. Digital transformation of public governance in migration: legal challenges and perspectives 165
Nasonov A. A. On the prospects for the development of the criminal procedure institute of consent 170

Nasonova I. A. The principle of freedom of evidence assessment and the problems of its legal regulation 174
Akhmedov U. N. Peculiarities of granting minors the criminal procedural status, its change and dynamics in Russian criminal proceedings 178
Belousova A. N., Zaporozhtseva E. A. Features of using internet advertising services to involve minors in fraudulent activities 185
Budanova E. A., Shikalova E. R. Criminological analysis of modern extremism: traditional and digital forms of manifestation 191
Kolesnikov R. V., Yuryeva Ya. V. Public calls to carry out extremist activities using the media or information and telecommunication networks, including the internet: concept, qualification issues, and court practice 198
Konik A. A. Administrative and legal regulation and innovative approaches to the use of unmanned aerial vehicles in the activities of the internal affairs agencies of the Russian Federation 207
Mozhaeva S. Yu., Polyakova N. V. About some of the features of the event pre-investigation checks based on reports on crimes provided for in article 314.1 the Criminal Code of the Russian Federation 214
Novikova E. P., Getmanova L. A. School shootings: history, causes, prevention 221
Pidusov E. A. Factors contributing to the commission of fraudulent acts using telecommunications 227
Puchnin A. V., Polshikov A. V., Demidova O. V. A comprehensive approach to early prevention of involvement of minors in subversion and terrorist activities 232
Puchnina M. Yu., Bezuglaya U. V. Criminological characteristics of modern terrorism: armed violence, school shooting, digital recruitment 240
Azarova I. V. Criminological portrait of a person who committed fraudulent acts in order to receive payments 247
Volkodavova G. N. Institute of leadership in the system of the ministry of internal affairs of Russia: the moral aspect of professional activities 255
Kochkina M. S. Stealthing as a form of sexualized and reproductive violence 262
Kurashova M. M. Towards a philosophy of ethical and legal regulation of digital transformation of public administration 268
Sentsov V. V. Criminal and legal characteristics of fictitious registration and accounting of foreign citizens and stateless persons: problems of theory and practice 274
Sidorova E. I. Investigative team as an optimal organizational form of interaction between an investigator and operational units in the investigation of crimes 280
Smagin P. G. The digital ruble as a tool for countering financial crimes: prospects and limitations 286
Chachkhiani M. N. Systematization of activities in the field of prevention of illicit trafficking in narcotic drugs and psychotropic substances 292
Chunikhina E. I. Administrative responsibility in the system of means of countering the dissemination of information that encroaches on traditional Russian spiritual and moral values 299

Information for authors 307

МВД РОССИИ: ПРОШЛОЕ, НАСТОЯЩЕЕ, БУДУЩЕЕ

А. П. Нахимов, *кандидат философских наук*
А. В. Кирнос, *кандидат политических наук, доцент*
В. А. Колесников, *кандидат политических наук, доцент*

ВОРОНЕЖСКАЯ ГОРОДСКАЯ МИЛИЦИЯ В КОНЦЕ ПЕРВОГО ДЕСЯТИЛЕТИЯ СОВЕТСКОЙ ВЛАСТИ: ОРГАНИЗАЦИЯ И ФУНКЦИОНАЛЬНОЕ СОСТОЯНИЕ (по материалам инспекторских обследований в марте 1927 г.)

VORONEZH CITY POLICE AT THE END OF THE FIRST DECADE OF SOVIET POWER: ORGANIZATION AND FUNCTIONAL STATUS (based on inspection surveys in march 1927)

В статье на основе анализа архивных источников рассмотрены основные черты воронежской городской милиции в конце 1920-х гг. — ее территориальная и кадровая организация и основные направления функционирования. Осуществлена попытка выявления ключевых особенностей административной деятельности и борьбы с преступностью пяти отделений милиции г. Воронежа. Проведен анализ объективных причин недостатков функционирования воронежской городской милиции. Сделаны заключения о специфике обследования территориальных подразделений городской милиции в ходе инспекторских проверок.

Based on the analysis of archival sources, the article examines the main features of the Voronezh city police in the late 1920s - its territorial and personnel organization and the main areas of operation. An attempt has been made to identify the key features of administrative activities and the fight against crime in five Voronezh police departments. The analysis of objective reasons of shortcomings of functioning of the Voronezh city militia is carried out. Conclusions were drawn about the specifics of the inspection of the territorial divisions of the city police during the inspections.

Вторую половину 1920-х гг. для советской рабоче-крестьянской милиции, как и всего советского общества и государства, можно охарактеризовать как период кратковременной «передышки» между радикальными потрясениями революций 1917 г. и гражданской войны, с одной стороны, и масштабными социально-экономическими преобразованиями, трансформациями политического режима, включая конституционную реформу, старт, направления и размах которым открыл «год великого перелома» [1. — С. 117—135], — с другой. Преодоление наследия «военного коммунизма», относительная стабилизация экономики в период НЭПа, прежде всего в сельском хозяйстве и отраслях легкой промышленности привели к относительному улучшению материального положения населения. Отход на второй план идейного ориентира «мировой революции», оформление, несмотря на появление первых тоталитарных симптомов, в общих чертах политической системы СССР, структурного облика «первого в истории социалистического государства», стимулировали тенденции к концептуализации и прагматизации государственного строительства [2]. Его обновленные идейные ориентиры чуть позднее диалектически сформулировал И. В. Сталин: «Уничтожение классов… достигается не путем потухания классовой борьбы, а путем ее усиления. Отмирание государства при-

дет не через ослабление государственной власти, а через ее максимальное усиление…» [3. — С. 509].

В этих условиях в общих чертах оформилась советская правоохранительная система, одним из важнейших элементов которой являлись органы внутренних дел [4. — С. 16—20], которые в соответствии с принципами классовости и партийности претерпели несколько волн систематических «чисток» [5. — С. 6]. В то же время к концу 1920-х гг. утвердились организационно-правовые основы советской милиции, оформленные Положениями «О Советской рабоче-крестьянской милиции» 1920 г. [6], «О Народном комиссариате внутренних дел РСФСР» 1922 г. [7], «О службе рабоче-крестьянской милиции» 1925 г. [8] и др.

В состав советской рабоче-крестьянской милиции, согласно Положению 1920 г., наряду с другими видами милиции входила и городская, непосредственно подчинявшаяся административным отделам губернских и областных исполнительных комитетов, начальники которых являлись одновременно и начальниками губернской милиции [9].

Следствием относительной стабилизации функционирования воронежской городской милиции стало не только усиление внимания к анализу ее отчетов, направляемых в вышестоящие инстанции по различным союзным и губернским запросам [см., напр.: 10—17], но и организация хронологически синхронизированных комплексных проверок состояния всех ее подразделений. Это позволило создать необходимый минимум объективной информации об этом важнейшем правоохранительном органе, полученной непосредственно в ходе «полевых исследований» инспекторов-специалистов.

В то же время важно отметить и некоторую несформированность методики подобного рода инспекторских обследований. Так, в частности, анализ архивных материалов, лежащих в основе настоящей статьи, показывает отсутствие концептуальной проработки всего спектра инспектируемых объектов. К примеру, в них совершенно отсутствует детальное изучение материально-технического состояния проверявшихся отделений городской милиции, вещевого и денежного содержания милиционеров, а анализ кадровых проблем выглядит довольно скудно. Безусловно, это, если рассматривать проблемы воронежской милиции с точки зрения исторического подхода, не позволило инспекторам сформировать более объёмную картину ее состояния. Впрочем, в сравнении с предшествующими периодами качество инспекторских проверок заметно выросло.

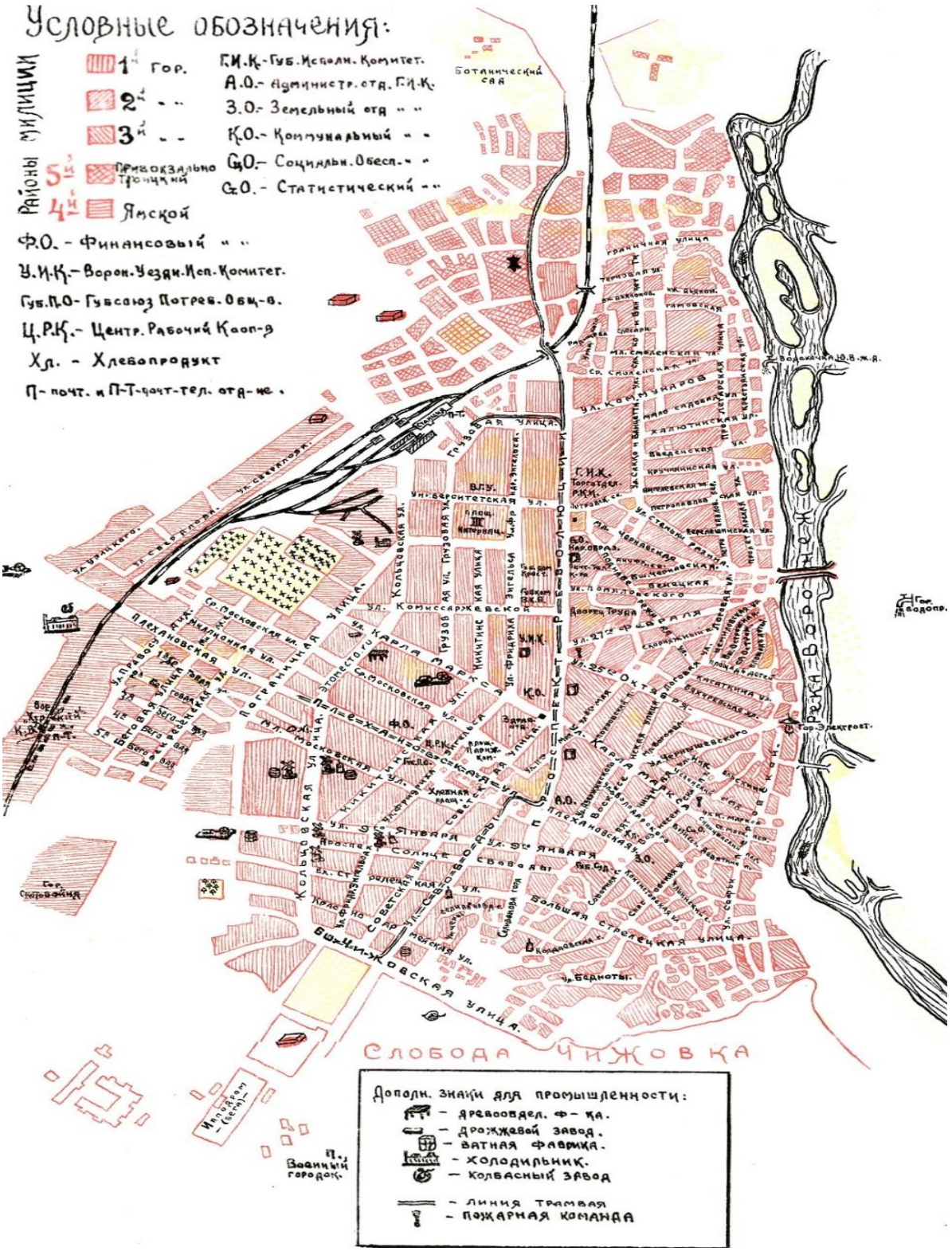
Основанием для комплексных обследований воронежской городской милиции стало предписание начальника Административного отдела Губисполкома, начальника милиции Воронежской губернии К. В. Григорьева от 17 марта 1927 г. № 06 [18. — Л. 1]. Начальник Инспекторской части Административного отдела И. И. Щемелинов с этой целью назначил двух наиболее ответственных работников — А. П. Драчева и И. И. Метелкина. Ими были обследованы пять городских отделений милиции: 19 марта — Первое (нач. Андреев) и Третье (нач. Ломакин), 22 марта — Второе (нач. Талдыкин), 26 марта — Троицко-Привокзальное (нач. Масленников) и 27 марта — Ямское (нач. Шедогубов). Драчев проинспектировал Первое и Троицко-Привокзальное отделения, остальные для проверки были поручены Метелкину.

Опытность ответственных работников Административного отдела не вызвала сомнений. Так, в частности, послужной список А. П. Драчева, бывшего до революции учителем, включал в себя руководство милицией Воронежской губернии, воронежскими милицейскими курсами начала 1920-х гг. и 3-й Воронежской школой младшего комсостава [19. — Л. 1—7]. Оба инспектора на момент проверки являлись преподавателями указанной образовательной организации. Следует отметить, что при осуществлении инспекции А. П. Драчев был более, чем его коллега, склонен не только к рассмотрению определенных предписанием начальника Административного отдела аспектов милицейской деятельности (постовая служба, административная работа, борьба с преступностью, делопроизводство), но и к тщательному анализу основных направлений рационализации функционирования отделений.

Территориальные зоны ответственности городских отделений милиции определялись январским 1926 г. приказом начальника городской милиции № 1с [18. — Л. 21] (рисунок). В ходе проверки в целом было выявлено общее недостаточное количество милицейских постов и слабая связь между ними.

Первое отделение несло службу в части города, основными постовыми пунктами которой являлись железнодорожная станция Воронеж 1, улицы Старо-Московская, Фридриха Энгельса, Никитинская, Плехановская, Большая Петровская, Свобода, Кольцовская, площадь III Интернационала. Всего на них было организовано 4 суточных и 2 ночных поста [18. — Л. 2]. Инспектор отмечал, что обслуживание суточными нарядами территории Первого отделения «надо признать недостаточно удовлетворительным». Так, к примеру, слишком большим было расстояние без организованных постов между Народным домом и новостроящимся кладбищем (4,5 версты в длину и 1, 25 верст в ширину). Это приводило к отсутствию «зрительной и слуховой» связи между имевшимися постами. Драчев предлагал перераспределить обязанности между сотрудниками отделения и увеличить число постов до 7—5 суточных и 2 ночных [18. — Л. 2].

Размещение отделений воронежской городской милиции в 1928 г.



В районе, обслуживаемом Третьим отделением, в наличии было 4 суточных и 3 ночных милицейских поста, расположенных на значительном удалении друг от друга и неизбежно не имевших как зрительной, так и звуковой связи. Более того, большая часть района от улицы Большая Стрелецкая вообще выпадала из-под постоянного милицейского надзора. Как «крайнюю потребность» инспектор определил организацию трех новых постов на улицах Большая Стрелецкая и Бедноты, пересечении улиц Софьи Перовской и Карла Маркса (у Каменного моста) [18. — Л. 21].

Ямское отделение милиции выставляло два суточных поста на Заставе — углу улицы Профсоюзной и площади III Интернационала и один ночной у трамвайного парка. При этом довольно большой район улиц Урицкого и Свердловской (рабочий поселок), а также Чугуновского кладбища постами не обслуживался. Более того, в летнее время ночной пост от трамвайного парка передислоцировался к глазной лечебнице — на угол улицы Карла Маркса и проспекта Революции [18. — Л. 28 об. — 29].

Границы территории, обслуживаемой Троцко-Привокзальным отделением, начинались от бывшего Девичьего монастыря, далее по берегу Воронежа до бывшей Архиерейской рощи и от моста через железнодорожный путь, охватывая железнодорожный поселок при станции Воронеж 1 до Ботанического Сада. Кроме того, в компетенцию отделения входила территория, прилегавшая к Сельскохозяйственному институту. Имевшиеся здесь два суточных поста и один ночной, как в ходе проверки выяснил Драчев, были совершенно лишены всякой связи. По мнению инспектора, общее количество постов было явно недостаточным [18. — Л. 33].

Базовым структурным элементом территории каждого отделения милиции являлся участок. Территории Первого и Третьего отделений были разбиты на 5 участков, Второго — на 4, Троицко-Привокзального — на 3, Ямского — на 2.

Учитывая объективные социально-экономические и политические характеристики хронологического периода инспектирования, на основании анализа мартовских 1927 г. актов обследования городских отделений милиции целесообразно выделить следующие основные направления их повседневной работы:

- охрана общественного порядка и безопасности путем несения постовой службы, регулирования уличного движения, патрулирования и т. д.;

- борьба с преступностью в форме производства дознания, гласного и негласного наблюдения за криминальным элементом, оперативно-розыскных мероприятий;

- противодействие нарушениям обязательных постановлений, привлечение виновных к ответственности в административном и судебном порядке;

- борьба с наиболее актуальными административными правонарушениями — самогонокурением, пьянством, хулиганством, проституцией, шинкарством и другими «видами паразитизма»;

- оказание содействия иным, кроме НКВД, ведомствам — НКПС (взыскание за безбилетный проезд), Военмору (проведение призывных кампаний, выявление уклонистов и т. д.), ГПУ (содействие в задержании и производство вызовов), ГУБРО (борьба с беспризорностью и правонарушениями малолетних) и т. д.;

- содействие контролю за всеми видами торговли;

- контроль за соблюдением паспортного режима;

- борьба со стихийными бедствиями [18. — Л. 10 — 10 об.];

- содействие ведению актов гражданского состояния;

- осуществление надзора по отдельным заданиям Губисполкома за некоммерческими и религиозными обществами и т. д. [18. — Л. 28 об.]

Как видно из перечисленного, реальная работа городских отделений милиции Воронежа носила, как и в прежние годы, разнообразный и многоаспектный характер, составляя исполнительскую основу для реализации государственной власти в губернском центре.

Самым многочисленным в начале 1927 г. был штат Первого отделения — 60 человек: 3 — комсостава (начальник, помощник и старший участковый надзиратель), 16 участковых, 37 младших милиционеров и 4 человека из технического персонала [18. — Л. 1]. Самое меньшее количество работников милиции было в штате Ямского отделения — 24 человека, где помимо начальника трудились еще 2 участковых, 1 старший и 18 младших милиционеров, а также 2 сотрудника из технического персонала [18. — Л. 31].

Наиболее тщательно были распределены служебные обязанности среди работников Первого отделения, которое обеспечивало общественный порядок в самом центре города, где располагались Губком ВКП (б) и Губисполком, а также иные административные учреждения и центральный рынок (см. рисунок). Из 16 участковых надзирателей штата Первого отделения 1 являлся комендантом рынка, 1 отвечал за производство дознаний, по 2 обслуживали четыре участка, на одном участке работали 3 человека. Трое участковых несли службу по отделению. 37 младших милиционеров были распределены следующим образом: 5 обслуживали рынок, 12 несли службу в

резерве (по 4 в смене), 16 заступали на пост (на суточных постах — 12 и на ночных — 4). Четыре милиционера числились «в подмене» [18. — Л. 1].

Значительной оставалась текучесть кадров. Так, в период с октября 1926 по март 1927 г. в Первом отделении переведено или уволено было 6 человек комсостава, 16 участковых и 21 милиционер (соответственно 25% увольнений и 46,4% переводов от общего количества личного состава). Один милиционер погиб при исполнении служебных обязанностей [18. — Л. 1]. По мнению Драчева, именно «текучесть и переводы являются основной причиной упадка работоспособности в органах милиции» [18. — Л. 1 об.]. В Ямском отделении кадровая ситуация в силу меньшей загруженности и численности личного состава была несколько более оптимистичной — с декабря 1926 по март 1927 г. убыло или переведено только 16 человек, включая 15 младших милиционеров [18. — Л. 31].

Служебная нагрузка на участковых надзирателей не слишком различалась в зависимости от удаленности участка от центра города. Так, чуть меньше, чем за полгода — с 1 октября 1926 г. по 21 марта 1927 г. — на 1-м, 2-м и 4-м участках (по выражению инспектирующего, двух «слабых» и одном «сильном») к производству было принято 868 дел, взысканий и требований [18. — Л. 2 об.]. За те же шесть месяцев на участках Троицко-Привокзального отделения исполнялось 877 поручений [18. — Л. 34 об.].

По подсчетам инспектора Драчева, в среднем на одного участкового в Первом отделении в истекший период в месяц приходилось 15,5 дознаний, 11,5 денежных взысканий и 23,1 административных наказаний, а также 2,2 исполнения отдельных требований, т. е. всего — 52,3 исполнительных производства. Соответственно, в сутки на одного участкового приходилось в среднем по $1\frac{2}{3}$ поручения. Все это позволило инспектору сделать вывод: «считать, что участковые милиционеры перегружены технической работой, нет никакого основания» [18. — Л. 3], последние заняты технической работой от 2 до 3 часов в сутки. По мнению Драчева, «остальное время их работы 5 часов в сутки» должно быть использовано для «периодических обходов участка, осмотров санитарного состояния улиц, дворов, площадей» [18. — Л. 34 об.], для чего в плановом порядке целесообразно создать «систему обслуживания территории Отделения» [18. — Л. 35].

Административная деятельность городских отделений милиции определялась исполнением обязательных постановлений губернских органов государственной власти. Как отмечалось в инспекторских отчетах, основным недостатком в этой сфере было несвоевременное прямое предоставление распоряжений из Административного отдела, усугублявшееся отсутствием подписки на официальный печатный орган «Воронежская коммуна», в котором публиковались эти документы [18. — Л. 5 об.]. Более того, за актами губернских властей из отделений приходилось ежедневно направлять в Административный отдел милиционеров из резерва, отвлекая их от исполнения основных служебных функций. Так, для доставки корреспонденции в Троицко-Привокзальное отделение «командированным» милиционерам приходилось каждый день преодолевать расстояние в 5 верст до Административного отдела и обратно [18. — Л. 37].

Вследствие этого в отделениях практически не велся учет обязательных постановлений. Так, во Втором отделении в период с 1924 г. по март 1927 г. имелось всего лишь 9 актов Губисполкома и 4 постановления Горсовета за 1926 г. — март 1927 г. [18. — Л. 11] Между тем, как правило, общее ежегодное количество административных предписаний этих органов исчислялось десятками.

Участковые милиционеры руководствовались лишь отдельными обязательными постановлениями, которые попадали им «на руки» либо потому, что они, об этом «проявляя личную заботливость» [18. — Л. 29], выписывали газету самостоятельно, либо «путем покупки отдельных номеров». В отделениях также отсутствовали и инструктивные указания Административного отдела, касающиеся специфики исполнения изданных обязательных постановлений губернских властей [18. — Л. 6].

Результативность административной деятельности городских отделений милиции по результатам инспектирования устанавливалась по количеству составленных протоколов. Фактическими основаниями для них чаще всего являлись состояние алкогольного опьянения в общественных местах («пьянство»), антисанитария, нарушения правил содержания и выгула домашних животных (прежде всего, собак), нарушения правил торговли, отсутствие прописки в домовой книге, хулиганство, шинкарство, нарушения правил дорожного движения и проезда в трамвае [18. — Л. 6 об., 11 об., 21 об., 29 — 29 об.].

По вполне понятным причинам больше всего пресекалось административных проступков в центральной части города. Так, в частности за период с 01.01.1926 по 01.01.1927 во Втором отделении всего по различным обязательным постановлениям было выписано 863 протокола об административных правонарушениях [18. — Л. 11 об.], в Третьем — 1971 [18. — Л. 21 об.], а в

Первом отделении только непосредственно на месте их совершения в октябре 1926 г. — марте 1927 г. милиционерами было составлено 725 правоприменительных актов о назначении штрафа. Общая же сумма взысканных штрафов по Первому отделению за указанный период составила 929 рублей по 145 постановлениям [18. — Л. 6 об.]. Милицией Ямского отделения за 1926 г. было составлено всего 193 протокола [18. — Л. 29 об.], а Троицко-Привокзального за отчетные полгода — 112 [18. — Л. 37].

В последнем случае инспектор Драчев критиковал «сравнительно слабую» деятельность участковых надзирателей, указывая, что, несмотря на очень большую площадь, находящуюся в ведении этого отделения, за антисанитарию граждане были привлечены к административной ответственности только в 37 случаях, за нарушения правил выгула собак — в 46, за хулиганство — в 11 [18. — Л. 37]. По его мнению, это свидетельствовало не столько об успехах правоохранительной деятельности местной милиции, сколько об отсутствии надлежащего надзора, поскольку «незаконные порубки в Ботаническом саду до настоящего времени все еще имеют место, хулиганство в летние месяцы в том же саду — большое» [18. — Л. 37 об.].

В материалах обследования особенно отмечались неутешительные результаты деятельности городской милиции по перерегистрации охотничьего оружия, которая, к примеру, в Первом отделении была охарактеризованы Драчевым как «полный провал»: из 81 зарегистрированных на пяти участках охотников на перерегистрацию не явились 61, а протоколов в отношении нарушителей было составлено всего 6 [18. — Л. 5], остальные «уклонисты» участковыми инспекторами не были выявлены.

Метелкин, подытоживая административную деятельность проинспектированных им отделений, заключил, что «указанный вид работ в систему не введен, личный состав с обязательными постановлениями знаком поверхностно, зачастую не имеет сведений об отмененных постановлениях, и проводятся таковые постольку, поскольку нарушение их выявляется более выпукло» [18. — Л. 11 об.]. Наиболее слабая профессиональная подготовленность и «мягкотелость» была отмечена у участковых надзирателей Троицко-Привокзального отделения [18. — Л. 37 об.].

В ходе инспектирования административной деятельности воронежской городской милиции были сформулированы некоторые практические предложения по ее совершенствованию. Так, в частности, Драчев предлагал «в целях приближения органов милиции к трудовым вопросам крестьянства и населения… проводить публикацию в местной прессе а) о приблудном скоте, хотя бы 1 раз в месяц, б) о находках». Он же рекомендовал применять «к буйствующим пьяным усмирительной рубашки, не причиняющей никакой боли», сетуя на то, что «за последнее время буйство в камере настолько частое явление, что днем работать… невозможно. Двери, окна и печи неоднократно разламывались» [18. — Л. 4 об.].

Особое внимание в ходе комплексного обследования городской милиции традиционно привлекала борьба с уголовной преступностью, причем наиболее детальный анализ по работе в данном направлении Первого отделения содержался в отчете А. П. Драчева (табл. 1).

Таблица 1 [18. — Л. 7 –7 об.]

Работа по борьбе с преступностью в Первом отделении за 1926 г.

Виды преступлений	**За 1926 г.**									**За 1927 г.**		
	2 квартал			**3 квартал**			**4 квартал**			**1 квартал**		
	Зафикс.	Раскр.	Прекр.	Зафикс.	Раскр.	Прекр.	Зафикс.	Раскр.	Прекр.	Зафикс.	Раскр.	Прекр.
Против порядка управления	16	9	6	26	14	11	21	18	3	28	19	8
Должностные	-	-	-	7	2	4	1	-	1	2	1	1
Самогоноварение	35	12	13	42	15	12	24	17	3	36	2	29
Хозяйственные	-	-	-	-	-	-	1	1	-	2	1	1
Убийство	1	1	-	1	1	-	-	-	-	-	-	-
Хулиганство	16	11	1	16	13	1	61	54	2	60	8	44
Против личности	32	11	16	59	20	25	32	6	8	61	19	32
Простые кражи			246	124	124	247	211	62	121	272	94	94

Виды преступлений	**За 1926 г.**									**За 1927 г.**		
	2 квартал			**3 квартал**			**4 квартал**			**1 квартал**		
	Зафикс.	Раскр.	Прекр.	Зафикс.	Раскр.	Прекр.	Зафикс.	Раскр.	Прекр.	Зафикс.	Раскр.	Прекр.
Квалиф. кражи	35	20	14	25	8	12	-	-	-	22	13	9
Присвоение и растрата	8	6	2	8	6	-	4	3	1	7	2	5
Поджог и истребление имущества	4	1	1	-	-	-	1	-	1	7	4	3
Военные	-	-	-	-	-	-	1	-	1	2	-	2
Всего	**393**	**195**	**173**	**619**	**203**	**312**	**357**	**161**	**141**	**499**	**163**	**228**

Как видно из таблицы 1, основное направление борьбы составляли простые кражи, что объясняется исключительной в масштабах города концентрированностью на подконтрольной Первому отделению территории публичных мест, включая площади и рынок. Что касается других видов преступной деятельности, то примерно в равных долях к ним относились самогоноварение и незаконный сбыт алкогольной продукции, преступные посягательства против личности и квалифицированные кражи. В конце 1926 — начале 1927 г. существенно усилилась борьба с хулиганством.

Из зафиксированных за год 1868 преступлений раскрыто было 722. Общая раскрываемость преступлений по Первому отделению без учета прекращенных, переданных в другие органы и неоконченных дел, по подсчету Драчева, составила 44,91% [18. — Л. 7 об.]. Единственный тормоз к поднятию процента раскрываемости преступлений инспектор усматривал в «несколько медлительном производстве дознаний по заявлениям граждан». Он предлагал изменить существовавший порядок дознания, установив в качестве обязательного максимального срока 24 часа [18. — Л. 8]. При анализе приведенной статистики антикриминальной деятельности Первого отделения обращает на себя внимание большое количество неоконченных, находившихся в производстве и направленных в другие органы дел (около 300), особенно в 3 квартале 1926 г. и 1 квартале 1927 г.

Выделив для анализа данные по антикриминальной деятельности Первого отделения с учетом объективных особенностей условий его функционирования, уместным представляется попытаться рассмотреть в комплексе усилия по борьбе с городской преступностью воронежских милиционеров из четырех других отделений (табл. 2).

Таблица 2 [18. — Л. 12 об., 22, 30, 38]

Деятельность Второго, Третьего, Ямского и Троицко-Привокзального отделений воронежской городской милиции по борьбе с преступностью (с 01.01.1926 по 01.01.1927)

Отделение	**Количество преступлений**					
	1-е полугодие		**2-е полугодие**		**Всего за год**	
	Зафикс.	Раскр.	Зафикс.	Раскр.	Зафикс.	Раскр.
Второе	379	170	352	132	731	302
Третье	406	191	404	210	810	401
Ямское	94	50	155	54	249	104
Троицко-Привокзальное	нет данных	нет данных	нет данных	нет данных	104	58

Основными объектами дознания во всех четырех отделениях являлись простые кражи и преступления против личности (76,6% всех зарегистрированных преступлений во Втором отделении [18. — Л. 12 об.], 46,8% в Третьем [18. — Л. 22], 39,2% в Ямском [18. — Л. 30], 37,9% в Троицко-Привокзальном [18. — Л. 38]). Значительно по количеству им уступают материалы дознаний по преступлениям против порядка управления. Во Втором отделении за отчетный период было зарегистрировано 77 [18. — Л. 12 об.], в Третьем — 69 [18. — Л. 22], в Троицко-Привокзальном — 15 [18. — Л. 38], в Ямском — 13 [18. — Л. 30] таких противоправных деяний, что вдвое-втрое меньше, нежели число простых краж и преступлений против личности. Только в Троицко-Привокзальном отделении преступления против порядка управления находились на втором после простых краж месте по количеству материалов дознания. Что касается других преступлений (должностных, хозяйственных, квалифицированных краж и т. д.), то в структуре антикриминальной деятельности воронежской городской милиции они занимали существенно менее значительные места. Обращает на себя внимание также и крайне малое количество тяжких преступлений, становившихся объектом дознания со стороны всех пяти отделений. Так, за анализируемый инспекторами год (с 1.01.1926 по 1.01.1927) только одно убийство было расследовано в Первом отделении [18. — Л. 7].

Указанное обстоятельство свидетельствует не только о сравнительно благоприятной криминогенной ситуации в Воронеже на исходе первого десятилетия Советской власти, но и о специфике милицейской деятельности, значительно уступавшей в своей функциональной направленности в данной области народным следователям и органам прокуратуры.

Раскрываемость преступлений во Втором отделении за отчетный период составила 41,3% [18. — Л. 12 об.], 49,5% — в Третьем [18. — Л. 22 об.], 41,8% — в Ямском [18. — Л. 30], 55,8% — в Троицко-Привокзальном [18. — Л. 38]. Успешность проведенных дознаний была явно неодинаковой, если рассматривать ее в контексте анализа борьбы с отдельными категориями преступлений. Так, к примеру, раскрываемость краж во Втором отделении составила 21,6%, должностных преступлений — 25% [18. — Л. 12 об.]. Сходная ситуация была и в других подразделениях городской милиции. Внутреннее содержание материалов дознания по всем расследуемым преступлениям, как отмечали в своих отчетах инспекторы, было явно недостаточно проработано, о чем свидетельствовал сравнительно высокий процент (в среднем 41%) прекращенных дел [18. — Л. 22 об.].

В целом, совершенно очевидным был слабый уровень результативности воронежской городской милиции в ее борьбе с преступностью, что объяснялось «низкой квалификацией сотрудников розыскной сферы, формальным отношением к работе и, наконец, как следствие, слабой продуктивной работой личного состава» [18. — Л. 12 об.]. Особенно, если это касалось дознаний по незначительным преступлениям на бытой почве. В частности, инспектировавший Второе отделение Метелкин, приводил такой пример: материал дознания, сформированный 27 ноября 1926 г. по заявлению гражданина о краже ткани, был направлен народному следователю только 28 января 1927 г. с целью прекращения дела по причине неустановления виновных. Инспектор делал в этой связи вполне логичное заключение: «трудно верить, что… участковый надзиратель исчерпал все возможности к раскрытию кражи» в такие длительные сроки. Тогда как более подготовленные работники, согласно сведениям инспектора, такие процессуальные действия осуществляли в день возбуждения уголовного дела [18. — Л. 12 об. — 13].

Сформированные в инспекторских отчетах выводы проверяющих в целом представляют комплексную картину состояния борьбы с преступностью во всех отделениях воронежской городской милиции. В то же время по итогам анализа статистических материалов, приведенных в отчетах инспекторов, с сожалением приходится констатировать весьма значительное количество ошибок в подсчетах и опечаток цифр, что приводило к необходимости более тщательной проверки и даже реконструкции аутентичных архивных данных. Примером могут служить цифровые выкладки по количеству отдельных видов преступлений, а также данные об их раскрываемости, приведенные в отчетах и Драчева, и Метелкина по всем пяти городским отделениям милиции.

Отчеты по обследованию воронежской городской милиции были составлены в четырех экземплярах (непосредственно инспекторский, в Адмотдел, для проверенного отделения, а также направляемый в Губисполком и Горсовет), подписаны инспекторами и начальниками отделений.

По итогам обследований функциональное состояние воронежской городской милиции было признано «вполне удовлетворительным» (в материалах по Первому отделению) [18. — Л. 8], а в их деятельности «грубых упущений в области производства дознаний, административных взысканий и технической работы канцелярии», как это определялось, к примеру, в отчете по Троицко-Привокзальному отделению, установлено не было [18. — Л. 39 об.].

Вместе с тем инспекторы как в целом, так и в отдельных направлениях работы милиционеров г. Воронежа предлагали провести ряд мер по ее улучшению:

- устранить текучесть милицейских кадров и частые перемещения личного состава [18. — Л. 8 об.];

- более последовательно проводить в жизнь принцип своевременного «выдвижения» работников на новые, включая вышестоящие, должности [18. — Л. 14];

- ввести практику более тщательного инструктажа участковых надзирателей со стороны начальствующего состава и работников Административного отдела [18. — Л. 40];

- наладить регулярное снабжение отделений городской милиции со стороны Адмотдела напечатанными текстами обязательных постановлений Губисполкома и Горсовета [18. — Л. 14, 31 об.];

- «углубить административную деятельность в области надзора за проведением в жизнь обязательных постановлений Президиума Губисполкома и Горсовета, а также в области наблюдения за деятельностью обществ всех видов» [18. — Л. 8 — 8 об.];

- уменьшить количество установленных приказами Административного отдела делопроизводственных книг, признав их «излишними»;

- сократить сроки исполнения милиционерами всех видов поручений за счет введения более действенной системы учета индивидуальной нагрузки участковых и проверки сроков ее реализации [18. — Л. 8 об.];

- обратить особое внимание на рациональное использование рабочего времени участковыми надзирателями, в том числе и на основе тщательного учета их работы по обслуживанию участков, так как по результатам инспекторского анализа их деятельности степень их повседневной фактической загруженности не превышала 3,5 часа в сутки [18. — Л. 39 об.];

- усилить борьбу с мелкой уголовной преступностью за счет введения обаятельного максимума времени в сутки, отпускаемого на производство дознания «по заявлениям граждан по свежим следам» [18. — Л. 8 об.];

- решить вопрос о возвращении милиционеру права ношения и пользования табельным оружием «вне его служебных часов», поскольку лишение его этого права в предыдущий период не только «не достигло целей, из-за которых данное мероприятие проводилось», но и не давало «возможности милиционеру оказать в нужную минуту содействие, благодаря чему личность милиционера теряет свой авторитет» [18. — Л. 23];

- устранить кадровую недостаточность технического персонала [18. — Л. 14].

Как видно из вышесказанного, наряду с весьма продуктивными соображениями, высказанными Драчевым и Метелкиным, некоторые инспекторские предложения оставались весьма нереалистичными, как, например, изжитие текучести кадров, которая только в Первом отделении в отчетный год составила, по оценке проверяющего, 71,4% [18. — Л. 8 об.], или совсем уж декларативными, как, к примеру, связанные с «текучкой» рекомендации о «кадровых выдвижениях».

Имелись в отчетах инспекторов и предложения по отдельным подразделениям городской милиции. Так, в отношении Третьего отделения был заострен вопрос о необходимости более тщательного контроля за обмундированием личного состава, а также улучшения состояния его материально-технического оснащения — расширения помещений и оснащения их служебной мебелью [18. — Л. 23]. Для Ямского отделения, находившегося на северной окраине города, в качестве актуальной меры была определена настоятельная потребность в организации арестного помещения и камеры для хранения вещественных доказательств [18. — Л. 31 об.].

Особое внимание в ходе инспектирования было обращено на окраинное и большое по территории Троицко-Привокзальное отделение, которое еще не вполне воспринималось в рассматриваемый период «городским». По справедливому замечанию Драчева, его работа носила «особо специфический характер» и значительно отличалась «от городских отделений по причине того, что район населен в большей части рабочими и городской беднотой», что требовало «несколько иного» подхода. Для этого инспектор предлагал более тщательно инструктировать работников «поселковой милиции», прежде всего участковых надзирателей, по вопросам специфики их деятельности среди местного населения, а также гораздо чаще устраивать доклады начальника Троицко-Привокзального отделения на собраниях рабочих. Кроме того, поскольку в этом подразделении городской милиции большие по территории участки предполагали только по одному надзирателю, настоятельно требовалось «принять меры к замене слабых участковых… более технически и практически подготовленными» [18. — Л. 39].

Недостатки работы, обнаружившиеся в ходе инспекторских проверок в марте 1927 г., нашли свое отражение в приказаниях начальника Административного отдела Губисполкома начальникам Первого, Ямского и Троицко-Привокзального отделений [18. — Л. 9, 32 – 32 об., 40].

О мероприятиях по их устранению предлагалось доложить в инспекторскую часть Адмотдела не позднее 1 мая 1927 г.

Подводя итог анализу архивных материалов, свидетельствующих о функциональном состоянии воронежской городской милиции, на наш взгляд, целесообразно отметить некоторые характерные черты, во многом определявшиеся объективными обстоятельствами ее функционирования.

Во-первых, следует отметить неравный фактический статус отделений, обусловленный как территориальным размещением — степенью близости к административному центру губернского города, так и продолжительностью существования и, соответственно, наличием организационно-служебного опыта работы. Следствием этого были весьма существенные различия в кадровом обеспечении отделения (разница в численности, степень профессиональной подготовленности и т. д.), материально-техническом снабжении, интенсивности административной и уголовно-розыскной работы и т. д. Безусловно, особое место в этом отношении занимало Первое отделение, отличавшееся наиболее качественным функциональным состоянием, а окраинные Ямское и, особенно, Троицко-Привокзальное еще не завершили своего организационного становления.

В-вторых, в рассматриваемый период для воронежской городской милиции наблюдалась относительная стабилизация ее организационно-правового положения и деятельности, обусловленная, с одной стороны, оформлением (хоть и не всегда последовательным и порой предполагающим излишнюю бюрократизацию) системы ведомственных предписаний, определяющих городскую милицейскую службу, с другой — налаживанием более-менее устойчивых функциональных связей как между ее структурными подразделениями и с руководящими органами в лице Административного отдела Губисполкома, так и с иными органами и учреждениями государственной власти Воронежской губернии.

В-третьих, по-прежнему наиболее острой проблемой ее кадрового обеспечения была недостаточная служебная подготовленность, причем не только в среде младших милиционеров, но и участковых надзирателей, обусловленная как текучестью личного состава, так и слабостью повседневного профессионального обучения милиционеров [20. — Л. 1—33, 21, 22]. Что касается функционировавшей с 1925 г. 3-й Воронежской школы младшего начсостава милиции, то она в большей степени была ориентирована на межобластную работу по подготовке милицейских кадров, чем на подготовку местной городской милиции [23, 24].

Тем не менее необходимо с большой долей уверенности констатировать, что достаточно объективные данные материалов инспекторских проверок, осуществленных в марте 1927 г., убеждают в общей функциональной подготовленности воронежской городской милиции к выполнению служебных обязанностей по охране общественного порядка и борьбе с уголовной преступностью настолько, насколько того требовала текущая социально-экономическая и политическая ситуация в стране к исходу первого десятилетия установления Советской власти.

ЛИТЕРАТУРА

1. Сталин И. В. Год великого перелома: к XII годовщине Октября // Сталин И. В. Сочинения. — М., 1949. — Т. 12. — С. 118—135.

2. Земцов Б. Н. Становление первого социалистического государства: теория и реальность // Гуманитарный вестник МГТУ им. Н. Э. Баумана. —2017. — № 12(62).

3. Сталин И. В. Вопросы ленинизма. — М., 1934. — 611 с.

4. Камалова Г. Т. Советская модель правоохранительной системы: теоретический аспект // Вестник ЮУрГУ. Серия : Право. — 2014. — Т. 14. — № 2. — С. 16—20.

5. Токмаков И.В. Становление и деятельность органов советской милиции 1917—1930 годов (на материалах Центрального Черноземья) : дис. … канд. ист. наук. — Курск, 2003. — 195 с.

6. О Советской рабоче-крестьянской милиции : положение, утвержденное Декретом Всероссийского Центрального Исполнительного Комитета Советов и Совета Народных Комиссаров от 10 июня 1920 г. // Собрание узаконений и распоряжений рабочего и крестьянского правительства. —1920. — № 79.

7. О Народном комиссариате внутренних дел РСФСР : положение ВЦИК и СНК РСФСР от 24 мая 1922 г. // Собрание узаконений и распоряжения правительства за 1922 г. — 1922. — № 77. — Отд. 1. — Ст. 649.

8. О введении в действие Положения о службе рабоче-крестьянской милиции : декрет ВЦИК и СНК РСФСР от 28 сентября 1925 г. // Собрание узаконений РСФСР. — 1925. — Отд. 1. — № 68. — Ст. 539.

9. Об Административном отделе губернских и областных исполнительных комитетов : положение от 11 августа 1924 г., утвержденное декретом Всероссийского Центрального Исполнительного Комитета и Совета Народных Комиссаров // Собрание узаконений и распоряжений Рабочего и Крестьянского правительства за 1924 г. — 1924. — № 70. — Отд. 1 — Ст. 690.

10. Государственный архив Воронежской области (далее ГАВО). — Ф. Р-5. — Оп. 1. — Д. 7.
11. ГАВО. — Ф. Р-5. — Оп. 1. — Д. 60.
12. ГАВО. — Ф. Р-5. — Оп. 1. — Д. 101.
13. ГАВО. — Ф. Р-5. — Оп. 1. — Д. 224.
14. ГАВО. — Ф. Р-5. — Оп. 1. — Д. 230.
15. ГАВО. — Ф. Р-5. — Оп. 1. — Д. 306.
16. ГАВО. — Ф. Р-5. — Оп. 3. — Д. 5.
17. ГАВО. — Ф. Р-5. — Оп. 3. — Д. 23.
18. ГАВО. — Ф. Р-5. — Оп. 2. — Д. 681.
19. ГАВО. — Ф. Р-38. — Оп. 2. — Д. 1097.
20. ГАВО. — Ф. Р-5. — Оп. 2. —Д. 472.
21. ГАВО. — Ф. Р-38. — Оп. 3. — Д. 20.
22. Нахимов А. В., Кирнос А. В., Колесников В. А. Предпосылки перестройки милицейского образования в Воронежской губернии в 1923—1925 гг. // Вестник Воронежского института МВД России. — 2017. — № 4. — С. 9—19.
23. ГАВО. — Ф. Р-5. — Оп. 2. Доп. — Д. 13.
24. Третья школа младшего комсостава рабоче-крестьянской милиции в системе образовательных организаций НКВД РСФСР : монография / А. П. Нахимов, А. В. Кирнос, В. А. Колесников, А. В. Артемченко. — Воронеж, 2019. — 209 с.

REFERENCES

1. Stalin I. V. God velikogo pereloma: k XII godovshchine Oktyabrya // Stalin I. V. Sochineniya. — M., 1949. — T. 12. — S. 118—135.
2. Zemtsov B. N. Stanovlenie pervogo sotsialisticheskogo gosudarstva: teoriya i real′nost′ // Gumanitarnyj vestnik MGTU im. N. E. Baumana. —2017. — № 12(62).
3. Stalin I. V. Voprosy leninizma. — M., 1934. — 611 s.
4. Kamalova G. T. Sovetskaya model′ pravookhranitel′noj sistemy: teoreticheskij aspekt // Vestnik YuUrGU. Seriya : Pravo. — 2014. — T. 14. — № 2. — S. 16—20.
5. Tokmakov I.V. Stanovlenie i deyatel′nost′ organov sovetskoj militsii 1917—1930 godov (na materialakh Tsentral′nogo Chernozem′ya) : dis. … kand. ist. nauk. — Kursk, 2003. — 195 s.
6. O Sovetskoj raboche-krest′yanskoj militsii : polozhenie, utverzhdennoe Dekretom Vserossijskogo Tsentral′nogo Ispolnitel′nogo Komiteta Sovetov i Soveta Narodnykh Komissarov ot 10 iyunya 1920 g. // Sobranie uzakonenij i rasporyazhenij rabochego i krest′yanskogo pravitel′stva. —1920. — № 79.
7. O Narodnom komissariate vnutrennikh del RSFSR : polozhenie VTsIK i SNK RSFSR ot 24 maya 1922 g. // Sobranie uzakonenij i rasporyazheniya pravitel′stva za 1922 g. — 1922. — № 77. — Otd. 1. — St. 649.
8. O vvedenii v dejstvie Polozheniya o sluzhbe raboche-krest′yanskoj militsii : dekret VTsIK i SNK RSFSR ot 28 sentyabrya 1925 g. // Sobranie uzakonenij RSFSR. — 1925. — Otd. 1. — № 68. — St. 539.
9. Ob Administrativnom otdele gubernskikh i oblastnykh ispolnitel′nykh komitetov : polozhenie ot 11 avgusta 1924 g., utverzhdennoe dekretom Vserossijskogo Tsentral′nogo Ispolnitel′nogo Komiteta i Soveta Narodnykh Komissarov // Sobranie uzakonenij i rasporyazhenij Rabochego i Krest′yanskogo pravitel′stva za 1924 g. — 1924. — № 70. — Otd. 1 — St. 690.
10. Gosudarstvennyj arkhiv Voronezhskoj oblasti (dalee GAVO). — F. R-5. — Op. 1. — D. 7.
11. GAVO. — F. R-5. — Op. 1. — D. 60.
12. GAVO. — F. R-5. — Op. 1. — D. 101.
13. GAVO. — F. R-5. — Op. 1. — D. 224.
14. GAVO. — F. R-5. — Op. 1. — D. 230.
15. GAVO. — F. R-5. — Op. 1. — D. 306.
16. GAVO. — F. R-5. — Op. 3. — D. 5.
17. GAVO. — F. R-5. — Op. 3. — D. 23.
18. GAVO. — F. R-5. — Op. 2. — D. 681.
19. GAVO. — F. R-38. — Op. 2. — D. 1097.
20. GAVO. — F. R-5. — Op. 2. —D. 472.
21. GAVO. — F. R-38. — Op. 3. — D. 20.
22. Nakhimov A. V., Kirnos A. V., Kolesnikov V. A. Predposylki perestrojki militsejskogo obrazovaniya v Voronezhskoj gubernii v 1923—1925 gg. // Vestnik Voronezhskogo instituta MVD Rossii. — 2017. — № 4. — S. 9—19.
23. GAVO. — F. R-5. — Op. 2. Dop. — D. 13.
24. Tret′ya shkola mladshego komsostava raboche-krest′yanskoj militsii v sisteme obrazovatel′nykh organizatsij NKVD RSFSR : monografiya / A. P. Nakhimov, A. V. Kirnos, V. A. Kolesnikov, A. V. Artemchenko. — Voronezh, 2019. — 209 s.

СВЕДЕНИЯ ОБ АВТОРАХ

Нахимов Александр Павлович. Начальник института. Кандидат философских наук.
Воронежский институт МВД России.
E-mail: chief@vimvd.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Кирнос Андрей Викторович. Доцент кафедры теории и истории государства и права. Кандидат политических наук, доцент.
Воронежский институт МВД России.
E-mail: andrej-kirnos@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Колесников Владимир Александрович. Доцент кафедры теории и истории государства и права. Кандидат политических наук, доцент.
Воронежский институт МВД России.
E-mail: vkolesnikov3@gmail.com
Россия, 394065, Воронеж, проспект Патриотов, 53.

Nakhimov Alexander Pavlovich. Head of the Institute. Candidate of Philosophical Sciences.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: chief@vimvd.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Kirnos Andrey Viktorovich. Associate Professor of the chair of Theory and History of State and Law. Candidate of Political Sciences, Associate Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: andrej-kirnos@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Kolesnikov Vladimir Alexandrovich. Associate Professor of the chair of Theory and History of State and Law. Candidate of Political Sciences, Associate Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: vkolesnikov3@gmail.com
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: НКВД; милиция; городская милиция; воронежская милиция; территориальное деление г. Воронежа; Воронежский губисполком; Административный отдел Губисполкома; Воронежский Горсовет; административная деятельность милиции; уголовно-розыскная деятельность милиции; обязательные постановления органов государственной власти.

Key words: NKVD; militia; city militia; Voronezh militia; territorial division of Voronezh; Voronezh Gubernatorial Executive Committee; Administrative Department of the Gubernatorial Executive Committee; Voronezh City Council; administrative activities of the militia; criminal investigative activities of the militia; mandatory resolutions of state authorities.

УДК 351.74

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

И. Г. Дровникова, *доктор технических наук, профессор*
Т. Ю. Тужикова, *адъюнкт*

ВЕРБАЛЬНАЯ МОДЕЛЬ ПРОЦЕССА РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ С ИСПОЛЬЗОВАНИЕМ ФЕЙКОВЫХ САЙТОВ

VERBAL MODEL OF THE PROCESS OF IMPLEMENTING INFORMATION SECURITY THREATS IN AUTOMATED SYSTEMS OF INTERNAL AFFAIRS BODIES USING FAKE SITES

В статье рассмотрены типичные для автоматизированных систем (АС) органов внутренних дел (ОВД) угрозы безопасности информации (УБИ), реализуемые посредством фишинг-атак, и используемые для их реализации уязвимости ИТ-активов системы. Представлена вербальная модель процесса реализации угрозы УБИ с использованием фейкового сайта в виде структурной схемы описания угрозы и результатов анализа ее элементов применительно к типичным для АС ОВД угрозам. Перспективы использования предложенной вербальной модели связаны с разработкой графовых моделей процесса реализации УБИ в АС ОВД с использованием фейковых сайтов и разработкой методического обеспечения количественной оценки рисков их реализации посредством фишинг-атак.

The article discusses information security threats (ISGs) typical for automated systems (AS) of internal affairs bodies (IAOs), which are implemented through phishing attacks, and the vulnerabilities of the system's IT assets used to implement them. A verbal model of the process of implementing a UBI threat using a fake site is presented in the form of a structural diagram describing the threat and the results of analyzing its elements in relation to typical threats for ATS. The prospects for using the proposed verbal model are related to the development of graph models of the process of implementing UBI in the ATS of the Interior Ministry using fake sites and the development of methodological support for quantifying the risks of their implementation through phishing attacks.

Введение. В настоящее время компьютерная преступность, основанная на реализации угроз несанкционированного доступа (НСД) посредством фишинг-атак, оказывает все более ощутимое влияние на большинство процессов функционирования современных объектов информатизации органов внутренних дел (ОВД). Одним из наиболее по-

пулярных способов реализации фишинг-атаки является создание фейкового сайта. Фейковость сайта рассматривается как фундаментальный компонент фишинг-атаки, определяющий успешность социальной инженерии [1].

В этой связи особую значимость приобретает решение задачи управления рисками информационной безопасности современных автоматизированных систем (АС) ОВД, связанными с реализацией фишинг-атак, что требует проведения количественной оценки рисков с использованием соответствующего методического обеспечения.

Решение задачи разработки методического обеспечения оценки рисков реализации угроз безопасности информации (УБИ) в АС ОВД с использованием фейковых сайтов требует выявления типичных для АС ОВД угроз, реализуемых посредством фишинг-атак, и используемых для их реализации уязвимостей ИТ-активов системы, а также предполагает разработку вербальной модели процесса реализации таких УБИ, что является целью данной статьи.

Основная часть. В общем случае описание УБИ представляет собой фрейм, состоящий из 9 слотов [2]. Отдельные слоты фрейма могут также рассматриваться как фреймы со сложной структурой либо вообще отсутствовать. Обязательными слотами описания УБИ являются первые 6 слотов, однако при необходимости описание конкретной угрозы может быть расширено добавлением новых слотов из последних трех, указанных на рисунке 1.

$$U = \left\langle \begin{array}{l} < \textit{наименование угрозы} >, < \textit{источник угрозы} >, \\ < \textit{используемая уязвимость} >, < \textit{сценарий реализации угрозы} >, \\ < \textit{объект воздействия} >, < \textit{несанкционированное действие}, \\ \textit{выполняемое при реализации угрозы} >, < \textit{время существования} \\ \textit{угрозы} >, < \textit{время, необходимое на реализацию угрозы} >, \\ < \textit{опасность угрозы} > \end{array} \right\rangle$$

Рис. 1. Структура описания УБИ в АС ОВД

Проанализируем каждый слот представленного фрейма применительно к УБИ в АС ОВД, реализуемым посредством фишинг-атак.

Именуется угроза, как правило, по наименованию выполняемого при ее реализации несанкционированного действия.

В ходе оценивания рисков реализации УБИ в АС ОВД с использованием фейковых сайтов должны быть определены возможные антропогенные источники данных угроз, к которым в соответствии с [3] относятся лица (группы лиц), осуществляющие реализацию УБИ путем НСД и (или) несанкционированного воздействия на информационные ресурсы АС ОВД — злоумышленники.

УБИ, реализуемую посредством фишинг-атаки, будем считать актуальной, если ее реализация приводит к существенным негативным последствиям (очень большому или недопустимому ущербу) для АС ОВД. Соответственно, злоумышленника считаем актуальным для АС ОВД, когда возможные цели реализации им УБИ с использованием

фейковых сайтов могут привести к существенным для системы негативным последствиям и рискам [3].

В зависимости от уровня возможностей (потенциала, оснащенности и мотивации) по реализации УБИ злоумышленники подразделяются на злоумышленников, обладающих: базовыми возможностями (низким потенциалом), базовыми повышенными возможностями, средними возможностями (средним потенциалом), высокими возможностями (высоким потенциалом). Злоумышленник является внешним, если он не имеет прав доступа в контролируемую зону и (или) полномочий по доступу к ИТ-активам АС ОВД и преднамеренно реализует УБИ с использованием фейковых сайтов. Соответственно, внутренний злоумышленник — это злоумышленник, имеющий такие права и полномочия, преднамеренно реализующий УБИ с использованием фейковых сайтов.

В результате анализа 227 угроз БИ и 78 505 уязвимостей, представленных в банке данных угроз (БДУ) Федеральной службы по техническому и экспортному контролю (ФСТЭК) России [4], а также результатов опроса специалистов в области защиты информации (ЗИ) на объектах информатизации ОВД были выделены 8 типичных для АС ОВД УБИ, реализуемых посредством фишинг-атак. Выбранные УБИ и уязвимости ИТ-активов АС ОВД, эксплуатируемые злоумышленником для реализации данных угроз, представлены в таблице 1.

Таблица 1

Типичные УБИ в АС ОВД, реализуемые посредством фишинг-атак, и используемые уязвимости

№ п/п	Идентификатор угрозы	Название угрозы	Идентификаторы используемых уязвимостей
1	УБИ.031	Угроза использования механизмов авторизации для повышения привилегий	BDU:2025-05473 BDU:2018-00827
2	УБИ.041	Угроза межсайтового скриптинга	BDU:2023-02442 BDU:2022-04856 BDU:2014-00051
3	УБИ.042	Угроза межсайтовой подделки запроса	BDU:2025-14893 BDU:2015-03352
4	УБИ.159	Угроза «форсированного web-браузинга»	BDU:2025-06016 BDU:2025-07728
5	УБИ.167	Угроза заражения компьютера при посещении неблагонадежных сайтов	BDU:2018-00838 BDU:2018-00840

№ п/п	Идентификатор угрозы	Название угрозы	Идентификаторы используемых уязвимостей
6	УБИ.174	Угроза «фарминга»	BDU:2025-14834 BDU:2025-14836 BDU:2018-00952
7	УБИ.175	Угроза «фишинга»	BDU:2025-13739 BDU:2024-04811 BDU:2021-03115
8	УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	BDU:2025-01793 BDU:2022-03226

Результаты подробного анализа выделенных УБИ с учетом их источников, объектов воздействия и возможных последствий реализации в виде причиненного информационного ущерба, а также используемых уязвимостей ИТ-активов АС ОВД приведены в [5].

Следует подчеркнуть, что описание уязвимости (информация о выявленной уязвимости) представляет собой составную часть описания угрозы, реализуемой с использованием этой уязвимости. Отсутствие указания на используемую уязвимость приводит к неопределенности описания способа реализации угрозы, а следовательно, и описания самой УБИ [2].

Возникновение рассмотренных УБИ и их реализация посредством фишинг-атак в АС ОВД осуществляются при сочетании определенных факторов и условий, позволяющих злоумышленниками проникать в защищенные АС ОВД и получать доступ к информации ограниченного распространения [6].

Факторы возникновения УБИ, реализуемых посредством фишинг-атак, и условия их реализации в АС ОВД приведены в таблице 2.

Актуальность УБИ определяется наличием хотя бы одного сценария ее реализации [3]. Под построением сценария реализации УБИ посредством фишинг-атаки на АС ОВД будем понимать определение последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным злоумышленником с учетом уровня его возможностей (потенциала, оснащенности, мотивации) для реализации УБИ при наличии рассмотренных выше факторов и условий.

Таблица 2

Факторы возникновения и условия реализации УБИ в АС ОВД посредством фишинг-атак

№ пп	Название	Содержание
Факторы возникновения УБИ в АС ОВД, реализуемых посредством фишинг-атак		
Основные факторы		
1	Технические (технологические)	Уязвимости ИТ-активов АС ОВД: аппаратных (физических), программных (лицензионного

№ пп	Название	Содержание
		и специализированного программного обеспечения (ПО), нематериальных (прав и цифровых ресурсов), информационных (данных и ценной информации) [3]
		Использование вредоносного ПО
		Сложности в архитектуре инфраструктуры
		Проблемы с конфигурацией
		Развитие информационно-коммуникационных технологий
		Использование технологий подмены и клонирования
2	Организационные и социальные	Высокая загруженность и спешка
		Отсутствие четких регламентов или их игнорирование
		Отсутствие культуры информирования
		Недостаток киберграмотности
		Утечка данных
3	Психологические	Когнитивные искажения: эффект авторитета, иллюзия контроля, эффект подтверждения
		Эмоциональные триггеры: любопытство и жадность, жалость, страх и неопределенность, чувство вины
		Дефицит времени: срочность и давление
		Автоматизмы: использование привычных сценариев общения, на которые у людей сформированы автоматические реакции
4	Особенности целевой аудитории	Малоосведомленные пользователи
		Пожилые люди и доверчивые личности
		Сотрудники с расширенными правами доступа
		Сотрудники с очень коротким и длительным стажем
		Сотрудники в состоянии эмоционального дисбаланса
Дополнительные факторы		Стрессовые ситуации
		Удаленная работа
		Доступность открытых данных
		Использование искусственного интеллекта и других современных технологий
Условия реализации фишинг-атак на АС ОВД		
Основные условия		
1	Технические	Устаревшие версии ПО и аппаратура
		Отсутствие или недостаточная эффективность мер ЗИ в АС ОВД
		Незащищенные каналы связи
		Слабые настройки сетевой инфраструктуры — наличие у злоумышленников возможности доступа к следующим типам интерфейсов объектов воздействия АС ОВД:

№ пп	Название	Содержание
		- внешним сетевым интерфейсам, обеспечивающим взаимодействие с сетью Интернет, смежными (взаимодействующими) системами или сетями; - внутренним сетевым интерфейсам, обеспечивающим взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы; - интерфейсам для пользователей; - интерфейсам для использования съемных машинных носителей информации и периферийного оборудования; - интерфейсам для установки, настройки, испытаний, пусконаладочных работ обеспечения функционирования компонентов АС ОВД
		Наличие у злоумышленников возможности доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам АС ОВД [3]
2	Организационные	Недостаточный уровень обучения сотрудников
		Нарушение регламентов безопасности информации
		Отсутствие четких процедур реагирования на инциденты
		Недостаточный контроль доступа
3	Социально-инженерные	Использование методов социальной инженерии
		Персонализация фишинг-атак
		Массовые рассылки с маскировкой под официальную переписку
Дополнительные условия		Человеческий фактор
		Зависимость от сторонних сервисов
		Недостаточный аудит и мониторинг

На основе анализа процесса реализации типовой фишинг-атаки в информационной системе построен сценарий реализации злоумышленником УБИ в АС ОВД посредством фишинг-атаки с описанием используемых возможных тактик и соответствующих им техник (табл. 3) [3].

Таблица 3

Сценарий реализации злоумышленником УБИ в АС ОВД
посредством фишинг-атаки

№ пп	Название этапа и используемые тактики	Используемые техники
1	Сбор информации об АС ОВД:	Сбор информации из публичных источников: официальный сайт организации МВД России, средства массовой информации, социальные сети,

№ пп	Название этапа и используемые тактики	Используемые техники
	1. Определение целевой аудитории (сотрудники, администраторы, руководители). 2. Изучение функционирующих сервисов (открытых портов). 3. Инвентаризация сети. 4. Определение уровней доступа и ролей пользователей	сайты поставщиков и вендоров, материалы конференций
		Сбор конфигурационной информации при помощи поисковых систем
		Пассивный сбор (прослушивание) информации и анализ данных телеметрии
		Направленное сканирование при помощи специального ПО подключенных к сети устройств
		Сбор информации путем перебора
		Сбор информации, предоставляемой DNS-сервисами
		Сбор информации о пользователе при посещении им сайтов
		Сбор информации путем поиска ее в памяти, файлах, каталогах, базах данных (БД), прошивках устройств, репозиториях исходных кодов ПО, включая поиск паролей в исходном и кэшированном виде, криптографических ключей
		Кража цифровых сертификатов, включая кражу физических токенов
		Сбор личной идентификационной информации сотрудников при условии, что они используют одни и те же пароли на работе и за ее пределами
		Получение доступа к системам физической безопасности и видеонаблюдения
		Получение контроля над личными устройствами сотрудников для скрытой прослушки и видеофиксации
		Получение доступа к БД результатов проведенных инвентаризаций, реестрам установленного оборудования и ПО, данным проведенных аудитов безопасности через компрометацию подрядчиков и партнеров
2	Вторжение: 1. Получение прав на доступ к ИТ-активам АС ОВД. 2. Обход стандартных мер ЗИ. 3. Осуществление доступа к ИТ-активу АС ОВД	Создание фейкового сайта
		Использование методов социальной инженерии
		Создание и доставка фишинг-письма
		Поиск уязвимостей ИТ-активов АС ОВД
		Определение объекта доступа (ИТ-актива) для выполнения несанкционированного воздействия на информацию в ходе реализации УБИ
		Выявление наличия (отсутствия) ограничений на получение доступа к объекту доступа и возможностей их преодоления

№ пп	Название этапа и используемые тактики	Используемые техники
		Использование штатных средств удаленного доступа и управления операционной системы (ОС)
		Использование ошибок конфигурации сетевого оборудования и мер ЗИ, в том числе слабых паролей и паролей по умолчанию для подбора пароля
		Использование вредоносного ПО и эксплойтов
		Эксплуатация уязвимостей ИТ-актива АС ОВД
3	Реализация несанкционированных действий: 1. Закрепление (сохранение доступа) в системе. 2. Управление вредоносным ПО и (или) ИТ-активом АС ОВД, к которому был получен доступ. 3. Повышение привилегий по доступу к ИТ-активу АС ОВД. 4. Получение доступа (распространение доступа) к другим ИТ-активам АС ОВД. 5. Сбор и вывод из системы информации, необходимой для дальнейших действий при реализации УБИ или реализации новых угроз. 6. НСД и (или) несанкционированное воздействие на информационные ресурсы АС ОВД, приводящие к существенным негативным последствиям (очень большому или недопустимому ущербу)	Перехват/сбор введенных учетных данных пользователя
		Незаконное использование учетных данных: копирование, модификация, уничтожение, блокирование.
		Перемещение по сети через скомпрометированные аккаунты
		Несанкционированный запуск приложений
		Формирование скрытых точек доступа («черных входов»), обеспечивающих долгосрочное присутствие злоумышленника в системе
4	Ликвидация следов фишинг-атаки:	Удаление или модификация записей из журнала аудита

№ пп	Название этапа и используемые тактики	Используемые техники
	1. Использование мер сокрытия следов несанкционированной активности. 2. Стремление злоумышленника затруднить применение мер ЗИ, способных обнаружить его действия или помешать им	Восстановление временно модифицированной информации
		Подмена IP-адреса злоумышленника
		Использование сторонних компьютеров в качестве базы фишинг-атаки
		Шифрование фишинг-атаки
		Фрагментация фишинг-атаки
		Сокрытие процессов за счет применения специальных утилит и вредоносных программ

В таблице 4 представлены способы реализации типичных УБИ в АС ОВД, использующих фейковые сайты, определенные на основе анализа БДУ ФСТЭК России [4]. Таблица показывает, что существует несколько способов реализации одной УБИ, в то же время один и тот же способ может использоваться для реализации различных угроз.

Таблица 4

Способы реализации типичных УБИ в АС ОВД
посредством фишинг-атак

№ пп	Идентификатор угрозы	Способы реализации	Содержание способов
1	УБИ.031	СП.2.11	Использование недостатков, связанных с некорректной настройкой прав доступа
		СП.17.1	Перебор паролей к учетной записи
		СП.17.3	Перебор утекших пар пользователь/пароль (Credential Stuffing)
		СП.17.8	Восстановление аутентификационной информации из сетевого трафика
		СП.18.2	Использование ошибок или отсутствия проверки прав доступа
		СП.22.6	Обход механизмов разграничения доступа
2	УБИ.041	СП.2.1	Использование недостатков, связанных с неполнотой проверки вводимых (входных) данных
		СП.22.3	Межсайтовый скриптинг (XSS) с запросами через сервер
		СП.22.4	Межсайтовый скриптинг (XSS) без участия сервера
		СП.22.16	Получение чувствительной информации со страниц приложения или из ответов сервера

№ пп	Идентификатор угрозы	Способы реализации	Содержание способов
3	УБИ.042	СП.2.3	Использование недостатков, связанных с отсутствием проверки достоверности отправителя и/или получателя
		СП.18.2	Использование ошибок или отсутствия проверки прав доступа
		СП.22.7	Нелегитимная отправка (подделка) запросов от имени пользователя (CSRF)
4	УБИ.159	СП.8.7	Обнаружение директорий сайтов
		СП.18.1	Доступ без авторизации
		СП.22.6	Обход механизмов разграничения доступа
		СП.22.20	Выход за пределы каталога (Path Traversal)
5	УБИ.167	СП.4.3	Внедрение вредоносного ПО через посещение сайтов
		СП.4.6	Внедрение вредоносного ПО через средства установки/обновления ПО
		СП.4.10	Внедрение вредоносного ПО через скомпрометированные обновления ПО или ОС
		СП.22.13	Использование уязвимых библиотек и компонентов
6	УБИ.174	СП.3.1	Эксплуатация недостатков незащищенных протоколов передачи данных
		СП.7.4	Перенаправление трафика
		СП.10.3	Атака типа «человек посредине» (MITM) через DNS-сервер
7	УБИ.175	СП.13.3	Web-фишинг
		СП.13.4	Почтовый фишинг
		СП.13.5	Рассылка SMS-сообщений или сообщений в мессенджерах (SMS-фишинг)
		СП.17.3	Перебор утекших пар пользователь/пароль (Credential Stuffing)
		СП.17.11	Перехват одноразовых паролей
8	УБИ.186	СП.4.3	Внедрение вредоносного ПО через посещение сайтов
		СП.4.9	Внедрение вредоносного ПО через мессенджеры, системы видео-конференц-связи
		СП.22.13	Использование уязвимых библиотек и компонентов
		СП.22.29	Загрузка произвольных файлов

В соответствии с [3] объектами воздействия УБИ являются ИТ-активы системы, НСД к которым или воздействие на которые в ходе реализации указанных угроз может привести к существенным негативным последствиям. С учетом результатов проведен-

ного анализа типичных для АС ОВД УБИ, реализуемых посредством фишинг-атак, изложенных в [5], определены объекты их воздействия в АС ОВД: системное ПО, прикладное ПО, сетевое ПО, сетевой узел, рабочая станция, сетевой трафик.

К несанкционированным действиям, выполняемым при реализации УБИ посредством фишинг-атаки, которые могут привести к существенным негативным последствиям для АС ОВД, относятся: создание поддельных ресурсов, маскировка ссылок и адресов, перехват учетных записей пользователей, перенаправление трафика, распространение фишинг-сообщений, внедрение вредоносного ПО, выявление данных, копирование данных, несанкционированная скрытная передача информации во внешние сети (нарушение конфиденциальности информации), стирание, модификация, несанкционированная запись информации (нарушение целостности информации), блокирование, отказ в обслуживании (нарушение доступности информации), несанкционированный запуск приложений и др.

Время (продолжительность) существования УБИ в АС ОВД, реализуемой посредством фишинг-атаки, определяется содержанием самой УБИ, длительностью существования источника угрозы или факторов возникновения угрозы [7].

Время, необходимое на реализацию УБИ в АС ОВД с использованием фейкового сайта, представляет собой временной интервал активных действий злоумышленника, требуемый для успешного проведения фишинг-атаки на АС ОВД, с момента сбора информации о системе до ликвидации следов атаки. Данный параметр зависит от: инфраструктуры и ресурсов злоумышленников; эмоционального состояния, уровня внушаемости и киберграмотности пользователей; наличия и эффективности используемых мер ЗИ; содержания уязвимостей ИТ-активов АС ОВД, наличия этих уязвимостей в известных БД; уровня возможностей злоумышленника; наличия эксплойтов и др. Например, при осуществлении доступа к ИТ-активу АС ОВД для злоумышленника с высокими возможностями реализация УБИ путем использования известной уязвимости с помощью готового эксплойта может занять минуты или даже секунды. В то же время реализация УБИ путем использования уязвимости «нулевого дня» [8] с предварительной разработкой эксплойта может занять несколько недель или месяцев. Если УБИ реализована посредством фишинг-атаки, то это не означает, что данная угроза перестала существовать.

В соответствии с [3] опасность УБИ, реализуемой с использованием фейкового сайта, определяется размером риска от ее реализации, который представляет собой сочетание возможности (вероятности) реализации угрозы и нанесения ущерба и величины возможного ущерба.

Для практического анализа и количественной оценки риска указанные компоненты традиционно объединяются в классическую модель, согласно которой величина риска (R) определяется как произведение вероятности реализации УБИ (P) и величины потенциального ущерба (D):

$$R = P \times D. \quad (1)$$

Вероятность реализации фишинг-атаки характеризует степень реальности наступления инцидента безопасности, тогда как величина ущерба отражает масштаб возможных последствий для ИТ-активов системы. Такой подход позволяет системно оценивать и сопоставлять риски, связанные с различными УБИ, реализуемыми с использованием фейковых сайтов посредством фишинг-атак, а также обосновывать выбор и приоритизацию мер ЗИ в АС ОВД.

Вместе с тем в ряде практико-ориентированных методик количественной оценки рисков применяется расширенная модель расчета, учитывающая значимость защищаемых ИТ-активов АС для деятельности организации. В этом случае величина риска определяется как произведение потенциального ущерба, вероятности реализации УБИ и приоритета (критичность) ИТ-актива (K):

$$R = P \times D \times K. \quad (2)$$

Введение в формуле (2) дополнительного множителя, отражающего критичность ИТ-актива АС для деятельности организации, позволит более точно учитывать влияние инцидентов информационной безопасности на ключевые процессы и повышает обоснованность управленческих решений в области ЗИ.

Применительно к АС ОВД использование как классической, так и расширенной моделей количественной оценки риска представляется обоснованным, поскольку ее ИТ-активы обладают высокой степенью критичности[1].

Для актуальных для АС ОВД УБИ, реализация которых посредством фишинг-атак приводит к существенным негативным последствиям (очень большому и недопустимому ущербу), опасность угрозы обусловлена в основном возможностью ее реализации в системе.

Выводы. В статье рассмотрена вербальная модель процесса реализации УБИ в АС ОВД с использованием фейковых сайтов. Приведена общая структурная схема описания такого вида угроз и проанализированы ее составные элементы применительно к типичным для АС ОВД угрозам.

Сформированная вербальная модель может быть положена в основу разработки графовых моделей процесса реализации УБИ в АС ОВД с использованием фейковых сайтов, анализ которых позволит разработать методическое обеспечение количественной оценки рисков реализации данных угроз посредством фишинг-атак.

ЛИТЕРАТУРА

1. Привалов А. Н., Смирнов В. А. К вопросу обнаружения фейковых сайтов // Современные проблемы физико-математических наук : материалы VII Всероссийской научно-практической конференции с международным участием, Орел, 18–21 ноября 2021 года / под общ. ред. Т. Н. Можаровой. — Орел : Орловский государственный университет имени И. С. Тургенева, 2021. — С. 384—391.

2. Язов Ю. К., Соловьев С. В. Защита информации в информационных системах от несанкционированного доступа : учебное пособие. — Воронеж : Кварта, 2015. — 440 с.

3. Методика оценки угроз безопасности информации : методический документ : утвержден ФСТЭК России 5 февраля 2021 г. // ФСТЭК России. — URL:

[1] АС ОВД являются системами специального назначения, которые в большинстве своем не относятся к значимым объектам критической информационной инфраструктуры Российской Федерации, но их, безусловно, можно отнести к системам критического применения (ведомственные АС обрабатывают, как правило, служебную информацию ограниченного распространения, выход их из строя ведет к существенным негативным последствиям в сфере деятельности ОВД).

https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g-2 (дата обращения: 27.02.2026).

4. Банк данных угроз ФСТЭК России. — URL: http://bdu. fstec.ru/threat (дата обращения: 26.02.2026).

5. Дровникова И. Г., Тужикова Т. Ю. Анализ угроз безопасности информации в автоматизированных системах органов внутренних дел, реализуемых посредством фишинг-атак // Вестник Дагестанского государственного технического университета. Технические науки. — 2026. — Т. 53. — № 2.

6. О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России : приказ МВД России от 9 ноября 2018 г. № 755 (Зарегистрировано в Минюсте России 05.12.2018 № 52870) // СПС «КонсультантПлюс». — URL: https://www.mvd.consultant.ru/document/1056600/ (дата обращения: 28.02.2026).

7. Попова А. Д. Динамические модели оценки защищенности программного обеспечения автоматизированных систем органов внутренних дел : дис. … канд. техн. наук : 2.3.6 / Попова Арина Дмитриевна. — Воронеж, 2026. — 183 с.

8. Уязвимость нулевого дня: современные угрозы кибербезопасности. — URL: https://blog.ishosting.com/ru/zero-day-vulnerability (дата обращения: 28.02.2026).

REFERENCES

1. Privalov A. N., Smirnov V. A. K voprosu obnaruzheniya fejkovykh sajtov // Sovremennye problemy fiziko-matematicheskikh nauk : materialy VII Vserossijskoj nauchno-prakticheskoj konferentsii s mezhdunarodnym uchastiem, Orel, 18–21 noyabrya 2021 goda / pod obshch. red. T. N. Mozharovoj. — Orel : Orlovskij gosudarstvennyj universitet imeni I. S. Turgeneva, 2021. — S. 384—391.

2. Yazov Yu. K., Solov′ev S. V. Zashchita informatsii v informatsionnykh sistemakh ot nesanktsionirovannogo dostupa : uchebnoe posobie. — Voronezh : Kvarta, 2015. — 440 s.

3. Metodika otsenki ugroz bezopasnosti informatsii : metodicheskij dokument : utverzhden FSTEK Rossii 5 fevralya 2021 g. // FSTEK Rossii. — URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g-2 (data obrashcheniya: 27.02.2026).

4. Bank dannykh ugroz FSTEK Rossii. — URL: http://bdu. fstec.ru/threat (data obrashcheniya: 26.02.2026).

5. Drovnikova I. G., Tuzhikova T. Yu. Analiz ugroz bezopasnosti informatsii v avtomatizirovannykh sistemakh organov vnutrennikh del, realizuemykh posredstvom fishing-atak // Vestnik Dagestanskogo gosudarstvennogo tekhnicheskogo universiteta. Tekhnicheskie nauki. — 2026. — T. 53. — № 2.

6. O nekotorykh voprosakh obrashcheniya so sluzhebnoj informatsiej ogranichennogo rasprostraneniya v sisteme MVD Rossii : prikaz MVD Rossii ot 9 noyabrya 2018 g. № 755 (Zaregistrirovano v Minyuste Rossii 05.12.2018 № 52870) // SPS «Konsul′tantPlyus». — URL: https://www.mvd.consultant.ru/document/1056600/ (data obrashcheniya: 28.02.2026).

7. Popova A. D. Dinamicheskie modeli otsenki zashchishchennosti programmnogo obespecheniya avtomatizirovannykh sistem organov vnutrennikh del : dis. … kand. tekhn. Nauk : 2.3.6 / Popova Arina Dmitrievna. — Voronezh, 2026. — 183 s.

8. Uyazvimost′ nulevogo dnya: sovremennye ugrozy kiberbezopasnosti. — URL: https://blog.ishosting.com/ru/zero-day-vulnerability (data obrashcheniya: 28.02.2026).

СВЕДЕНИЯ ОБ АВТОРАХ

Дровникова Ирина Григорьевна. Профессор кафедры автоматизированных информационных систем органов внутренних дел. Доктор технических наук, профессор.
Воронежский институт МВД России.
E-mail: idrovnikova@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Тужикова Татьяна Юрьевна. Адъюнкт.
Воронежский институт МВД России.
E-mail: kashirskaya.tania@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Drovnikova Irina Grigoryevna. Professor of the chair of Automatic Information Systems. Doctor of Technical Sciences, Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: idrovnikova@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tuzhikova Tatyana Yuryevna. Post-graduate cadet.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: kashirskaya.tania@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: автоматизированная система органов внутренних дел; угроза безопасности информации; структура описания угрозы; фишинг-атака; фейковый сайт; вербальная модель,

Key words: automated system of internal affairs bodies; information security threat; the structure of the threat description; phishing attack; fake site; the verbal model.

УДК 004.056

О. В. Ланкин, *доктор технических наук, доцент*
И. И. Застрожнов, *кандидат технических наук*
А. Д. Попов, *кандидат технических наук, доцент*

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ УТЕЧКИ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

MODELING OF INFORMATION LEAKAGE AND RECOVERY PROCESSES IN SECURITY SYSTEMS

В статье рассматривается применение метода исключения Гаусса для моделирования процессов утечки и восстановления информации в системах защиты. В основе подхода лежит представление канала утечки в виде системы линейных уравнений, коэффициенты которой определяются свойствами канала или структурой алгоритмов кодирования. Этапы метода — нормировка, прямой ход, формирование треугольной матрицы и обратный ход — интерпретируются как декомпозиция модели, последовательное выделение и восстановление информационных параметров. Рассматриваются вопросы численной устойчивости, вырожденности систем и применения итерационных методов. Показано использование моделей для криптоанализа линейных регистров сдвига, оценки помехоустойчивых кодов и анализа утечки по побочным электромагнитным излучениям. Результаты могут быть применены при проектировании систем защиты информации с повышенной стойкостью к линейным методам криптоанализа.

This article examines the application of the Gaussian elimination method for modeling information leakage and recovery processes in security systems. The approach is based on representing the leakage channel as a system of linear equations, whose coefficients are determined by channel properties or the structure of encoding algorithms. The stages of the method — normalization, forward elimination, formation of the triangular matrix, and back substitution — are interpreted as model decomposition, sequential extraction, and recovery of information parameters. Issues of numerical stability, system degeneracy, and the application of iterative methods are discussed. The use of models for cryptanalysis of linear feedback shift registers, evaluation of error-correcting codes, and analysis of leakage through electromagnetic side channels is demonstrated. The results can be applied in the design of security systems with enhanced resistance to linear cryptanalysis methods.

Введение. Актуальность обеспечения информационной безопасности в современных телекоммуникационных системах и вычислительных сетях обусловлена стремительным ростом объёмов передаваемых данных, увеличением числа угроз несанкционированного доступа и усложнением методов криптоанализа [1]. Одним из ключевых направлений защиты информации является разработка и анализ математических моделей, описывающих процессы формирования, передачи и перехвата сигналов, а также процессов восстановления информации по наблюдаемым данным. В основе многих таких моделей лежат системы линейных уравнений, решение которых позволяет злоумыш-

леннику восстановить ключевую информацию, параметры кодирования или передаваемые сообщения. С другой стороны, понимание структуры и свойств этих систем даёт возможность разработчикам средств защиты создавать более устойчивые алгоритмы кодирования, вводить нелинейные искажения и эффективно противодействовать атакам [2]. В данной статье рассматривается применение классического алгоритма решения систем линейных уравнений — метода исключения Гаусса — в контексте моделирования процессов утечки информации и восстановления защищаемых данных. Особое внимание уделяется интерпретации этапов метода (прямой ход, приведение к треугольному виду, обратный ход) с точки зрения построения моделей криптоанализа, моделей помехоустойчивых кодов и моделей оценки уязвимости каналов утечки информации. Математический аппарат, представленный в виде системы (1) и последующих формул (2) — (8), служит основой для построения вычислительных процедур, используемых как при проектировании систем защиты, так и при моделировании атак на них [3].

В задачах моделирования защиты информации часто возникает необходимость описания канала передачи данных или канала утечки информации с помощью системы линейных уравнений (1). Пусть имеется $n-1$ неизвестных параметров $q_i(v)$, которые могут представлять собой информационные символы, коэффициенты линейного регистра сдвига, параметры модуляции или иные значимые величины, подлежащие защите. Эти неизвестные связаны с наблюдаемыми величинами $h_{i,n}(v)$, характеризующими свойства канала связи, аппаратные особенности устройства или структуру применяемого кода.

В обобщённой форме такая модель записывается как (1).

Метод исключения Гаусса:

$$\|h_{ij}(v)\|\, q_i(v) = h_{i,n}(v),$$
$$i = \overline{1, n-1};$$
$$j = \overline{1, n-1}.$$

Для удобства будем подразумевать:

$$h_{ij} = h_{ij}(v);$$
$$q_i = q_i(v);$$
$$h_{i,n} = h_{i,n}(v),$$

и получим систему линейных уравнений:

$$\begin{cases} h_{11}q_1 + h_{12}q_2 + \ldots + h_{1,n-1}q_{n-1} = h_{1,n}; \\ h_{21}q_1 + h_{22}q_2 + \ldots + h_{2,n-1}q_{n-1} = h_{2,n}; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ h_{n-1,1}q_1 + h_{n-1,2}q_2 + \ldots + h_{n-1,n-1}q_{n-1} = h_{n-1,n}. \end{cases} \quad (1)$$

Данная модель является отправной точкой для применения метода Гаусса и лежит в основе многих криптоаналитических атак, в частности атак на основе известного открытого текста, атак на линейные генераторы псевдослучайных последовательностей и

методов восстановления ключей по побочным излучениям. Для успешного решения смоделированной системы необходимо, чтобы выполнялись определённые условия, прежде всего — отличность от нуля ведущих коэффициентов. Если первый коэффициент h_{11} равен нулю, то уравнения системы следует переставить местами, что в практических задачах моделирования может интерпретироваться как изменение порядка обработки сигналов или переупорядочивание перехваченных пакетов данных. После обеспечения ненулевого ведущего коэффициента выполняется нормировка первого уравнения, в результате чего получается приведённое уравнение (2), где коэффициенты вычисляются по формуле (3).

Если $h_{11} \neq 0$, разделив все члены первого уравнения на h_{11}, получим приведенное уравнение (1):

$$q_1 + \quad h_{12}^{(0)} q_2 \quad + \ldots + h_{1,n-1}^{(0)} q_{n-1} = h_{1,n}^{(0)}, \tag{2}$$

$$\text{где } h_{1j}^{(0)} = \frac{h_{1j}}{h_{11}}, \quad j = \overline{1,n}. \tag{3}$$

Для исключения q_1 из остальных уравнений системы (1) домножим приведенное уравнение (2) на соответствующий коэффициент при q_1 в каждом из уравнений системы (1) — h_{i1} и полученное уравнение вычтем из i-го уравнения ($i = \overline{2,n-1}$).

Получим следующую систему уравнений:

$$\begin{cases} q_1 + h_{12}^{(0)} q_2 + \ldots + h_{1,n-1}^{(0)} q_{n-1} = h_{1,n}^{(0)}; \\ \quad h_{22}^{(1)} q_2 + \ldots + h_{2,n-1}^{(1)} q_{n-1} = h_{2,n}^{(1)}; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \quad h_{n-1}^{(1)} q_2 + \ldots + h_{n-1,n-1}^{(1)} q_{n-1} = h_{n-1,n}^{(1)}. \end{cases} \tag{4}$$

Этот этап критически важен для численной устойчивости всего последующего моделирования, поскольку от точности вычисления нормированных коэффициентов зависит накопление ошибок округления при исключении неизвестных в рамках вычислительной модели.

Прямой ход метода Гаусса в контексте моделирования заключается в последовательном исключении неизвестных из системы. На первом шаге приведённое уравнение (2) используется для исключения переменной q_1 изо всех остальных уравнений. Для этого приведённое уравнение умножается на коэффициент h_{i1} при q_1 в каждом из уравнений исходной модели, после чего полученное уравнение вычитается из соответствующего i-го уравнения. В результате формируется система (4), в которой неизвестное q_1 исключено из последних $n - 2$ уравнений. Новые коэффициенты этой системы вычисляются по рекуррентной формуле (5), представляющей собой вычитание произведения исключаемого коэффициента на нормированный коэффициент из исходного значения.

$$h_{i,j}^{(1)} = h_{i,j} - h_{i,1} h_{1,j}^{(0)}, \tag{5}$$

$$\text{где } i = \overline{2, n-1},\ j = \overline{2, n}.$$

Если $h_{22}^{(1)} \neq 0$, то из системы (4) указанным выше приемом можно исключить неизвестное и получим новые коэффициенты, которые будут вычисляться по формулам типа (5) и т. д. — (прямой ход) (1).

В контексте моделирования защиты информации данный этап может интерпретироваться как декомпозиция сложной модели канала утечки на последовательность независимых подмоделей, либо как процесс последовательного выделения информационных символов в линейных кодах при построении модели декодирования [4, 5]. Если на каком-либо шаге ведущий коэффициент $h_k^{(k-1)}$ оказывается равным нулю, то дальнейшее применение метода в стандартной форме невозможно. В такой ситуации требуется перестановка уравнений, что в моделях реальных систем может соответствовать изменению порядка обработки сигналов или перестановке принятых символов. Если же после всех возможных перестановок ведущий коэффициент остаётся нулевым, это свидетельствует о линейной зависимости уравнений модели, что в задачах защиты информации может указывать на наличие избыточности в коде, на существование скрытых каналов передачи данных или на вырожденность математической модели, требующей применения итерационных методов моделирования.

В результате последовательного выполнения шагов исключения формируется треугольная матрица коэффициентов с единичной диагональю, представленная в виде (6). Коэффициенты этой матрицы вычисляются по обобщённой рекуррентной формуле (7), которая учитывает как начальные коэффициенты модели, так и все последующие преобразования.

В результате преобразований получим треугольную матрицу коэффициентов с единичной диагональю:

$$\begin{Vmatrix} 1 & h_{12}^{(0)} & h_{13}^{(0)} & \dots & h_{1,n-1}^{(0)} \\ 0 & 1 & h_2^{(1)} & \dots & h_{2,n-1}^{(1)} \\ 0 & 0 & 1 & \dots & h_{3,n-1}^{(2)} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{Vmatrix} \times \begin{Vmatrix} q_1 \\ q_2 \\ q_3 \\ \dots \\ q_{n-1} \end{Vmatrix} = \begin{Vmatrix} h_{1,n}^{(0)} \\ h_{2,n}^{(1)} \\ h_{3,n}^{(2)} \\ \dots \\ h_{n-1,n}^{(n-2)} \end{Vmatrix}, \tag{6}$$

$$\text{где} \qquad h_{i,j}^{(k)} = h_{i,j}^{(k-1)} - h_{i,k}^{(k-1)} \frac{h_{k,j}^{(k-1)}}{h_{k,k}^{(k-1)}}. \tag{7}$$

$k = \overline{1, n-2};$

$i = \overline{k+1, n-1};$

$j = \overline{k+1, n}.$

Если $i = 1$, то $h_{ij}^{(0)}$ нужно вычислять по формуле (3). Если $i \neq 1$, тогда $h_{ij}^{(0)} = h_{ij}$.

Отсюда последовательно находим неизвестные (обратный ход) (1).

Треугольная форма является удобной для последующего восстановления неизвестных в рамках обратной задачи моделирования, поскольку каждое уравнение содержит не более одного нового неизвестного. В задачах криптоаналитического моделирования треугольная матрица позволяет определить минимальное количество независимых параметров, необходимых для полного восстановления ключа, выявить структуру линейных зависимостей между передаваемыми сигналами и оценить возможность существования скрытых каналов передачи данных, образованных за счёт линейных связей между различными элементами моделируемой системы [6, 7]. Кроме того, вид треугольной матрицы даёт возможность судить о численной обусловленности исходной модели: если диагональные элементы существенно различаются по величине, это может свидетельствовать о плохой обусловленности и, следовательно, о высокой чувствительности решения к малым возмущениям входных данных, что в контексте моделирования защиты информации может быть как недостатком (уязвимость к шумам), так и преимуществом (сложность точного восстановления для злоумышленника в рамках его модели атаки).

После приведения модели к треугольному виду выполняется обратный ход метода Гаусса, позволяющий последовательно вычислить значения всех неизвестных q_i.

Соотношения для обратного хода представлены в (8).

$$\begin{cases} q_{n-1} = h_{n-1,n}^{(n-2)}; \\ q_{n-2} = h_{n-2,n}^{(n-3)} - h_{n-2,n-1}^{(n-3)} q_{n-1}; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ q_1 = h_{1,n}^{(0)} - h_{1,n-1}^{(0)} q_{n-1} - h_{1,n-2}^{(0)} q_{n-2} - \ldots - h_{1,2} q_2. \end{cases} \quad (8)$$

Коэффициент, на который делятся все члены уравнения для представления его в приведенном виде, называется «ведущим коэффициентом». Если очередной «ведущий коэффициент» окажется равным нулю, то уравнения системы следует переставить местами надлежащим образом. Если «ведущие коэффициенты» всех уравнений равны нулю — система уравнений несовместна и метод Гаусса не применим. В этом случае следует применять метод Гаусса — Зайделя (метод последовательного приближения), в котором поиск решения начинается с приближения $q_i = 0$, $i = \overline{1, n-1}$ (2). Итерации продолжаются до выполнения заданного уровня точности.

Начиная с последнего уравнения, в котором остаётся только одно неизвестное, вычисляется q_{n-1}, затем, подставляя найденное значение в предпоследнее уравнение, находится q_{n-2}, и так далее до первого уравнения. В контексте моделирования защиты информации обратный ход интерпретируется как процесс восстановления исходных данных из перехваченных сигналов или как этап криптоаналитического моделирования, на котором злоумышленник, обладая перехваченными значениями наблюдаемых величин, последовательно восстанавливает ключевую информацию. Именно на этом этапе становится возможной количественная оценка стойкости моделируемой системы защиты: если решение существует и единственно, причём процесс восстановления устойчив к малым погрешностям измерений, то модель демонстрирует уязвимость системы для атак, основанных на решении линейных уравнений. В противном случае, если решение отсутствует или сильно зависит от погрешностей входных данных, моделируемая система может считаться более защищённой при условии, что эта неопределённость не может быть

устранена злоумышленником за счёт дополнительной информации, что также должно быть учтено в модели угроз.

Важную роль при использовании метода Гаусса в задачах моделирования защиты информации играет ситуация вырожденности и то, как её можно обойти в вычислительных моделях [8, 9]. Если на каком-то шаге прямого хода ведущий коэффициент обнуляется, а перестановка строк не даёт ненулевого элемента, система считается вырожденной. В таком случае обычный метод Гаусса уже не работает, и приходится обращаться к итерационным схемам — например, к методу Гаусса — Зайделя. Здесь решение ищут, начиная с нулевого приближения $q_i = 0$, и повторяют шаги, пока не выйдут на нужную точность.

В системах защиты информации вырожденность может появляться либо из-за специально добавленной избыточности (чтобы повысить помехоустойчивость), либо при использовании помехоустойчивых кодов. С точки зрения злоумышленника это означает, что однозначно восстановить информацию без дополнительных данных не выйдет, что только повышает устойчивость моделируемой системы. Но для разработчика средств защиты здесь важнее другое: вырожденность сама по себе ещё не гарантирует безопасности. Даже в вырожденных системах итерационные методы способны сходиться к достаточно точному решению, особенно если удачно выбрано начальное приближение или есть дополнительные измерения. И этот момент обязательно нужно учитывать в комплексной модели угроз.

Одним из классических примеров использования линейных моделей в криптоанализе является моделирование взлома генераторов псевдослучайных последовательностей на основе линейных регистров сдвига с обратной связью (LFSR). Выходная последовательность такого генератора удовлетворяет линейному рекуррентному соотношению, коэффициенты которого могут быть восстановлены по известному отрезку последовательности путём построения и решения системы линейных уравнений (1). Применение метода Гаусса с использованием формул (3), (5), (7) и (8) позволяет в рамках модели атаки злоумышленнику, перехватившему достаточное количество битов выходной последовательности, определить начальное состояние регистра или коэффициенты обратной связи, что эквивалентно полному компрометированию генератора. Для защиты от подобных атак при моделировании систем защиты применяются нелинейные усложнения, такие как использование нелинейных комбинаций выходов нескольких регистров, введение неравномерного тактирования или добавление обратной связи по переносу, что выводит модель из класса линейных и делает невозможным прямое применение метода исключения в рамках стандартной модели атаки.

В системах передачи информации с помехоустойчивым кодированием моделирование процесса декодирования линейных кодов часто требует решения системы уравнений, связывающей принятые символы с информационными [10]. Метод Гаусса позволяет не только выполнить моделирование декодирования, но и оценить корректирующую способность кода в рамках имитационной модели. Если в процессе приведения к треугольному виду (6) возникает нулевой ведущий коэффициент, это может указывать на наличие ошибки в принятой комбинации, которую код способен исправить. Таким образом, метод исключения служит не только инструментом решения, но и средством диагностики состояния канала связи в рамках построенной модели. В моделях систем защиты информации, использующих помехоустойчивое кодирование как один из эшелонов защиты, важно, чтобы декодер, построенный на основе метода Гаусса, был устойчив

к ошибкам округления и обеспечивал корректное исправление ошибок в условиях реальных каналов с шумами. При этом при моделировании действий злоумышленника, перехватывающего зашумлённые сигналы, применение метода Гаусса позволяет оценить возможность восстановления информации в условиях наличия помех, что даёт количественную оценку стойкости системы [12, 13].

Ещё одной важной областью применения рассматриваемого математического аппарата является моделирование побочных электромагнитных излучений (ПЭМИН) как канала утечки информации. При обработке данных в цифровых устройствах, таких как процессоры, контроллеры и средства криптографической защиты, возникают электромагнитные излучения, параметры которых линейно связаны с обрабатываемой информацией. Построение математической модели такого канала утечки приводит к системе (1), где коэффициенты h_{ij} определяются конструктивными особенностями устройства, трассировкой печатной платы, используемыми элементами и режимами работы. Решение этой системы методом Гаусса в рамках модели атаки позволяет злоумышленнику, оснащённому специальной измерительной аппаратурой, восстановить обрабатываемые данные по перехваченным сигналам. Для защиты от таких атак при моделировании систем защиты применяются методы маскировки, такие как генерация широкополосного шума, синхронизация тактовых частот с некоррелированными источниками, а также использование нелинейных преобразований данных, нарушающих линейность модели. Однако даже при наличии нелинейных искажений в некоторых случаях возможно линеаризовать модель в малой окрестности рабочей точки, что вновь делает применимым метод Гаусса, поэтому моделирование защиты от ПЭМИН требует комплексного подхода, учитывающего как аппаратные, так и алгоритмические меры [11].

При реальном программировании вычислительных моделей, где метод Гаусса применяется для задач защиты информации, на первый план выходят численная устойчивость и точность расчётов. Если использовать формулы (5) и (7), ошибки округления будут накапливаться и в системах большой размерности или при плохой обусловленности матрицы результат может сильно исказиться. В криптоаналитических моделях даже маленькая погрешность иногда приводит к неверному восстановлению ключа, так что требования к точности здесь жёсткие.

Чтобы модель работала устойчивее, обычно выбирают главный элемент по столбцу или по всей матрице, масштабируют уравнения, чтобы выровнять порядки коэффициентов, и используют повышенную разрядность — вплоть до двойной или произвольной точности. Иногда выгоднее взять целочисленный вариант метода Гаусса в поле Галуа: тогда ошибки округления исчезают полностью, но зато появляются ограничения на тип исходных данных. В моделях защиты информации, где коэффициенты и неизвестные заданы в конечных полях, метод Гаусса в полях GF (2) или $GF(2^m)$ давно стал стандартным инструментом — например, при криптоанализе регистров сдвига или линейных кодов.

В системах защиты информации итерационные методы используют, например, для моделирования восстановления сигнала при сильных помехах, когда точного решения всё равно не получить из-за низкого отношения сигнал/шум, для оценки параметров канала при неполных данных, а также для анализа того, насколько криптосистема устойчива к атакам с неточными входными данными. Важно отметить, что сходимость итерационных методов зависит от свойств матрицы системы и в некоторых случаях они могут не сходиться или сходиться медленно, что делает их неприменимыми для реальных временных масштабов. Поэтому при проектировании систем защиты, устойчивых к атакам,

на этапе моделирования стремятся к тому, чтобы матрица системы была либо вырожденной, либо плохо обусловленной, либо имела спектральные характеристики, затрудняющие сходимость итерационных методов.

Заключение. Метод исключения Гаусса представляет собой не только фундаментальный инструмент вычислительной математики, но и важнейшее средство моделирования процессов утечки и восстановления информации в системах защиты. Рассмотренный математический аппарат, включающий исходную модель (1), формулы приведения (2) и (3), рекуррентные соотношения прямого хода (4) — (7), а также соотношения обратного хода (8), позволяет строить адекватные модели процессов утечки информации по линейным каналам, модели восстановления ключевых параметров по перехваченным данным, модели оценки уязвимостей помехоустойчивых кодов и криптографических генераторов. Понимание структуры линейных моделей и особенностей их решения даёт возможность разработчикам средств защиты информации эффективно противодействовать криптоаналитическим атакам путём введения нелинейных преобразований, использования вырожденных или плохо обусловленных моделей, а также применения итерационных методов декодирования, устойчивых к шумам. В то же время для специалистов по криптоанализу владение методом Гаусса и его модификациями является необходимым условием успешного моделирования и оценки стойкости защищённых систем. Таким образом, глубокое понимание данного математического аппарата, выходящее за рамки формального применения, составляет основу для построения надёжных и сбалансированных моделей систем обеспечения информационной безопасности в условиях современных угроз.

ЛИТЕРАТУРА

1. Авраменко В. С., Саенко И. Б., Котенко И. В. Прогнозная модель защищенности информации в инфокоммуникационных системах на основе рекуррентной нейронной сети // Правовая информатика. — 2025. — № 2. — С. 140—147.

2. Будзко В. И., Беленков В. Г. Кибербезопасность систем, реализующих интенсивное использование данных и использующих технологии искусственного интеллекта // Системы высокой доступности. — 2025. — Т. 21. — № 1. — С. 52—62.

3. Гаврилов В. Е., Зацаринный А. А. Некоторые системотехнические вопросы использования интеллектуального анализа данных для обеспечения защиты информации в ситуационных центрах // Системы и средства информатики. — 2018. — Т. 28. — № 1. — С. 89—98.

4. Гаврилов В. Е., Зацаринный А. А. Некоторые системотехнические и нормативно-методические вопросы обеспечения защиты информации в автоматизированных информационных системах на облачных технологиях с использованием методов искусственного интеллекта // Системы и средства информатики — 2016. — Т. 26. — № 4. — С. 38—50.

5. Даирбекова Ж. М., Полуян А. Ю. Анализ возможностей искусственного интеллекта в выявлении и предотвращении кибератак // Системная инженерия и информационные технологии. — 2025. — Т. 7. — № 2(21). — С. 56—67.

6. Модель оценки эффективности программных систем защиты информации в системах электронного документооборота / С. А. Змеев, Д. В. Солод, Е. И. Сиренький, И. И. Застрожнов // Вестник Воронежского института ФСИН России. — 2013. — № 1. — С. 82—85.

7. Исакова Т. А. Аналитический обзор методов искусственного интеллекта в обнаружении сетевых вторжений // Современные тенденции развития науки и мирового сообщества в эпоху цифровизации : сборник материалов XXVI Международной научно-практической конференции. — М., 2024. — С. 202—205.

8. Модель оценки эффективности конфигурации системы защиты информации на базе генетических алгоритмов / И. М. Космачева, Н. В. Давидюк, И. В. Сибикина, И. Ю. Кучин // Моделирование, оптимизация и информационные технологии. — 2020. — Т. 8. — № 3(30).

9. Автоматизированная система анализа слабоструктурированных данных кибер-разведки с использованием больших языковых моделей / А. И. Луцкович, В. И. Васильев, А. М. Вульфин [и др.] // Информационно-управляющие системы. — 2025. — № 2(135). — С. 50—67.

10. Менисов А. Б., Ломако А. Г., Дудкин А. С. Метод защиты нейронных сетей от компьютерных бэкдор-атак на основе идентификации триггеров закладок // Научно-технический вестник информационных технологий, механики и оптики. — 2022. — Т. 22. — № 4. — С. 742—750.

11. Методика обнаружения атак типа SQL-инъекция на основе алгоритмов искусственного интеллекта, методом задачи классификации / М. В. Митрофанов, А. М. Крибель, А. С. Фроленков, О. Л. Спицын // Наукоемкие технологии в космических исследованиях Земли. — 2021. — Т. 13. — № 5. — С. 96—102.

12. Ревякина Е. А., Кучерова С. В. Разработка модели выявления ложной и вредоносной информации на основе нейросетевых технологий // Научно-исследовательские публикации. — 2025. — № 4. — С. 44—54.

13. Скрыль С. В., Окрачков А. А. Метод количественной оценки показателей эффективности систем защиты информации от несанкционированного доступа // Вестник Воронежского института МВД России. — 2013. — № 3. — С. 78—83.

REFERENCES

1. Avramenko V. S., Saenko I. B., Kotenko I. V. Prognoznaya model′ zashchishchennosti informatsii v infokommunikatsionnykh sistemakh na osnove rekurrentnoj nejronnoj seti // Pravovaya informatika. — 2025. — № 2. — S. 140—147.

2. Budzko V. I., Belenkov V. G. Kiberbezopasnost′ sistem, realizuyushchikh intensivnoe ispol′zovanie dannykh i ispol′zuyushchikh tekhnologii iskusstvennogo intellekta // Sistemy vysokoj dostupnosti. — 2025. — T. 21. — № 1. — S. 52—62.

3. Gavrilov V. E., Zatsarinnyj A. A. Nekotorye sistemotekhnicheskie voprosy ispol′zovaniya intellektual′nogo analiza dannykh dlya obespecheniya zashchity informatsii v situatsionnykh tsentrakh // Sistemy i sredstva informatiki. — 2018. — T. 28. — № 1. — S. 89—98.

4. Gavrilov V. E., Zatsarinnyj A. A. Nekotorye sistemotekhnicheskie i normativno-metodicheskie voprosy obespecheniya zashchity informatsii v avtomatizirovannykh informatsionnykh sistemakh na oblachnykh tekhnologiyakh s ispol′zovaniem metodov iskusstvennogo intellekta // Sistemy i sredstva informatiki — 2016. — T. 26. — № 4. — S. 38—50.

5. Dairbekova Zh. M., Poluyan A. Yu. Analiz vozmozhnostej iskusstvennogo intellekta v vyyavlenii i predotvrashchenii kiberatak // Sistemnaya inzheneriya i informatsionnye tekhnologii. — 2025. — T. 7. — № 2(21). — S. 56—67.

6. Model′ otsenki effektivnosti programmnykh sistem zashchity informatsii v sistemakh elektronnogo dokumentooborota / S. A. Zmeev, D. V. Solod, E. I. Siren′kij, I. I. Zastrozhnov // Vestnik Voronezhskogo instituta FSIN Rossii. — 2013. — № 1. — S. 82—85.

7. Isakova T. A. Analiticheskij obzor metodov iskusstvennogo intellekta v obnaruzhenii setevykh vtorzhenij // Sovremennye tendentsii razvitiya nauki i mirovogo soobshchestva v epokhu tsifrovizatsii : sbornik materialov XXVI Mezhdunarodnoj nauchno-prakticheskoj konferentsii. — M., 2024. — S. 202—205.

8. Model′ otsenki effektivnosti konfiguratsii sistemy zashchity informatsii na baze geneticheskikh algoritmov / I. M. Kosmacheva, N. V. Davidyuk, I. V. Sibikina, I. Yu. Kuchin // Modelirovanie, optimizatsiya i informatsionnye tekhnologii. — 2020. — T. 8. — № 3(30).

9. Avtomatizirovannaya sistema analiza slabostrukturirovannykh dannykh kiberrazvedki s ispol′zovaniem bol′shikh yazykovykh modelej / A. I. Lutskovich, V. I. Vasil′ev, A. M. Vul′fin [i dr.] // Informatsionno-upravlyayushchie sistemy. — 2025. — № 2(135). — S. 50—67.

10. Menisov A. B., Lomako A. G., Dudkin A. S. Metod zashchity nejronnykh setej ot komp′yuternykh bekdor-atak na osnove identifikatsii triggerov zakladok // Nauchno-tekhnicheskij vestnik informatsionnykh tekhnologij, mekhaniki i optiki. — 2022. — T. 22. — № 4. — S. 742—750.

11. Metodika obnaruzheniya atak tipa SQL-in″ektsiya na osnove algoritmov iskusstvennogo intellekta, metodom zadachi klassifikatsii / M. V. Mitrofanov, A. M. Kribel′, A. S. Frolenkov, O. L. Spitsyn // Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli. — 2021. — T. 13. — № 5. — S. 96—102.

12. Revyakina E. A., Kucherova S. V. Razrabotka modeli vyyavleniya lozhnoj i vredonosnoj informatsii na osnove nejrosetevykh tekhnologij // Nauchno-issledovatel′skie publikatsii. — 2025. — № 4. — S. 44—54.

13. Skryl′ S. V., Okrachkov A. A. Metod kolichestvennoj otsenki pokazatelej effektivnosti sistem zashchity informatsii ot nesanktsionirovannogo dostupa // Vestnik Voronezhskogo instituta MVD Rossii. — 2013. — № 3. — S. 78—83.

СВЕДЕНИЯ ОБ АВТОРАХ

Ланкин Олег Викторович. Профессор кафедры автоматизированных информационных систем органов внутренних дел. Доктор технических наук, доцент.
Воронежский институт МВД России.
E-mail: oleg_lankin@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Застрожнов Игорь Иванович. Доцент кафедры автоматизированных информационных систем органов внутренних дел. Кандидат технических наук.
Воронежский институт МВД России.
E-mail: zasigor@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Попов Антон Дмитриевич. Доцент кафедры автоматизированных информационных систем органов внутренних дел. Кандидат технических наук, доцент.
Воронежский институт МВД России.
E-mail: antonholmes@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Lankin Oleg Viktorovich. Professor of the chair of Automated Information Systems of Internal Affairs Bodies. Doctor of Technical Sciences, Associate Professor.

Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: oleg_lankin@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Zastrozhnov Igor Ivanovich. Associate Professor of the chair of Automated Information Systems of Internal Affairs Bodies. Candidate of Technical Sciences.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: zasigor@yandex.ru.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Popov Anton Dmitrievich. Associate Professor of the chair of Automated Information Systems of Internal Affairs Bodies. Candidate of Technical Sciences, Associate Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: antonholmes@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: метод Гаусса; исключение неизвестных; моделирование утечки информации; восстановление информации; линейные системы уравнений; криптоанализ; помехоустойчивые коды; побочные электромагнитные излучения; линейные регистры сдвига; вырожденные системы; итерационные методы; метод Гаусса — Зайделя; треугольная матрица; прямой ход; обратный ход; численная устойчивость.

Key words: Gaussian elimination; elimination of unknowns; information leakage modeling; information recovery; linear systems of equations; cryptanalysis; error-correcting codes; electromagnetic side-channel emissions; linear feedback shift registers; degenerate systems; iterative methods; Gauss — Seidel method; triangular matrix; forward elimination; back substitution; numerical stability.

УДК 681.3

А. Е. Лоскутова
Н. А. Алейникова, *кандидат физико-математических наук, доцент*
М. Г. Матвеев, *доктор технических наук, профессор*

АВТОМАТИЗАЦИЯ МОНИТОРИНГА И УПРАВЛЕНИЯ КАЧЕСТВОМ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

AUTOMATION OF MONITORING AND MANAGEMENT OF THE EDUCATIONAL PROCESS QUALITY

В статье предложена технология автоматизированного мониторинга и управления успеваемостью в образовательных учреждениях. Технология основана на анализе динамики отметок учащихся с использованием дискретных цепей Маркова с нечеткими состояниями. Особенностью технологии является дифференцированный подход к оценке уровня усвоения знаний: на основе предварительной кластеризации учащихся по схожести их учебных показателей для каждой группы рассчитываются индивидуальные эталонные вероятности успеваемости. Текущая успеваемость оценивается через предельные вероятности нечетких состояний, что позволяет учитывать не только средний балл, но и вариативность, динамику и тенденции изменения отметок. При значимом отклонении фактических показателей от эталонных система автоматически генерирует сигнал преподавателю о необходимости педагогического вмешательства. Разработанная технология может быть интегрирована в существующие системы управления обучением для снижения нагрузки на преподавателей и повышения эффективности управления образовательным процессом.

The article proposes a technology for automating the monitoring and management of academic performance in educational institutions. The technology is based on analyzing the dynamics of student grades using discrete Markov chains with fuzzy states. A distinctive feature of the technology is a differentiated approach to assessing the level of knowledge acquisition: based on preliminary clustering of students according to the similarity of their learning indicators, individual reference probabilities of academic performance are calculated for each group. Current performance is assessed through the limit probabilities of fuzzy states, which allows taking into account not only the average score, but also the variability, dynamics, and trends in grade changes. When actual indicators significantly deviate from the reference ones, the system automatically generates a signal to the teacher about the need for pedagogical intervention. The developed technology can be integrated into existing learning management systems to reduce teacher workload and increase the efficiency of educational process management.

Введение. На современном этапе цифровизации образовательной среды наблюдается следующая ситуация: при широком внедрении систем управления обучением (LMS), электронных деканатов и образовательных платформ автоматизация охватывает преимущественно рутинные операции — фиксацию результатов промежуточной аттестации, расчет рейтингов, генерацию стандартных отчетов. По данным исследований [1,

2], существует значительный дисбаланс между автоматизацией учетно-административных функций и управлением образовательным процессом, в том числе с использованием искусственного интеллекта.

Перечислим некоторые ключевые проблемы автоматизации образовательного процесса:

- несмотря на хранящиеся в LMS данные об учащихся (отметки, посещаемость), они не вполне используются для получения готовых аналитических рекомендаций для преподавателей;

- недостаточно инструментов поддержки принятия педагогических решений, например, преподаватели, как и раньше, вынуждены вручную анализировать динамику успеваемости каждого учащегося;

- существующие системы не учитывают индивидуальных особенностей учащихся.

Это обусловливает актуальность разработки алгоритмов и моделей с искусственным интеллектом, автоматизирующих процессы поддержки принятия решений преподавателем.

Во всем мире ведутся интенсивные разработки технологий поддержки принятия педагогических решений на основе данных с использованием методов искусственного интеллекта [3—7]. Однако большинство технологий основано на методах машинного обучения, требующих привлечения большого объема разнородной информации об учащихся. Используемые в учебных заведениях системы и технологии не обеспечивают возможности автоматизированного сбора этой информации из-за существующих организационно-технических проблем, прежде всего, связанных со слабой интегрированностью между LMS и другими сервисами, используемыми в образовательных и аналитических целях. Следствием этого является отсутствие эффективного обмена данными, синхронизации процессов и единой цифровой среды, что приводит к фрагментации информации и невозможности создания целостного цифрового следа учащегося.

Необходимо разработать технологию, которая бы позволила автоматизировать мониторинг уровня усвоения учебного материала учащимися по относительно небольшому объему доступной информации и проведение ранней диагностики возможных проблем с успеваемостью каждого учащегося. Кроме того, технология должна основываться на дифференцированном подходе к оценке уровня усвоения знаний учащимися в зависимости от их способностей и индивидуальных особенностей.

В статье предлагается математический аппарат, основанный на моделях дискретных марковских цепей и нечетких множеств, позволяющий разработать такую технологию.

Благодаря внедрению технологии в существующие LMS преподаватели смогут автоматически получать сигнал о необходимости вмешательства в процесс обучения учащихся, если это требуется, что значительно снизит их нагрузку.

Постановка задачи. В педагогической литературе успеваемость рассматривается как количественная характеристика степени усвоения материала учащимися, выраженная в отметках (баллах), а, с другой стороны, как комплексный качественный показатель, измеряющий глубину, осознанность, системность знаний.

По отметкам можно лишь косвенно судить об успеваемости как о качественном показателе усвоения знаний. Отметка, полученная в ходе текущего контроля, по сути, является результатом выборочного контроля, что не всегда обеспечивает объективность

оценивания. Учащийся мог плохо себя чувствовать, переволноваться, случайно ошибиться в ключевом вычислении, хотя общий метод усвоил, или, наоборот, ему просто повезло. Одна отметка не отражает устойчивого состояния знаний. В то же время, если рассматривать успеваемость как комплексный показатель, то необходимо автоматизировать учет и анализ целой совокупности характеристик по каждому учащемуся, таких как академическая успеваемость, психометрические показатели, посещаемость, учебная активность. На современном этапе автоматизации это затруднительно прежде всего из-за существующих организационно-технических проблем, которые были перечислены во введении, отсутствия единых шкал оценивания результатов, методик сбора личностных характеристик, связанных с конфиденциальностью информации, и т. д.

В статье предлагается проводить оценку уровня усвоения учебного материала на основе отметок учащегося, но при этом перейти от отдельных отметок к анализу их динамики. Несколько отметок по одной теме действительно могут выявить тренд. Стабильно низкие отметки с высокой вероятностью указывают на проблемы в усвоении учебного материала. На проблемы усвоения может указывать также большая вариативность отметок, что может свидетельствовать о нестабильности в усвоении материала, о наличии пробелов в знаниях. Анализируя динамику отметок, можно судить о вероятности того или иного уровня усвоения учебного материала, о наличии проблем и о необходимости дальнейшей диагностики.

Таким образом, первая задача, решению которой посвящена статья, — разработать технологию автоматического мониторинга и управления успеваемостью, которая бы основывалась на анализе динамики отметок, полученных учащимися. В рамках этой задачи также надо разработать показатель, который бы измерял уровень знаний при той или иной динамике отметок в категориях, понятных преподавателю.

Вторая задача, которую необходимо решить в рамках разрабатываемой технологии, — это учет индивидуальных особенностей учащихся при автоматической оценке их достижений. Система оценивания в образовательных учреждениях исторически сложилась как унифицированная: ко всем учащимся предъявляются одинаковые требования, и их достижения оцениваются по единой шкале (единому эталону).

Однако такая унификация не учитывает:

- разный уровень способностей учащихся;
- разную мотивацию и познавательные интересы;
- разный темп усвоения материала;
- разные стартовые условия (базовый уровень подготовки);
- индивидуальные психофизиологические особенности.

Унифицированное оценивание является проблемой как для учащегося, так и для преподавателя. Для учащегося такой способ оценки ведет прежде всего к демотивации («я все равно не могу достичь уровня отличников»), к возникновению ощущения несправедливости («меня оценивают так же, как тех, кому легче дается учеба»), к потере уверенности в своих силах, к формированию заниженной самооценки. Для преподавателя негативными последствиями такого оценивания являются невозможность адекватно оценить прогресс слабого учащегося, сложность постановки реалистичных целей для разных групп учащихся.

Необходимо разработать компромиссное решение между полной индивидуализацией (нереалистичной из-за трудоемкости) и унифицированным подходом (несправедливым) в виде дифференцированного подхода, который бы заключался в разделении учащихся на группы по схожести их успеваемости по результатам предыдущих периодов

обучения. Для каждой группы необходимо разработать свои целевые установки к уровню усвоения учебного материала, учитывающие особенности учащихся. В статье предлагаются методы формализации таких целевых установок. Далее рассмотрим решение каждой из перечисленных задач.

Разработка показателя уровня усвоения учебного материала и его категорий. Как уже отмечалось выше, в высших учебных заведениях нет единой шкалы для оценки успеваемости. Отметки могут выставляться в 4-балльной шкале, в 50-балльной и т. д. Для унификации успеваемости как показателя уровня усвоения знаний предлагается перейти к единой шкале путем нормировки отметок:

$$s_t = \frac{x_t}{x_t^{\max}} \in [0;1], \tag{1}$$

где x_t — отметка (в виде балла), полученная в момент времени t, $x_t^{\max}$ — максимально возможный балл.

Показатель (1) может принимать бесконечное множество значений, тогда как для понятия об уровне усвоения материала и принятия решения достаточно нескольких категорий. Можно разбить диапазон значений этого показателя на непересекающиеся интервалы и каждому интервалу поставить в соответствие характеристику степени усвоения материала в виде категорий «Плохо», «Удовлетворительно», «Хорошо» и «Отлично». Например, если значение s_t от 0,95 до 1, то степень усвоения материала учащимся на «Отлично». Таким образом будет происходить переход от непрерывной шкалы от нуля до единицы к дискретной категориальной шкале. Но на практике одно и то же значение s_t можно с разной степенью уверенности отнести сразу к двум соседним категориям. Поэтому во избежание потери информации обо всех потенциальных состояниях успеваемости как текущего уровня усвоения материала на множестве значений показателя (1) предлагается ввести нечеткие категории, описываемые нечеткими множествами $\tilde{S}_i, i = \overline{1,4}$, где

$$\tilde{S}_1 = \text{«Плохо»},\ \tilde{S}_2 = \text{«Удовлетворительно»},\ \tilde{S}_3 = \text{«Хорошо»},\ \tilde{S}_4 = \text{«Отлично»}. \tag{2}$$

Введем в рассмотрение лингвистическую переменную «Успеваемость», термами которой являются нечеткие категории (2). Обозначим ее через $\tilde{S}$. Пусть

$$\mu_{\tilde{S}_i}(s_t),\ i = \overline{1,4} \tag{3}$$

— функции принадлежности термов (2).

Для упрощения расчетов в качестве (3) предлагается использовать треугольные или трапециевидные функции [8]. Например, функции принадлежности могут быть заданы следующим образом:

$$\mu_{\tilde{S}_1}(x) = \begin{cases} 1, & 0 \le x \le 0{,}5, \\ \dfrac{0{,}6 - x}{0{,}1}, & 0{,}5 \le x \le 0{,}6, \\ 0, & \textit{иначе.} \end{cases} \qquad \mu_{\tilde{S}_2}(x) = \begin{cases} 0, & x < 0{,}5 \textit{ или } x > 0{,}75, \\ \dfrac{x - 0{,}5}{0{,}1}, & 0{,}5 \le x \le 0{,}6, \\ \dfrac{0{,}75 - x}{0{,}15}, & 0{,}6 < x \le 0{,}75. \end{cases}$$

$$\mu_{\tilde{S}_3}(x)=\begin{cases}0, & x<0{,}7 \text{ или } x>0{,}95,\\ \dfrac{x-0{,}7}{0{,}1}, & 0{,}7\le x\le 0{,}8,\\ \dfrac{0{,}95-x}{0{,}15}, & 0{,}8<x\le 0{,}95.\end{cases} \qquad \mu_{\tilde{S}_4}(x)=\begin{cases}0, & x<0{,}85 \text{ или } x>1,\\ \dfrac{x-0{,}85}{0{,}1}, & 0{,}85\le x\le 0{,}95,\\ 1, & 0{,}95\le x\le 1.\end{cases}$$

Динамику успеваемости для определения уровня усвоения учебного материала в дальнейшем будем анализировать с точки зрения динамики нечетких термов переменной $\tilde{S}$.

Определение уровня усвоения учебного материала на основе анализа динамики отметок. Традиционный анализ успеваемости основан на вычислении среднего балла, что не позволяет учитывать динамику изменений и неопределенность в оценках. Основные недостатки традиционного подхода заключаются в потере информации о последовательности получения отметок; игнорировании вариативности и нестабильности отметок; отсутствии учета нечеткости границ между уровнями знаний; невозможности с помощью статичной отметки объективно измерить истинный уровень усвоения учебного материала учеником.

Для преодоления указанных недостатков традиционного подхода успеваемость в данной работе рассматривается как динамическая система с нечеткими состояниями в виде нечетких термов (2). Анализ динамики такой системы предлагается проводить на основе моделей дискретной марковской цепи.

Для перехода от отметок x_t, полученных учащимся в моменты времени t, к нечетким термам (2) сначала рассчитывается показатель (1). Затем его значения подставляют в функции принадлежности (3) и получают последовательность термов:

$$\tilde{S}_t = (\tilde{S}_{i,t} \big/ \mu_{\tilde{S}_i}(s_t) \neq 0,\ i=\overline{1,4}). \tag{4}$$

Отметим, что в каждый момент времени t может наблюдаться сразу несколько нечетких термов (2) лингвистической переменной $\tilde{S}$ с разными значениями функции принадлежности.

Классическая модель дискретной марковской цепи состоит из трех компонент:

$$(\mathbf{S}, \mathbf{M}, \mathbf{p}_0), \tag{5}$$

где $\mathbf{S}$ — совокупность состояний системы, $\mathbf{M}$ — матрица переходных вероятностей (или стохастическая матрица), элементы которой — вероятности p_{ij} перехода из состояния S_i в S_j за один шаг; $\mathbf{p}_0$ — вектор начальных вероятностей состояний системы.

Расчет марковской цепи производится с помощью формулы Колмогорова — Чепмена

$$\mathbf{p}_t = \mathbf{p}_{t-1} \cdot \mathbf{M}, \tag{6}$$

где $\mathbf{p}_t$ — вероятностное распределение состояний из $\mathbf{S}$ на шаге t.

С помощью формулы (6) можно получить вероятности термов лингвистической переменной $\tilde{S}$ на момент времени t, то есть, по сути, классифицировать уровни усвое-

ния учебного материала на текущий момент времени [9]. При этом информация о характере динамики отметок содержится в матрице $\mathbf{M}$, а начальный уровень знаний учащегося перед началом изучения дисциплины — в векторе $\mathbf{p}_0$.

Но в отличие от классической модели в нашем случае состояния системы — нечеткие термы (2) и в каждый момент времени их может быть несколько. В этих условиях необходимо найти матрицу $\mathbf{M}$ и $\mathbf{p}_0$.

Зафиксируем событие, когда лингвистическая переменная $\tilde{S}$ меняет терм с $\tilde{S}_i$ на шаге $t-1$ на терм $\tilde{S}_j$ на шаге t, в виде нечеткой импликации

$$(\tilde{S}_{i,t-1} \to \tilde{S}_{j,t}) \,|\, \mu_{ij}^t \,, \tag{7}$$

где $\mu_{ij}^t = \min\left(\mu_{\tilde{S}_{i,t-1}}; \mu_{\tilde{S}_{j,t}}\right)$, t — моменты времени, когда выставлялись отметки.

В работе [10] матрицу $\mathbf{M}$ к моменту времени t было предложено оценивать с помощью формулы

$$\mathbf{M}_t = \frac{1}{n-1}\begin{pmatrix} \sum\limits_{t=1}^{n-1} \mu_{11}^t & \cdots & \sum\limits_{t=1}^{n_k-1} \mu_{14}^t \\ \cdots & \cdots & \cdots \\ \sum\limits_{t=1}^{n-1} \mu_{41}^t & \cdots & \sum\limits_{t=1}^{n_k-1} \mu_{44}^t \end{pmatrix}, \tag{8}$$

где n — с одной стороны, количество отметок, полученных за период от начала оценивания до момента времени t, с другой — количество моментов времени, когда эти отметки выставлялись; μ_{ij}^t — значение функции принадлежности импликации (7) в момент времени t.

Матрицу $\mathbf{M}_t$ нормируют по строкам для достижения свойств стохастической матрицы.

Рассмотрим теперь способы оценки вероятностного распределения $\mathbf{p}_0$. Распределение $\mathbf{p}_0$ отражает достигнутый уровень успеваемости учащихся к моменту начала мониторинга дисциплины. Это достижения учащихся за предыдущий период времени. Для оценки этих достижений используется входной контроль, заключающийся, как правило, в тестировании учащихся. Но здесь возникают те же проблемы, что обсуждались ранее. Тестирование — это, по сути, одна из форм выборочного контроля, который не позволяет объективно оценить уровень знаний учащегося, лишь косвенно учитывает качество его учебы ранее. Для оценки $\mathbf{p}_0$ также важно учитывать динамику отметок, полученных учащимся в предыдущие периоды, важна направленность, тенденция динамики отметок, их вариативность. По этой же причине не подходят такие способы для оценивания $\mathbf{p}_0$, как средние баллы или подсчет относительных долей отметок, полученных учащимся за предыдущий период, так как эти методы также не позволяют анализировать характер его учебы в динамике.

Для оценки начального распределения $\mathbf{p}_0$ в работе предлагается использовать тот же математический аппарат, что и для текущего мониторинга — дискретные цепи Маркова с нечеткими состояниями, применяя его к отметкам предыдущего периода. Для оценки достигнутого уровня успеваемости учащихся предлагается найти предельные ве-

роятности его нечетких состояний. Предельные вероятности показывают, какое распределение оценок установится у учащегося в долгосрочной перспективе, если сохранятся текущие закономерности его обучения.

Предельные вероятности дают комплексную характеристику**,** учитывающую уровень знаний — через соотношение вероятностей; стабильность — через разброс вероятностей; тенденции — через смещение в сторону лучших или худших отметок; динамику — через матрицу переходных вероятностей, из которой они получены.

Оценка распределения $\mathbf{p}_0$ включает следующие шаги:

1. Сбор данных (отметок) за предыдущий период обучения по каждому учащемуся по выбранной дисциплине.
2. Нормировка отметок по формуле (1).
3. Фаззификация — расчет степеней принадлежности нормированных отметок к нечетким термам (2).
4. Построение матрицы переходных вероятностей $\mathbf{M}$ по формуле (8).
5. Расчет предельных вероятностей для описания начального вероятностного распределения $\mathbf{p}_0$ с помощью решения матричного уравнения:

$$\mathbf{p}_0 = \mathbf{p_0 M}, \tag{9}$$

при условии выполнения равенства единице суммы предельных вероятностей.

В статье [10] приводятся условия существования предельных вероятностей. В случае, если оценка предельных вероятностей производилась по нескольким дисциплинам, в статье [11] предлагается способ агрегирования этих вероятностей с учетом возможности разного вклада этих дисциплин в формирование итогового вероятностного распределения с помощью интеграла Шоке.

Приведем простые примеры, демонстрирующие преимущества использования предельных вероятностей для подведения итогов по успеваемости по сравнению с традиционными подходами в виде относительных долей отметок или средних баллов. Для сравнения итогового распределения вероятностей в виде предельных вероятностей и относительных долей отметок рассмотрим следующий пример: имеется два студента с одинаковыми наборами отметок, но разной динамикой. Вся информация представлена в таблице 1.

Таблица 1

Сравнение итоговых распределений, найденных с помощью относительных долей и предельных вероятностей в зависимости от направления динамики

Студент	Последовательность отметок	Относительные частоты	Предельные вероятности
А (спад)	5, 5, 5, 5, 5, 4, 4, 4, 4, 4	P(5) = 0.5, P(4) = 0.5	$\mathbf{p}_0 = (0, 0, 0.58, 0.42)$
Б (рост)	4, 4, 4, 4, 4, 5, 5, 5, 5, 5	P(5) = 0.5, P(4) = 0.5	$\mathbf{p}_0 = (0, 0, 0.42, 0.58)$

Следовательно, предельные вероятности отражают направление тренда, в то время как относительные частоты дают одинаковый результат. У студента Б наблюдается неубывающая тенденция в изменении отметок и вероятность терма «Отлично» больше, чем у студента А, у которого происходит спад отметок.

Покажем на еще одном простом примере чувствительность предельных вероятностей к вариации отметок. Рассмотрим двух студентов с одинаковым средним баллом, но разной вариацией отметок и покажем, что предельные вероятности дают разные результаты, отражающие эту вариацию. Информация представлена в таблице 2.

Таблица 2

Сравнение среднего балла и итоговой оценки на основе предельных вероятностей

Студент	Последовательность отметок	Средний балл	Предельные вероятности	Характеристика студента	Матем. ожидание (на основе $\mathbf{p}_0$)
А	4, 4, 4, 4, 4, 4, 4, 4, 4, 4	4.0	$p_0 = (0, 0, 1, 0)$	стабильный, все отметки одинаковые	4
Б	5, 3, 5, 3, 5, 3, 3, 3, 5, 5	4.0	$p_0 = (0, 0.56, 0, 0.4$	вариативный, чередование отметок	3.88

Выводы, которые можно сделать по таблице 2:

- средний балл одинаков у обоих студентов и равен 4, но предельные вероятности разные;
- предельные вероятности отражают структуру вариации:

студент А — стабильный «хорошист»;

студент Б — нестабильный, с чередованием «отлично» и «удовлетворительно»;

- для студента Б предельные вероятности показывают смещение к удовлетворительным результатам (56%) из-за более частого чередования отметок;
- математическое ожидание для студента Б (3.88) ниже, чем для студента А (4.0), несмотря на одинаковый средний балл. Это отражает тот факт, что предельные вероятности учитывают изменчивость динамики, а не только среднее.

Дифференцированный подход к оценке достижений учащихся. Для реализации дифференцированного подхода к оценке достижений учащихся предлагается проводить их предварительную кластеризацию в зависимости от результатов предыдущего периода обучения. В данной работе были выделены несколько показателей, которые бы с разных сторон характеризовали учебные достижения и способности учащихся и в то же время были доступны из LMS или личного портфолио.

Для оценки общего уровня академической успеваемости предлагается анализировать средние баллы за предыдущий период по ключевым дисциплинам профиля обучения, которые могут быть извлечены из LMS. Для измерения стабильности процесса обу-

чения по отметкам за предыдущий период предлагается рассчитывать коэффициенты вариации (CV) по ключевым дисциплинам, также из LMS извлекаются отметки о посещаемости. Для оценки вовлеченности в процесс обучения используется количество конкурсов, соревнований, состязаний за предыдущий период, в которых участвовал учащийся. Эта информация, в отличие от предыдущей, извлекается из личного портфолио.

Для кластеризации предлагается использовать метод k-means, с помощью которого учащиеся разбиваются на кластеры по схожести значений выбранных показателей.

Для каждого кластера необходимо разработать свои целевые установки к уровню усвоения учебного материала, учитывающие особенности учащихся. Целевые установки предлагается описывать в виде эталонного распределения вероятностей термов лингвистической переменной $\tilde{S}$ — это целевое распределение, показывающее, с какой вероятностью учащиеся из данного кластера должны достигать каждого уровня успеваемости (2), в случае если процесс обучения усвоения знаний происходит в нормальном режиме. Обозначим эталонное распределение через $\mathbf{p}^э$.

Для определения вероятностей эталонного распределения предлагается находить, как и ранее, предельные вероятности, но не для каждого учащегося по отдельности, а по отметкам целого кластера учащихся. Перечислим этапы определения вероятностей эталонного распределения:

1. Для каждого кластера собираются отметки всех учащихся, входящих в него, за предыдущий период по дисциплине. Объединенная последовательность сохраняет хронологический порядок для каждого учащегося, но рассматривается как единый массив данных.

2. По формуле (8) для всего массива данных кластера рассчитывается матрица переходных вероятностей.

3. При решении системы (9) определяются предельные вероятности термов (2).

Полученные предельные вероятности становятся эталонными для всех учащихся из данного кластера.

Текущий мониторинг и управление успеваемостью. В ходе текущего мониторинга успеваемости каждого учащегося через периоды времени, назначенные преподавателем, происходит сбор (накапливание) отметок, полученных им по дисциплине, с помощью которых оценивается матрица переходных вероятностей по формуле (8). Далее определяется фактическое распределение термов (2) $p_t = (p_1, p_2, p_3, p_4)$ на момент времени t по формуле (6).

Для сравнения эталонного распределения вероятностей и распределения вероятностей, полученного по формуле (6), предлагается воспользоваться критерием χ^2. С помощью этого критерия можно проверить, насколько статистически значимо фактическое распределение отличается от теоретического.

Формулируется нулевая гипотеза H_0 о том, что распределения не отличаются значимо. Альтернативная гипотеза H_1 состоит в том, что различия есть. Теоретическим распределением в нашем случае будет эталонное распределение. Пусть n — количество текущих отметок обучающегося, по которым была оценена матрица $\mathbf{M}$. Тогда фактическое значение критерия χ^2 рассчитывается по формуле

$$\chi^2 = \sum_{j=1}^{4}\left[n \cdot \frac{\left(p_j - p_j^э\right)^2}{p_j^э} \right] \tag{10}$$

и затем сравнивается с теоретическим значением $\chi^2(3;\alpha)$, где α — заданный уровень значимости (например, 0,05); 3 — число степеней свободы (так как одна из четырех вероятностей линейно зависит от остальных). Если

$$\chi^2 \geq \chi^2(3;\alpha), \tag{11}$$

то гипотезу H_0 отвергаем на уровне значимости α. То есть распределения отличаются значимо. Но в этом случае необходимо проанализировать, в какую сторону фактическое распределение отличается от эталонного: может учащийся учился даже лучше, чем ожидалось. В этом случае коррекция обучения также не нужна. А может, наоборот, учился существенно хуже, чем ожидалось. Тогда необходимо подать сигнал о том, что требуется коррекция процесса обучения. Для сравнения предлагается «оцифровать» термы лингвистической переменной $\tilde{S}$ в виде чисел 2, 3, 4 и 5 и найти с учетом распределения, определённого по формуле (6), и эталонного распределения математические ожидания таких оцифрованных термов по формулам:

$$M_э = 2 \cdot p_1^э + 3 \cdot p_2^э + 4 \cdot p_3^э + 5 \cdot p_4^э, \tag{12}$$

$$M_p = 2 \cdot p_1 + 3 \cdot p_2 + 4 \cdot p_3 + 5 \cdot p_4. \tag{13}$$

Если $M_p \geq M_э$, то корректировка процесса обучения не требуется. Фактический уровень усвоения учебного материала в среднем лучше, чем планировалось. Если $M_p < M_э$, то выдается сигнал о необходимости вмешательства в процесс обучения.

Этапы технологии автоматического мониторинга и управления уровнем усвоения учебного материала учащимися. Последовательность этапов разработанной технологии автоматического мониторинга и управления уровнем усвоения учебного материала учащимися приведена ниже:

1. Подготовительный этап.

1.1. Выбор показателей для кластеризации учащихся по их предыдущим достижениям.

1.2. Сбор данных за предыдущий период по каждому учащемуся: отметки, сведения о посещаемости, участие в конкурсах.

1.3. Формализация успеваемости как степени усвоения учебного материала и ее уровней: определение параметров функции принадлежности термов (2).

2. Кластеризация учащихся по выбранным в п. 1.2 показателям.

3. Расчет эталонных вероятностей для формализации целевых установок внутри каждого кластера.

3.1. Статистический анализ динамики отметок по каждому кластеру за предыдущий период обучения.

3.2. Расчет целевых распределений термов (2) успеваемости по каждому кластеру в виде распределений предельных вероятностей.

4. Расчет начального распределения вероятностей термов (2) успеваемости в виде распределения предельных вероятностей.

5. Текущий мониторинг.

5.1. Сбор текущих отметок.

5.2. Определение фактических распределений термов (2) успеваемости для каждого учащегося.

6. Принятие решений.

6.1. Сравнение фактического распределения успеваемости учащегося с эталонным для данного кластера.

6.2. Выдача сигналов преподавателю при необходимости.

Заключение. Разработанная технология автоматизированного мониторинга и управления успеваемостью позволяет преодолеть ограничения традиционных методов оценивания (средний балл, относительные частоты, разовое тестирование) за счет:

- анализа динамики, а не только статичных показателей;
- учета нечеткости границ между уровнями усвоения знаний;
- использования всей доступной информации о последовательности получения отметок.

Ее ключевыми особенностями являются:

- освобождение преподавателя от рутинного анализа;
- дифференцированный подход к определению целевых установок успеваемости в зависимости от способностей учеников за счет кластеризации;
- практическая реализуемость — не требует больших данных и сложной инфраструктуры**;**
- адаптивность — учет индивидуальных особенностей учащихся через кластеризацию;
- наглядность — интерпретируемые результаты и четкие критерии принятия решений для преподавателей.

Технология заполняет важный пробел между существующими учетными системами и потребностью в интеллектуальной поддержке педагогических решений, предлагая работоспособное и экономичное решение для образовательных организаций.

ЛИТЕРАТУРА

1. Строгецкая Е. В., Бетеев А. А. Цифровая трансформация высшего образования: вызовы и перспективы // Высшее образование в России. — 2020. — Т. 29. — № 8/9. — С. 34—45. — DOI 10.31992/0869-3617-2020-29-8-9-34-45.

2. Трудности и перспективы цифровой трансформации образования / А. Ю. Уваров, Э. Гейбл, И. В. Дворецкая [и др.] ; под ред. А. Ю. Уварова, И. Д. Фрумина. — М. : Издательский дом Высшей школы экономики, 2019. — 343 с.

3. Хлопотов М. В., Коцюба И. Ю. Методы интеллектуального анализа данных для мониторинга и диагностики качества образования // Дистанционное и виртуальное обучение. — 2014. — № 5(83). — С. 18—25.

4. Ranjan J., Malik K. Effective educational process: a data-mining approach // Vine. — 2007. — Vol. 37. — P. 502—515.

5. Enhancing education quality with hybrid clustering and evolutionary neural networks in a multi phase framework / S. Malik, C. Mahanty, J. Mohanty [et al.] // Scientific Reports. — 2025. — Vol. 15. — Article 21323. — DOI 10.1038/s41598-025-04622-z.

6. Wang Y. Artificial intelligence in student management systems to enhance academic performance monitoring and intervention // Scientific Reports. — 2025. — Vol. 15. — Article 35122. — DOI 10.1038/s41598-025-19159-4.

7. Romero C., Ventura S. Educational data mining: a review of the state of the art // IEEE Transactions on Systems, Man, and Cybernetics, Part C : Applications and Reviews. — 2010. — Vol. 40. — No. 6. — P. 601—618.

8. Матвеев М. Г., Лоскутова А. Е., Алейникова Н. А. Оценка успеваемости учащегося, как реализации случайного процесса с помощью дискретных цепей Маркова с нечеткими состояниями // Информатика: проблемы, методы, технологии : материалы XXV Международной научно-практической конференции имени Э. К. Алгазинова (Воронеж, 12—13 февраля 2025 г.). — Воронеж : Издательство Воронежского государственного университета, 2025. — С. 854—865. — EDN YCYDBL.

9. Лоскутова А. Е., Алейникова Н. А., Матвеев М. Г. Задача управления процессом обучения на основе нечетких цепей Маркова // Труды молодых ученых факультета компьютерных наук ВГУ : сборник научных трудов. — Воронеж : Издательство Воронежского государственного университета, 2025. — С. 491—498. — EDN UPPWHD.

10. Алейникова Н. А., Лоскутова А. Е., Матвеев М. Г. Задача управления успеваемостью с помощью дискретных цепей Маркова с нечеткими состояниями // Вестник Воронежского государственного университета. Серия : Системный анализ и информационные технологии. — 2025. — № 3. — С. 63—73. — DOI 10.17308/sait/1995-5499/2025/3/63-73. — EDN GCGASI.

11. Матвеев М. Г., Алейникова Н. А., Громковский А. А. Синтез дискретной нечеткой цепи Маркова на основе многомерных временных рядов // Информатика: проблемы, методы, технологии : материалы XXIII Международной научно-практической конференции им. Э. К. Алгазинова (Воронеж, 15—17 февраля 2023 г.). — Воронеж : Издательство Воронежского государственного университета, 2023. — С. 865—876. — EDN YPKZTG.

REFERENCES

1. Strogetskaya E. V., Beteev A. A. Tsifrovaya transformatsiya vysshego obrazovaniya: vyzovy i perspektivy // Vysshee obrazovanie v Rossii. — 2020. — T. 29. — № 8/9. — S. 34—45. — DOI 10.31992/0869-3617-2020-29-8-9-34-45.

2. Trudnosti i perspektivy tsifrovoj transformatsii obrazovaniya / A. Yu. Uvarov, E. Gejbl, I. V. Dvoretskaya [i dr.] ; pod red. A. Yu. Uvarova, I. D. Frumina. — M. : Izdatel′skij dom Vysshej shkoly ekonomiki, 2019. — 343 s.

3. Khlopotov M. V., Kotsyuba I. Yu. Metody intellektual′nogo analiza dannykh dlya monitoringa i diagnostiki kachestva obrazovaniya // Distantsionnoe i virtual′noe obuchenie. — 2014. — № 5(83). — S. 18—25.

4. Ranjan J., Malik K. Effective educational process: a data-mining approach // Vine. — 2007. — Vol. 37. — P. 502—515.

5. Enhancing education quality with hybrid clustering and evolutionary neural networks in a multi phase framework / S. Malik, C. Mahanty, J. Mohanty [et al.] // Scientific Reports. — 2025. — Vol. 15. — Article 21323. — DOI 10.1038/s41598-025-04622-z.

6. Wang Y. Artificial intelligence in student management systems to enhance academic performance monitoring and intervention // Scientific Reports. — 2025. — Vol. 15. — Article 35122. — DOI 10.1038/s41598-025-19159-4.

7. Romero C., Ventura S. Educational data mining: a review of the state of the art // IEEE Transactions on Systems, Man, and Cybernetics, Part C : Applications and Reviews. — 2010. — Vol. 40. — No. 6. — P. 601—618.

8. Matveev M. G., Loskutova A. E., Alejnikova N. A. Otsenka uspevaemosti uchashchegosya, kak realizatsii sluchajnogo protsessa s pomoshch′yu diskretnykh tsepej Markova s nechetkimi sostoyaniyami // Informatika: problemy, metody, tekhnologii : materialy XXV Mezhdunarodnoj nauchno-prakticheskoj konferentsii imeni E. K. Algazinova (Voronezh, 12—13 fevralya 2025 g.). — Voronezh : Izdatel′stvo Voronezhskogo gosudarstvennogo universiteta, 2025. — S. 854—865. — EDN YCYDBL.

9. Loskutova A. E., Alejnikova N. A., Matveev M. G. Zadacha upravleniya protsessom obucheniya na osnove nechetkikh tsepej Markova // Trudy molodykh uchenykh fakul′teta komp′yuternykh nauk VGU : sbornik nauchnykh trudov. — Voronezh : Izdatel′stvo Voro-nezhskogo gosudarstvennogo universiteta, 2025. — S. 491—498. — EDN UPPWHD.

10. Alejnikova N. A., Loskutova A. E., Matveev M. G. Zadacha upravleniya uspevaemost′yu s pomoshch′yu diskretnykh tsepej Markova s nechetkimi sostoyaniyami // Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya : Sistemnyj analiz i informatsionnye tekhnologii. — 2025. — № 3. — S. 63—73. — DOI 10.17308/sait/1995-5499/2025/3/63-73. — EDN GCGASI.

11. Matveev M. G., Alejnikova N. A., Gromkovskij A. A. Sintez diskretnoj nechetkoj tsepi Markova na osnove mnogomernykh vremennykh ryadov // Informatika: problemy, metody, tekhnologii : materialy XXIII Mezhdunarodnoj nauchno-prakticheskoj konferentsii im. E. K. Algazinova (Voronezh, 15—17 fevralya 2023 g.). — Voronezh : Izdatel′stvo Voronezhskogo gosudarstvennogo universiteta, 2023. — S. 865—876. — EDN YPKZTG.

СВЕДЕНИЯ ОБ АВТОРАХ

Лоскутова Анна Евгеньевна. Заместитель директора по учебно-воспитательной работе.
Муниципальное бюджетное общеобразовательное учреждение «Лицей № 1».
E-mail: anyaa02@yandex.ru
Россия, 394088, Воронеж, ул. Генерала Лизюкова, 81.

Алейникова Наталья Александровна. Доцент кафедры информационных технологий управления. Кандидат физико-математических наук, доцент.
Воронежский государственный университет.
E-mail: balbashovan@mail.ru
Россия, 394018, Воронеж, Университетская площадь, 1.

Матвеев Михаил Григорьевич. Заведующий кафедрой информационных технологий управления. Доктор технических наук, профессор.
Воронежский государственный университет.
E-mail: mgmatveev@yandex.ru
Россия, 394018, Воронеж, Университетская площадь, 1.

Loskutova Anna Evgenievna. Deputy director for educational work.
Municipal budgetary educational institution «Lyceum № 1».
E-mail: anyaa02@yandex.ru
Work address: Russia, 394088, Voronezh, Generala Lizyukova Str., 81.

Aleynikova Natalya Alexandrovna. Associate Professor of the chair of Information Technology Management. Candidate of Science in Physics and Mathematics, Associate Professor.
Voronezh State University
E-mail: balbashovan@mail.ru
Work address: Russia, 394018, Voronezh, Universitetskaya Sq., 1.

Matveev Mikhail Grigoryevich. Head of the chair of Information Technology Management. Doctor of Technical Sciences, Professor.
Voronezh State University.
E-mail: mgmatveev@yandex.ru
Work address: Russia, 394018, Voronezh, Universitetskaya Sq., 1.

Ключевые слова: успеваемость; мониторинг; нечеткие множества; цепи Маркова с нечеткими состояниями; кластеризация; предельные вероятности; динамика отметок.

Key words: academic performance; monitoring; fuzzy sets; Markov chains with fuzzy states; clustering; limit probabilities; grade dynamics.

УДК 519.217.6

В. В. Меньших, *доктор физико-математических наук, профессор*
А. Н. Никитенко, *адъюнкт*

ЧИСЛЕННЫЙ МЕТОД И АЛГОРИТМ МАКСИМИЗАЦИИ ПОЛЕЗНОСТИ ФУНКЦИОНИРОВАНИЯ ДЕЦЕНТРАЛИЗОВАННЫХ МУЛЬТИАГЕНТНЫХ СИСТЕМ

NUMERICAL METHOD AND ALGORITHM FOR MAXIMIZING THE UTILITY FUNCTION OF DECENTRALIZED MULTI-AGENT SYSTEMS

В статье рассматривается формализация процесса формирования коалиций на основе теоретико-игрового подхода. Основное внимание уделено разработке численного метода и алгоритма максимизации коллективной полезности агентов, в основе которого лежит генетический алгоритм поиска оптимальной коалиционной структуры с внутренней градиентной оптимизацией параметров «мягкого» управления. Представлено описание архитектуры генетического алгоритма, включая принципы кодирования решений и генетические операторы. Работоспособность предложенного метода подтверждена численным примером для системы из четырёх агентов.

The article proposes a formalization of the coalition formation process based on a game-theoretic approach. The main focus is on developing a numerical method and algorithm for maximizing the collective utility of agents, which is based on a genetic algorithm for finding the optimal coalition structure with internal gradient optimization of soft control parameters. The article provides a description of the genetic algorithm architecture, including the principles of solution encoding and genetic operators. The effectiveness of the proposed method is demonstrated through a numerical example for a system of four agents.

Введение. Приоритетными направлениями повышения качества информационно-аналитического обеспечения органов внутренних дел (ОВД) являются автоматизация процессов сбора и обработки данных, интеллектуализация процедур поддержки принятия решений, а также внедрение распределенных систем управления, способных функционировать в динамически меняющейся оперативной обстановке [1—3]. Решение указанных задач может быть обеспечено применением мультиагентных систем (МАС). При проектировании МАС, предназначенных для решения задач ОВД [4] ключевое значение имеет выбор архитектуры системы.

В теории МАС выделяются два фундаментальных подхода [5, 6]:

1) распределённый искусственный интеллект (РИИ);
2) децентрализованный искусственный интеллект (ДИИ).

Указанные подходы принципиально различаются механизмами координации и уровнем автономности технических агентов при принятии решений в динамически меняющейся оперативной обстановке.

Формализация задач, решаемых в рамках РИИ применительно к функционированию МАС в условиях «мягкого» управления, была представлена в работе [7]. В отличие

от указанного подхода, в настоящей статье основное внимание уделяется разработке численного метода и алгоритма для МАС, функционирующих в условиях ДИИ. Здесь каждый агент обладает высокой степенью автономности.

В условиях ограниченности ресурсов критически важной становится задача их оптимального перераспределения. В работах [8—10] предложен и формализован принцип организации межагентного взаимодействия, согласно которому в системе реализуются механизмы «мягкого» управления. В рамках данного подхода отдельные агенты-доноры могут временно снижать собственную полезность функционирования для выполнения приоритетных задач других агентов-реципиентов из множества потенциально выполнимых задач.

В рамках концепции ДИИ в системе могут формироваться подмножества агентов, совместное функционирование которых признается оптимальной стратегией. Таким образом, актуальной является задача разработки численного метода максимизации коллективной полезности агентов, основанного на поиске оптимальной коалиционной структуры, а также его соответствующей алгоритмической реализации.

Формализации задачи формирования коалиционной структуры. Формализованное описание принципа «мягкого» управления представлено в [11], где доказано, что на основании использования данного принципа отдельные агенты-реципиенты могут повышать свою полезность функционирования за счет помощи в выполнении их задач агентами-донорами. Представим данную формализацию применительно к использованию теоретико-игрового подхода [12—14].

Как было сказано выше, при децентрализованном построении системы агенты заинтересованы в повышении полезности функционирования при решении собственных задач, что может быть достигнуто за счет объединения отдельных агентов в различные подгруппы, так называемые коалиции, целью которых является достижение максимума полезности функционирования путём взаимодействия с другими агентами.

Таким образом, будем считать, что МАС M разбивается на T коалиций следующим образом:

$$\forall t, p \;\; t \neq p \quad S_t \cap S_p = \varnothing.$$

При этом множество задач агентов рассматриваемой системы состоит из:

множества назначенных задач, которое определяется соответствием $G: M \to W$ и задаётся матрицей $G = (g_i^k)_{\substack{i=1,\ldots,|M| \\ k=1,\ldots,|W|}}$, где

$$g_i^k = \begin{cases} 1, \text{ если задача } w^k \text{ назначена на выполнение агенту } m_i; \\ 0, \text{ если иначе;} \end{cases}$$

множества потенциально выполнимых задач, которое определяется соответствием $F: M \to W$ и задаётся матрицей $F = (f_i^k)_{\substack{i=1,\ldots,|M| \\ k=1,\ldots,|W|}}$, где

$$f_i^k = \begin{cases} 1, \text{ если задача } w^k \text{ может быть выполнена агентом } m_i; \\ 0, \text{ если иначе.} \end{cases}$$

В качестве множества игроков примем множество агентов МАС M. Характеристическая функция $v: 2^M \to \mathbb{R}$, которая ставит в соответствие каждой коалиции агентов $S_t \subseteq M$ её выигрыш $v(S_t)$ — это суммарная полезность агентов, включённых в данную

коалицию, которая определяется с учётом их важности в условиях применения принципа «мягкого» управления:

$$L_{S_t}\left(\mathrm{N}\right)=\sum_{j=1}^{|M|}\left(\beta_j\cdot\sum_{k=1}^{|W|}\left(\alpha^k\cdot g_j^k\sum_{t=1}^{T}\left(\gamma_{j,t}\cdot\sum_{i=1}^{|M|}\left(\tilde{q}_i^k(v_i^k)\cdot\gamma_{i,t}\cdot f_i^k\right)\right)\right)\right), \quad (1)$$

где

α^k — важность задачи w^k;

β_i — важность агента m_i;

$\tilde{q}_i^k(v_i^k)$ — полезность функционирования агента-донора m_i при выполнении задачи w^k агента-реципиента m_j:

$$\tilde{q}_i^k(v_i^k)=\begin{cases}\lambda_i^k\cdot\rho_i\cdot v_i^k, \text{ если } r_i^{k\min}\cdot g_i^k\le r\le r_i^{k\max}\cdot f_i^k;\\ 0-\text{во всех остальных случаях;}\end{cases}$$

$r_i^{k\ \min}$ — минимальный ресурс, который агент m_i должен выделить на выполнение задачи w^k;

$\rho_i=r_i-\sum_{k=1}^{|W|}\left(r_i^{k\ \min}\cdot g_i^k\right)$ — часть ресурса, которая останется у агента m_i после выделения минимальных объёмов ресарса $r_i^{k\ \min}$ для множества всех назначенных ему для выполнения задач;

$\gamma_{j,t}=\begin{cases}1, \text{если } m_j\in S_t;\\ 0, \text{если иначе;}\end{cases}$ — парметр, определяющий принадлежность агента к коалиции S_t.

В таком случае задача максимизации величины полезности функционирования агентов децентрализованной МАС в условиях «мягкого» управления может быть описана как совокупность задач:

$$\begin{cases}\mathrm{N}_{S_1}^*=\underset{\mathrm{N}_{S_1}^*\in\mathcal{N}_{S_1}}{Arg\max}\,L_{S_1}\left(\mathrm{N}_{S_1}\right);\\ \mathrm{N}_{S_2}^*=\underset{\mathrm{N}_{S_2}^*\in\mathcal{N}_{S_2}}{Arg\max}\,L_{S_2}\left(\mathrm{N}_{S_2}\right);\\ \ldots\\ \mathrm{N}_{S_T}^*=\underset{\mathrm{N}_{S_T}^*\in\mathcal{N}_{S_T}}{Arg\max}\,L_{S_T}\left(\mathrm{N}_{S_T}\right),\end{cases} \quad (2)$$

где $\mathrm{N}^*=\sum_{t=1}^{T}\mathrm{N}_{S_t}^*$ при следующих ограничениях на параметры мягкого управления ν_i^k:

$$\forall m_i\in M\quad\sum_{k=1}^{|W|}\nu_i^k\le 1; \quad (3)$$

$$\nu_i^k\in\left[0;\nu_i^{k\max}\right]\subseteq[0;1]. \quad (4)$$

Тогда полезность функционирования всей МАС определяется

$$L\left(\mathrm{N}^*\right)=\sum_{t=1}^{T}\left(L_{S_t}\left(\mathrm{N}_{S_t}^*\right)\right). \qquad (5)$$

Хотя целевая функция полезности коалиции агентов $L_{S_t}\left(\mathrm{N}_{S_t}^*\right)$ линейна, основная сложность заключается не в расчете ее величины, а в определении наилучшего варианта разбиения агентов на коалиции. Это связано с тем, что число допустимых коалиционных структур экспоненциально возрастает по мере увеличения количества агентов в системе, что описывается рассчитываемым рекуррентно числом Белла $B_{n+1}=\sum_{k=0}^{n}\left(C_k^n\cdot B_k\right)$.

В связи с этим возникает сложная комбинаторная задача формирования коалиционной структуры с учетом ограничений, которая дополнительно усложняется необходимостью определения оптимальных значений функций полезности агентов (1). Даже при относительно небольших размерах системы прямой перебор всех возможных вариантов разбиения на коалиции становится вычислительно неэффективным. В этих условиях методологически обоснованным представляется переход к применению эволюционных алгоритмов глобальной оптимизации [15].

Описание генетического алгоритма как метода решения задачи. Генетический алгоритм [16] (далее — ГА) представляет собой один из наиболее эффективных инструментов решения задач в данном контексте. Принцип работы ГА основан на имитации механизмов естественного отбора. Алгоритм оперирует множеством потенциальных решений, оценивая их пригодность в соответствии с заранее определенным критерием оптимальности. Формирование новых итераций решений осуществляется посредством операторов рекомбинации и мутации, обеспечивая направленный поиск в дискретном пространстве высокой размерности.

Рассмотрим основные понятия, которые будут использованы при описании численного метода и алгоритма в терминах эволюционной оптимизации.

Ген представляет собой наименьшую единицу информации в хромосоме, которая кодирует отдельный параметр, характеристику или переменную решения. В качестве гена примем номер коалиции S_T, в которую включён конкретный агент МАС. Максимальное количество коалиций соответствует числу агентов в системе, в то время как минимальная коалиция включает всех агентов системы, т. е. $1\le T\le\left|M\right|$.

Гены располагаются в локусах хромосомы. Локус представляет собой специфическое местоположение гена на хромосоме. В данном контексте локус определяется как порядковый номер агента, который распределяется в соответствующую коалицию по порядку от 1 до M.

Набор генов, определяющих распределение агентов $M=\left\{m_1,...,m_{|M|}\right\}$ в коалиции $\left\{S_{i_t},t=\overline{1,T}\right\}$ так, чтобы $\forall j,k\ \ j\ne k\ \ S_{i_j}\cap S_{i_k}=\varnothing$, является хромосомой. В данном контексте хромосома представляет собой отдельную особь. Номера коалиций могут быть расположены не по порядку, и некоторые из них могут отсутствовать.

Следовательно, каждую i-ю особь можно представить в виде вектора $O_i=\left(o_{i,1};o_{i,2};...;o_{i,|M|}\right)$, где $o_{i,1}$ — значение гена.

Совокупность различных распределений агентов, объединённых в коалиции, представляет собой популяцию.

На рисунке 1 изображен графический пример, демонстрирующий популяцию, состоящую из различных вариантов распределения агентов на коалиции в контексте генетического алгоритма.

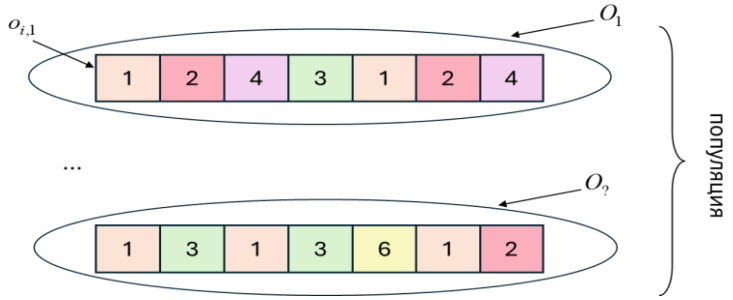


Рис. 1. Примеры вариантов распределения агентов на коалиции в контексте генетического алгоритма

Перейдём к рассмотрению основных этапов алгоритма решения задачи, основанного на её формализации, описанной выше.

На первом этапе реализации генетического алгоритма осуществляется инициализация начальной популяции:

правило 1 — случайным образом происходит разбиение коалиций, однако для обеспечения генетического разнообразия в начальную популяцию должны быть включены особи, содержащие одноэлементные коалиции.

Размер популяции, как в начальной, так и в последующих итерациях, определяется экспертом и зависит от размерности системы.

После формирования каждой популяции производится оценка приспособленности особей, входящих в её состав, согласно выражению (1).

Процесс формирования следующей популяции начинается с операции скрещивания родительских особей. В качестве родителей выступает каждая пара особей из текущей популяции.

В ходе рекомбинации гены наследуются потомками равномерно, т. е. каждый ген в потомстве выбирается случайным образом с равной вероятностью от одного из родителей.

Важно отметить, что в результате скрещивания может изменяться количество коалиций в потомстве, оно может как увеличиваться, так и уменьшаться, либо оставаться неизменным.

Для предотвращения преждевременной сходимости алгоритма применяется операция мутации:

правило 2 — с заданной вероятностью определяется количество мутирующих генов. После этого случайным образом выбираются локусы мутирующих генов. Для каждого локуса выбирается новое целочисленное значение гена из интервала $\left[1;\left|M\right|\right]$ с вероятностью $\frac{1}{\left|M\right|}$.

После применения генетических операторов, таких как скрещивание и мутация, формируются потомки, которые частично или полностью заменяют текущую популяцию в последующем поколении.

Для каждой особи рассчитывается значение функции приспособленности. Осуществляется поиск оптимальных параметров «мягкого» управления $\mathrm{N}^{*}_{S_1}$, обеспечивающих максимальную полезность функционирования агентов коалиции при текущем распределении коалиций. Поиск этих параметров проводится во внутреннем цикле алгоритма, в основе которого лежит градиентный метод.

Следующим этапом является селекция особей. В рамках текущей популяции выбираются пары особей для роли родителей в следующем поколении на основе принципа турнирной селекции, где родители определяются как особи с наибольшими значениями функции приспособленности.

Заключительным этапом итерации генетического алгоритма является проверка условия его завершения:

правило 3 — критерием остановки алгоритма является достижение n повторений значения функции приспособленности $L_{S_t}(\mathrm{N})$. При выполнении этого условия алгоритм останавливается и результатом становится «наилучшая» особь, представляющая оптимальное распределение агентов в коалициях.

Блок-схема алгоритма представлена на рисунке 2.

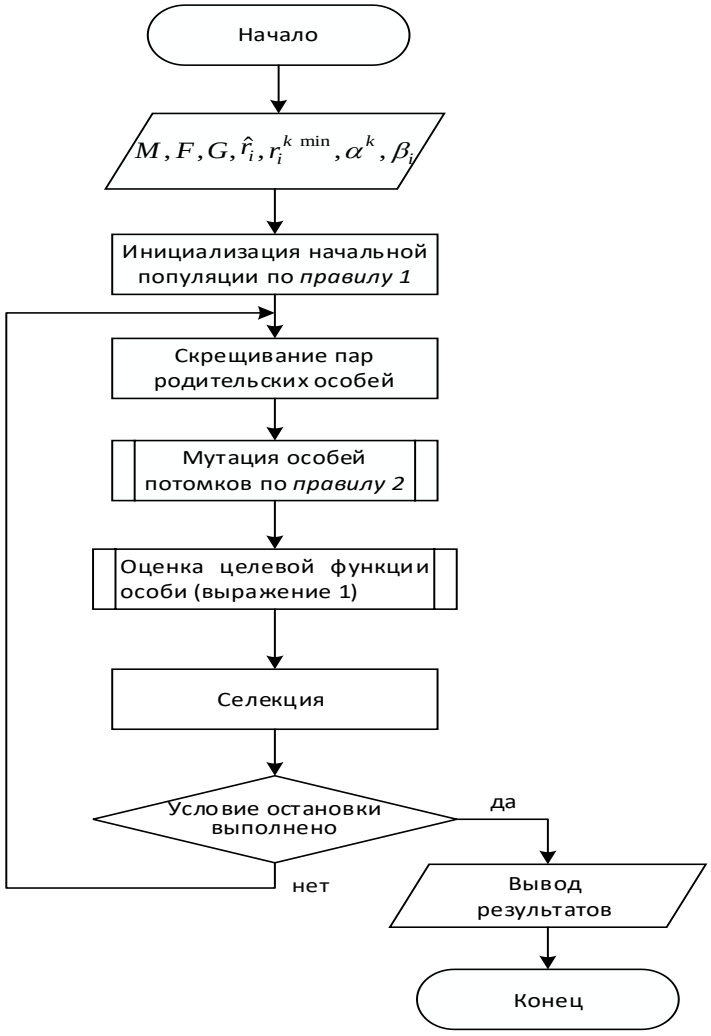


Рис. 2. Блок-схема алгоритма

Численный пример реализации алгоритма. Рассмотрим формирование коалиционной структуры на примере МАС, состоящей из четырёх агентов.

Пусть матрицы потенциально выполнимых и назначенных задач агентов представлены следующим образом:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \; F = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Ниже в таблицах представлены начальные параметры функционирования агентов системы.

Таблица 1

Важности β_j агентов и их ресурсный потенциал

	r_i	$r_i^{k\ \min}$	β_j
m_1	13	3	4
m_2	12	2	4
m_3	13	3	4
m_4	12	2	4

Таблица 2

Значения коэффициентов λ_i^k и важностей задач α^k

	w^1	w^2	w^3	w^4
α^k	3	4	3	5
m_1	3	6	0	0
m_2	6	3	0	9
m_3	0	9	3	6
m_4	0	0	6	3

В результате компьютерного моделирования была определена коалиционная структура системы, которая представлена на рисунке 3.

Чтобы убедиться в оптимальности распределения агентов, обратимся к анализу значений функций полезности L_i для каждого агента при разных вариантах коалиций, представленных в таблице 3.

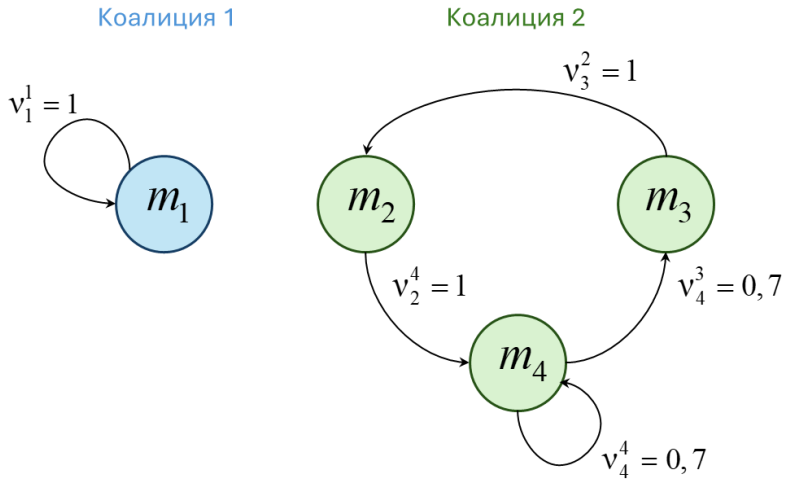


Рис. 3. Оптимальное разбиение на коалиции

Таблица 3

Значения полезностей функционирования

№	Варианты разбиения	L_1	L_2	L_3	L_4	L
1	$\{m_1\},\{m_2\},\{m_3\},\{m_4\}$	81	84	72	120	1428
2	$\{m_1,m_2\},\{m_3,m_4,\}$	153	300	189	255	3588
3	$\{m_1,m_3\},\{m_2,m_4,\}$	81	24	72	570	2988
4	$\{m_1,m_4\},\{m_2,m_3,\}$	81	444	27	120	2688
5	$\{m_1,m_2,m_3\},\{m_4\}$	153	660	27	120	3840
6	$\{m_1\},\{m_2,m_3,m_4\}$	**81**	**384**	**153**	**525**	**4572**
7	$\{m_1,m_2,m_3,m_4\}$	27	624	153	525	5316

Как следует из таблицы, для отдельных агентов функционирование в рамках разбиения на коалиции под номером 6 является самым оптимальным решением, в то же время при формировании такой коалиции увеличивается и значение полезности функционирования всей системы в целом, в отличие от независимого функционирования агентов системы. В таблице также представлен вариант функционирования агентов в рамках одной коалиции, что является примером РИИ, однако при таком разбиении хоть и увеличивается значение эффективности функционирования всей системы, но для отдельного агента m_1 такое взаимодействие приводит к снижению полезности функционирования.

Заключение. В работе разработаны численный метод и алгоритм максимизации полезности функционирования децентрализованных мультиагентных систем в условиях «мягкого» управления. Метод базируется на генетическом алгоритме поиска оптимальной коалиционной структуры с внутренней градиентной оптимизацией параметров «мяг-

кого» управления. Предложенная архитектура алгоритма учитывает особенности децентрализованного искусственного интеллекта и ориентирована на применение в распределенных системах управления органов внутренних дел. Работоспособность подхода подтверждена численным примером.

ЛИТЕРАТУРА

1. Вихляев А. А., Калинина С. В. Приоритетные направления деятельности и основные элементы информационно-аналитической работы подразделений ГИАЦ МВД России в условиях цифровизации органов внутренних дел // Научный портал МВД России. — 2023. — № 1(61). — С. 43—48.

2. Кубасов И. А., Лекарь Л. А., Кондрущенков О. М. Перспективные направления применения методов анализа больших данных в информационно-аналитическом обеспечении оперативно-разыскной деятельности // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы : сборник статей международной научно-практической конференции. — М., 2020. — С. 436—442.

3. О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года : указ Президента РФ от 07.05.2024 № 309 // СПС «Гарант». — URL: https://base.garant.ru/408992634/ (дата обращения: 03.04.2026).

4. Никитенко А. Н. О возможности применения мультиагентных технологий при решении задач органов внутренних дел // Общественная безопасность, законность и правопорядок в III тысячелетии. — 2025. — № 11-2. — С. 200—207.

5. Wooldridge M. An introduction to Multiaqent Systems. — Chichester, West Sussex, England : JOHN WILEY & SONS, LTD, 2002. — P. 492.

6. Бессмертный И. А. Искусственный интеллект. Введение в многоагентные системы : учебник для вузов. — М. : Юрайт, 2025. — 148 с. — (Высшее образование).

7. Меньших В. В., Никитенко А. Н. Задачи распределения ресурсов элементов мультиагентных систем в условиях «мягкого» управления // Информатика: проблемы, методы, технологии : материалы XXVI Международной научно-практической конференции им. Э. К. Алгазинова. — Воронеж : Воронежский государственный университет, 2026. — С. 658—665.

8. Menshikh V. V., Orlova D. E. Balance on Nash in «Soft» Control Problems for Systems of the Hierarchal Type // Bulletin of the South Ural State University. Series : Mathematical Modelling, Programming and Computer Software. — 2019. — Vol. 12. — No. 1. — P. 144—149.

9. Меньших В. В., Никитенко А. Н. Формализация задачи «мягкого» управления мультиагентными системами // Математика и математики на службе Родине (ко Дню математики) : сборник научных статей всероссийской научно-практической конференции. — Саратов : Саратовский военный ордена Жукова Краснознаменный институт войск национальной гвардии РФ, 2025. — С. 43—48.

10. Меньших В. В., Никитенко А. Н. Модель оценки эффективности функционирования мультиагентной системы в условиях использования «мягкого» управления // Вестник Воронежского института МВД России. — 2025. — № 1. — С. 40—48.

11. Никитенко А. Н. Компьютерное моделирование «мягкого» управления в мультиагентных системах // Моделирование систем критического применения. — 2025. — № 2. — С. 27—34.

12. Новиков Д. А., Чхартишвили А. Г. Рефлексивные игры. — М. : СИНТЕГ, 2003. — 149 с

13. Новиков Д. А. Теория управления организационными системами. 3-е изд., испр. и доп. — М. : Издательство физико-математической литературы, 2012. — 604 с.

14. Новиков Д. А. Теория игр и мультиагентные системы // Proceeding of the International Workshop «Networking games and management» (NGM-2012, Petrozavodsk). — Petrozavodsk : Karelian Research Center RAS, 2012. — С. 47—50.

15. Саймон Д. Алгоритмы эволюционной оптимизации / пер. с англ. А. В. Логунова. — М. : ДМК Пресс, 2020. — 1002 с.

16. Карпенко А. П. Современные алгоритмы поисковой оптимизации. Алгоритмы, вдохновленные природой : учебное пособие для вузов. — М. : Изд-во МГТУ им. Н. Э. Баумана, 2014. — 446 с.

REFERENCES

1. Vikhlyaev A. A., Kalinina S. V. Prioritetnye napravleniya deyatel′nosti i osnovnye elementy informatsionno-analiticheskoj raboty podrazdelenij GIATs MVD Rossii v usloviyakh tsifrovizatsii organov vnutrennikh del // Nauchnyj portal MVD Rossii. — 2023. — № 1(61). — S. 43—48.

2. Kubasov I. A., Lekar′ L. A., Kondrushchenkov O. M. Perspektivnye napravleniya primeneniya metodov analiza bol′shikh dannykh v informatsionno-analiticheskom obespechenii operativno-razysknoj deyatel′nosti // Strategicheskoe razvitie sistemy MVD Rossii: sostoyanie, tendentsii, perspektivy : sbornik statej mezhdunarodnoj nauchno-prakticheskoj konferentsii. — M., 2020. — S. 436—442.

3. O natsional′nykh tselyakh razvitiya Rossijskoj Federatsii na period do 2030 goda i na perspektivu do 2036 goda : ukaz Prezidenta RF ot 07.05.2024 № 309 // SPS «Garant». — URL: https://base.garant.ru/408992634/ (data obrashcheniya: 03.04.2026).

4. Nikitenko A. N. O vozmozhnosti primeneniya mul′tiagentnykh tekhnologij pri reshenii zadach organov vnutrennikh del // Obshchestvennaya bezopasnost′, zakonnost′ i pravoporyadok v III tysyacheletii. — 2025. — № 11-2. — S. 200—207.

5. Wooldridge M. An introduction to Multiaqent Systems. — Chichester, West Sussex, England : JOHN WILEY & SONS, LTD, 2002. — P. 492.

6. Bessmertnyj I. A. Iskusstvennyj intellekt. Vvedenie v mnogoagentnye sistemy : uchebnik dlya vuzov. — M. : Yurajt, 2025. — 148 s. — (Vysshee obrazovanie).

7. Men′shikh V. V., Nikitenko A. N. Zadachi raspredeleniya resursov elementov mul′tiagentnykh sistem v usloviyakh «myagkogo» upravleniya // Informatika: problemy, metody, tekhnologii : materialy XXVI Mezhdunarodnoj nauchno-prakticheskoj konferentsii im. E. K. Algazinova. — Voronezh : Voronezhskij gosudarstvennyj universitet, 2026. — S. 658—665.

8. Menshikh V. V., Orlova D. E. Balance on Nash in «Soft» Control Problems for Systems of the Hierarchal Type // Bulletin of the South Ural State University. Series : Mathematical Modelling, Programming and Computer Software. — 2019. — Vol. 12. — No. 1. — P. 144—149.

9. Men′shikh V. V., Nikitenko A. N. Formalizatsiya zadachi «myagkogo» upravleniya mul′tiagentnymi sistemami // Matematika i matematiki na sluzhbe Rodine (ko Dnyu matematiki) : sbornik nauchnykh statej vserossijskoj nauchno-prakticheskoj konferentsii. — Saratov : Saratovskij voennyj ordena Zhukova Krasnoznamennyj institut vojsk natsional′noj gvardii RF, 2025. — S. 43—48.

10. Men′shikh V. V., Nikitenko A. N. Model′ otsenki effektivnosti funktsionirovaniya mul′tiagentnoj sistemy v usloviyakh ispol′zovaniya «myagkogo» upravleniya // Vestnik Voronezhskogo instituta MVD Rossii. — 2025. — № 1. — S. 40—48.

11. Nikitenko A. N. Komp′yuternoe modelirovanie «myagkogo» upravleniya v mul′tiagentnykh sistemakh // Modelirovanie sistem kriticheskogo primeneniya. — 2025. — № 2. — S. 27—34.

12. Novikov D. A., Chkhartishvili A. G. Refleksivnye igry. — M. : SINTEG, 2003. — 149 s

13. Novikov D. A. Teoriya upravleniya organizatsionnymi sistemami. 3-e izd., ispr. i dop. — M. : Izdatel′stvo fiziko-matematicheskoj literatury, 2012. — 604 s.

14. Novikov D. A. Teoriya igr i mul′tiagentnye sistemy // Proceeding of the International Workshop «Networking games and management» (NGM-2012, Petrozavodsk). — Petrozavodsk : Karelian Research Center RAS, 2012. — S. 47—50.

15. Sajmon D. Algoritmy evolyutsionnoj optimizatsii / per. s angl. A. V. Logunova. — M. : DMK Press, 2020. — 1002 s.

16. Karpenko A. P. Sovremennye algoritmy poiskovoj optimizatsii. Algoritmy, vdokhnovlennye prirodoj : uchebnoe posobie dlya vuzov. — M. : Izd-vo MGTU im. N. E. Baumana, 2014. — 446 s.

СВЕДЕНИЯ ОБ АВТОРАХ

Меньших Валерий Владимирович. Профессор кафедры математики и моделирования систем. Доктор физико-математических наук, профессор.
Воронежский институт МВД России.
E-mail: menshikh@list.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Никитенко Анастасия Николаевна. Адъюнкт.
Воронежский институт МВД России.
E-mail: nikitenkoan27@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Menshikh Valery Vladimirovich. Professor of the chair of Mathematics and Modeling Systems. Doctor of Physical and Mathematical Sciences, Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: menshikh@list.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Nikitenko Anastasia Nikolaevna. Post-graduate cadet.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: nikitenkoan27@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: мультиагентные системы; «мягкое» управление; децентрализованный искусственный интеллект; коалиции; кооперативные игры; генетический алгоритм; градиентный метод; оптимизация коалиционной структуры; распределение ресурсов.

Key words: multi-agent systems; «soft» control; decentralized artificial intelligence; coalitions; cooperative games; genetic algorithm; gradient method; coalition structure optimization; resource allocation.

УДК 004.94

О. В. Пьянков, *доктор технических наук, профессор*
Е. А. Казанцева, *адъюнкт*

РАЗРАБОТКА МЕТОДИКИ АНАЛИЗА И ПРОГНОЗИРОВАНИЯ ПОТРЕБНОСТЕЙ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ МВД РОССИИ В ТЕХНИЧЕСКИХ СРЕДСТВАХ ОБУЧЕНИЯ

DEVELOPMENT OF A METHODOLOGY FOR ANALYZING AND FORECASTING THE NEEDS OF EDUCATIONAL ORGANIZATIONS OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA IN TECHNICAL TRAINING FACILITIES

В работе обосновывается актуальность проведения анализа и прогнозирования потребностей образовательных организаций в технических средствах обучения. Исследуются текущие нормативные требования, определяющие материально-техническое обеспечение в образовательных организациях МВД России. Предлагается методика, позволяющая определить и спрогнозировать потребности образовательной организации МВД России в технических средствах обучения, а также принять решение об их удовлетворении. Приводятся результаты вычислительного эксперимента, проведенного с использованием регрессионного анализа временных рядов.

The paper substantiates the relevance of analyzing and forecasting the needs of educational organizations in technical training facilities. The current regulatory requirements defining logistical support in educational institutions of the Ministry of Internal Affairs of Russia are being investigated. A methodology is proposed that makes it possible to identify and predict the needs of the educational organization of the Ministry of Internal Affairs of Russia in technical training facilities, as well as to make a decision on their satisfaction. The results of a computational experiment conducted using regression analysis of time series are presented.

Введение. Во всех образовательных организациях уже давно вошло в практику использование технических средств обучения для обеспечения высокого качества учебного процесса: повышения наглядности, сокращения времени на объяснение материала, активизации познавательного интереса обучающихся, моделирования различных ситуаций и процессов и т. п. Как составная часть материально-технического обеспечения учебного процесса технические средства обучения (ТСО) используются и в образовательных организациях МВД России, для которых одним из направлений методической деятельности является их внедрение в учебно-воспитательный процесс и разработка соответствующих педагогических технологий, осуществляемых кафедрами (циклами) [1]. Нормы положенности основных технических средств обучения, криминалистической и специальной техники, а также технических средств обучения, необходимых для освоения специализированных учебных программ, определяются по предложениям начальника соответствующей кафедры (цикла), и их количество рассчитывается в соответствии с [2], где одним из факторов является количество обучающихся.

Своевременное оснащение кафедр средствами ТСО требует проведения анализа текущих потребностей и состояния учебно-материальной базы, включающего инвентаризацию существующего оборудования, изучение рабочих программ учебных дисциплин, оценку нагрузок на оборудование, учёт количественного изменения обучающихся. Результаты такого анализа позволяют строить прогнозы потребностей в ТСО на ближайшую и далекую перспективу, принимать меры по обеспечению высокого качества учебного процесса. Однако методики проведения такого анализа, и тем более прогнозирования потребностей в ТСО, в настоящее время нет, что определило актуальность проводимого исследования.

Постановка задачи. Разработать методику проведения анализа и прогнозирования потребностей в ТСО в образовательных организациях системы МВД России для проведения своевременной работы по материально-техническому обеспечению учебного процесса.

Обоснование выбора направления разработки методики.

Среди основных подходов к анализу потребностей можно выделить [3]:

1. Системный подход — рассматривает образовательную организацию как единую систему, где ТСО интегрированы в учебный процесс, методическое обеспечение и материально-техническую базу. Учитываются взаимосвязи между различными элементами: учебными программами, тематическими планами кафедр, потребностями структурных подразделений.

2. Анализ учебных программ и планов — изучение образовательных стандартов, примерных программ профессиональной подготовки, рабочих программ учебных дисциплин позволяет определить требования к ТСО для реализации конкретных учебных задач. Например, для огневой подготовки могут потребоваться стрелковые тренажёры, а для криминалистической — специализированное лабораторное оборудование.

3. Оценка текущей материально-технической базы — инвентаризация имеющегося оборудования, выявление изношенного или устаревшего, а также определение дефицитов. Включает анализ спортивных сооружений, тренажёрных комплексов, учебных полигонов, лабораторий и других объектов.

4. Экспертные оценки — привлечение преподавателей, обучающихся, специалистов из практических подразделений ОВД для выявления потребностей в ТСО. Опросы и интервью помогают выявить запросы на конкретные технологии, а также проблемы, связанные с использованием существующих средств.

5. Анализ тенденций развития технологий — учёт перспективных направлений, таких как цифровизация, внедрение искусственного интеллекта, робототехники, виртуальной и дополненной реальности. Например, технологии VR могут использоваться для моделирования оперативно-служебных ситуаций.

6. Нормативно-правовой анализ — изучение приказов и распоряжений МВД России, федеральных законов и подзаконных актов, которые регулируют образовательную деятельность и требования к материально-техническому обеспечению.

Все перечисленные подходы несомненно представляют собой значимые весомые пути решения задачи по определению потребностей в ТСО, однако их применение требует тщательного детального анализа и значительного времени на проведение при отсутствии строгих, как уже было сказано выше, методик. В то же время существующие модели определения зависимостей между различными объектами позволяют их применять для проведения экспресс-анализа потребностей и разрабатывать прогноз на перспективу [4, 5].

Описание исходных данных. Рассмотрим данные, которые представляют собой эмпирическую базу, на которой можно разрабатывать методику анализа и прогнозирования потребностей.

Учитывая, что к ТСО можно отнести несколько десятков различных наименований соответствующих средств, для примера выберем только три, наиболее широко используемых в вузах, типа:

1. Рабочие станции (РС).
2. Портативные персональные электронно-вычислительные машины (ПЭВМ).
3. Мультимедийные проекторы (МП).

В таблицах 1—3 приведены данные по числу имеющихся и используемых в учебном процессе персональных компьютеров (РС), ноутбуков, мультимедийных проекторов на отдельных кафедрах вуза за период с 2020 по 2025 год. Кафедры пронумерованы от 1 до 7 и не включают всех кафедр, существующих в вузе.

Таблица 1

Количество РС

Номер учебной кафедры	Год					
	2020	2021	2022	2023	2024	2025
№ 1	45	44	44	55	71	58
№ 2	55	57	52	56	55	42
№ 3	36	5	36	36	36	60
№ 4	168	78	72	96	145	156
№ 5	38	37	35	36	34	34
№ 6	17	17	17	19	19	19
№ 7	26	26	26	28	37	39
Всего	385	264	282	326	397	408

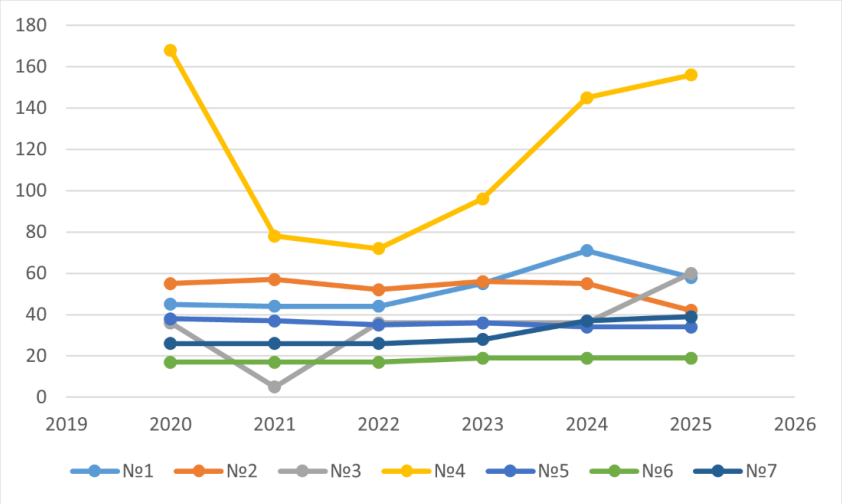


Рис. 1. График динамики оснащения кафедр компьютерами

Анализ данных таблицы 1 показывает неравномерную динамику оснащения кафедр РС (рис. 1). Кафедра № 4 имеет наибольшее количество РС, однако наблюдается

значительное снижение со 168 единиц оборудования в 2020 году до 156 в 2025 году. Кафедра № 3 демонстрирует аномальное снижение до 5 единиц оборудования в 2021 году с последующим восстановлением.

Таблица 2

Количество ноутбуков

Номер учебной кафедры	Год					
	2020	2021	2022	2023	2024	2025
№ 1	3	3	3	3	3	3
№ 2	67	48	47	48	48	45
№ 3	4	1	4	5	5	5
№ 4	11	11	11	11	10	10
№ 5	14	14	14	5	14	14
№ 6	8	8	8	8	8	8
№ 7	3	3	3	2	4	4
Всего	110	88	90	82	92	89

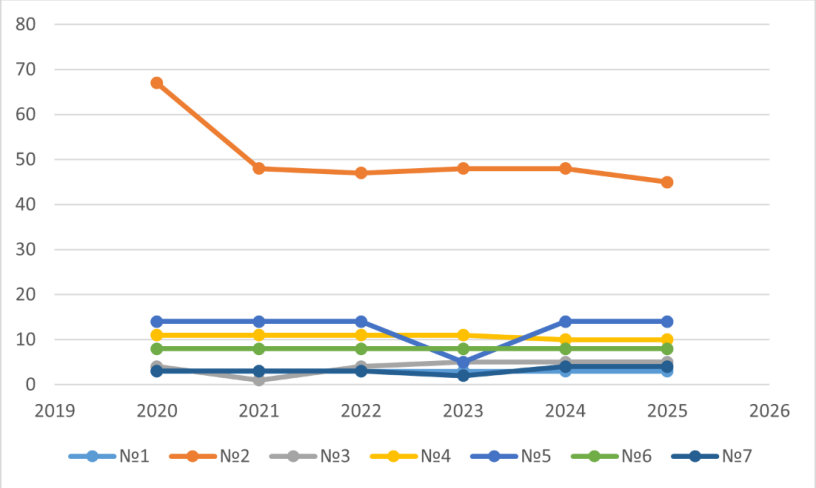


Рис. 2. График динамики оснащения кафедр ноутбуками

Анализ данных таблицы 2 показывает динамику оснащения кафедр ноутбуками (рис. 2). За исключением кафедры № 3, где наблюдается спад с 4 единиц оборудования в 2020 году до 1 в 2021 году, и кафедры № 5, где имеется резкий спад с 14 единиц оборудования в 2022 году до 5 в 2023 году с последующим восстановлением, имеющееся оборудование принимает стабильную динамику, в некоторых случаях неизменяющуюся. Общее количество портативных ПЭВМ демонстрирует тенденцию к снижению со 110 единиц в 2020 году до спрогнозированных 78 единиц в 2026 году, что составляет снижение на 29,1 % (рис. 2).

Анализы данных таблицы 3, так же как и в таблице 1, показывает неравномерную динамику оснащения кафедр МП (рис. 3). За исключением кафедры № 3 где наблюдается резкий спад с 5 единиц оборудования в 2020, 2022 годах до нуля (2021 и 2023 год), и кафедры № 4, с 10 единиц оборудования в 2020 году до 2 в 2021 году, а после до нуля в 2022 году,

имеющееся оборудование принимает стабильную динамику, в случае с кафедрой № 6 неизменяющуюся. Количество мультимедийных проекторов сократилось с 32 единиц в 2020 году до 23 в 2025 году, с спрогнозированным дальнейшим снижением до 17 единиц в 2026 году (снижение на 46,9 % за период).

Таблица 3

Количество МП

Номер учебной кафедры	Год					
	2020	2021	2022	2023	2024	2025
№ 1	2	3	3	3	4	4
№ 2	7	2	4	2	2	3
№ 3	5	0	5	0	5	5
№ 4	10	2	0	2	3	2
№ 5	3	3	4	4	4	4
№ 6	3	3	3	3	3	3
№ 7	2	3	3	2	2	2
Всего	32	16	22	16	23	23

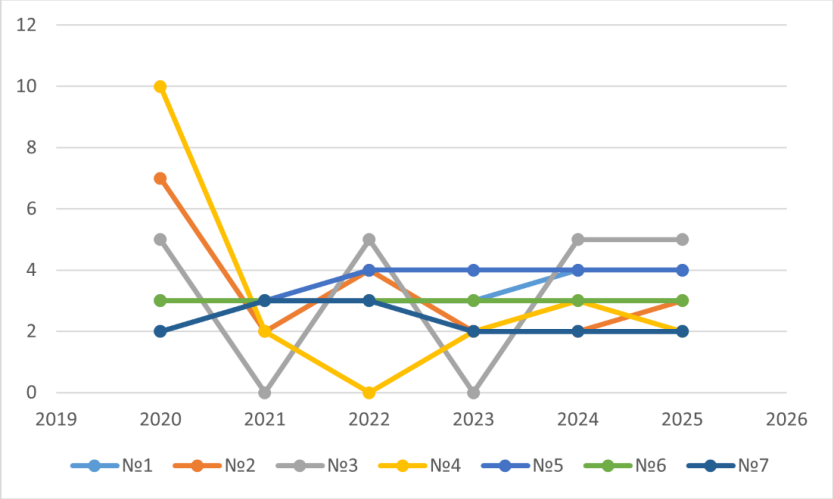


Рис. 3. График динамики оснащения кафедр МП

Далее, поскольку имеется предположение о наличии связи между количеством рассматриваемых типов ТСО с числом обучающихся в вузе, приведем данные с разбивкой по факультетам (см. табл. 4).

Таблица 4

Количество обучающихся

Обучающиеся	2020	2021	2022	2023	2024	2025
Радиотехнический факультет	517	519	568	617	612	580
Юридический факультет	773	775	764	706	781	799
Всего	1290	1294	1332	1323	1393	1379

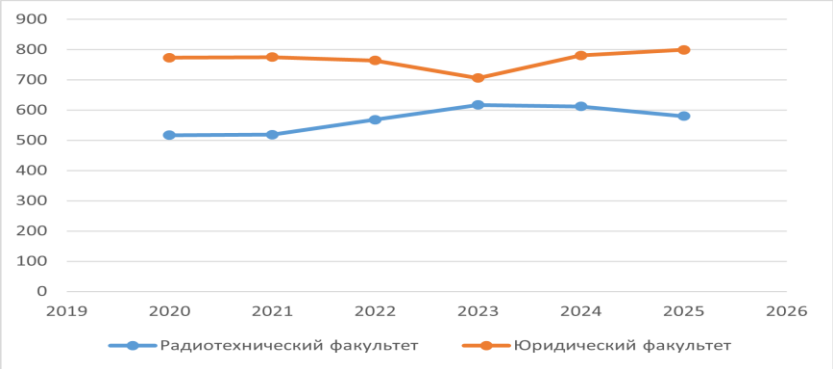


Рис. 4. График динамики числа обучающихся

Анализ данных таблицы 4 показывает неравномерную динамику обучающихся института (рис. 4). Общий контингент обучающихся демонстрирует рост с 1290 человек в 2020 году до спрогнозированного 1441 обучающегося в 2026 году (прирост 11,7%).

Для проверки предположения найдем значения коэффициентов корреляции между типами ТСО и количеством обучающихся за рассматриваемый период, результаты приведены в таблице 5.

Таблица 5

Коэффициенты корреляции

	№ 1	№ 2	№ 3	№ 4	№ 5	№ 6	№ 7
РС	0,87	-0,55	0,62	0,34	-0,95	0,76	0,92
ПЭВМ	0	-0,56	0,64	-0,92	0,14	0	0,71
МП	0,91	-0,45	0,48	-0,4	0,78	0	-0,4

Из результатов расчета видно, что в подавляющем большинстве случаев, существует средняя (больше 0,3) или сильная (больше 0,7) связь между ними (только в 4 ячейках таблицы значения коэффициентов меньше 0,3). Это позволяет осуществить следующую методику анализа и прогнозирования потребностей.

Методика анализа и прогнозирования потребностей. Для анализа связи между типами ТСО и числом обучающихся предлагается найти уравнение регрессии [6, 7]

$$Y = a + bX + \varepsilon,$$

где Y — зависимая переменная (то, что мы хотим предсказать — количество оборудования данного типа); X — независимая переменная (предиктор — количество обучающихся); a — свободный член (значение Y, когда $X = 0$); b — коэффициент регрессии (на сколько единиц изменится Y при увеличении X на 1 единицу); ε — ошибка модели (неучтённые факторы и случайность).

Исходя из значения коэффициента b, можно делать следующие выводы:

$b > 1$ — оснащенность растет быстрее числа обучающихся (возможный избыток ресурсов);

$b = 1$ — пропорциональное развитие инфраструктуры;

$b < 1$ — оснащенность отстает от роста числа обучающихся или развивается консервативно.

По результатам исследования на основе исходных данных (таблицы 1—4) были рассчитаны коэффициенты регрессии для каждой кафедры по каждому типу оборудования. Сводные результаты представлены в таблице 6.

Таблица 6

Коэффициент регрессии b

Оборудование	Коэффициент регрессии b кафедр							Среднее значение по институту
	№ 1	№ 2	№ 3	№ 4	№ 5	№ 6	№ 7	
РС	3,45	-4,23	1,52	0,34	-24,87	29,83	6,52	1,79
ПЭВМ	0	-2,96	17,75	-76,25	1,62	0	40,18	-2,81
МП	51,82	-9,74	8	-4,88	64,75	0	-33,25	10,95

Анализируя результаты по РС:

- кафедры № 1, 3, 6 и 7 демонстрируют опережающий рост оснащенности;
- кафедры № 2 и 5 имеют отрицательные коэффициенты, что свидетельствует о снижении оснащенности;
- кафедра № 4 демонстрирует консервативный рост оснащенности.
- значение по институту указывает на значительное увеличение оснащения.

Вывод, который можно сделать за весь институт, состоит в следующем: по данному типу ТСО оснащение института можно признать удовлетворительным, при этом имеется возможность перераспределения РС между кафедрами по согласованию с руководством кафедр.

Результаты по портативным ПЭВМ (Notebook):

- кафедры № 3, 5 и 7 демонстрируют рост;
- кафедры № 2 и 4 имеют отрицательные коэффициенты, что свидетельствует о снижении оснащенности;
- кафедры № 1 и 6 демонстрируют отсутствие динамики, количество оборудования не меняется при изменении числа обучающихся;
- значение по институту свидетельствует о существенном уменьшении технической оснащенности.

Вывод, который можно сделать за весь институт, состоит в следующем: по данному типу ТСО оснащение института нельзя признать удовлетворительным, имеется возможность перераспределения ПЭВМ между кафедрами по согласованию с руководством кафедр.

Результаты по МП:

- кафедры № 1, 3 и 5 демонстрируют опережающий рост оснащенности;
- кафедры № 2, 4 и 7 показывают снижение оснащенности;
- кафедра № 6 демонстрирует отсутствие динамики, количество оборудования не меняется при изменении числа обучающихся.
- значение по институту указывает на значительное увеличение оснащения.

Вывод, который можно сделать за весь институт, состоит в следующем: по данному типу ТСО оснащение института нельзя признать удовлетворительным, имеется возможность перераспределения МП между кафедрами по согласованию с руководством кафедр.

Данные выводы приводят нас к тому, что необходимо равномерно распределять ресурсы между кафедрами, так как коэффициенты варьируются от минуса к плюсу.

Необходимо пересмотреть стратегии материально-технического обеспечения с учетом регрессионных коэффициентов для каждой кафедры, а также выделить некоторые кафедры, где требуется увеличить количество единиц технических средств обучения.

Для прогнозирования потребностей можно воспользоваться одним из следующих подходов:

1. Исходя из планируемой численности обучающихся на следующий год (с учетом выпуска окончивших обучение и приема новых обучающихся), по полученным уравнениям регрессии для каждого типа ТСО рассчитать прогнозируемые потребности.

2. По значениям временного ряда с помощью подходящей модели (AR, MA, ARIMA и др.) определить значение на будущий период.

Каждый из подходов обладает своими преимуществами и недостатками, ни один из них не является идеальным. Для первого требуется значительный объем вычислений, кроме того, необходим подбор функции, описывающей зависимость $Y(X)$ с наименьшей ошибкой ε. При этом уравнение регрессии не обязательно будет лучшим решением.

Второй подход, к сожалению, ограничен объемом исходных данных. Количество отсчетов требуется гораздо большее, чем имеется в распоряжении, а их увеличение нецелесообразно. Поэтому подбор подходящей модели для работы с временным рядом в 5—8 отсчетов становится бесперспективным решением.

Исходя из вышеизложенного, для рассматриваемых исходных данных воспользуемся первым подходом с применением уравнений регрессий, рассчитанных ранее. Результаты расчётов приведены в таблице 7.

Таблица 7

Прогнозные значения на 2026 год

Тип ТСО	Кафедры							
	№ 1	№ 2	№ 3	№ 4	№ 5	№ 6	№ 7	Институт
РС	60	37	68	180	32	17	41	435
ПЭВМ	3	43	2	7	13	8	2	78
МП	1	2	3	2	4	3	2	17

В целом полученные прогнозные значения позволяют принять решение о необходимости закупки необходимых объемов ТСО по каждому типу.

Заключение. В ходе исследования были определены количественные значения по типам ТСО, используемых на кафедрах института. Разработана методика анализа и прогнозирования потребностей в ТСО, отличающаяся учетом исторических данных, представленных в виде временных рядов, для принятия решений о необходимости приобретения соответствующего оборудования. Данная методика может быть использована для дальнейшего обоснования заявок на закупку оборудования и разработки долгосрочной программы развития материально-технической базы образовательных организаций МВД России, а также иных учреждений.

ЛИТЕРАТУРА

1. Об утверждении Особенностей организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования, программам бакалавриата, программам специалитета, программам магистратуры, дополнительным профессиональным программам и основным программам профессионального обучения, Особенностей организации и осуществления методической и научной (научно-исследовательской) деятельности в области подготовки кадров в интересах

обеспечения законности и правопорядка, а также деятельности федеральных государственных организаций, осуществляющих образовательную деятельность и находящихся в ведении Министерства внутренних дел Российской Федерации : приказ МВД России от 19.09.2022 № 691 // СТРАС «Юрист» (дата обращения: 09.04.2026).

2. О некоторых вопросах обеспечения федеральных государственных образовательных учреждений высшего профессионального образования, дополнительного профессионального образования, общего среднего образования Министерства внутренних дел Российской Федерации, центров профессиональной подготовки управлений на транспорте Министерства внутренних дел Российской Федерации по федеральным округам, МВД, ГУВД, УВД по субъектам Российской Федерации основными видами технических средств обучения, средств связи, вычислительной и организационной техники : приказ МВД России от 21.01.2009 № 37 // СТРАС «Юрист» (дата обращения: 09.04.2026).

3. Челпанов В. В. Методики анализа и прогнозирования потребностей образовательных организаций МВД России в технических средствах обучения : автореф. дис. … канд. пед. наук : 13.00.01. — СПб. : СПВИ ВВ МВД России, 2003. — 24 с.

4. Басовский Л. Е. Прогнозирование и планирование в условиях рынка : учеб. пособие. — М. : ИНФРА-М, 2023. — 260 с.

5. Пьянков О. В., Терентьев А. А. Модели и методики прогнозирования потребностей органов внутренних дел в средствах и системах связи : научно-практическое пособие. — Воронеж : Воронежский институт МВД России, 2025. — 98 с.

6. Герасимов А. Н., Громов Е. И., Скрипченко Ю. С. Социально-экономическое прогнозирование : учеб. пособие. — М. : СтГАУ : Агрус, 2017. — 144 с.

7. Себер Дж. Линейный регрессионный анализ. — М. : Мир, 1980. — 456 с.

REFERENCES

1. Ob utverzhdenii Osobennostej organizatsii i osushchestvleniya obrazovatel′noj deyatel′nosti po obrazovatel′nym programmam srednego professional′nogo obrazovaniya, programmam bakalavriata, programmam spetsialiteta, programmam magistratury, dopolnitel′nym professional′nym programmam i osnovnym programmam professional′nogo obucheniya, Osobennostej organizatsii i osushchestvleniya metodicheskoj i nauchnoj (nauchno-issledovatel′skoj) deyatel′nosti v oblasti podgotovki kadrov v interesakh obespecheniya zakonnosti i pravoporyadka, a takzhe deyatel′nosti federal′nykh gosudarstvennykh organizatsij, osushchestvlyayushchikh obrazovatel′nuyu deyatel′nost′ i nakhodyashchikhsya v vedenii Ministerstva vnutrennikh del Rossijskoj Federatsii : prikaz MVD Rossii ot 19.09.2022 № 691 // STRAS «Yurist» (data obrashcheniya: 09.04.2026).

2. O nekotorykh voprosakh obespecheniya federal′nykh gosudarstvennykh obrazovatel′nykh uchrezhdenij vysshego professional′nogo obrazovaniya, dopolnitel′nogo professional′nogo obrazovaniya, obshchego srednego obrazovaniya Ministerstva vnutrennikh del Rossijskoj Federatsii, tsentrov professional′noj podgotovki upravlenij na transporte Ministerstva vnutrennikh del Rossijskoj Federatsii po federal′nym okrugam, MVD, GUVD, UVD po sub″ektam Rossijskoj Federatsii osnovnymi vidami tekhnicheskikh sredstv obucheniya, sredstv svyazi, vychislitel′noj i organizatsionnoj tekhniki : prikaz MVD Rossii ot 21.01.2009 № 37 // STRAS «Yurist» (data obrashcheniya: 09.04.2026).

3. Chelpanov V. V. Metodiki analiza i prognozirovaniya potrebnostej obrazovatel′nykh organizatsij MVD Rossii v tekhnicheskikh sredstvakh obucheniya : avtoref. dis. … kand. ped. nauk : 13.00.01. — SPb. : SPVI VV MVD Rossii, 2003. — 24 s.

4. Basovskij L. E. Prognozirovanie i planirovanie v usloviyakh rynka : ucheb. posobie. — M. : INFRA-M, 2023. — 260 s.

5. P′yankov O. V., Terent′ev A. A. Modeli i metodiki prognozirovaniya potrebnostej organov vnutrennikh del v sredstvakh i sistemakh svyazi : nauchno-prakticheskoe posobie. — Voronezh : Voronezhskij institut MVD Rossii, 2025. — 98 s.

6. Gerasimov A. N., Gromov E. I., Skripchenko Yu. S. Sotsial′no-ekonomicheskoe prognozirovanie : ucheb. posobie. — M. : StGAU : Agrus, 2017. — 144 s.

7. Seber Dzh. Linejnyj regressionnyj analiz. — M. : Mir, 1980. — 456 s.

СВЕДЕНИЯ ОБ АВТОРЕ

Пьянков Олег Викторович. Заместитель начальника кафедры инфокоммуникационных систем и технологий. Доктор технических наук, профессор.
Воронежский институт МВД России.
E-mail: ovpyankov@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Казанцева Ева Алексеевна. Адъюнкт.
Воронежский институт МВД России.
E-mail: kazaneva@gmail.com
Россия, 394065, Воронеж, проспект Патриотов, 53.

Pyankov Oleg Viktorovich. Deputy Head of the chair of Information and Communication Systems and Technologies. Doctor of Technical Sciences, Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: ovpyankov@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Kazantseva Eva Alekseevna. Post-graduate cadet.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: kazaneva@gmail.com
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: прогнозирование; множественная линейная регрессия; коэффициент регрессии; техническая оснащенность; управление ресурсами, образование.

Key words: forecasting; multiple linear regression; regression coefficient; technical equipment; resource management; and education.

УДК 519.7

А. В. Власенко, *кандидат технических наук, доцент*
А. К. Назаров, *кандидат физико-математических наук*

АСИМПТОТИЧЕСКИЙ АНАЛИЗ ОДНОЙ МОДЕЛИ ЭПИДЕМИИ В КОМПЬЮТЕРНЫХ СЕТЯХ С БЫСТРООСЦИЛЛИРУЮЩИМИ ПАРАМЕТРАМИ

ASYMPTOTIC ANALYSIS OF A MODEL OF EPIDEMICS IN COMPUTER NETWORKS WITH FAST-OSCILLATING PARAMETERS

В статье исследуется возможность применения метода усреднения Крылова — Боголюбова, распространенного для систем с большими высокочастотными слагаемыми, к задачам моделирования киберугроз. На примере модифицированной сетевой эпидемиологической модели SIS (Susceptible — Infected — Susceptible) показано, как высокочастотные колебания сетевой активности влияют на динамику распространения вредоносного программного обеспечения. Результаты позволяют предложить новый математически обоснованный подход к анализу скрытых угроз в условиях сильного фонового сетевого шума.

The article explores the possibility of applying the Krylov — Bogolyubov averaging method, which is commonly used for systems with large high-frequency terms, to the problem of modeling cyber threats. Using a modified SIS (Susceptible — Infected — Susceptible) network epidemiological model, the article demonstrates how high-frequency fluctuations in network activity affect the spread of malicious software. The results provide a new mathematically sound approach for analyzing hidden threats in the presence of strong background network noise.

Введение. Современный ландшафт киберугроз характеризуется стремительной эволюцией от примитивных массовых атак к сложным, целенаправленным операциям, получившим название Advanced Persistent Threat (APT). Отличительной чертой APT-атак является их скрытый, растянутый во времени характер: злоумышленники месяцами могут незаметно находиться в сети, маскируя свою активность под легитимный трафик, медленно перемещаясь между системами и собирая информацию. Выявление таких угроз методами классического сигнатурного анализа или пороговых правил становится крайне затруднительным, поскольку атака не представляет собой аномалию в конкретный момент, а является медленным трендом, скрытым в «шумной» динамике обычных сетевых процессов.

Таким образом, актуальной задачей кибербезопасности становится разработка математических моделей и аналитических методов, способных разделять временные масштабы в наблюдаемых данных: выделять медленную, стратегическую составляющую (деятельность злоумышленника) из-под маскирующего слоя быстрых, высокочастотных воздействий (нормальная сетевая активность).

В данной статье для решения таких задач применен метод усреднения, который является инструментом анализа нелинейных колебательных систем, находящихся под

воздействием высокочастотных сил [1—3]. Классическая теория, однако, предполагает, что амплитуда этих сил мала. В реальных сетевых условиях фоновый трафик может быть не только быстрым, но и соизмеримым по амплитуде с основными процессами или даже превосходить их. В настоящей работе метод усреднения применен для построения и анализа математических моделей динамики скрытых киберугроз в условиях интенсивной высокочастотной сетевой активности.

1. Модифицированная сетевая модель SIS с высокочастотным воздействием. Рассмотрим модель SIS для сети из N устройств, где в момент времени t $C(t)$ — количество здоровых, но уязвимых устройств, $Z(t)$ — количество заражённых устройств, $N = C(t) + Z(t) = \text{const}$.

Динамику процессов определим в следующем виде:

1) заражение: скорость перехода $C \to Z$ пропорциональна числу контактов между заражёнными и здоровыми устройствами и равна

$$p_Z \cdot Z(t) \cdot C(t),$$

где p_Z — вероятность заражения при контакте;

2) очистка: скорость перехода $Z \to C$ пропорциональна числу заражённых устройств, и равна

$$p_C \cdot Z(t),$$

где p_C — количество выздоровлений за единицу времени.

Изменение числа заражённых устройств описывается уравнением:

$$\frac{dZ}{dt} = p_Z \cdot Z(t) \cdot C(t) - p_C \cdot Z(t).$$

Введём долю заражённых устройств: $z(t) = \frac{Z(t)}{N}$. Поскольку $C(t) = N - Z(t)$, то доля здоровых устройств равна $c(t) = 1 - z(t)$.

После подстановки и преобразований получаем уравнение SIS-модели:

$$\frac{dz}{dt} = p_Z \cdot N \cdot z(t) \cdot (1 - z(t)) - p_C \cdot z(t).$$

Для компактности записи произведение $p_Z \cdot N$ обозначим как новый эффективный коэффициент P_Z. Таким образом, окончательный вид:

$$\frac{dz}{dt} = P_Z \cdot z(t) \cdot (1 - z(t)) - p_C \cdot z(t).$$

Здесь выражение $P_Z \cdot z(t) \cdot (1 - z(t))$ — это скорость распространения угрозы. Она растёт, когда в сети много и заражённых (распространителей), и здоровых (целей).

Второе слагаемое $p_C \cdot z(t)$ — это скорость противодействия (выздоровления), пропорциональная текущему числу зараженных.

Угроза «укореняется» в сети (т. е. начинается эпидемия), если $P_Z > p_C$. В противном случае система безопасности успевает очищать узлы быстрее, чем происходит заражение.

Добавим к данной SIS-модели слагаемое вида

$\sqrt{\omega} \cdot \phi(z, t, \omega \cdot t)$,

которое будем интерпретировать как случайный шум (например, активность пользователей), интенсивность которого растет с частотой ω (к примеру, в периоды высокой нагрузки). Этот шум может как мешать атаке, так и помогать ей, маскируя ее следы при анализе рисков. Зависимость от $\omega \cdot t$ означает, что восприимчивость сети к шуму меняется в такт с ее регулярной активностью (день/ночь, рабочие/выходные дни).

После добавления слагаемого получаем:

$$\frac{dz}{dt} = P_Z \cdot z(t) \cdot (1 - z(t)) - p_C \cdot z(t) + \sqrt{\omega} \cdot \phi(z, t, \omega \cdot t). \quad (1)$$

Такая модель описывает ситуацию, когда основные механизмы заражения и очистки (P_Z и p_C) постоянны, но на их работу накладывается высокочастотный сетевой шум, интенсивность которого растет с общей активностью сети. Порог $P_Z > p_C$ становится «размытым». Заражение может случайно закрепиться даже при $P_Z < p_C$ или, наоборот, не развиться при $P_Z > p_C$ (из-за влияния $\sqrt{\omega} \cdot \phi(z, t, \omega \cdot t)$).

2. Метод усреднения для систем с большими высокочастотными слагаемыми. Рассмотрим уравнение (1) с начальными условиями. Пусть D — ограниченная область в n-мерном пространстве вещественных чисел, $T>0$, $\Omega=\{(z,t,\tau)$: $z=(z_1,\ldots,z_n)^{tr} \in D$, $t \in [0,T]$, $\tau \in [0,+\infty)\}$, где tr обозначает операцию транспонирования. На множестве Ω рассмотрим задачу с начальными условиями для системы уравнений вида (1):

$$\frac{dz}{dt} = f(z,t, \tau) + \sqrt{\omega} \cdot \phi(z, t, \tau), \quad (2)$$

$$z(t_0)=z^0, \quad (3)$$

где значения функции $f(z,t, \tau)$ вычисляются по формуле

$$f(z,t, \tau) \equiv P_Z \cdot z(t) \cdot (1 - z(t)) - p_C \cdot z(t),$$

$t_0 \in [0, T]$, $z^0 \in D$, $\tau = \omega \cdot t$.

Относительно данных задачи (2) — (3) будем считать, что компоненты вектор-функций $f(z,t, \tau)$ и $\phi(z, t, \tau)$ вместе с частными производными любого порядка по всем переменным определены, непрерывны и равномерно ограничены на Ω. Также предположим, что компоненты вектор-функции $\phi(z, t, \tau)$ и ее частных производных по z, t обладают «нулевыми средними» по τ. Последнее можно интерпретировать как активность пользователей, при которой пики отправки и приема данных компенсируют друг друга в среднем за определенный период. Несмотря на это условие, влияние $\phi(z, t, \tau)$ может значительно ускорить или замедлить распространение угрозы ввиду большой амплитуды.

Наряду с задачей (2) — (3), которую будем называть возмущенной, рассмотрим следующую задачу, которую будем называть усредненной:

$$\frac{dy}{dt} = F(y,t), \quad (4)$$

$$y(t_0)=z^0, \quad (5)$$

где значения функции $F(y,t)$ определяются тождеством

$$F(y,t) \equiv \lim_{K\to\infty} \frac{1}{K} \int_0^K (f(z,t,\tau)+\frac{\partial \phi}{\partial z} z\,(z,t,\tau) \int_0^\tau \phi(z,t,\theta)d\theta)d\tau\ ,t \in [0,T].$$

Если задача (4) — (5) определена и имеет решение со значениями в D, то в силу теоремы 1 из [1] существует решение исходной (2) — (3). Таким образом, решение усредненного уравнения можно использовать для анализа долгосрочного поведения системы (2) — (3), причем согласно вышеупомянутой теореме ожидаемый уровень заражения в сети $z(t)$ будет близок к решению $y(t)$ системы (4) — (5) при достаточно больших частотах ω. Другими словами, система защиты и сетевая среда формируют ожидаемый уровень заражения $y(t)$, который можно вычислить. Задача системы защиты будет заключаться в снижении уровня заражения $y(t)$ до приемлемого минимума. Решение $y(t)$ показывает, как система будет эволюционировать в среднем: расти к некоторому $\bar{y}$ или затухать до нуля. Это позволит перейти от реагирования на инциденты к проактивному управлению рисками. Модель в таком случае может дать прогноз, например, что при текущих параметрах через определенный период времени доля зараженных узлов в среднем стабилизируется на уровне $\bar{y}$.

Заметим при этом, что точность модели зависит от ω (чем больше ω, тем точнее приближенное решение), поэтому на практике необходимо оценивать погрешность. Усредненная модель не описывает конкретные пики заражения или другие конкретные реализации случайного процесса, а описывает типичное, наиболее вероятное поведение и может быть использована как инструмент анализа угроз, прогнозирования их развития в среднесрочной перспективе.

3. Численная верификация результатов. Рассмотрим полученные результаты на конкретных примерах.

Возьмём упрощенную модель, в которой

$f(z,t,\tau) \equiv -\delta \cdot z, \qquad \delta > 0,$

$\phi(z,t,\tau) \equiv \alpha \cdot \sin(\tau), \qquad \alpha > 0,$

а начальное условие

$z(0)=1.$

Тогда система (2) — (3) примет вид:

$$\frac{dz}{dt} = -\delta \cdot z + \sqrt{\omega} \cdot \alpha \cdot \sin(\tau), \tag{6}$$

$$z(t_0)=1, \tag{7}$$

где $t_0 \in [0, T]$, $z^0 \in D$, $\tau = \omega \cdot t$.

Здесь δ — коэффициент затухания, α — амплитуда воздействия, ω — большая частота.

Применим описанный выше метод усреднения, тогда получим следующее усредненное уравнение:

$$\frac{dy}{dt} = -\delta \cdot y,$$

у которого существует решение, причем единственное для начальных данных (7). Таким образом, высокочастотное гармоническое воздействие не меняет усреднённую динамику

и при достаточно больших значениях ω решения усреднённой и возмущенной задач близки.

Для наглядности предположим, что коэффициент затухания $\delta = 0.1$, амплитуда воздействия $\alpha = 0.5$, большая частота $\omega = 10000$, а начальное условие z(0)=1. Проведем численное интегрирование вышеупомянутых систем с помощью метода Рунге — Кутта.

Ниже представлены результаты, полученные с помощью набора вычислительных алгоритмов на сайте www.wolframalpha.com:

При совмещении данные графики показывают, что быстрые мелкие колебания находятся вокруг плавно убывающей кривой затухания. Таким образом, усредненная модель верно описывает основную динамику. Даже когда исходная система (z(t)) постоянно находится под воздействием «шума», ее системный тренд (y(t)) подчиняется простому предсказуемому закону. Это дает специалисту по кибербезопасности инструмент, который позволяет, игнорируя «шум», прогнозировать развитие угрозы.



Рис. 1. Возмущенная система

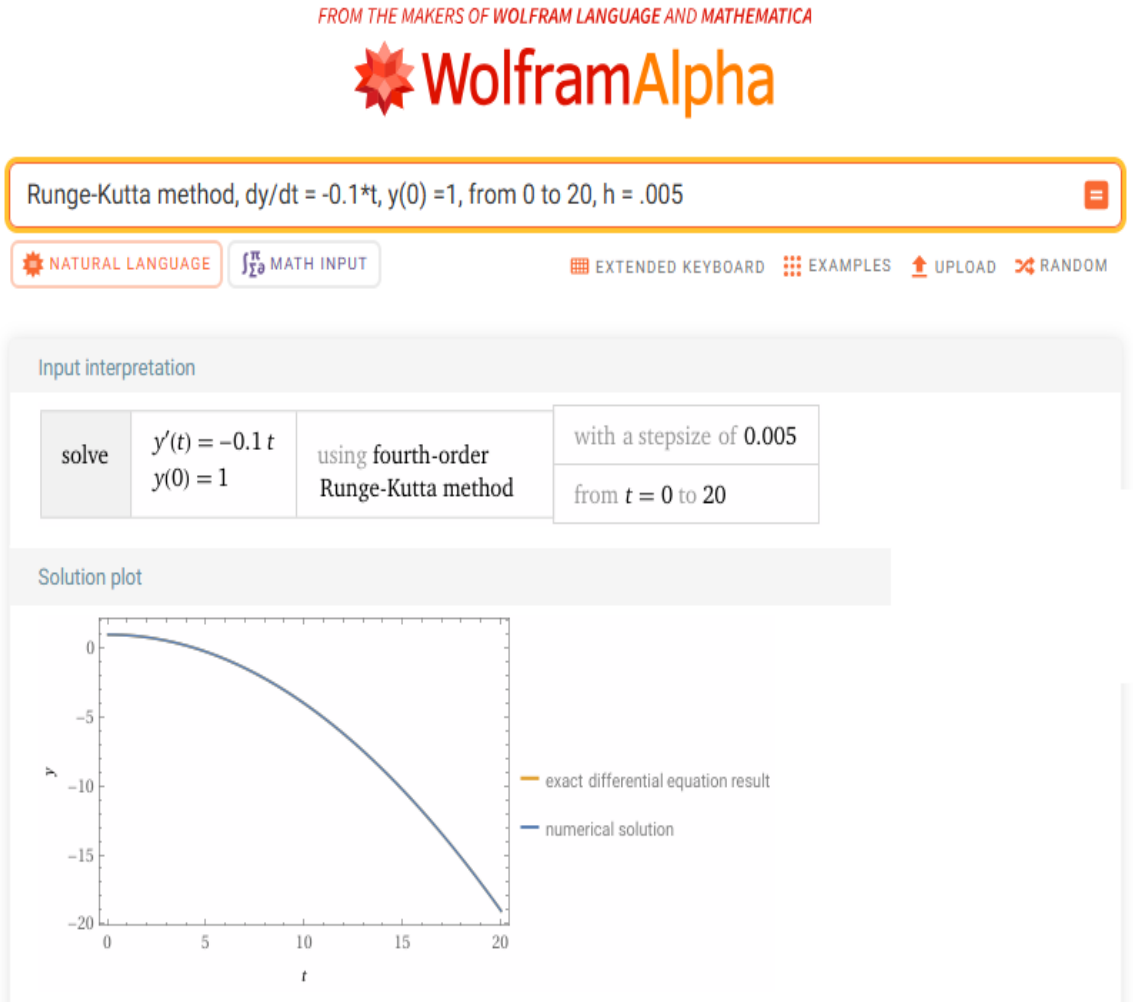


Рис. 2. Усредненная система

Заключение. В работе исследована возможность применения метода усреднения Крылова — Боголюбова для анализа динамики скрытых сетевых угроз. Для модифицированной модели SIS с высокочастотным воздействием получено усредненное уравнение, описывающее долгосрочную динамику системы. Результаты работы могут быть использованы для разработки алгоритмов проактивного обнаружения APT-атак путем фильтрации сетевого «шума» и прогнозирования развития угрозы.

ЛИТЕРАТУРА

1. Левенштам В. Б. Дифференциальные уравнения с большими высокочастотными слагаемыми (усреднение и асимптотики). — Ростов-на-Дону : Изд-во Южного федерального университета, 2008. — 366 с.

2. Назаров А. К. Усреднение уравнений в частных производных 1-го порядка // Экологический вестник научных центров ЧЭС. — 2015. — № 4. — С. 62—68.

3. Назаров А. К. Асимптотический анализ эволюционных высокочастотных задач : дис. … канд. физ.-мат. наук : 01.01.02 / Назаров Артур Карапетович ; Южный федеральный университет. — Ростов-на-Дону, 2018. — 123 с. — РГБ ОД, 9 18-1/120.

REFERENCES

1. Levenshtam V. B. Differentsial′nye uravneniya s bol′shimi vysokochastotnymi slagaemymi (usrednenie i asimptotiki). — Rostov-na-Donu : Izd-vo Yuzhnogo federal′nogo universiteta, 2008. — 366 s.

2. Nazarov A. K. Usrednenie uravnenij v chastnykh proizvodnykh 1-go poryadka // Ekologicheskij vestnik nauchnykh tsentrov ChES. — 2015. — № 4. — S. 62—68.

3. Nazarov A. K. Asimptoticheskij analiz evolyutsionnykh vysokochastotnykh zadach : dis. … kand. fiz.-mat. nauk : 01.01.02 / Nazarov Artur Karapetovich ; Yuzhnyj federal′nyj universitet. — Rostov-na-Donu, 2018. — 123 s. — RGB OD, 9 18-1/120.

СВЕДЕНИЯ ОБ АВТОРАХ

Власенко Александра Владимировна. Заведующий кафедрой информационной безопасности. Кандидат технических наук, доцент.
Краснодарский университет МВД России.
E-mail: alex_vlasenko@list.ru
Россия, 350005, Краснодар, ул. Ярославская, 128.

Назаров Артур Карапетович. Доцент кафедры информационной безопасности. Кандидат физико-математических наук.
Краснодарский университет МВД России.
E-mail: anazarovkrumvd@yandex.ru
Россия, 350005, Краснодар, ул. Ярославская, 128.

Vlasenko Alexandra Vladimirovna. Head of the chair of Information Security. Candidate of Technical Sciences, Associate Professor.
Krasnodar University of the Ministry of the Interior of Russia.
E-mail: alex_vlasenko@list.ru
Work address: Russia, 350005, Krasnodar, Yaroslavskaya Str., 128.

Nazarov Artur Karapetovich. Associate Professor of the chair of Information Security. Candidate of Physical and Mathematical Sciences.
Krasnodar University of the Ministry of the Interior of Russia.
E-mail: anazarovkrumvd@yandex.ru
Work address: Russia, 350005, Krasnodar, Yaroslavskaya Str., 128.

Ключевые слова: кибербезопасность; метод усреднения Крылова — Боголюбова; сетевая эпидемиологическая модель SIS; вредоносное программное обеспечение.

Key words: cybersecurity; Krylov — Bogoliubov averaging method; SIS network epidemiological model; malicious software.

УДК 004.7+517.9

М. А. Гудков, *кандидат технических наук*
А. А. Гапеев, *кандидат химических наук*
А. В. Мещеряков, *кандидат технических наук*
Е. С. Герасименко, *кандидат технических наук*

ИНТЕГРАТИВНЫЙ ПОДХОД К ОЦЕНКЕ КАЧЕСТВА ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ

INTEGRATIVE APPROACH TO ASSESSING THE QUALITY OF EDUCATIONAL PROGRAMS

В статье предложен интегративный подход к оценке качества образовательных программ по направлению «Техносферная безопасность», основанный на сочетании методов кластерного анализа компетенций и статистического контроля качества (SPC). Разработана и апробирована комплексная методика, позволяющая объективно анализировать сбалансированность структуры учебного плана, выявлять тематические группы дисциплин, обнаруживать дублирование модулей и определять критические области в подготовке инженеров. Проведённый анализ позволил выделить семь тематических кластеров, оценить качество кластеризации и идентифицировать проблемные дисциплины с превышением допустимого уровня неудовлетворительных результатов. Применение контрольных карт Шухарта подтвердило стабильность образовательного процесса на групповом уровне и выявило необходимость корректирующих мер по отдельным направлениям. Предложенный подход обеспечивает переход от субъективной оценки к количественно обоснованному управлению качеством образования, что способствует повышению конкурентоспособности выпускников и соответствию требованиям работодателей.

The article proposes an integrative approach to assessing the quality of educational programs in the field of technosphere safety, based on the combination of competency cluster analysis and statistical process control (SPC). A comprehensive methodology has been developed and tested, enabling an objective analysis of the balance in the curriculum structure, identification of thematic discipline groups, detection of duplicated modules, and pinpointing critical areas in engineer training. The analysis allowed for the identification of seven thematic clusters, assessment of clustering quality, and detection of problem disciplines with an excess of unsatisfactory results. The application of Shewhart control charts confirmed the stability of the educational process at the group level and highlighted the need for corrective actions in specific areas. The proposed approach facilitates a transition from subjective assessment to quantitatively grounded quality management in education, thereby enhancing graduate competitiveness and alignment with employer requirements.

Введение. Положительный результат в научной деятельности во многом обусловлен синергетическим взаимодействием знаний из различных предметных областей. В современной науке границы между дисциплинами становятся всё более условными: успешные исследования и инновационные разработки возникают на стыке физики и био-

логии, математики и гуманитарных наук, инженерии и медицины. Такой междисциплинарный подход позволяет расширять горизонты познания, находить нестандартные решения сложнейших задач и ускорять процесс внедрения новых технологий.

Симбиоз знаний из разных областей способствует не только появлению оригинальных идей, но и обеспечивает более глубокую верификацию результатов: методы одной науки усиливают надёжность выводов другой. Только комплексное соединение теоретических основ, экспериментальных методик и практического опыта разных специальностей даёт возможность исследователям достигать действительно значимых и устойчивых научных достижений [1—4].

Современная наука выходит за пределы узкой специализации. Новые открытия всё чаще возникают на стыке дисциплин — там, где инструменты одной области дополняют теории и методы другой. Такой междисциплинарный симбиоз становится ключом к решению самых сложных задач.

Механизмы симбиоза знаний:

1. Совместное использование методик:

- применение машинного обучения (информатика) для анализа медицинских снимков (радиология);

- методы статистики и теории вероятностей (математика) в биоинформатике для обработки геномных данных.

2. Трансфер теоретических моделей. Перенос понятий из одной области в другую позволяет увидеть проблему под новым углом:

- сетевые модели (теория графов) используются для изучения социальных взаимодействий и распространения эпидемий;

- принципы термодинамики вдохновляют разработку алгоритмов оптимизации в компьютерных науках.

3. Инструментальная интеграция. Развитие аппаратного обеспечения и лабораторных установок требует знаний как из физики, так и из инженерии, материаловедения и даже химии:

- расширение возможностей оптических микроскопов за счёт наноструктурированных покрытий.

- создание биосенсоров с использованием полимерных композитов и микроэлектроники [5—8].

Отталкиваясь от представленного положительного опыта, допустим, что процесс формирования будущего специалиста аналогичен производственному процессу, и рассмотрим ситуацию, когда по результатам обратной связи работодателя имеются недочеты по компетенциям. В качестве инструментария оценки качества подготовки выпускника используем методы статистической оценки брака.

Расчетная часть. Рассмотрим в качестве примера основную профессиональную образовательную программу высшего образования по направлению 20.03.01 «Техносферная безопасность», профиль — «Пожарная безопасность», очной формы обучения. Результат освоения основной профессиональной образовательной программы высшего образования, согласно ФГОС, определяется приобретенными выпускником компетенциями, т. е. способностью применять знания, умения и личные качества в соответствии с задачами профессиональной деятельности, результативность которых определяется

уровнем освоения компетенций: универсальные, общепрофессиональные, профессиональные, — каждая из которых имеет определенный набор индикаторов достижения [9—10]. Для различных дисциплин набор компетенций свой, но также есть дисциплины, в которых реализуются одинаковые компетенции. Совокупность последовательности дисциплин с реализуемыми компетенциями образует матрицу компетенций.

Для оценки сбалансированности структуры образовательной программы, включающей все необходимые компоненты профессиональной подготовки: фундаментальную, общепрофессиональную, специальную техническую и практическую составляющие, проведем кластерный анализ матрицы компетенций (рис. 1).

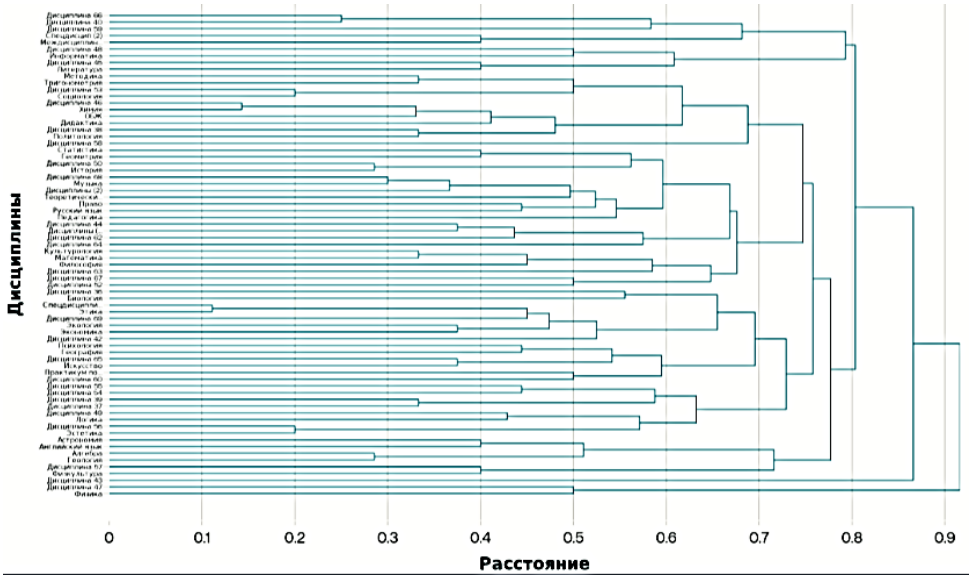


Рис. 1. Дендрограмма кластерного анализа

Дендрограмма демонстрирует четкую иерархическую организацию дисциплин с выраженными тематическими кластерами и оптимальным разбиением на семь основных групп. Диапазон расстояний слияния от 0,0 до 2,3957, что указывает на наличие как абсолютно идентичных профилей компетенций у некоторых дисциплин, так и существенных различий между отдельными группами. Среднее расстояние слияния составляет 0,7319 при стандартном отклонении 0,6352, что свидетельствует о неравномерном распределении дисциплин по степени сходства.

Анализ скачков расстояний выявил основные разделительные границы в структуре данных. Наибольший скачок (0,5073) происходит на шаге 3, разделяя дисциплины на два крупных супер-кластера при расстоянии 1,8760—2,3832. Второй значимый скачок (0,1686) на шаге 52 при расстоянии 0,0238—0,1925 указывает на формирование более детальных тематических групп.

Силуэт-анализ (рис. 2) демонстрирует постоянное повышение качества кластеризации с увеличением количества групп, достигая максимума 0,3617 при 10 кластерах. Однако для практической интерпретации рекомендуется использование 7 кластеров как компромисс между качеством разбиения (силуэт 0,2324) и содержательной интерпретируемостью результатов.

Кластер 4: Практические и оперативно-тактические дисциплины (30 дисциплин, 41,7%). Доминирующий кластер объединяет максимальное количество дисциплин с наивысшей насыщенностью компетенциями (350 общих назначений, 11,67 в среднем на дисциплину). Профиль характеризуется смешанным составом: 79,4% профессиональных, 20,6% универсальных и 15,1% общепрофессиональных компетенций. Высокая внутренняя неоднородность (стандартное отклонение 19,72) обусловлена включением как базовых технических дисциплин, так и специализированных курсов практической подготовки.

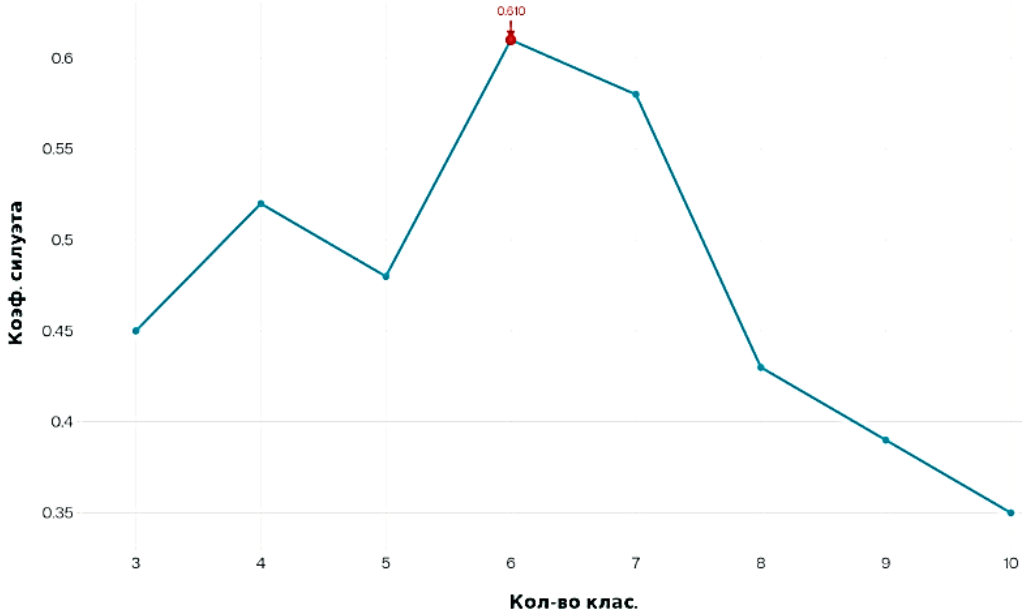


Рис. 2. Силуэт-анализ для выбора оптимального количества кластеров дисциплин

Кластер 1: Специализированные технические дисциплины пожарной безопасности (14 дисциплин, 19,4%). Второй по размеру кластер демонстрирует абсолютное доминирование профессиональных компетенций (100% от общего профиля) при умеренной внутренней вариативности (стандартное отклонение 3,29). Включает ключевые технические дисциплины: теория горения и взрыва, физико-химические основы тушения пожаров, пожарная автоматика, что формирует техническое ядро профессиональной подготовки.

Кластер 6: Фундаментальные естественнонаучные дисциплины (8 дисциплин, 11,1%). Кластер характеризуется преобладанием универсальных компетенций (78,8%) над профессиональными (21,2%) при среднем количестве 6,5 компетенций на дисциплину. Объединяет базовые естественнонаучные дисциплины (физика, химия, математика) с мировоззренческими курсами, формирующими теоретический фундамент инженерного образования.

Малые специализированные кластеры. Кластеры 2 (экономические дисциплины), 3 (правовые дисциплины) и 5 (гуманитарные дисциплины) демонстрируют высокую внутреннюю однородность (стандартные отклонения 0,87, 0,96 и 1,13 соответственно) и четкую тематическую специализацию.

Качество и валидность кластеризации. Метрики качества разбиения. Максимальный коэффициент силуэта 0,3617 при 10 кластерах указывает на умеренно хорошее качество кластеризации, что типично для образовательных данных с высокой степенью

междисциплинарности. Выбранное разбиение на 7 кластеров с силуэтом 0,2324 обеспечивает баланс между статистическим качеством и педагогической интерпретируемостью.

Внутрикластерная однородность. Анализ внутренней вариативности выявил наиболее однородные группы: экономические (σ = 0,87), правовые (σ = 0,96) и гуманитарные (σ = 1,13) дисциплины, что подтверждает корректность их группировки. Высокая неоднородность практического кластера (σ = 19,72) отражает разнообразие включенных дисциплин — от базовых до высокоспециализированных.

Профили сходства дисциплин. Обнаружено 10 пар дисциплин с абсолютно идентичными профилями компетенций (расстояние 0,0000), включая связанные курсы типа «Электротехника и электроника» — «Пожарная безопасность электроустановок». Максимальные различия (расстояние 1,0000) наблюдаются между узкоспециализированными практическими и общекультурными дисциплинами.

Структурная сбалансированность программы. Дендрограмма подтверждает оптимальную архитектуру образовательной программы с представленностью всех необходимых компонентов: фундаментального (кластер 6), общепрофессионального (кластеры 1, 4), специализированного (кластеры 2, 3) и общекультурного (кластер 5) блоков. Доминирование практического кластера (41,7% дисциплин) соответствует прикладной направленности инженерного образования [11—13].

Допустим ситуацию, что пришел негативный отзыв на выпускника, в котором указано, что он обладает недостаточными навыками оценки эффективности огнетушащих составов. Данная область знаний соответствует индикатору достижений ИД-3.ПК-1, который реализуется на следующих дисциплинах:

- «Общая и специальная химия»;
- «Теория горения и взрыва»;
- «Физико-химические основы развития и тушения пожаров»;
- «Теплотехника и прогнозирование опасных факторов»;
- «Пожарная безопасность технологических процессов»;
- «Практика»;
- «Преддипломная практика».

Для исключения или подтверждения системности указанной проблемы рассмотрим среднюю успеваемость группы по указанным дисциплинам. Представим успеваемость группы по дисциплинам в виде контрольной карты Шухарта (рис. 3).

Чтобы оценить наличие «промаха» (выброса) балла, анализируются две статистические границы:

- Центральная линия (CL): среднее значение балла по всем дисциплинам;
- Верхняя и нижняя контрольные границы (UCL и LCL) [15—17].

Признаком индивидуального «промаха» является балл крайне ниже центральной линии, лежащий ниже LCL, либо балл стабильно ниже среднего, если нет системных отклонений у всей группы. Если средний балл по всем дисциплинам превышает 3 и ни одна из точек не выходит за допустимые пределы, проблема носит индивидуальный характер и не является системной для выпуска [18, 19].

Проведенный анализ успеваемости группы из 30 обучающихся по семи дисциплинам, связанным с оценкой эффективности огнетушащих составов, выявил важные закономерности в образовательном процессе. Статистический анализ с применением контрольной карты Шухарта показал, что все средние оценки по дисциплинам находятся в

пределах контрольных границ (UCL = 4,655, LCL = 3,916), что свидетельствует о статистически управляемом процессе обучения на групповом уровне.

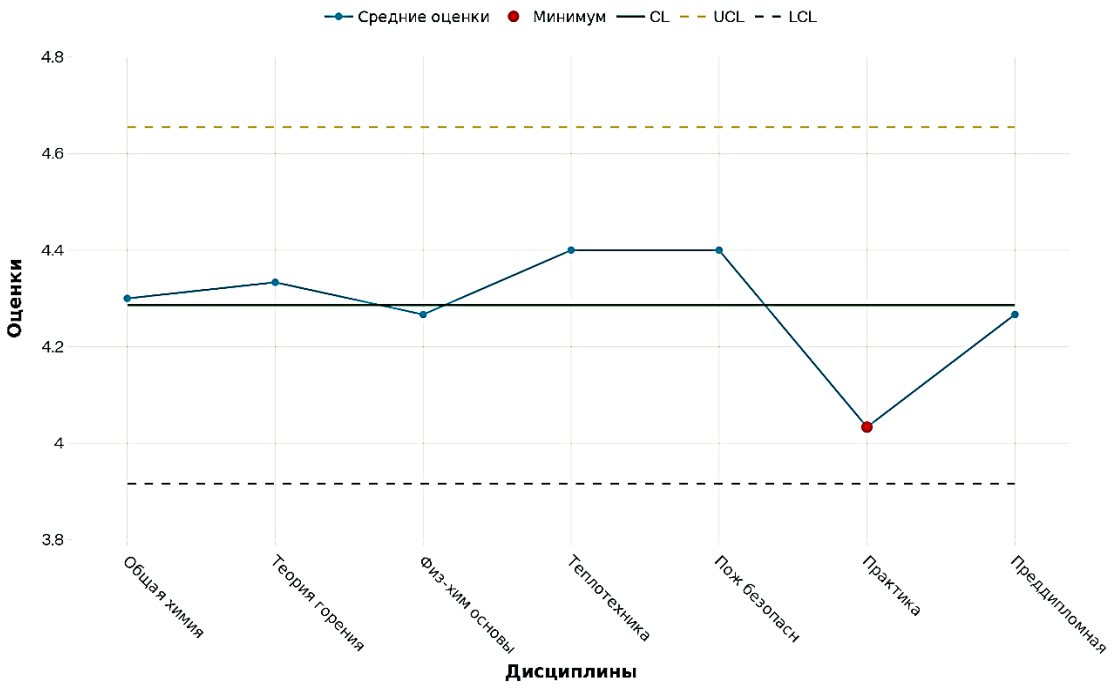


Рис. 3. Анализ средних оценок по дисциплинам по контрольной карте Шухарта

Анализ средних оценок по всем дисциплинам индикатора ИД-3.ПК-1 демонстрирует достаточно высокий уровень подготовки студентов. «Общая и специальная химия» показала средний балл 4,30 ± 0,70, что находится в пределах нормы контрольной карты. «Теория горения и взрыва» имеет средний показатель 4,33 ± 0,71, несмотря на наличие студентов с низкими оценками. «Физико-химические основы развития и тушения пожаров» характеризуются средним баллом 4,27 ± 0,74, демонстрируя стабильные результаты обучения.

«Теплотехника и прогнозирование опасных факторов» и «Пожарная безопасность технологических процессов» показали наиболее высокие средние баллы — по 4,40, что может указывать на эффективность методик преподавания этих дисциплин. «Практика» имеет самый низкий средний балл 4,03 ± 0,56, что может требовать дополнительного внимания к организации практических занятий. «Преддипломная практика» показала средний результат 4,27 ± 0,58, что соответствует общему уровню подготовки группы.

Контрольная карта Шухарта (I-карта индивидуальных значений) была построена для анализа средних оценок по дисциплинам с центральной линией CL = 4,286. Все точки данных находятся в пределах контрольных границ, что подтверждает статистическую управляемость образовательного процесса. Отсутствие выбросов за контрольные границы свидетельствует о том, что вариабельность успеваемости по дисциплинам не превышает естественных флуктуаций системы.

По дисциплине «Теория горения и взрыва» выявлено следующее распределение оценок: 46,7% студентов (14 человек) получили оценку «5», 40,0% (12 человек) — оценку «4», и 13,3% (4 человека) — оценку «3». Среднее значение составляет 4,33 балла

при стандартном отклонении 0,71, что указывает на умеренную вариабельность результатов.

Четыре студента показали неудовлетворительные результаты по данной дисциплине: Студент № 5, Студент № 15, Студент № 22 и Студент № 28. Доля студентов с оценкой «3» составляет 13,3% от общего числа обучающихся, что превышает критический порог в 10% и может указывать на системные проблемы в преподавании дисциплины.

Студент № 15 демонстрирует парадоксальную картину успеваемости: при получении оценки «3» по «Теории горения и взрыва» (отклонение — 1,33 от среднего), он показывает отличные результаты по смежным дисциплинам. По «Общей и специальной химии» получена оценка «5» (+0,70 от среднего), по «Физико-химическим основам развития и тушения пожаров» — также «5» (+0,73), по «Практике» — «5» (+0,97). Такой паттерн оценок указывает на специфические трудности именно с теоретическими аспектами горения и взрыва, а не на общую неподготовленность студента.

Анализ показывает, что проблема носит системный характер, поскольку 13,3% студентов испытывают трудности с дисциплиной «Теория горения и взрыва». Это превышает пороговое значение случайных флуктуаций и требует принятия корректирующих мер. Негативный отзыв работодателя на выпускника № 15 подтверждается статистическими данными о его слабой подготовке именно в области теоретических основ горения.

Корреляционный анализ дисциплин. Успеваемость по «Теории горения и взрыва» показывает различную степень корреляции с другими дисциплинами. Наиболее высокая корреляция наблюдается с «Физико-химическими основами развития и тушения пожаров» и «Пожарной безопасностью технологических процессов», что логично с точки зрения содержательной близости курсов.

Результаты и их обсуждение. Проведенное исследование демонстрирует эффективность применения методов кластерного анализа и статистического контроля качества для оценки структуры образовательных программ и выявления системных проблем в подготовке специалистов.

Кластерный анализ матрицы компетенций выявил оптимальную структурную организацию образовательной программы с семью тематически обособленными группами дисциплин. Доминирующий кластер практических и оперативно-тактических дисциплин (41,7% от общего числа) соответствует прикладной направленности инженерного образования в области пожарной безопасности. Выделение специализированного кластера технических дисциплин пожарной безопасности (19,4%) подтверждает формирование профессионального ядра программы, включающего теорию горения и взрыва, физико-химические основы тушения пожаров и пожарную автоматику.

Высокие метрики качества кластеризации (коэффициент силуэта 0,2324 для семи кластеров) свидетельствуют о корректности группировки дисциплин и обоснованности структуры учебного плана. Обнаружение десяти пар дисциплин с идентичными профилями компетенций указывает на необходимость пересмотра дублирования образовательного контента.

Применение контрольных карт Шухарта для анализа успеваемости группы по дисциплинам, связанным с индикатором ИД-3.ПК-1, выявило статистически управляемый процесс обучения на групповом уровне. Все средние оценки находятся в пределах контрольных границ (UCL = 4,655, LCL = 3,916), что подтверждает стабильность образовательного процесса.

Однако детальный анализ успеваемости по дисциплине «Теория горения и взрыва» показал превышение критического порога неудовлетворительных результатов: 13,3% студентов получили оценку «3», что превышает допустимые 10% и указывает на системные проблемы в преподавании данной дисциплины. Выявленный парадоксальный паттерн успеваемости отдельных студентов, демонстрирующих высокие результаты по смежным дисциплинам при низких оценках по теории горения, подтверждает специфические трудности в усвоении теоретических основ предмета.

Представленная методология комплексного анализа образовательной программы позволяет объективно оценивать сбалансированность структуры подготовки специалистов и своевременно выявлять проблемные области. Применение статистических методов контроля качества к образовательному процессу обеспечивает переход от субъективных оценок к количественным метрикам, повышающим точность диагностики недостатков в подготовке выпускников.

Предложенный подход позволяет дифференцировать индивидуальные проблемы студентов от системных недостатков образовательного процесса, что критически важно для принятия адекватных управленческих решений в области повышения качества образования.

Представленная методология может быть масштабирована для анализа других образовательных программ инженерного профиля и адаптирована к специфике различных направлений подготовки. Дальнейшее развитие исследования предполагает интеграцию методов машинного обучения для прогнозирования образовательных результатов и автоматизации процессов контроля качества подготовки специалистов.

Применение принципов статистического контроля качества к образовательным процессам открывает новые возможности для создания адаптивных систем управления качеством образования, способных оперативно реагировать на изменения требований работодателей и корректировать образовательные траектории в режиме реального времени.

ЛИТЕРАТУРА

1. Гусев А. А., Миронова Н. В. Междисциплинарные исследования: методологические основания и практики // Вестник Томского государственного университета. Философия. Социология. Политология. — 2020. — Т. 54. — № 2. — С. 5 — 22.

2. Кейс Т. В., Кузнецов И. А. Междисциплинарность в современной науке: драйвер инноваций и трансфера технологий // Управление наукой: теория и практика. — 2019. — Т. 1. — № 3. — С. 34 — 49.

3. Новиков Д. А. Методология научных исследований. — М. : Логос, 2016.

4. Мироушкин С. В. Научные коммуникации и конвергенция дисциплин // Вопросы образования. — 2021. — № 1. — С. 112—131.

5. Жаринов И. О., Панова А. Е. Машинное обучение в медицинской диагностике: обзор отечественных исследований // Медицинская техника. — 2022. — Т. — 56. — № 4. — С. 7—21.

6. Колчанова А. А., Федоров В. В. Методы статистики и анализа больших данных в биоинформатике // Прикладная информатика. — 2018. — Т. 13. — № 5. — С. 5—18.

7. Бычков И. В., Гноевых А. И. Сетевой анализ распространения эпидемий: модели и приложения // Математическое моделирование. — 2020. — Т. 32. — № 11. — С. 3—27.

8. Литвинов В. И. Термодинамические принципы и их аналоги в оптимизации сложных систем // Управляющие системы и машины. — 2017. — № 5. — С. 3—15.

9. Латыпова Л. Г., Сабирова Д. Р. Компетентностный подход в высшем образовании: модели, индикаторы, оценка. — Казань : Изд-во КФУ, 2018.

10. Филиппов В. М. Практико-ориентированная подготовка инженеров: от учебного плана к образовательным результатам // Высшее образование в России. — 2019. — Т. 28. — № 6. — С. 5—18.

11. Хайкин С. Нейронные сети и методы машинного обучения. — 3-е изд. — СПб. : Питер, 2020.

12. Копченков А. А., Соловьев А. Н. Кластерный анализ в задачах образования: методика и программные средства // Открытое образование. — 2021. — Т. 25. — № 4. — С. 30—47.

13. Ушаков Д. В. Интерпретируемость кластерных решений: критерии и эвристики выбора числа кластеров // Программные продукты и системы. — 2017. — № 3. — С. 78—85.

14. Дубовик В. П., Селезнев П. А. Анализ матриц компетенций и выявление дублирования учебных модулей // Университетское управление: практика и анализ. — 2022. — Т. 26. — № 2. — С. 66—82.

15. Шухарт У. А. Экономический контроль качества производственного процесса. — М. : Стандарты и качество, 2018.

16. Елисеев А. Н. Статистические методы управления качеством. — 2-е изд. — М. : Юрайт, 2020.

17. Кузьмина Н. В., Романов П. С. Применение контрольных карт в мониторинге образовательных результатов // Педагогические измерения. — 2019. — № 2. — С. 15—27.

18. Меньших В. В., Подольских А. В. Модель и алгоритм оптимизации процесса организации подготовки групп специалистов к действиям в кризисных ситуациях // Моделирование систем критического применения. — 2025. — № 1. — С. 22—32.

19. Меньших В. В., Подольских А. В. Обоснование состава программного комплекса оптимизации процессов подготовки групп и переподготовки специалистов // Вестник Воронежского института МВД России. — 2025. — № 4. — С. 73—83.

REFERENCES

1. Gusev A. A., Mironova N. V. Mezhdistsiplinarnye issledovaniya: metodologicheskie osnovaniya i praktiki // Vestnik Tomskogo gosudarstvennogo universiteta. Filosofiya. Sotsiologiya. Politologiya. — 2020. — T. 54. — № 2. — S. 5 — 22.

2. Kejs T. V., Kuznetsov I. A. Mezhdistsiplinarnost′ v sovremennoj nauke: drajver innovatsij i transfera tekhnologij // Upravlenie naukoj: teoriya i praktika. — 2019. — T. 1. — № 3. — S. 34 — 49.

3. Novikov D. A. Metodologiya nauchnykh issledovanij. — M. : Logos, 2016.

4. Miroushkin S. V. Nauchnye kommunikatsii i konvergentsiya distsiplin // Voprosy obrazovaniya. — 2021. — № 1. — S. 112—131.

5. Zharinov I. O., Panova A. E. Mashinnoe obuchenie v meditsinskoj diagnostike: obzor otechestvennykh issledovanij // Meditsinskaya tekhnika. — 2022. — T. — 56. — № 4. — S. 7—21.

6. Kolchanova A. A., Fedorov V. V. Metody statistiki i analiza bol′shikh dannykh v bioinformatike // Prikladnaya informatika. — 2018. — T. 13. — № 5. — S. 5—18.

7. Bychkov I. V., Gnoevykh A. I. Setevoj analiz rasprostraneniya epidemij: modeli i prilozheniya // Matematicheskoe modelirovanie. — 2020. — T. 32. — № 11. — S. 3—27.

8. Litvinov V. I. Termodinamicheskie printsipy i ikh analogi v optimizatsii slozhnykh sistem // Upravlyayushchie sistemy i mashiny. — 2017. — № 5. — S. 3—15.

9. Latypova L. G., Sabirova D. R. Kompetentnostnyj podkhod v vysshem obrazovanii: modeli, indikatory, otsenka. — Kazan′ : Izd-vo KFU, 2018.

10. Filippov V. M. Praktiko-orientirovannaya podgotovka inzhenerov: ot uchebnogo plana k obrazovatel′nym rezul′tatam // Vysshee obrazovanie v Rossii. — 2019. — T. 28. — № 6. — S. 5—18.

11. Khajkin S. Nejronnye seti i metody mashinnogo obucheniya. — 3-e izd. — SPb. : Piter, 2020.

12. Kopchenkov A. A., Solov′ev A. N. Klasternyj analiz v zadachakh obrazovaniya: metodika i programmnye sredstva // Otkrytoe obrazovanie. — 2021. — T. 25. — № 4. — S. 30—47.

13. Ushakov D. V. Interpretiruemost′ klasternykh reshenij: kriterii i evristiki vybora chisla klasterov // Programmnye produkty i sistemy. — 2017. — № 3. — S. 78—85.

14. Dubovik V. P., Seleznev P. A. Analiz matrits kompetentsij i vyyavlenie dublirovaniya uchebnykh modulej // Universitetskoe upravlenie: praktika i analiz. — 2022. — T. 26. — № 2. — S. 66—82.

15. Shukhart U. A. Ekonomicheskij kontrol′ kachestva proizvodstvennogo protsessa. — M. : Standarty i kachestvo, 2018.

16. Eliseev A. N. Statisticheskie metody upravleniya kachestvom. — 2-e izd. — M. : Yurajt, 2020.

17. Kuz′mina N. V., Romanov P. S. Primenenie kontrol′nykh kart v monitoringe obrazovatel′nykh rezul′tatov // Pedagogicheskie izmereniya. — 2019. — № 2. — S. 15—27.

18. Men′shikh V. V., Podol′skikh A. V. Model′ i algoritm optimizatsii protsessa organizatsii podgotovki grupp spetsialistov k dejstviyam v krizisnykh situatsiyakh // Modelirovanie sistem kriticheskogo primeneniya. — 2025. — № 1. — S. 22—32.

19. Men′shikh V. V., Podol′skikh A. V. Obosnovanie sostava programmnogo kompleksa optimizatsii protsessov podgotovki grupp i perepodgotovki spetsialistov // Vestnik Voronezhskogo instituta MVD Rossii. — 2025. — № 4. — S. 73—83.

СВЕДЕНИЯ ОБ АВТОРАХ

Гудков Максим Андреевич. Доцент кафедры процессов горения и экологической безопасности (в составе учебно-научного комплекса процессов горения и экологической безопасности). Кандидат технических наук.

Академия ГПС МЧС России.

E-mail: gudokmaksim@yandex.ru

Россия, 129366, Москва, ул. Бориса Галушкина, 4.

Гапеев Артем Александрович. Заместитель начальника кафедры процессов горения и экологической безопасности (в составе учебно-научного комплекса процессов горения и экологической безопасности). Кандидат химических наук.

Академия ГПС МЧС России.

E-mail: kratos_1987@mail.ru

Россия, 129366, Москва, ул. Бориса Галушкина, 4.

Мещеряков Алексей Викторович. Начальник кафедры процессов горения и экологической безопасности (в составе учебно-научного комплекса процессов горения и экологической безопасности). Кандидат технических наук.
Академия ГПС МЧС России.
Россия, 129366, Москва, ул. Бориса Галушкина, 4.

Герасименко Евгений Сергеевич. Старший преподаватель кафедры математики и моделирования систем. Кандидат технических наук.
Воронежский институт МВД России.
E-mail: jenya35353@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Gudkov Maxim Andreevich. Associate Professor of the chair of Combustion Processes and Environmental Safety (as part of the educational and scientific complex of combustion processes and environmental safety). Candidate of Technical Sciences.
Academy of the Ministry of Emergency Situations of Russia.
E-mail: Gudokmaksim@yandex.ru
Work address: Russia, 129366, Moscow, Borisa Galushkina Str., 4.

Gapeev Artem Alexandrovich. Deputy head of the chair of Combustion Processes and Environmental Safety (as part of the educational and scientific complex of combustion processes and environmental safety). Candidate of Chemical Sciences.
Academy of the Ministry of Emergency Situations of Russia.
E-mail: kratos_1987@mail.ru
Work address: Russia, 129366, Moscow, Borisa Galushkina Str., 4.

Meshcheryakov Alexey Viktorovich. Head of the chair of Combustion Processes and Environmental Safety (as part of the educational and scientific complex of combustion processes and environmental safety). Candidate of Technical Sciences.
Academy of the Ministry of Emergency Situations of Russia.
Work address: Russia, 129366, Moscow, Borisa Galushkina Str., 4.

Gerasimenko Evgeny Sergeevich. Senior lecturer of the chair of Mathematics and Systems Modeling.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: jenya35353@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: кластерный анализ; контроль качества; техносферная безопасность; компетенции; контрольные карты Шухарта; статистический мониторинг.

Key words: cluster analysis; quality control; technosphere safety; competencies; Shewhart control charts; statistical monitoring.

УДК 37.014.6:519.237:005.7

Д. Д. Зверева, *кандидат технических наук*

ДИНАМИЧЕСКИЕ МОДЕЛИ ИЗМЕНЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ ТРАНСПОРТНОЙ СЕТИ ПРИ ДЕГРАДАЦИИ И ВОССТАНОВЛЕНИИ КАНАЛОВ

DYNAMIC MODELS OF TRANSPORT NETWORK CAPACITY CHANGE UNDER CHANNEL DEGRADATION AND RECOVERY

Работа посвящена моделированию пропускной способности транспортных сетей снабжения при разрушении и последующем восстановлении их элементов. Сеть представляется мультиграфом с параметрами пропускной способности, времени и стоимости. В развитие статического подхода предложены динамические модели деградации и восстановления пропускной способности каналов с использованием гладких функций времени, позволяющие учитывать постепенное изменение состояния сети. Дано физическое, математическое и практическое обоснование выбора экспоненциальных и сигмоидальных (логистических) функций. Рассмотрены ограничения подхода и его связь со ступенчатыми моделями (как предельным случаем).

The paper is devoted to modeling the capacity of transportation supply networks under the degradation and subsequent recovery of their components. The network is represented as a multigraph characterized by capacity, transit time, and cost parameters. Extending the traditional static approach, dynamic models of channel capacity degradation and recovery are proposed using smooth time-dependent functions, which make it possible to account for gradual changes in the network state. Physical, mathematical, and practical justifications are provided for the use of exponential and sigmoidal (logistic) functions. The limitations of the proposed approach and its relationship to step-function models (as a limiting case) are also discussed.

Введение. Современные логистические и транспортные системы отличаются высокой сложностью, объединяя инфраструктурные объекты, материальные потоки и управляющие воздействия. Нарушения в работе одного из элементов нередко вызывают цепные задержки по всей цепочке поставок. Рост объёмов перевозок и активное развитие межмодальных технологий предъявляют повышенные требования к полноте учёта характеристик сети и её способности изменяться под влиянием внешних факторов.

Разнообразие видов транспорта (автомобильный, железнодорожный, водный, воздушный) требует единой формализации их свойств с фиксацией ограничений по скорости, пропускной способности и эксплуатационным затратам, включая расходы на переход между разными видами транспорта. Для анализа необходимы корректные математические модели, позволяющие описывать как стационарные, так и нестационарные режимы работы.

Центральная задача состоит в выборе маршрутов по нескольким критериям: временным затратам, пропускной способности, стоимости, надёжности. Наличие альтернативных путей между одними и теми же пунктами усложняет оценку их совместного влияния и делает необходимым применение методов многокритериальной оптимизации.

Анализ повреждений инфраструктуры даёт возможность оценить снижение общей пропускной способности, перераспределение потоков между оставшимися участками и возникновение локальных «узких мест». На основе такого анализа формируются рекомендации по приоритизации перевозок и организации временных маршрутов. В военной сфере такие модели нужны для планирования ремонта дорог, раздачи ресурсов, создания запасных маршрутов и слежения за тем, как загружены уцелевшие участки. Сценарное и имитационное моделирование помогает заранее найти слабые места сети и проработать вопрос о том, как переключать потоки при авариях.

Традиционные методы считают разрушение или ремонт пути мгновенными: ребро либо убирают из графа, либо сразу возвращают назад. Но на деле деградация (износ асфальта, подтопление, трещины) и восстановление (открытие полос по очереди, установка временных опор) длятся какое-то время и идут непрерывно. Поэтому нужны динамические модели, в которых пропускная способность меняется как гладкая функция времени. Они дают более точные прогнозы, позволяют лучше оценить риски и построить адаптивное управление потоками.

Цель работы — построение модели анализа пропускной способности транспортной сети, учитывающей временную динамику деградации и восстановления её участков, описываемую гладкими функциями.

Теоретические основы моделирования транспортных сетей. Для описания транспортной сети используется математический аппарат теории графов [1—3].

Вершины V: склады, промежуточные логистические узлы, города-потребители.

Дуги E: транспортные пути (железная дорога, автомобильная дорога, авиация, водный транспорт).

Модель: ориентированный мультиграф:

$$G = (V, E), \tag{1}$$

где допускается несколько дуг между парой вершин, отражающих альтернативные маршруты.

Каждая дуга $e \in E$ характеризуется набором параметров:

- пропускной способностью $c(e)$ (тонн/сутки);
- временем доставки $t(e)$ (часы);
- стоимостью перевозки $w(e)$.

Таким образом, транспортная сеть может быть представлена в виде системы:

$$G = (V, E, c, t, w), \tag{2}$$

где каждой дуге приписаны значения $c(e), t(e), w(e)$.

Методы определения пропускной способности сети (статические). Ключевой характеристикой является максимальный поток от источника s к стоку t [4].

Классическая задача:

$$\Phi_{\max}(G) = \max_{f} \sum_{e \in \delta^+(s)} f(e), \tag{3}$$

где $0 \le f(e) \le c(e) \quad \forall e \in E, \quad \sum_{e \in \delta^+(v)} f(e) = \sum_{e \in \delta^-(v)} f(e) \quad \forall v \in V \setminus \{s, t\}$.

Величина $\Phi_{\max}(G)$ — это максимальный суммарный поток, который можно направить из источника s в сток t. Он определяется как максимум суммы потоков по всем дугам, выходящим из источника s (обозначение $\delta^+(s)$). Суммируются потоки $f(e)$ на каждой дуге, которая начинается в s.

Для определения максимального потока могут быть применены алгоритмы:

- Форда — Фалкерсона,

- Эдмондса — Карпа,
- Диница.

Потеря мощности сети при разрушении канала:

$$\Delta\Phi = \Phi_{\text{исх}} - \Phi_{\text{после}}, \quad (4)$$

где $\Phi_{\text{исх}}$ — исходный поток, $\Phi_{\text{после}}$ — поток после разрушения.

Моделирование разрушений и перестроек (статические сценарии).

Типы разрушений:

1. Полное удаление дуги (например, разрушен мост):

$$G' = (V, E \setminus \{e\}). \quad (5)$$

2. Блокировка вершины (недоступность логистического узла) приводит к удалению всех дуг, инцидентных данной вершине v.

3. Частичное разрушение дуги (снижение пропускной способности) описывается формулой:

$$c'(e) = \beta \cdot c(e), \qquad 0 < \beta < 1, \quad (6)$$

где β — коэффициент остаточной пропускной способности дуги после частичного разрушения. Он показывает, какая доля от исходной пропускной способности $c(e)$ сохраняется.

Динамические модели изменения пропускной способности во времени. В реальных сетях разрушение и восстановление происходят не мгновенно. Для учёта этого введём зависящую от времени пропускную способность дуги e: $c_e(t)$, где $t \in \mathbb{R}_+$ (неотрицательное вещественное время). Будем рассматривать $c_e(t)$ как гладкую (непрерывно дифференцируемую) или кусочно-гладкую функцию времени, что позволяет моделировать постепенное изменение состояния.

Обоснование использования гладких функций. Выбор гладких функций (экспоненциальных, сигмоидальных, логистических) для описания деградации и восстановления пропускной способности имеет три уровня обоснования: физический (процессный), математический и практический.

Физическое обоснование. Реальные процессы ухудшения и ремонта инфраструктуры почти никогда не являются мгновенными или строго линейными. Они подчиняются законам накопления повреждений, инерционности ремонтных работ и ограничениям технологических процессов:

1. Экспоненциальная деградация возникает, когда скорость ухудшения пропорциональна текущему «запасу прочности» (дифференциальное уравнение $dc/dt = -\lambda(c - c_{\min})$). Это типично для износа дорожного покрытия, заиливания каналов, распространения трещин, а также для надёжности технических систем (постоянная интенсивность отказов).

2. Сигмоидальная (логистическая) деградация описывает процессы с начальным медленным ухудшением, затем ускорением и последующим замедлением при приближении к пределу. Примеры: усталостные разрушения материалов, прогрессирующее обрушение конструкций, нарастание коррозионных повреждений.

3. Восстановление с плавной динамикой моделируется как поэтапный ремонт. Сначала идёт медленный рост пропускной способности (развёртывание бригад), затем быстрая фаза восстановления, а на завершающем этапе темп снова замедляется. Плавность таких процессов обусловлена физической инерцией — мгновенно повысить пропускную способность, например с 50 до 100 автомобилей в час, технически невозможно.

Математическое обоснование:

1. Функция $c(t)$ непрерывно дифференцируема, значит, её скорость изменения всегда конечна. Это позволяет применять обычные численные методы — разрывы производных, ведущие к неустойчивости счёта, тут отсутствуют.

2. Экспоненту и логистическую функцию легко интегрировать аналитически. Для расчёта интегральных показателей, например общего объёма перевозок, $V(T) = \int_0^T \Phi_{\max}(t)dt$ (у экспоненты первообразная выписывается сразу, у логистической — через логарифмы).

3. Модель настраивается под разные сценарии за счёт введения нескольких параметров: можно получить быстрое или медленное разрушение, раннее или позднее восстановление, не меняя структуру алгоритма.

Практическое обоснование.

Реальные данные по авариям и ремонтам на транспорте дают следующие соответствия:

1. Заторы из-за сужения дороги — снижение потока хорошо описывается экспонентой (это подтверждает теория транспортных потоков).

2. Распространение коррозии на рельсах или образование колеи — сигмоидальные модели («эпидемия» повреждений).

3. Открытие полос после ремонта моста — логистическая кривая качественно повторяет реальные графики.

Гладкие функции давно применяются в теории надёжности, биологии, экономике. Для транспортных сетей их пригодность также показана в ряде работ [5—9].

Основные динамические модели изменения пропускной способности во времени.

1. Экспоненциальная деградация. Начальная пропускная способность c_0 снижается до $c_{\min}$ по закону:

$$c(t) = c_{\min} + (c_0 - c_{\min}) \cdot e^{-\lambda t}, \qquad t \geq 0, \tag{7}$$

где $\lambda > 0$ — скорость процесса. При $t = 0$ получаем $c(0) = c_0$, при больших t имеем $c(t) \to c_{\min}$. Такой вариант подходит для износа, накопления дефектов или медленного заиливания.

2. Сигмоидальное падение с последующим подъёмом. Для цепочки «разрушение → ремонт» удобна логистическая функция:

$$c(t) = c_{\text{норм}} - \frac{\Delta c}{1 + e^{-k(t-t_0)}} + \frac{\Delta c_{\text{восст}}}{1 + e^{-m(t-t_1)}}. \tag{8}$$

Первое слагаемое отвечает за спад от $c_{\text{норм}}$ до $c_{\text{норм}} - \Delta c$ с крутизной k около момента t_0. Второе — за плавный подъём с крутизной m, начиная с t_1. Чтобы восстановление не превышало исходный уровень, нужно, чтобы $0 \leq \Delta c_{\text{восст}} \leq \Delta c$. Если $\Delta c_{\text{восст}} = \Delta c$, функция возвращается к исходному значению; если меньше — восстанавливается лишь часть.

Параметры $k,\ m$ выбираются так, чтобы вне переходной области отклонение от предельных значений ($c_{\text{норм}}$ до деградации и $c_{\text{норм}} - \Delta c$ после деградации) было пренебрежимо мало. Моменты $t_0,\ t_1$ соответствуют центрам переходных интервалов. Поэтому в начальный момент $t = 0$ функция не обязана строго равняться $c_{\text{норм}}$, однако при достаточно больших k и $t_0 > 0$ это отличие может быть сделано сколь угодно малым.

3. Кусочно-постоянная модель со сглаженными переходами. На практике часто удобно задавать несколько интервалов с постоянной пропускной способностью, но

сглаживать резкие скачки (например, при мгновенном разрушении и последующем восстановлении). Гладкая аппроксимация ступенчатой функции использует гиперболический тангенс:

$$c(t) = c_0 - \frac{c_0 - c_1}{2}\left(1 + \tanh\frac{t - T_1}{\delta}\right) + \frac{c_0 - c_1}{2}\left(1 + \tanh\frac{t - T_2}{\delta}\right). \quad (9)$$

Здесь δ — параметр гладкости. При $\delta \to 0$ функция приближается к кусочно-постоянной со скачками в точках T_1 и T_2. В такой модели нет линейных участков, только плавные переходы между постоянными уровнями.

Определение пропускной способности при использовании динамических моделей. Максимальный поток определяется как функция времени (квазистатическое приближение). Для каждого момента t решается статическая задача максимального потока. Задержки движения грузов по дугам не учитываются — поток мгновенно подстраивается под текущую пропускную способность. Это допустимо, если время изменения $c_e(t)$ заметно больше времени доставки.

При переменных $c_e(t)$ максимальный поток зависит от времени:

$$\Phi_{\max}(t) = \max_f \sum_{e \in \delta^+(s)} f(e,t), \quad (10)$$

при ограничениях: $0 \le f(e,t) \le c_e(t) \quad \forall e \in E, \quad \sum_{e\in\delta^+(v)} f(e,t) = \sum_{e\in\delta^-(v)} f(e,t)$ $\forall v \in V \setminus s,t.$

$\Phi_{\max}(t)$ — это наибольшая возможная величина потока, которую можно передать из s в t в момент t.

Интегральные характеристики:

- суммарный объём груза за время $[0,T]$:

$$V(T) = \int_0^T \Phi_{\max}(t)\, dt; \quad (11)$$

- время перевозки заданного объёма;
- момент падения пропускной способности ниже порога.

Ограничения подхода и связь со ступенчатыми моделями. Предложенные гладкие модели имеют определённые ограничения, которые важно учитывать при практическом применении.

Ограничения:

1. Предположение о детерминированности — функции $c_e(t)$ известны точно. Реальные сценарии деградации и восстановления часто включают случайные составляющие (разброс времени ремонта, вероятностные отказы). Переход к стохастической модели потребовал бы использования методов теории случайных процессов.

2. Независимость дуг — модель предполагает, что пропускная способность каждой дуги меняется автономно. Однако на практике возможны корреляции (к примеру, землетрясение повреждает целый ряд участков одновременно). Чтобы учесть такие случаи, достаточно ввести в модель общие внешние факторы, воздействующие на несколько дуг.

3. Гладкость не везде уместна — некоторые события (взрыв, внезапное обрушение моста, мгновенное перекрытие движения) происходят практически скачкообразно. В этих случаях гладкая функция с очень большой крутизной (почти ступенька) может быть вычислительно неудобна.

Связь со ступенчатыми функциями. Ступенчатая функция (функция Хевисайда) $H(t - t_0)$ является предельным случаем сигмоидальной (логистической) функции при стремлении параметра крутизны к бесконечности:

$$\lim_{k\to\infty}\frac{1}{1+e^{-k(t-t_0)}}=\begin{cases}0, & t<t_0,\\ 0.5, & t=t_0,\\ 1, & t>t_0.\end{cases} \qquad (12)$$

Любое мгновенное изменение пропускной способности аппроксимируется гладкой сигмоидой с большим параметром k с любой требуемой точностью. Следовательно, предложенный гладкий подход включает ступенчатые модели как частный случай. При достаточно больших k в численных расчётах допустима замена на кусочно-постоянные функции, однако при этом утрачивается возможность аналитического интегрирования.

Численный пример: нормализация движения после ликвидации аварии. Возьмём участок дороги с 4 полосами. Пропускная способность $c_0 = 100$ авт./ч. В момент $t = 0$ авария перекрывает две полосы, и пропускная способность падает до 50 авт./ч (работают только две полосы). Начинаются работы и первые два часа ($0 \le t \le 2$) осуществляется подготовка (приезд служб, разбор завалов), пропускная способность остаётся 50. На интервале [2, 6] ч постепенно открывают сначала одну дополнительную полосу, затем последнюю. Этот процесс идёт по логистической (сигмоидальной) кривой: сначала медленно, потом быстрее, а к концу снова замедляется (восстановление после затора). После $t = 6$ ч все четыре полосы работают, пропускная способность достигает 100.

Для описания используем нормированную логистическую функцию:

$$c(t) = 50 + 50\cdot\frac{\sigma(t)-\sigma(2)}{\sigma(6)-\sigma(2)}, \qquad \sigma(t)=\frac{1}{1+e^{-k(t-t_0)}}, \qquad (13)$$

где $t_0 = 4$ — точка перегиба (момент максимальной скорости восстановления), $k = 1.5$ — крутизна логистической кривой. При $t \ge 6$ ч пропускная способность возвращается к исходному уровню $c = 100$ авт./ч.

На рисунке 1 сопоставлена полученная динамическая зависимость со ступенчатой моделью, в которой восстановление происходит мгновенно в момент $t = 6$.

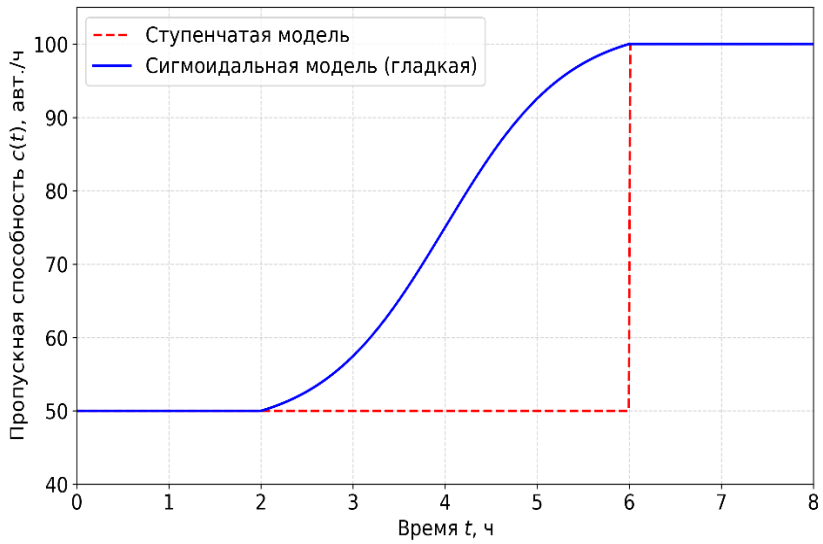


Рис. 1. Сравнение ступенчатой
и сигмоидальной моделей восстановления пропускной способности

В отличие от скачкообразного изменения, сигмоидальная кривая даёт плавный переход от повреждённого состояния к полной пропускной способности. Такое поведение соответствует реальным процессам восстановления после аварийных ситуаций.

Количество автомобилей, прошедших за 8 часов, вычисляется по формуле

$$V(8) = \int_0^8 c(t)\, dt. \tag{14}$$

Аналитическое интегрирование (при необходимости — численная проверка квадратурными формулами с шагом 10^{-3}) приводит к следующим значениям:

- для сигмоидальной модели $V_{\text{sig}} = 600$ авт.;
- для ступенчатой модели $V_{\text{step}} = 50 \cdot 6 + 100 \cdot 2 = 500$ авт.

Таким образом, учёт плавного (гладкого) характера восстановления позволяет учесть дополнительный проезд $\Delta V = 100$ автомобилей (на 20% больше) за тот же период (рис. 2). Это подтверждает, что динамические модели с гладкими функциями способны давать более точную оценку пропускной способности по сравнению со ступенчатыми упрощениями.

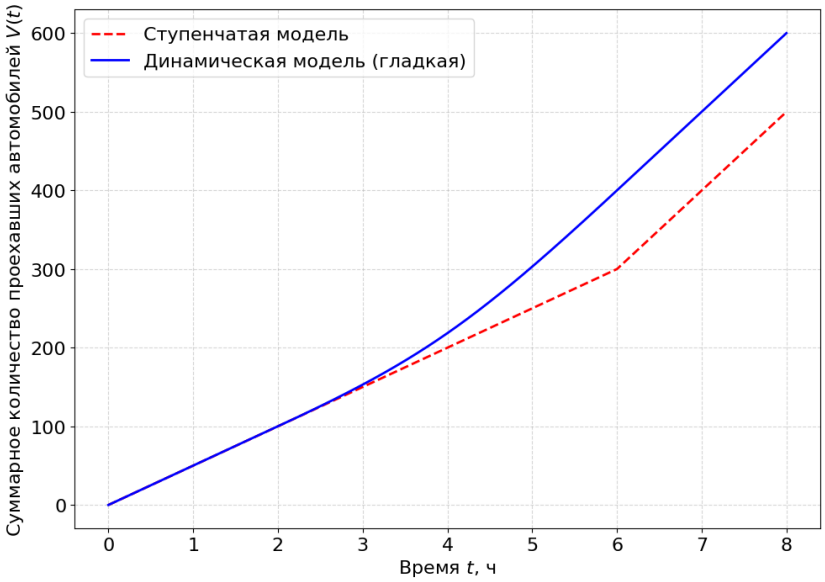


Рис. 2. Сравнение суммарного количества проехавших автомобилей

Заключение. В работе показано, что в реальных транспортно-логистических сетях между одними и теми же пунктами часто существует несколько альтернативных маршрутов. Мультиграфовое представление даёт возможность применять методы теории графов для расчёта максимального потока, многокритериальной оптимизации маршрутов и анализа уязвимости сети.

Предложены динамические модели с гладкими функциями, описывающие постепенную деградацию (износ, накопление повреждений) и восстановление (ремонт, открытие полос). Обоснован выбор экспоненциальных и сигмоидальных функций, указана их связь со ступенчатыми моделями. Установлено, что предложенные зависимости применимы к разным видам транспорта.

ЛИТЕРАТУРА

1. Menshikh V. V., Zvereva D. D. Models and algorithms of optimal structure synthesis of infocommunication network with specified parameters // Journal of Physics : Conference Series. — 2019 — Vol. 1203. — DOI: 10.1088/1742-6596/1203/1/012067.

2. Zvereva D. D., Menshikh V. V., Seifer A. V. Optimization of processes of modernization and operating conditions of infocommunication networks // Global Smart Industry Conference (Chelyabinsk, 13—15 Nov. 2018). — Chelyabinsk, 2018. — P. 1—6.

3. Меньших В. В., Зверева Д. Д. Модель оптимизации выбора вариантов изменения инфокоммуникационной сети (сегмента сети) // Вестник Воронежского института МВД России. — 2018. — № 1. — С. 21—26.

4. Зверева Д. Д. Модели и алгоритмы оптимизации выбора вариантов модернизации инфокоммуникационных сетей органов внутренних дел : дис. … канд. техн. наук : 05.13.18 / Зверева Дарья Дмитриевна. — Воронеж, 2020. — 139 с.

5. Resilience Quantification and Recovery Prediction of Highway Toll-Station Nodes Under Rainfall Disturbances / Z. Wang, J. Jia, X. Wang [at al.] // Sustainability. — 2026. — Vol. 18. — No. 9. — Art. 4455. — DOI: 10.3390/su18094455.

6. Comparative Analysis of Three Modeling Approaches for Predicting Pavement Conditions / J. Wang, G. Comert, N. Begashaw [at al.] // Transportation Research Record : Journal of the Transportation Research Board. — 2024. — Vol. 2678. — No. 10. — P. 547—560. — DOI: 10.1177/03611981241234924.

7. Gao Y., Levinson D. A multistage spatial queueing model with logistic arrivals and departures consistent with the microscopic fundamental diagram and hysteresis // Transportation Research. Part B : Methodological. — 2024. — Vol. 186. — Art. 103015. — DOI: 10.1016/j.trb.2024.103015.

8. Fürstenau N., Mittendorf M., Kamo S. Nonlinear dynamics approach for modeling of air traffic performance disruption and recovery // 7th International Conference on Research in Air Transportation (ICRAT 2016). — Philadelphia, 2016. — P. 1—8.

9. Evaluation of Corrosion Residual Life Prediction Methods for Metal Pipelines / L. Zuo, C. Zeng, X. Hu [at al.] // Materials. — 2022. — Vol. 15. — No. 16. — P. 5624. — DOI: 10.3390/ma15165624.

REFERENCES

1. Menshikh V. V., Zvereva D. D. Models and algorithms of optimal structure synthesis of infocommunication network with specified parameters // Journal of Physics : Conference Series. — 2019 — Vol. 1203. — DOI: 10.1088/1742-6596/1203/1/012067.

2. Zvereva D. D., Menshikh V. V., Seifer A. V. Optimization of processes of modernization and operating conditions of infocommunication networks // Global Smart Industry Conference (Chelyabinsk, 13—15 Nov. 2018). — Chelyabinsk, 2018. — P. 1—6.

3. Men′shikh V. V., Zvereva D. D. Model′ optimizatsii vybora variantov izmeneniya infokommunikatsionnoj seti (segmenta seti) // Vestnik Voronezhskogo instituta MVD Rossii. — 2018. — № 1. — S. 21—26.

4. Zvereva D. D. Modeli i algoritmy optimizatsii vybora variantov modernizatsii infokommunikatsionnykh setej organov vnutrennikh del : dis. … kand. tekhn. nauk : 05.13.18 / Zvereva Dar′ya Dmitrievna. — Voronezh, 2020. — 139 s.

5. Resilience Quantification and Recovery Prediction of Highway Toll-Station Nodes Under Rainfall Disturbances / Z. Wang, J. Jia, X. Wang [at al.] // Sustainability. — 2026. — Vol. 18. — No. 9. — Art. 4455. — DOI: 10.3390/su18094455.

6. Comparative Analysis of Three Modeling Approaches for Predicting Pavement Conditions / J. Wang, G. Comert, N. Begashaw [at al.] // Transportation Research Record : Journal of the Transportation Research Board. — 2024. — Vol. 2678. — No. 10. — P. 547—560. — DOI: 10.1177/03611981241234924.

7. Gao Y., Levinson D. A multistage spatial queueing model with logistic arrivals and departures consistent with the microscopic fundamental diagram and hysteresis // Transportation Research. Part B : Methodological. — 2024. — Vol. 186. — Art. 103015. — DOI: 10.1016/j.trb.2024.103015.

8. Fürstenau N., Mittendorf M., Kamo S. Nonlinear dynamics approach for modeling of air traffic performance disruption and recovery // 7th International Conference on Research in Air Transportation (ICRAT 2016). — Philadelphia, 2016. — P. 1—8.

9. Evaluation of Corrosion Residual Life Prediction Methods for Metal Pipelines / L. Zuo, C. Zeng, X. Hu [at al.] // Materials. — 2022. — Vol. 15. — No. 16. — P. 5624. — DOI: 10.3390/ma15165624.

СВЕДЕНИЯ ОБ АВТОРЕ

Зверева Дарья Дмитриевна. Старший преподаватель кафедры информационной безопасности. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: zubzv@yandex.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Zvereva Daria Dmitrievna. Senior Lecturer of the chair of Information Security. Candidate of Technical Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: zubzv@yandex.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: транспортная сеть; пропускная способность; максимальный поток; динамическая модель; гладкая функция; деградация; восстановление; живучесть; ступенчатая функция.

Key words: transport network; capacity; maximum flow; dynamic model; smooth function; degradation; recovery; survivability; step function.

УДК 004.94

Д. С. Звягин, *кандидат технических наук*
О. В. Пименова, *кандидат технических наук*

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ИНДИКАТОРОВ ПОЛЯ И ЧАСТОТОМЕРОВ ПРИ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

FEATURES OF USING FIELD INDICATORS AND FREQUENCY METERS IN IMPLEMENTING SECURITY OF CONFIDENTIAL INFORMATION

В статье рассматриваются вопросы практического применения индикаторов поля и частотомеров как ключевых инструментов технической защиты информации при проведении поисковых мероприятий по выявлению электронных устройств негласного получения информации. Проведён обзор современных отечественных приборов (ST 111, RAKSA-121, NR-D, РИЧ-8 (MFP-8000)), проанализированы их функциональные особенности и области применения. Особое внимание уделено многоканальному измерителю РИЧ-8, как устройству, совмещающему функции индикатора поля, частотомера, измерителя мощности и анализатора сигнатур. На основе анализа архитектуры и режимов работы данного прибора предложена математическая модель процесса поиска электронных устройств негласного получения информации с использованием аппарата сетей Петри. Разработанная модель описывает последовательность действий оператора, смену режимов работы и условия принятия решений, что позволяет формализовать и оптимизировать процесс обследования защищаемых помещений.

This article examines the practical application of field indicators and frequency meters as key tools for technical information security during search operations to detect electronic devices for covert information acquisition. A review of modern domestic devices (ST 111, RAKSA-121, NR-D, RICH-8 (MFP-8000)) is provided, along with an analysis of their functional features and applications. Particular attention is paid to the RICH-8 multichannel meter as a device combining the functions of a field indicator, frequency meter, power meter, and signature analyzer. Based on an analysis of the device's architecture and operating modes, a mathematical model of the search for electronic devices for covert information acquisition using Petri nets is proposed. The developed model describes the sequence of operator actions, operating mode changes, and decision-making conditions, thereby formalizing and optimizing the process of inspecting protected premises.

Введение. В современном мире, характеризующемся высокой геополитической напряженностью и ожесточенной конкурентной борьбой в бизнесе, вопросы обеспечения информационной безопасности выходят на первый план. Особую уязвимость представляют собой конфиденциальные встречи и деловые переговоры, в ходе которых обсуждаются сведения, составляющие государственную тайну, коммерческую тайну или иную информацию ограниченного доступа. Угроза несанкционированного съема информации с помещений для переговоров посредством радиопередающих электронных

устройств негласного получения информации (далее — ЭУ НПИ) остается чрезвычайно высокой, что требует применения эффективных и надежных методов противодействия [1]. В этой связи техническая защита информации, и в частности проведение поисковых мероприятий, приобретает критическое значение для собственников бизнеса, руководителей организаций и государственных служащих.

Техническое обеспечение поисковой деятельности базируется на применении специализированных приборов, позволяющих выявить факт несанкционированной передачи данных. Среди всего многообразия средств поиска ключевую роль играют индикаторы поля и частотомеры, которые служат первичным инструментом для обнаружения работающих радиопередающих устройств. Актуальность использования данных приборов в рамках обеспечения защиты конфиденциальных встреч и переговоров продиктована самой природой современных ЭУ НПИ, которые для передачи перехваченной информации используют каналы связи в широком диапазоне радиочастот — от единиц МГц до нескольких ГГц. Компактные и простые в эксплуатации индикаторы поля позволяют оперативно оценить электромагнитную обстановку в помещении и выявить аномальные источники радиоизлучения. Частотомеры, в свою очередь, дают возможность точно определить несущую частоту обнаруженного сигнала, что необходимо для его последующей идентификации и локализации источника.

Таким образом, исследование технических характеристик, методологии применения и эффективности современных индикаторов поля и частотомеров в контексте поиска ЭУ НПИ является важной научно-практической задачей. Совершенствование методов инструментального поиска направлено на повышение гарантий конфиденциальности проводимых мероприятий и минимизацию рисков утечки информации по радиоканалу. Настоящая работа посвящена анализу функциональных возможностей данных устройств и их роли в комплексе мер по защите переговорных помещений от современных углубленных угроз технической разведки.

Современный рынок технических средств защиты информации предлагает широкий спектр отечественных индикаторов поля и частотомеров, предназначенных для поиска ЭУ НПИ. Ниже представлен краткий обзор наиболее актуальных приборов, включая детектор поля ST 111, селективный индикатор RAKSA-121 и компонентный индикатор NR-D. Особое внимание в конце обзора уделено прибору РИЧ-8 (MFP-8000), который занимает уникальную нишу на рынке [2].

Детектор поля ST 111 является представителем класса широкополосных детекторов поля. Его работа основана на измерении напряженности электрического поля в широкой полосе частот. Прибор охватывает впечатляющий диапазон до 7 ГГц (50—2500 МГц и 2500—7000 МГц) и способен идентифицировать распространенные типы сигналов (GSM, DECT, Bluetooth, Wi-Fi). Отличительной особенностью модели является наличие режима осциллографа, позволяющего проводить анализ сигналов во временной области, что полезно для отсеивания импульсных помех (рис. 1).

Селективный индикатор поля RAKSA-121 принципиально отличается от широкополосных детекторов тем, что построен по схеме супергетеродинного приемника. Это позволяет ему проводить частотно-селективный анализ, эффективно разделяя сигналы даже в условиях плотного радиочастотного фона. Его главные преимущества — сверхкомпактность и наличие интеллектуальных алгоритмов работы, таких как режим «Охрана» с вычитанием фонового спектра и режим «Поиск с вычитанием спектра», которые значительно повышают вероятность обнаружения локальных источников излучения (рис. 2).



Рис. 1. Детектор поля ST 111



Рис. 2. Селективный индикатор поля RAKSA-121

Индикатор поля-NR-D — это компонентный индикатор ближнего поля, особенностью которого является наличие двух каналов обработки сигнала: канала детектора мощности и компонентного канала. Такая архитектура предназначена для более глубокого анализа сигнальной обстановки и локализации источников. Прибор ориентирован на длительный автономный мониторинг благодаря большому объему энергонезависимой памяти (до 2048 событий). По верхней границе частотного диапазона (до 3500 МГц) он уступает лидерам рынка, а точность измерения частоты импульсных сигналов является его основной характеристикой (рис. 3).

РИЧ-8 (MFP-8000) занимает особое положение среди средств поиска ЭУ НПИ, так как позиционируется не просто как индикатор, а как портативный универсальный измеритель, объединяющий в одном корпусе функции четырех приборов: измерителя мощности, частотомера, индикатора поля и анализатора сигнатуры (сигнатурного анализатора). (рис. 4) Ключевыми особенностями данного поискового средства являются:

- Рекордный частотный диапазон — обеспечивает обнаружение устройств в самом широком спектре — от 0,1 до 8000 МГц, что перекрывает все актуальные диапазоны связи, включая верхние этажи гражданских частот (до 8 ГГц).

- Высочайшая точность измерений — отличается прецизионной точностью измерения частоты и мощности.

- Функция сигнатурного анализа — позволяет идентифицировать во входном сигнале признаки протоколов сотовой связи (GSM) и беспроводных телефонов (DECT).

- Интеграция в системы — благодаря встроенному интерфейсу RS-232 РИЧ-8 может использоваться в качестве измерительного элемента в составе автоматизированных комплексов для управления внешними панорамными приемниками.



Рис. 3. Индикатор поля-NR-D



Рис. 4. РИЧ-8 (MFP-8000)

Таким образом, если ST 111, RAKSA-121 и NR-D являются оптимизированными инструментами для решения конкретных поисковых задач (оперативный поиск, селективный анализ, мониторинг), то РИЧ-8 (MFP-8000) представляет собой эталонный измерительный прибор для профессионалов, которым требуется не только обнаружение, но и высокоточное определение параметров сигнала в максимально широком диапазоне.

Постановка задачи. Работа с индикаторами поля и частотомерами требует определенных навыков и знаний, необходимых для качественного и полноценного проведения поисковых мероприятий. Учитывая это, в основу моделирования процесса поиска ЭУ НПИ при помощи индикаторов поля следует положить модели, в которых учитывается смена состояний взаимосвязанных процессов. Наиболее удобным средством построения таких моделей являются сети Петри [3, 4].

Решение. Эффективность поисковых мероприятий, направленных на обнаружение ЭУ НПИ, находится в прямой зависимости не только от тактики проведения осмотра, но и от глубины понимания оператором физических принципов функционирования применяемого инструментария. Индикатор поля, являясь первичным звеном в цепи обнаружения, представляет собой сложный радиоизмерительный прибор, грамотная эксплуатация которого невозможна без всестороннего изучения его архитектуры, режимов работы и метрологических характеристик.

Современные индикаторы поля, такие как селективные модели, могут содержать в себе алгоритмы цифровой обработки сигналов: режимы вычитания спектральной маски, идентификацию типов сигналов (GSM, LTE, Wi-Fi), функции осциллографа или анализатора спектра. Глубокое знание архитектуры позволяет оператору корректно выбирать режим работы под конкретную задачу.

Обобщенная UML-диаграмма работы индикатора поля представлена на рисунке 5.

В связи с тем что в рамках данного исследования мы выделили индикатор поля РИЧ - 8 (MFP-8000), дальнейшую математическую модель будем строить на примере данного поискового прибора.

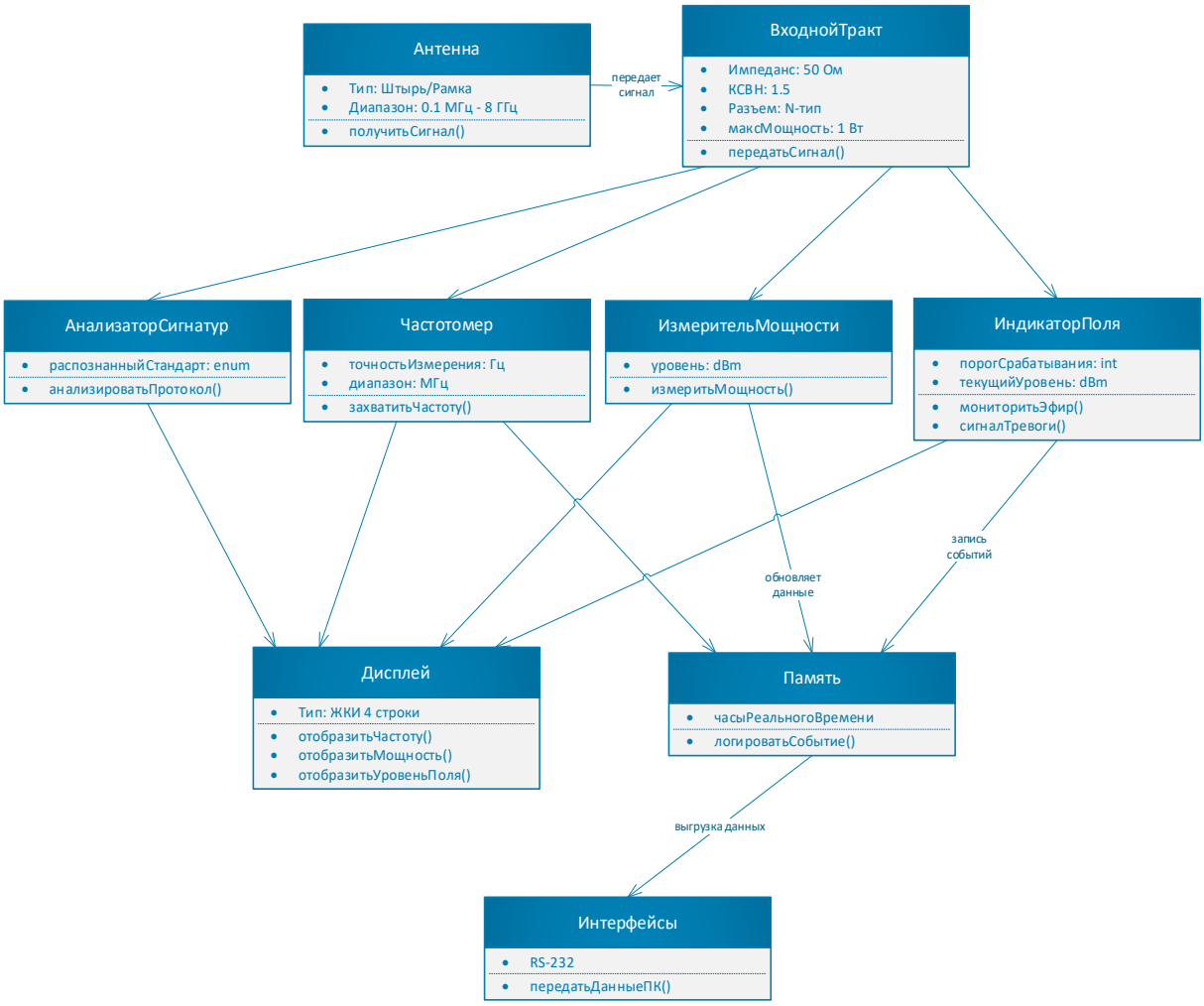


Рис. 5. UML-диаграмма работы индикатора поля

Сети Петри — это математический процесс моделирования динамических параллельных и асинхронных систем, являющийся совокупностью множеств $C = \{P, T, I, O\}$, где P и T — это множество позиций и переходов, а I и O — входная и выходная функции соответственно [5, 6].

Рассматривая процесс поиска ЭУ НПИ при помощи индикаторов поля РИЧ-8, построим его математическую модель при помощи аппарата сети Петри (рис. 6).

В этой сети Петри:

$P = \{p_1, p_2, \dots p_{22}\}$; $T = \{t_1, t_2, \dots t_{18}\}$;

$I(t_1) = \{p_1\}$; $I(t_2) = \{p_2\}$; $I(t_3) = \{p_3\}$; $I(t_4) = \{p_4\}$; $I(t_5) = \{p_5, p_6\}$; $I(t_6) = \{p_6, p_7\}$; $I(t_7) = \{p_8\}$; $I(t_8) = \{p_9\}$; $I(t_9) = \{p_{10}, p_{11}\}$; $I(t_{10}) = \{p_{11}, p_{12}\}$; $I(t_{11}) = \{p_{13}\}$; $I(t_{12}) = \{p_{14}\}$; $I(t_{13}) = \{p_{15}\}$; $I(t_{14}) = \{p_{16}\}$; $I(t_{15}) = \{p_{17}\}$; $I(t_{16}) = \{p_{18}, p_{19}\}$; $I(t_{17}) = \{p_{19}, p_{20}\}$; $I(t_{18}) = \{p_{21}\}$;

$O(t_1) = \{p_2\}$; $O(t_2) = \{p_3\}$; $O(t_3) = \{p_4\}$; $O(t_4) = \{p_6\}$; $O(t_5) = \{p_4\}$; $O(t_6) = \{p_8\}$; $O(t_7) = \{p_9\}$; $O(t_8) = \{p_{11}\}$; $O(t_9) = \{p_{13}\}$; $O(t_{10}) = \{p_{15}\}$; $O(t_{11}) = \{p_{14}\}$; $O(t_{12}) = \{p_{15}\}$; $O(t_{13}) = \{p_{16}\}$; $O(t_{14}) = \{p_{17}\}$; $O(t_{15}) = \{p_{19}\}$; $O(t_{16}) = \{p_{21}\}$; $O(t_{17}) = \{p_{17}\}$; $O(t_{18}) = \{p_{22}\}$.

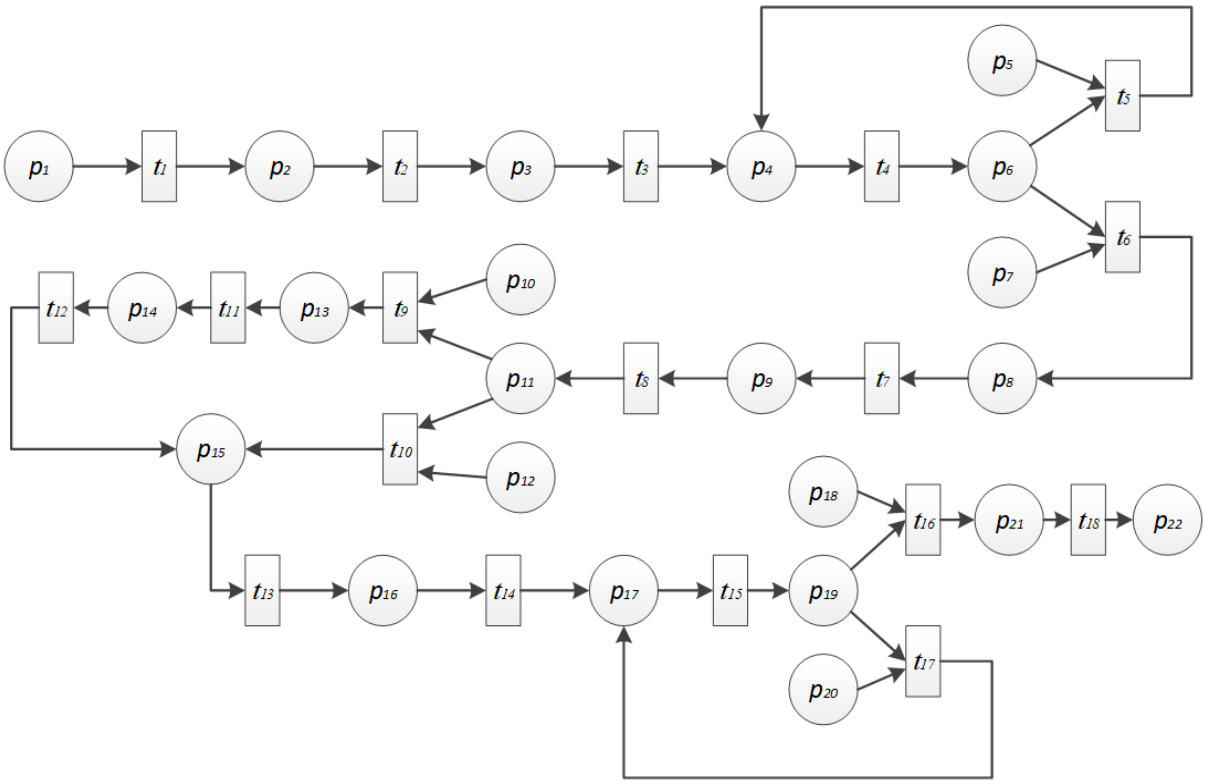


Рис. 6. Модель поиска ЭУ НПИ при помощи индикаторов поля РИЧ-8

В таблице 1 представлено описание всех позиций разработанной математической модели процесса поиска ЭУ НПИ при помощи индикаторов поля РИЧ-8.

Таблица 1.

Описание позиций модели поиска ЭУ НПИ при помощи индикаторов поля РИЧ-8

Позиции	Описание позиции
p_1	включение прибора РИЧ-8
p_2	выбор режима работы
p_3	включение режима «Индикатор поля»
p_4	мониторинг эфира в режиме «Индикатор поля»
p_5	сигнал не обнаружен
p_6	анализ уровня сигнала
p_7	сигнал обнаружен
p_8	фиксация частоты сигнала
p_9	включение режима «Частотомер»
p_{10}	требуется идентификация сигнала
p_{11}	измерение несущей частоты
p_{12}	не требуется идентификация сигнала
p_{13}	активация «Анализатор сигнатур»

Позиции	Описание позиции
p_{14}	сравнение с базами GSM/DECT/WiFi и вывод результата на экран
p_{15}	включение режима «Измеритель мощности»
p_{16}	наблюдение за уровнем *P* (дБм)
p_{17}	перемещение оператора с антенной
p_{18}	уровень мощности сигнала достиг максимума
p_{19}	фиксация текущего уровня мощности
p_{20}	уровень мощности растет
p_{21}	фиксация положения антенны
p_{22}	запись результата

Заключение. Разработанная модель позволит оптимизировать процесс поиска ЭУ НПИ при обследование защищаемых помещений с использованием индикаторов поля РИЧ-8 (MFP-8000).

Вариативное размещение меток в позициях разработанной модели позволяет сформировать ряд наблюдений, позволяющих найти закономерности в осуществлении процесса поиска ЭУ НПИ при помощи индикаторов поля и, используя данную информацию, осуществлять проведение данного мероприятия на более качественном уровне.

ЛИТЕРАТУРА

1. Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) : постановление Правительства РФ от 16 апреля 2012 г. № 314 // СПС «КонсультантПлюс».

2. Сайт компании Detector Systems. — URL: http://detsys.ru/

3. Питерсон Дж. Теория сетей Петри и моделирование систем. — М. : Мир, 1984. — 264 с.

4. Котов В. Е. Сети Петри. — М. : Наука. Главная редакция физико-математической литературы, 1984. — 160 с.

5. Пьянков О. В., Звягин Д. С. Моделирование процесса производства судебной почерковедческой экспертизы при помощи сетей Петри // Вестник Воронежского института МВД России. — 2020. — № 1. — С. 57—64.

6. Лескин А. А., Мальцев П. А., Спиридонов А. М. Сети Петри в моделировании и управлении. — Л. : Наука, 1989. — 133 с.

REFERENCES

1. Ob utverzhdenii Polozheniya o litsenzirovanii deyatel′nosti po vyyavleniyu elektronnykh ustrojstv, prednaznachennykh dlya neglasnogo polucheniya informatsii (za isklyucheniem sluchaya, esli ukazannaya deyatel′nost′ osushchestvlyaetsya dlya obespecheniya sobstvennykh nuzhd yuridicheskogo litsa ili individual′nogo predprinimatelya) : postanovlenie Pravitel′stva RF ot 16 aprelya 2012 g. № 314 // SPS «Konsul′tantPlyus».

2. Sajt kompanii Detector Systems. — URL: http://detsys.ru/

3. Piterson Dzh. Teoriya setej Petri i modelirovanie sistem. — M. : Mir, 1984. — 264 s.

4. Kotov V. E. Seti Petri. — M. : Nauka. Glavnaya redaktsiya fiziko-matematicheskoj literatury, 1984. — 160 s.

5. P′yankov O. V., Zvyagin D. S. Modelirovanie protsessa proizvodstva sudebnoj pocherkovedcheskoj ekspertizy pri pomoshchi setej Petri // Vestnik Voronezhskogo instituta MVD Rossii. — 2020. — № 1. — S. 57—64.

6. Leskin A. A., Mal′tsev P. A., Spiridonov A. M. Seti Petri v modelirovanii i upravlenii. — L. : Nauka, 1989. — 133 s.

СВЕДЕНИЯ ОБ АВТОРАХ

Звягин Данил Сергеевич. Доцент кафедры информационной безопасности. Кандидат технических наук.

Воронежский институт МВД России.
E-mail: danil_exp@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Пименова Оксана Владимировна. Доцент кафедры информационной безопасности учебно-научного комплекса информационных технологий. Кандидат технических наук.

Московский университет МВД России имени В. Я. Кикотя.
E-mail: okcana.pimenova@yandex.ru
Россия, 117437, Москва, ул. Академика Волгина, 12.

Zvyagin Danil Sergeevich. Associate Professor of the chair of Information Security. Candidate of Technical Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: danil_exp@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Pimenova Oksana Vladimirovna. Associate Professor of the chair of Information Security of the Educational and Scientific Complex of Information Technologies. Candidate of Technical Sciences.

Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot.
E-mail: okcana.pimenova@yandex.ru
Work address: Russia, 117437, Moscow, Akademika Volgina Str., 12.

Ключевые слова: моделирование; сети Петри; индикатор поля; защита информации.

Key words: modeling; Petri nets; field indicator; information security.

УДК 004.056

А. Ю. Телков, *кандидат физико-математических наук, доцент*
М. М. Жуков, *кандидат технических наук, доцент*
Д. И. Полухин

ЗАЩИЩЕННЫЙ МАРШРУТИЗАТОР С ПОДДЕРЖКОЙ L3 VPN И МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ НА БАЗЕ ASTRA LINUX SE В СЦЕНАРИЯХ ПРИМЕНЕНИЯ «СЕТЬ-СЕТЬ» И «СЕТЬ-ПОЛЬЗОВАТЕЛЬ»

SECURE ROUTER WITH L3 VPN AND MULTIFACTOR AUTHENTICATION SUPPORT BASED ON ASTRA LINUX SE FOR NETWORK-TO-NETWORK AND NETWORK-TO-USER APPLICATION SCENARIOS

В статье рассматриваются вопросы реализации функционала защищенного маршрутизатора-концентратора сетевых потоков на отечественной операционной системе (ОС) Astra Linux Special Edition (ALSE). Исследуется возможность интеграции технологий VPN и двухфакторной (2FA) или многофакторной (MFA) аутентификации для организации безопасного удаленного доступа в топологии «сеть-пользователь», а также возможные решения для реализации топологий «сеть-сеть». Приводятся результаты анализа актуальности разработки, обзор технологий, схемы реализации на базе встроенного в ОС ALSE программного обеспечения. Формулируются выводы о целесообразности и основных особенностях развертывания подобного решения.

This article examines the implementation of a secure network flow concentrator router on the domestic Astra Linux Special Edition (ALSE) operating system (OS). It explores the feasibility of integrating VPN technologies and two-factor or multi-factor authentication (2FA and MFA) to provide secure remote access in a network-to-user topology, as well as potential solutions for implementing network-to-network topologies. The article presents the results of an analysis of the development's relevance, a technology overview, and implementation schemes based on OS-embedded software. Conclusions are drawn regarding the feasibility and key considerations for deploying such a solution.

Введение. В условиях глобальной цифровой трансформации и ужесточения требований к кибербезопасности, особенно на фоне санкционного давления и продолжения разработки решений согласно политике импортозамещения, задача создания отечественных средств защиты периметра и удаленного доступа является стратегически важной [1]. Традиционные межсетевые экраны (МЭ) или Firewall эволюционировали в решения класса Next-Generation Firewall (NGFW), которые интегрируют функции глубокой инспекции пакетов (DPI), предотвращения вторжений (IPS), контроля приложений, а также безопасных виртуальных частных сетей (VPN) и гибких механизмов аутентификации [2, 3].

В настоящее время российский рынок информационной безопасности по-прежнему нуждается в гибких, сертифицированным по требованиям регуляторов —

ФСТЭК России и ФСБ России — решениях, которые могут быть развернуты как на специализированном оборудовании, так и на серверах (аппаратных платформах) универсального назначения. Особую важность приобретают гибридные сценарии, требующие одновременного обслуживания постоянных зашифрованных туннелей между филиалами либо между филиалами и центральным сетевым сегментом (топология «сеть-сеть») и предоставления безопасного доступа мобильным сотрудникам и удаленным рабочим местам (топология «сеть-пользователь»). Реализация такого функционала на базе российской ОС ALSE, имеющей сертификаты соответствия требованиям по безопасности информации (пока только для обработки информации, но не для использования в качестве сертифицированных межсетевых экранов[1]) и входящей в реестр Минцифры[2], представляется логичным и перспективным направлением развития отечественной сетевой инфраструктуры. Несмотря на актуальность темы, объем информации по реализации указанного функционала на универсальной аппаратной платформе и на базе ОС ALSE авторы считают явно недостаточным, а саму информацию разрозненной, что и определяет направленность данного исследования.

Целью настоящей работы является определение схем реализации защищенного маршрутизатора с поддержкой технологий L3 VPN и многофакторной аутентификации на базе ОС ALSE в сценариях применения «сеть-сеть» и «сеть-пользователь» и демонстрационная реализация одной из таких схем с выявлением ее особенностей, связанных с работой ОС ALSE в усиленном режиме безопасности.

Для достижения указанной цели рассмотрим и решим следующие задачи. Сначала выясним актуальность имеющихся на текущий момент технологий VPN, затем проанализируем существующие в ОС ALSE подсистемы и модули для реализации актуальных технологий VPN и на завершающем этапе предложим и исследуем методику реализации одного из предложенных решений. По итогам исследований обобщим полученные результаты, сформулируем выводы и рекомендации.

I. Существующие технологии VPN, их роль и место. Процесс развития технологий VPN при его анализе в исторической ретроспективе может быть разбит на насколько этапов.

Первый этап. Ранние протоколы (PPTP, L2TP). Отличались относительной простотой настройки, но имели фундаментальные уязвимости в области криптографии (PPTP) или не предоставляли встроенного шифрования (L2TP, которое часто комбинировалось с IPsec). PPTP — один из старейших протоколов туннелирования, разработанный в конце 1990-х годов компаниями Microsoft и Cisco. Его спецификация опубликована как информационный документ RFC 2637 [4], однако протокол не был ратифицирован IETF (Internet Engineering Task Force). Первоначально протокол создавался для организации удаленного доступа сотрудников к корпоративным сетям через коммутируемые соединения (dial-up). Протокол функционирует на канальном уровне модели OSI и основывается на инкапсуляции кадров PPP (Point-to-Point Protocol) в IP-пакеты. Для установки соединения используется два канала: во-первых, управляющее соединение на TCP-порту 1723 для инициации и управления туннелем и, во-вторых, туннель данных через протокол GRE (Generic Routing Encapsulation) для передачи инкапсулированных

[1] Сертификат соответствия Министерства обороны Российской Федерации № 1339. Операционная система специального назначения «Astra Linux Special Edition». — М. : НПО «Эшелон», 2010. — 24 сент.

[2] Astra Linux Special Edition. Сертификация // Справочный центр Astra Linux : [сайт]. — URL: https://wiki.astralinux.ru/ (дата обращения: 19.03.2026).

пакетов. Шифрование реализуется через протокол MPPE (Microsoft Point-to-Point Encryption), использующий поточный шифр RC4. Аутентификация может выполняться различными механизмами, среди которых наиболее распространены MS-CHAPv2 и EAP-TLS. В настоящее время PPTP считается устаревшим и нерекомендуемым для использования протоколом. Компания Apple исключила его поддержку из macOS Sierra и iOS 10 по соображениям безопасности, многие VPN-сервисы отказались от его поддержки. Теоретическое применение ограничено узкими сценариями, где безопасность не является критическим требованием, а скорость выступает приоритетом — например, сервер доступа в сеть Интернет, размещенный внутри защищенной локальной сети организации. Достоинства и недостатки протокола PPTP указаны в таблице 1.

Протокол L2TP (Layer 2 Tunneling Protocol) — протокол туннелирования канального уровня, объединяющий лучшие функции PPTP (от Microsoft) и L2F (Layer 2 Forwarding, от Cisco). Стандарт был предложен в 2000 году, его спецификация опубликована как информационный документ RFC 2661 [5]. При изолированном использовании он не обеспечивает шифрования и конфиденциальности, поэтому практически всегда применяется в связке с IPSec — такая комбинация известна как L2TP/IPsec. L2TP использует архитектуру «клиент-сервер» с двумя основными компонентами: во-первых, LAC (L2TP Access Concentrator) — устройство на стороне клиента или оператора связи, и, во-вторых, LNS (L2TP Network Server) — сервер, обрабатывающий подключения. Протокол инкапсулирует пакеты PPP в UDP-дейтаграммы (порт 1701) для передачи через IP-сети. При использовании с IPSec применяется двойная инкапсуляция: сначала L2TP, затем IPSec, что увеличивает накладные расходы. Функции безопасности обеспечиваются протоколом только в связке с IPSec, при этом используются алгоритмы шифрования AES и 3DES (до 256 бит), а аутентификация обеспечивается протоколами IPSec и целостность данных гарантируется механизмами IPSec. Наиболее широкое применение протокол L2TP нашел в корпоративных VPN-решениях, провайдерских схемах удаленного PPP-доступа, сценариях BRAS/BNG (Broadband Remote Access Server), так же как альтернатива PPPoE в DSL/FTTH-сетях. Достоинства и недостатки протокола L2TP указаны в таблице 2.

Таблица 1

Достоинства и недостатки протокола PPTP

Преимущества	Недостатки
Высокая скорость соединения (минимальные накладные расходы на шифрование)	Критическая уязвимость протоколов аутентификации (MS-CHAPv2 взламывается словарными атаками)
Простота настройки и встроенная поддержка в устаревших версиях ОС	Использование ненадежного шифра RC4 с возможностью атак подмены битов
Минимальные требования к вычислительным ресурсам	Проблемы с прохождением через NAT и МЭ (требуется поддержка PPTP Passthrough)

Таблица 2

Достоинства и недостатки протокола L2TP

Преимущества	Недостатки
Высокий уровень безопасности при использовании с IPSec	Замедление соединения из-за двойной инкапсуляции
Широкая поддержка в ОС и оборудовании	Использование фиксированных UDP-портов (500, 1701, 4500), что позволяет блокировать протокол с помощью МЭ
Возможность туннелирования без шифрования (удобно для провайдерских сценариев CGNAT и DPI)	Потенциальные сложности при работе через NAT (требуется поддержка NAT-T)

Второй этап. Период IPsec (Internet Protocol Security). Протокол IPSec стал де-факто стандартом для организации безопасных туннелей «сеть-сеть» на сетевом (L3) уровне. Он обеспечивает аутентификацию, целостность и конфиденциальность данных, описан в информационном документе RFC 6071 [6]. Возможные режимы работы — Tunnel и Transport, используемые протоколы — AH и ESP, а также применение протокола IKE (Internet Key Exchange) для управления ключами сделали его надежным, но относительно сложным в конфигурации решением. Решение IPSec представляет собой не отдельный протокол, а комплект протоколов для обеспечения безопасности на сетевом уровне модели OSI. Изначально оно разрабатывалось как обязательный компонент протокола IPv6. Решение обеспечивает три ключевые функции: аутентификацию, целостность и конфиденциальность передаваемых данных. Архитектура решения представлена протоколами первого уровня (защита данных) — AH (Authentication Header) — протокол заголовка аутентификации, он обеспечивает аутентификацию отправителя и целостность данных, но не предоставляет шифрования (данные передаются открыто). Имеются известные проблемы при работе через механизм NAT, так как протокол защищает неизменяемость IP-заголовка. Далее ESP (Encapsulating Security Payload) — протокол инкапсулированной защищенной нагрузки. Он обеспечивает аутентификацию, целостность и конфиденциальность. Может использоваться как с шифрованием, так и без него, но алгоритмы конфиденциальности применяются обязательно. Протокол поддерживает защиту от атак воспроизведения (replay attacks) через порядковые номера. Возможны два режима работы: во-первых, транспортный режим: защищается только полезная нагрузка IP-пакета, исходный заголовок сохраняется. Он используется для сквозных соединений «end-to-end». Во-вторых, поддерживается туннельный режим — защищается весь IP-пакет целиком, который инкапсулируется в новый пакет с новым заголовком. Этот режим применяется для соединений «шлюз-шлюз» или «клиент-шлюз».

Также имеются компоненты управления — во-первых, IKE (Internet Key Exchange) — протокол обмена ключами, функционирующий на UDP-порту 500. Обеспечивает согласование алгоритмов безопасности, генерацию и распределение ключей; во-вторых — SA (Security Association) — ассоциация безопасности, содержащая параметры защищенного соединения (алгоритмы, ключи, время жизни); в-третьих, SPD (Security Policy Database) — база данных политик безопасности, определяющая, какие пакеты требуют защиты и каким образом.

Рассматриваемое решение поддерживает и механизмы аутентификации — такие как PSK (Pre-Shared Key) (предварительный обмен симметричными ключами — обеспечивает простоту настройки, высокую скорость, однако существует риск компрометации ключа и ограничения масштабирования) и подход на основе цифровых сертификатов (предполагается использование инфраструктуры открытых ключей — Public Key Infrastructure (PKI) и центров сертификации). Последний подход обеспечивает высокую безопасность и масштабируемость при большей сложности настройки и более высоких затратах на инфраструктуру. Достоинства и недостатки протокола IPSec указаны в таблице 3.

Таблица 3

Достоинства и недостатки протокола IPSec

Преимущества	Недостатки
Высокий уровень безопасности (поддержка AES, 3DES)	Сложность конфигурации и управления
Гибкость (различные режимы и алгоритмы)	Совместимость с NAT требует дополнительных механизмов (NAT-T)
Широкая поддержка в оборудовании и ОС	Накладные расходы на установку соединения

Третий этап. Протоколы SSL/TLS VPN. Появление OpenVPN [7] и подобных гибридных решений, работающих на уровнях с канального по сессионный (L2-L5), упростило создание туннелей «сеть-пользователь». Клиентское программное обеспечение (ПО) часто представляло собой простой исполняемый файл. Протоколы SSL/TLS (Secure Sockets Layer / Transport Layer Security) [8, 9] — криптографические протоколы, обеспечивающие безопасную связь между клиентом и сервером на транспортном уровне (выше сетевого, но ниже прикладного). Наиболее распространенное применение — защита вебтрафика в протоколе HTTPS, а также организация VPN-соединений (например, OpenVPN). TLS является преемником SSL. SSL признан устаревшим и небезопасным (последняя версия SSL — 3.0). Использование устаревших версий TLS (1.0, 1.1) на практике также не рекомендуется. Актуальными версиями являются TLS 1.2 и TLS 1.3.

Этапы установления соединения (рукопожатие или handshake) включают следующие шаги. Сначала клиент запрашивает доступ к защищенному ресурсу. Затем сервер отвечает отправкой своего сертификата, содержащего открытый ключ. После этого клиент проверяет действительность сертификата (через доверенный центр сертификации). Клиент генерирует симметричный сеансовый ключ и шифрует его открытым ключом сервера. Сервер расшифровывает сеансовый ключ своим закрытым ключом. Обе стороны используют симметричный ключ для шифрования всего последующего трафика.

В процессе использования протоколов поддерживается асимметричное шифрование: используется пара открытый/закрытый ключ для аутентификации и безопасного обмена сеансовым ключом. Применяются алгоритмы RSA, ECC. Также может быть использовано симметричное шифрование — одноразовые сеансовые ключи для шифрования передаваемых данных. Используются алгоритмы AES, ChaCha2. Наиболее популярным решением де-факто является технология OpenVPN, которая использует SSL/TLS для организации VPN. Преимущества и недостатки решений VPN, основанных на протоколах SSL/TLS, показаны в таблице 4.

Таблица 4

Достоинства и недостатки решений VPN, основанных на протоколах SSL/TLS

Преимущества	Недостатки
Широкое распространение и стандартизация	Накладные расходы на установку соединения
Поддержка совершенной прямой секретности (Perfect Forward Secrecy) в современных реализациях	Зависимость от инфраструктуры открытых ключей (PKI) для серверных сертификатов

Рассмотренные протоколы представляют различные поколения развития технологий защищенных сетевых соединений. Протокол PPTP, исторически первый широко распространенный протокол, в настоящее время не рекомендуется к использованию из-за критических уязвимостей. Протокол L2TP в связке с IPSec обеспечивает приемлемый уровень защиты, однако уступает современным решениям в эффективности из-за двойной инкапсуляции. Протокол IPSec представляет собой комплексное решение для защиты на сетевом уровне, сохраняющее актуальность для построения корпоративных VPN. Протоколы SSL/TLS, особенно в реализации OpenVPN, получили широкое распространение благодаря универсальности и способности адаптироваться к различным сетевым условиям.

Информация, ключевым образом характеризующая имеющиеся особенности и различия между технологиями VPN, представлена в таблице 5.

Таблица 5

Сравнительная таблица протоколов VPN

Характеристика	PPTP	L2TP/IPsec	IPSec	SSL/TLS
Уровень OSI	Канальный (L2)	Канальный (L2)	Сетевой (L3)	Канальный/ сетевой/ транспортный/ сеансовый (L2-L5)
Шифрование	MPPE (RC4)	AES, 3DES (через IPsec)	AES, 3DES, DES	AES, ChaCha 2.0
Аутентификация	MS-CHAP, EAP	Сертификаты, PSK	Сертификаты, PSK	Сертификаты
Порты, протоколы	TCP 1723, GRE	UDP 500, 1701, 4500	UDP 500, ESP/AH	TCP 443 (HTTPS), UDP 1194, TCP 1194
Скорость	Высокая	Средняя	Высокая	Средняя
Безопасность	Крайне низкая	Высокая	Высокая	Высокая
Современный статус	Устаревший	Используется	Актуальный	Актуальный

Четвертый этап. Современные тенденции. В настоящее время акцент при создании решений VPN смещается на безопасность, удобство и централизованное управление. Ключевыми требованиями [10] стали:

- многофакторная аутентификация (MFA): обязательное использование второго фактора (TOTP, SMS, Push-уведомления, аппаратные токены) помимо пароля;
- адаптивный доступ (Zero Trust): проверка контекста (состояние устройства, геолокация) перед предоставлением доступа;
- упрощение инфраструктуры: конвергенция возможностей для топологий «сеть-сеть» и «сеть-пользователь» в рамках единого шлюза.

Для реализации защищенного маршрутизатора в рамках данной работы в качестве базовой L3 VPN технологии в ряде задач целесообразно выбирать протокол IPsec ввиду его зрелости, высокой производительности, стандартизации и широкой поддержки как в сетевом оборудовании, так и в ПО, а в ряде задач — протоколы, использующие TLS, ввиду их широкого распространения и стандартизации, а также поддержки «Совершенной прямой секретности».

II. Возможность реализации технологий маршрутизации и VPN на ОС ALSE. Системное ПО — ОС ASLE специально создана для работы с информацией, составляющей государственную тайну[1]. Ее ядро, подсистемы безопасности (мандатный контроль доступа, система регистрации, подсистема безопасности PARSEC) и пакетный фонд потенциально предоставляют надежную основу для построения сетевых шлюзов безопасности. Реализация VPN-функционала на данной ОС возможна и целесообразна по следующим причинам.

1. Наличие встроенных и репозиторных пакетов. В составе дистрибутива или из официальных репозиториев доступны все необходимые компоненты: strongSwan (реализация IPsec IKEv1/IKEv2), libreswan, xl2tpd, OpenVPN, freeRADIUS (для централизованной аутентификации).

2. Интеграция с подсистемой безопасности. Процессы VPN-демонов могут функционировать под контролем мандатной политики безопасности, что изолирует их от других компонентов системы и повышает общую устойчивость к компрометации.

3. Производительность сетевого стека. ОС оптимизирована для работы в высоконагруженных сетевых средах, поддерживает аппаратное ускорение шифрования (при наличии соответствующих процессорных инструкций или карт), что критично для VPN маршрутизатора.

4. Поддержка MFA. Интеграция с системами аутентификации, поддерживающими протоколы RADIUS или TACACS+, позволяет подключить внешние провайдеры MFA (например, на базе Time-based One-Time Password - TOTP) или развернуть собственный (например, privacyIDEA в связке с FreeRADIUS).

Таким образом, ALSE представляет собой не просто возможную, но и предпочтительную программную платформу для создания VPN маршрутизаторов и, в дальнейшем, сертифицированных решений класса NGFW.

Ниже рассмотрим возможные схемы применения встроенных программных средств ОС ALSE при реализации функционала защищенного маршрутизатора. Архитектура решения строится на комбинации проверенных Open Source инструментов, интегрированных под управлением ОС ALSE.

[1] Astra Linux Special Edition. Сертификация // Справочный центр Astra Linux : [сайт]. — URL: https://wiki.astralinux.ru/ (дата обращения: 19.03.2026).

Предлагаемая базовая схема реализации состоит из четырех пунктов.

Пункт 1. Ядро и сетевая подсистема — используется встроенный сетевой стек ядра Linux с включенными функциями netfilter/iptables (или nftables) для фильтрации и трансляции адресов (NAT), а также политик маршрутизации и приоритезации трафика;

Пункт 2. Решение L3 VPN (IPsec) на базе strongSwan — пакет strongSwan выступает в роли демона IKE, отвечающего за установление и поддержание защищенных IPsec-туннелей.

Пункт 3. Подсистема многофакторной аутентификации (MFA) — в качестве центра аутентификации разворачивается сервер FreeRADIUS. Служба StrongSwan настраивается на использование аутентификации через RADIUS (плагин eap-radius). Служба FreeRADIUS интегрируется с бэкендом для проверки первого фактора (например, LDAP/Active Directory или локальная база пользователей) и вторым фактором. Для второго фактора может использоваться модуль, поддерживающий TOTP (например, google-authenticator или privacyIDEA). Пользователь при подключении вводит одноразовый код из мобильного приложения (Google Authenticator, Яндекс.Ключ и т. д.) вместе с паролем.

Пункт 4. Управление и мониторинг — для конфигурации strongSwan и iptables (nftables) могут быть разработаны скрипты или веб-интерфейс на базе, например, webmin или собственной панели управления. Для мониторинга состояния туннелей и системы используется штатный инструментарий (ipsec status, systemctl) и системы логирования (rsyslog), интегрированные с ОС.

Для сценария «сеть-сеть» настраивается туннель между двумя шлюзами strongSwan. Аутентификация производится на основе предварительных общих ключей (PSK) или сертификатов X.509. После установления туннеля трафик между защищаемыми сетями маршрутизируется через него.

Для сценария «сеть-пользователь» настраивается пакет StrongSwan в роли сервера IKEv2 с поддержкой EAP (Extensible Authentication Protocol). Это позволяет использовать для аутентификации не только сертификаты, но и логин/пароль.

Предлагаемая возможная схема взаимодействия для сценария «сеть-пользователь» содержит пункты, приведенные ниже.

1. Удаленный пользователь инициирует подключение IKEv2 к шлюзу на ОС ALSE.

2. Служба StrongSwan запрашивает учетные данные, используя метод EAP-MSCHAPv2 или EAP-TLS.

3. Учетные данные (логин/пароль + OTP-код) пересылаются на сервер FreeRADIUS.

4. FreeRADIUS проверяет логин/пароль в LDAP, а OTP-код — через TOTP-модуль.

5. При успешной проверке обоих факторов FreeRADIUS возвращает strongSwan положительный ответ.

6. StrongSwan завершает фазу аутентификации IKE и устанавливает IPsec SA (Security Association).

7. Клиенту назначается внутренний IP-адрес, и его трафик, направленный в защищенную сеть, проходит через зашифрованный туннель, подвергаясь проверке правилами iptables (nftables).

III. Реализация маршрутизатора с поддержкой технологий L3 VPN с двухфакторной аутентификацией, объединением сценариев взаимодействия «сеть-сеть» и «сеть-пользователь» на основе служб OpenVPN, samba и nftables. Ниже приведем конкретный пример методики создания и настройки маршрутизатора в соответствии с общей целью работы в контексте решения частной прикладной задачи.

Частная прикладная задача заключается в необходимости маршрутизации сетевого трафика и получения доступа к удаленным сетевым устройствам, работающим в сети Интернет, каналы связи с которыми не предполагают наличия статических IP адресов на внешних интерфейсах граничных маршрутизаторов удаленных сетевых сегментов (рис. 1). Данная задача является типовой, она сопровождает часто встречающиеся на практике сценарии доступа к IP-камерам, видеорегистраторам, счетчикам различных ресурсов (воды, электроэнергии и др.), системам «Умный дом», в тех случаях, когда для связи с ними не используются специализированные облачные сервисы.

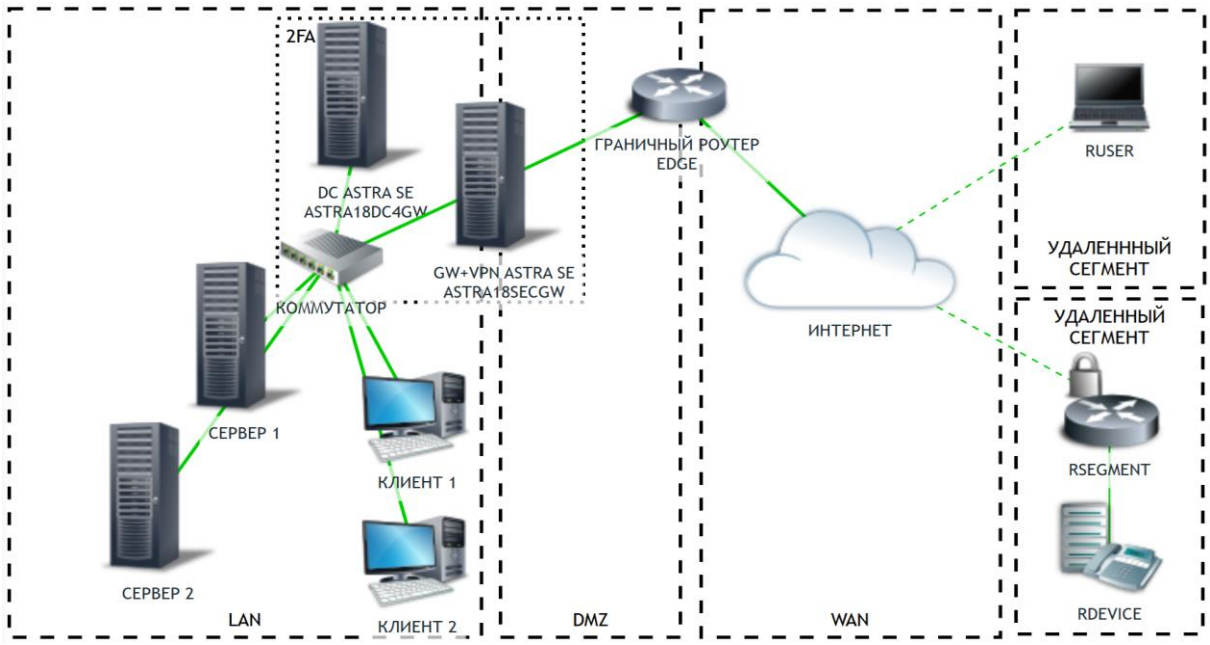


Рис. 1. К пояснению решения прикладной задачи

Предполагается следующий вариант работы: серверная площадка, на которой расположен центральный маршрутизатор с ОС ALSE, имеет статический, «общественный» или «белый» IP адрес. Удаленные сетевые сегменты могут находиться за NAT интернет-провайдеров (например, при работе через сети пакетной передачи данных сотовых операторов связи — 3G/4G/5G). В таких же условиях (без статических IP адресов, за NAT) могут находиться рабочие места пользователей информационных систем, с которых требуется получать доступ к устройствам в удаленных сетевых сегментах.

Специфика прикладной задачи определяется так, что необходимо обеспечить доступ к сетевым устройствам по их «частным» IP адресам — то есть тем IP, которые устройства имеют в своих локальных сетях. Адреса устройств показаны в табл. 6. В дополнение к напрямую требующемуся по условию задачи функционалу еще необходимо обеспечить возможность работы устройств, находящихся в локальной сети центрального

сегмента LAN в сети Интернет через NAT, с фильтрацией, приоритезацией трафика и т. п. традиционными задачами сетевого управления и сетевой безопасности.

Таблица 6

Адреса устройств в прикладной задаче

№ п/п	Хост	Интерфейс	IPv4 адрес	Сетевой префикс	Шлюз по умолчанию, DNS сервер	Примечание
1.	EDGE	WAN	IP_0	n/a	n/a	Граничный NAT- роутер центрального сегмента
		LAN	192.168.29.1	/24	нет	
2.	ASTRA18SECGW	ens18	192.168.29.25	/24	192.168.29.1	Основной роутер с ОС ALSE
		ens 19	10.236.72.1	/24	нет	
		tun0	10.36.22.1	/24	нет	
		tun1	10.159.8.1	/24	нет	
3.	ASTRA18DC4GW	ens18	10.236.72.2	/24	10.236.72.1	Контроллер домена с ОС ALSE
4.	RSEGMENT	WAN	n/a	n/a	n/a	Граничный роутер удаленного сегмента
		LAN	192.168.48.254	/24	нет	
		tun1	10.36.22.33	/30	10.36.22.34; 10.36.22.1	
5.	RDEVICE	LAN	192.168.48.253	/24	192.168.48.254	Устройство в удаленном сегменте
6.	RUSER	LAN	n/a	n/a	n/a	Удаленный пользователь
		tun1	10.159.8.21	/30	10.159.8.22; 10.159.8.1	

Решение задачи обеспечивается развертыванием и настройкой на центральном маршрутизаторе с ОС ALSE двух серверных служб OpenVPN. Одна из этих служб обеспечивает функционирование сегментов «сеть-сеть» (для связи удаленных сегментов с устройствами с сегментом центрального маршрутизатора). Эта служба VPN работает с первым набором параметров безопасности, здесь используется однофакторная аутентификация по сертификатам и ключам, сгенерированным с помощью имеющейся инфраструктуры открытых ключей (пакет EasyRSA). Вторая служба обеспечивает работу сегментов «сеть-пользователь» (для связи информационных систем пользователей с сегментом центрального маршрутизатора), здесь используется второй (уникальный) комплект сертификатов и ключей, сгенерированный аналогичным образом. Кроме того, данная служба настроена на использование второго фактора аутентификации — логина и пароля, для чего в центральном локальном сегменте развернут контроллер домена на базе все той же ОС ALSE и роли sambadc, а в конфигурационный файл второй службы VPN добавлен вызов внешнего shell-скрипта для проверки логина и пароля (для реализации 2FA) по протоколу LDAP на контроллере домена sambadc. Данный скрипт был дополнительно разработан авторами, т. к. в реализации ОС ALSE отсутствует подключаемый модуль аутентификации (PAM — Pluggable Authentication Module) openvpn-auth-ldap, который имеется в большинстве представителей семейств «обычных» ОС Linux. В терминах сетей на основе доменов защищенный шлюз-маршрутизатор настроен клиентом домена, который поддерживается другой виртуальной машиной с ролью контроллера (сервера)

домена. Вторая серверная служба VPN настроена с усиленными параметрами безопасности: она дополнительно использует статический стартовый ключ (для защиты от DDoS) и более сильные алгоритмы аутентификации и шифрования. Связь информационных систем пользователей с удаленными устройствами осуществляется при взаимодействии двух указанных серверных служб VPN и службы nftables, которая отвечает за маршрутизацию в ядре ОС ALSE. Совместное использование указанных служб и сервисов согласуется с предложенной выше базовой схемой реализации рассматриваемого функционала, состоящего из четырех пунктов.

Руководство администратора ОС ALSE [11] предписывает развертывание ролей сервера и клиента службы sambadc (контроллер и член домена samba) на «чистые», свободные от других установленных ролей и служб, операционные системы. Данная рекомендация определяет начальные этапы методики создания защищенного маршрутизатора, создание которого, в целом, включает следующие укрупненные шаги.

1. Установка двух ОС ALSE на узлы ASTRA18SECGW (защищенный маршрутизатор) и ASTRA18DC4GW (контроллер домена для второго фактора аутентификации).
2. Отключение на время интеграции в домен на узлах ASTRA18DC4GW и ASTRA18SECGW службы ufw — встроенного персонального межсетевого экрана.
3. Проверка сетевой связности, задание адресов и имен на хостах, установка роли контроллера домена на узел ASTRA18DC4GW с помощью консольной команды *apt install astra-sambadc*. Инициализация домена с помощью консольной команды *astra-sambadc-d agw.net–px*, где agw.net — имя домена.
4. Установка на узел ASTRA18SECGW графического инструмента, позволяющего подключить узел-маршрутизатор к домену в качестве клиента с помощью команды *apt install fly-admin-ad-sssd-client*.
5. Ввод узла ASTRA18SECGW в домен через графический инструмент, с обязательным указанием IP адреса внутреннего интерфейса маршрутизатора в качестве IP адреса клиента. Результат выполнения показан на рис. 2.

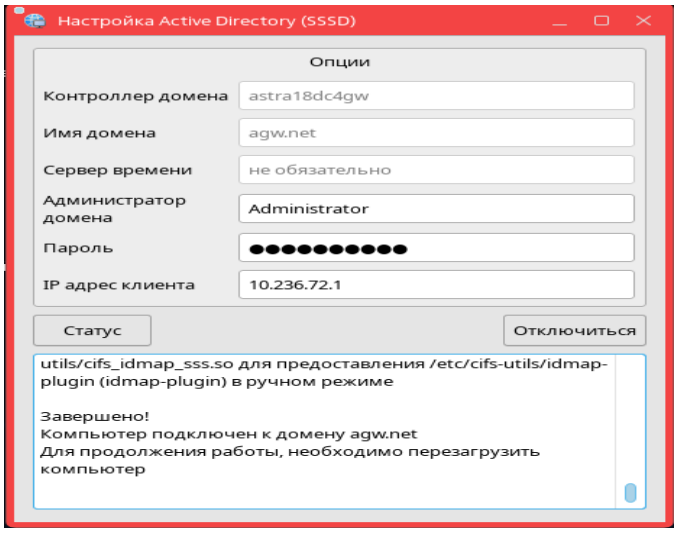


Рис. 2. Результат ввода в домен узла-маршрутизатора

6. Развертывание и настройка на ASTRA18SECGW службы маршрутизации nftables. Настройка службы nftables [12], настройка ее автозапуска, проверка правил получившегося транзитного МЭ. При настройке МЭ необходимо учесть, что данный узел является членом домена, взаимодействует по внутренней сети с контроллером домена по

протоколу LDAP. Необходимо, также, предусмотреть транзитную маршрутизацию между удаленными пользователями и удаленными устройствами. Таблица маршрутизации центрального роутера после всех настроек показана на рис. 3.

7. Установка и настройка на узле ASTRA18SECGW двух сервисов OpenVPN, включающая подготовку двух экземпляров инфраструктуры открытых ключей (PKI), генерацию серверных и клиентских сертификатов, подготовку конфигурационных файлов, подключение к одной из служб скрипта проверки второго фактора аутентификации, запуск служб VPN, и настройка их автоматического запуска. Окончательный перечень сетевых интерфейсов маршрутизатора показан на рис. 4.

```
root@astra18secgw:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.29.1    0.0.0.0         UG    100    0        0 ens18
10.36.22.0      10.36.22.2      255.255.255.0   UG    0      0        0 tun0
10.36.22.2      0.0.0.0         255.255.255.255 UH    0      0        0 tun0
10.159.8.0      10.159.8.2      255.255.252.0   UG    0      0        0 tun1
10.159.8.2      0.0.0.0         255.255.255.255 UH    0      0        0 tun1
10.236.72.0     0.0.0.0         255.255.255.0   U     101    0        0 ens19
192.168.29.0    0.0.0.0         255.255.255.0   U     100    0        0 ens18
192.168.48.0    10.36.22.2      255.255.255.0   UG    0      0        0 tun0
```

Рис. 3. Таблица маршрутизации узла ASTRA18SECGW

```
root@astra18secgw:~# ifconfig -a
ens18: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.29.25  netmask 255.255.255.0  broadcast 192.168.29.255
        inet6 fe80::40ba:62e7:3360:8d3f  prefixlen 64  scopeid 0x20<link>
        ether bc:24:11:ea:64:51  txqueuelen 1000  (Ethernet)
        RX packets 802081  bytes 239539272 (228.4 MiB)
        RX errors 0  dropped 482887  overruns 0  frame 0
        TX packets 255560  bytes 201914366 (192.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens19: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.236.72.1  netmask 255.255.255.0  broadcast 10.236.72.255
        inet6 fe80::3c32:8d54:e063:7d10  prefixlen 64  scopeid 0x20<link>
        ether bc:24:11:43:83:97  txqueuelen 1000  (Ethernet)
        RX packets 110905  bytes 24031520 (22.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 143875  bytes 24204332 (23.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 3960 (3.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 3960 (3.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.36.22.1  netmask 255.255.255.255  destination 10.36.22.2
        inet6 fe80::1987:cbb9:13aa:d341  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 18555  bytes 21598780 (20.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9950  bytes 412811 (403.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun1: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.159.8.1  netmask 255.255.255.255  destination 10.159.8.2
        inet6 fe80::1e01:82aa:9e31:3dd5  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 10311  bytes 456797 (446.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18797  bytes 21650767 (20.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Рис. 4. Перечень интерфейсов ASTRA18SECGW

8. Запуск персонального межсетевого экрана ufw на узле ASTRA18DC4GW, открытие на нем портов для обеспечения возможности взаимодействия узлов

ASTRA18SECGW и ASTRA18DC4GW в ролях sssd+LDAP клиент и sambadc+LDAP сервер соответственно.

После завершения настройки центрального маршрутизатора с ОС ALSE необходимо настроить граничные маршрутизаторы удаленных устройств и программы-клиенты удаленных пользователей информационных систем, что производится без существенных особенностей.

IV. Обсуждение результатов. Предложенная в п. III методика использована для реализации тестовой схемы доступа с мобильного ноутбука с ОС Windows 11 с программным клиентом OpenVPN и прикладным программным обеспечением ODM (Synesis free GNU software) к удаленной IP видеокамере CORUM GS-410-IP. Видеокамера подключалась к маршрутизатору Mikrotik модели RB962UiGS-5HacT2HnT с встроенным клиентом OpenVPN и 3G/4G модемом Huawei модели E3372h-153 (для доступа в интернет). При создании маршрутизатора и контроллера домена использовался установочный носитель с образом ОС ALSA 1.8 — installation-1.8.1.6-27.06.2024_14.12.iso, предоставленный компанией-разработчиком ОС по запросу (для тестирования). Внешние репозитории при работе с ОС ALSE не использовались. Система устанавливалась на две двухядерные виртуальные машины с объемом оперативной памяти 4 Гб, виртуальными дисками объемом 64 Гб. При установке ОС выбирался режим усиленной безопасности — «Воронеж». Сетевые адреса устройств при этом обеспечивались в соответствии с таблицей 6. Схема показала устойчивою работу в течение длительного периода.

В процессе практической реализации решения необходимо было учесть ряд особенностей. Во-первых, виртуальные tun-интефейсы после старта служб VPN не появлялись. Проблема была решена заданием явного разрешения на создание сетевых интерфейсов в файле конфигурации подсистемы PARSEC для служб VPN. Во-вторых, поскольку серверных служб VPN использовалось две, от встроенного в ОС ALSE визуального интерфейса fly-admin-openvpn-server пришлось отказаться (при его использовании предполагается, что в системе существует только один «серверный» сервис VPN). Вместо этого работа с сервисами VPN велась с помощью консольных команд вида *systemctl restart openvpn-server@server4nets.service* и т. п., по этой же причине с помощью консольных команд велась подготовка ключей, сертификатов и конфигурационных файлов для этих сервисов. В-третьих, после добавления в функционал функций VPN сервера перестала запускаться служба nftables. Разбор журналов служб показал, что причиной является попытка применения политики маршрутизации для «несуществующих» виртуальных сетевых интерфейсов по причине того, что ядро маршрутизации в операционной системе стартует быстрее служб VPN и быстрее их активации. Этот вопрос был решен за счет создания shell-скрипта, проверяющего готовность виртуальных сетевых интерфейсов сервисов VPN и последующего повторного запуска службы nftables. На основе указанного скрипта была реализована служба под управлением systemd, обеспечивающего постоянную работу данного функционала. И, в-четвертых, как уже упоминалось, в имеющейся реализации ОС ALSE отсутствовал подключаемый модуль аутентификации PAM openvpn-auth-ldap, из за чего был разработан shell-скрипт с аналогичным функционалом, использующий вызов утилиты ldapsearch для проверки логина и пароля.

Заключение. Проведенное исследование демонстрирует техническую осуществимость развертывания защищенного маршрутизатора-концентратора сетевых потоков, включая поддержку L3 VPN и многофакторной аутентификации, на базе ОС ALSE. Стандартный пакетный фонд и сетевые возможности ОС в полной мере позволяют развернуть решение, объединяющее strongSwan (IPsec), OpenVPN, FreeRADIUS (MFA), sambadc,

netfilter и т. д. в единый защищенный комплекс. Предложенная архитектура эффективно покрывает оба ключевых сценария использования каналов VPN, во-первых, «сеть-сеть» и, во-вторых, «сеть-пользователь». Использование сертифицированной ОС, работающей под контролем мандатной системы защиты, способно обеспечить необходимый уровень доверия к платформе. Внедрение MFA значительно повышает устойчивость к компрометации учетных данных по сравнению с простой парольной аутентификацией или PSK. Разрабатываемый подход может составить основу для дальнейшего развития в сторону полноценного отечественного NGFW-решения — добавления DPI/IPS (на базе IPS SNORT/Suricata или собственных разработок), системы контроля приложений, централизованного управления кластером шлюзов и облачных сервисов аутентификации.

ЛИТЕРАТУРА

1. О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года : указ Президента РФ от 7 мая 2024 г. № 309 // Собрание законодательства Российской Федерации. — 2024. — № 20. — Ст. 2584.

2. Ермаков Г. С., Пантелеев Н. Н. Организация защиты информации с помощью NTA, NGFW и WAF в контексте защиты веб-приложений // Наукосфера. — 2024. — № 4(2). — С. 22—26.

3. Косинская А. Р., Демкин Д. А. Межсетевые экраны нового поколения (NGFW): обзор, технологии, представители // Вестник науки. — 2024. — Т. 1. — № 7(76). — С. 516—521.

4. Point-to-Point Tunneling Protocol (PPTP) / K. Hamzeh, G. Pall, W. Verthein [et al.] // IETF. RFC 2637. — 1999. — Jul. — URL: https://doi.org/10.17487/RFC2637.

5. Layer Two Tunneling Protocol "L2TP" / W. Townsley, A. Valencia, A. Rubens [et al.] // IETF. RFC 2661 — 1999.— Aug. — URL: https://doi.org/10.17487/RFC2661.

6. Frankel S., Krishnan S. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap // IETF. Informational. RFC 6071. — 2011. — Feb. — 63 p.

7. Skendzic A., Kovacic B. Open source system OpenVPN in a function of Virtual Private Network // IOP Conference Series : Materials Science and Engineering. — 2017. — Vol. 200. — Article 012065. — DOI 10.1088/1757-899X/200/1/012065.

8. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3 : RFC 8446. — IETF, 2018. — 160 p. — URL: https://tools.ietf.org/html/rfc8446 (дата обращения: 19.03.2026).

9. Sheffer Y., Holz R., Saint-Andre P. Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) : RFC 7525. — IETF, 2015. — 41 p. — URL: https://tools.ietf.org/html/rfc7525 (дата обращения: 19.03.2026).

10. Кадер М. (2025). Эволюция защищенного доступа в корпоративных сетях // IT Week. — 2025. — 24 июля. — URL: https://www.itweek.ru/security/article/detail.php?ID=232628.

11. Руководство администратора. Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) // Официальный сайт Группы «Астра». — URL: https://wiki.astralinux.ru/pages/viewpage.action?pageId=302043140 (дата обращения: 19.03.2026).

12. Власов П. Простой шлюз в сеть Интернет на nftables в ОС Astra Linux Special Edition // Habr : [сайт]. — 2024. — 14 ноября. — URL: https://habr.com/ru/companies/ astralinux/ articles/858390/ (дата обращения: 19.03.2026).

REFERENCES

1. O natsional′nykh tselyakh razvitiya Rossijskoj Federatsii na period do 2030 goda i na perspektivu do 2036 goda : ukaz Prezidenta RF ot 7 maya 2024 g. № 309 // Sobranie zakonodatel′stva Rossijskoj Federatsii. — 2024. — № 20. — St. 2584.

2. Ermakov G. S., Panteleev N. N. Organizatsiya zashchity informatsii s pomoshch′yu NTA, NGFW i WAF v kontekste zashchity veb-prilozhenij // Naukosfera. — 2024. — № 4(2). — S. 22—26.

3. Kosinskaya A. R., Demkin D. A. Mezhsetevye ekrany novogo pokoleniya (NGFW): obzor, tekhnologii, predstaviteli // Vestnik nauki. — 2024. — T. 1. — № 7(76). — S. 516—521.

4. Point-to-Point Tunneling Protocol (PPTP) / K. Hamzeh, G. Pall, W. Verthein [et al.] // IETF. RFC 2637. — 1999. — Jul. — URL: https://doi.org/10.17487/RFC2637.

5. Layer Two Tunneling Protocol \"L2TP\" / W. Townsley, A. Valencia, A. Rubens [et al.] // IETF. RFC 2661 — 1999.— Aug. — URL: https://doi.org/10.17487/RFC2661.

6. Frankel S., Krishnan S. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap // IETF. Informational. RFC 6071. — 2011. — Feb. — 63 p.

7. Skendzic A., Kovacic B. Open source system OpenVPN in a function of Virtual Private Network // IOP Conference Series : Materials Science and Engineering. — 2017. — Vol. 200. — Article 012065. — DOI 10.1088/1757-899X/200/1/012065.

8. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3 : RFC 8446. — IETF, 2018. — 160 p. — URL: https://tools.ietf.org/html/rfc8446 (data obrashcheniya: 19.03.2026).

9. Sheffer Y., Holz R., Saint-Andre P. Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) : RFC 7525. — IETF, 2015. — 41 p. — URL: https://tools.ietf.org/html/rfc7525 (data obrashcheniya: 19.03.2026).

10. Kader M. (2025). Evolyutsiya zashchishchennogo dostupa v korporativnykh setyakh // IT Week. — 2025. — 24 iyulya. — URL: https://www.itweek.ru/security/article/detail.php?ID=232628.

11. Rukovodstvo administratora. Astra Linux Special Edition RUSB.10015-01 (ocherednoe obnovlenie 1.8) // Ofitsial′nyj sajt Gruppy «Astra». — URL: https://wiki.astralinux.ru/pages/viewpage.action?pageId=302043140 (data obrashcheniya: 19.03.2026).

12. Vlasov P. Prostoj shlyuz v set′ Internet na nftables v OS Astra Linux Special Edition // Habr : [sajt]. — 2024. — 14 noyabrya. — URL: https://habr.com/ru/companies/ astralinux/ articles/858390/ (data obrashcheniya: 19.03.2026).

СВЕДЕНИЯ ОБ АВТОРАХ

Телков Александр Юрьевич. Заместитель начальника кафедры компьютерной безопасности и технической экспертизы. Кандидат физико-математических наук, доцент.

Воронежский институт МВД России.

E-mail: telkov@phys.vsu.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Жуков Михаил Михайлович. Начальник кафедры компьютерной безопасности и технической экспертизы. Кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: mzhukov25@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Полухин Дмитрий Игоревич. Старший преподаватель кафедры компьютерной безопасности и технической экспертизы.
Воронежский институт МВД России.
E-mail: dipoluhin@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Telkov Alexander Yurievich. Deputy head of the chair of Computer Security and Technical Expertise. Candidate of Physical and Mathematical Sciences, Associate Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: telkov@phys.vsu.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Zhukov Mikhail Mikhailovich. Head of the chair of Computer Security and Technical Expertise. Candidate of Technical Sciences, Associate Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: mzhukov25@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Polukhin Dmitry Igorevich. Senior lecturer of the chair of Computer Security and Technical Expertise.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: dipoluhin@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: Astra Linux SE; IPsec VPN; L3 VPN; PPTP; L2TP; Open VPN; PAM; 2FA; двухфакторная аутентификация; маршрутизатор; удаленный доступ; NGFW.

Key words: Astra Linux SE; IPsec VPN; L3 VPN; PPTP; L2TP; Open VPN; PAM; 2FA; two-factor authentication; router; remote access; NGFW.

УДК 004.056.5

А. А. Терентьев, *кандидат технических наук*
В. Я. Пославская

АЛГОРИТМ РАСЧЕТА ИНДЕКСА ЭФФЕКТИВНОСТИ ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКОГО ЦЕНТРА ОРГАНОВ ВНУТРЕННИХ ДЕЛ

ALGORITHM FOR CALCULATING THE EFFICIENCY INDEX OF THE EXPERT CRIMINALISTIC CENTER OF THE INTERNAL AFFAIRS BODIES

В статье рассматривается проблема оценки эффективности функционирования экспертно-криминалистических центров органов внутренних дел как организационно-технических систем. В работе представлен разработанный алгоритм расчета индекса эффективности, включающий в себя расчет трех показателей: время выполнения экспертиз, качество экспертных исследований и ресурсоемкость. Предложена методика их нормирования и агрегирования в единый индекс эффективности с учетом весовых коэффициентов.

The article discusses the problem of assessing the effectiveness of the functioning of forensic centers of internal affairs bodies as organizational and technical systems. The paper presents a developed algorithm for calculating the effectiveness index, which includes the calculation of three indicators: the time required for examinations, the quality of expert research, and the resource intensity. A methodology for standardizing and aggregating these indicators into a single effectiveness index is proposed, taking into account weight coefficients.

Введение. В современных условиях развития правоохранительной системы особую актуальность приобретает совершенствование механизмов оценки эффективности деятельности экспертно-криминалистических центров (ЭКЦ) органов внутренних дел. Актуальность исследования обусловлена растущими объемами экспертно-криминалистической деятельности и необходимостью оптимизации процессов принятия управленческих решений на основе объективных показателей эффективности.

Экспертно-криминалистический центр органов внутренних дел представляет собой сложный комплекс, чья деятельность направлена на решение задач судебной экспертизы в условиях постоянно растущих объемов информации [1].

Основными функциями таких центров являются [2, 3]:

1. Организационно-методическое обеспечение;
2. Осуществление экспертно-криминалистической деятельности;
3. Научно-методическое обеспечение производства экспертиз;
4. Организация экспертно-криминалистических учетов;
5. Организация метрологического обеспечения;
6. Апробация экспертных методик и технических средств.

Ранее в работе [4] уже было выдвинуто предположение, что ЭКЦ можно считать, организационно-технической системой (ОТС). На деятельность любой ОТС всегда оказывает влияние несколько показателей эффективности одновременно, ЭКЦ в данном

случае не является исключением. Для оценки эффективности функционирования ЭКЦ как организационно-технических систем требуется определить показатели, учитывающие специфику их деятельности и современные требования к качеству экспертного обслуживания.

Постановка задачи. Исследованию оценки эффективности функционирования организационно-технических систем посвящено достаточно много научных трудов [5—8]. Статья [5] посвящена проблеме оценки эффективности сложных информационных систем (ИС), что особенно актуально в условиях цифровизации государственного управления. Автор обоснованно указывает на необходимость развития методологии системного анализа и моделирования. В работе предложена теоретическая база оценки эффективности сложных ИС, сформулированы аксиомы и принципы оценки эффективности и разработан подход к моделированию адаптационных процессов. При этом в представленном исследовании отсутствуют конкретные алгоритмы расчета показателей эффективности системы.

Исследование [6] посвящено методологии оценки эффективности развития социально-экономических систем. Актуальность темы подтверждается растущей потребностью в комплексных подходах к оценке развития экономических объектов в условиях динамичной среды. В качестве научной новизны анализируемого исследования выступает оригинальный методологический подход к комплексной оценке эффективности, систематизировано направление оценивания: результативность, оптимальность, экономичность, а также обоснована необходимость сравнения с эталонными моделями. Несмотря на это, в статье имеются определенные ограничения, такие как отсутствие конкретных примеров расчета показателей эффективности, а также практическая апробация предложенной методологии оценки эффективности систем.

Работа [7] посвящена проблеме оценки эффективности функционирования сложных технических систем, что соответствует современным тенденциям развития технического сервиса и диагностики. Актуальность темы подтверждается растущей потребностью в оптимизации процессов технического обслуживания. В данной работе авторы предлагают оригинальный метод оценки с учетом особенностей связей элементов системы, разработан математический аппарат для характеристики интенсивности изменения параметров, систематизированы подходы к оценке параметрической надежности. При этом при анализе данного исследования можно выделить следующие ограничения: отсутствие конкретных примеров расчета показателей эффективности, наличие недостаточной детализации предложенного алгоритма расчета оценки эффективности сложных систем. Выделенные ограничения не позволяют в полном объёме оценить предложенный алгоритм и дать практическую составляющую данной методике.

Существующие методики оценки не в полной мере отражают взаимосвязь между различными показателями эффективности и не позволяют получить целостную картину функционирования экспертно-криминалистических центров органов внутренних дел. Таким образом, возникает задача определения показателей эффективности и разработки алгоритма расчета индекса эффективности экспертно-криминалистического центра как организационно-технической системы.

Решение задачи. Для решения поставленной задачи требуется комплексное решение, состоящее в применении методов математического моделирования. На первом этапе решения задачи требуется произвести моделирование системы при помощи теории графов [9]. Экспертно-криминалистический центр как целостная система состоит из подсистем, каждая из которых выполняет свои функции [10].

Таблица 1

Подсистемы ЭКЦ

№ п/п	Подсистема	Функции
1	Научно-методическая	Разработка и внедрение новых методов и методик
2	Технико-криминалистическая	Идентификация объектов, установление фактов и обстоятельств события преступления
3	Нормативно-правовая	Обеспечение правового регулирования деятельности ЭКЦ
4	Метрологическая	Обеспечение единства, точности и достоверности измерений, проводимых в ходе судебных экспертиз
5	Инженерно-эксплуатационная	Поддержание в работоспособном состоянии оборудования

Систему можно представить в виде множества $S = \{s_1, \dots, s_i\}$, где s_i — некоторые элементы, называемые агентами, которые выполняют свои функции для конкретной подсистемы, выступают в роли подсистем. Агенты в свою очередь также могут быть подразделены еще на несколько подсистем. Например, подсистема S_1 может подразделяться следующим образом:

$(s_{1i}, \dots, s_{1n})$ — эксплуатация специального оборудования, лабораторная база, материально-техническое снабжение.

В последующем $s_i = \{s_{ij}, \dots, s_{ij}\}$, где i соответствует номеру подсистемы, а j соответствует номеру элемента (агента).

Сами подсистемы будут выступать центрами и являться промежуточными в самой системе (рис. 1).

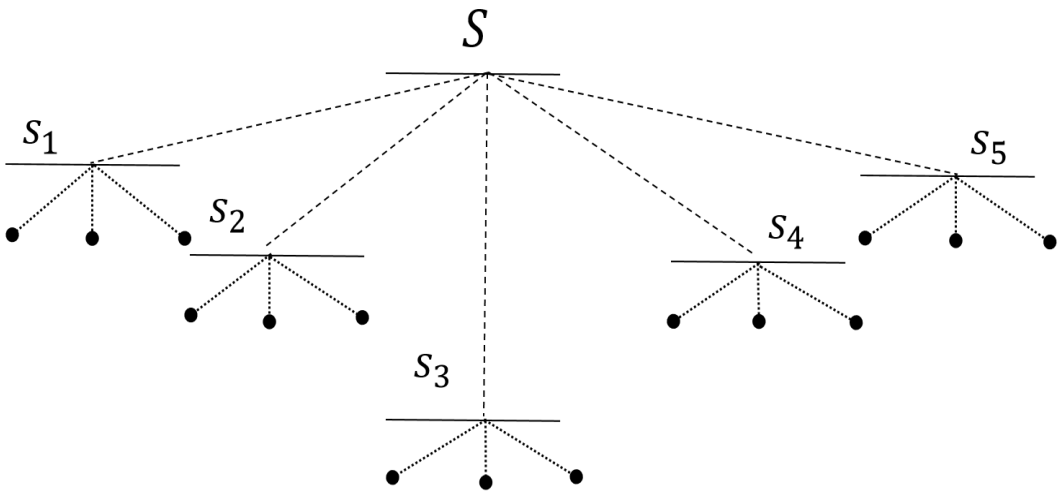


Рис. 1. Иерархическая структура организационно-технической системы на примере экспертно-криминалистического центра

Они представлены следующим образом:

s_1 — научно-методическая подсистема;

s_2 — технико-криминалистическая;

s_3 — нормативно-правовая;

s_4 — метрологическая;

s_5 — инженерно-эксплуатационная.

Иерархия системы будет называться ациклическим графом $G = (V, E)$ (рис. 2), где $V = \vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5$ — множество вершин, а $E = \{e_1, \dots, e_i\}$ — множество дуг, которые характеризуют отношения между подсистемами Существует единственная вершина (корневая вершина — ЭКЦ), в которую существуют пути изо всех промежуточных вершин (подсистем) $a_i \in S$.

Вершинами в графе будут служить подсистемы ЭКЦ:

ϑ_1 — научно-методическая подсистема;

ϑ_2 — технико-криминалистическая;

ϑ_3 — нормативно-правовая;

ϑ_4 — метрологическая;

ϑ_5 — инженерно-эксплуатационная.

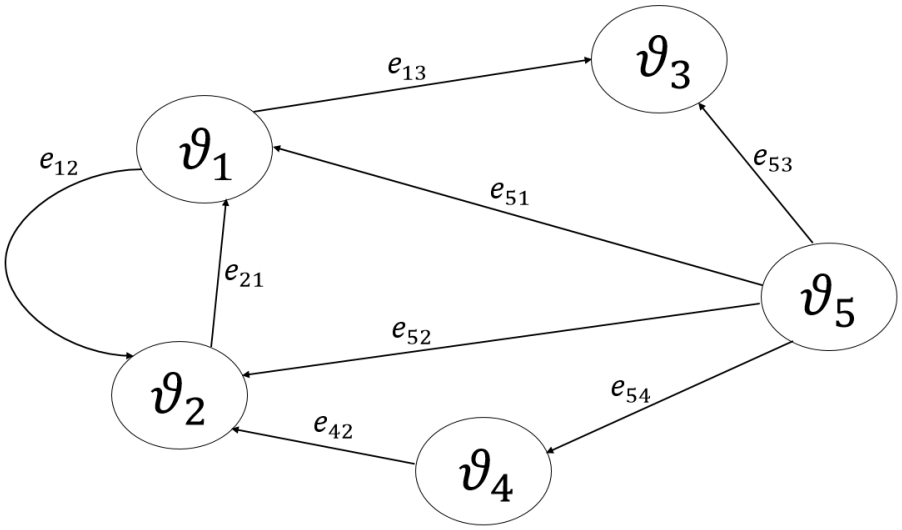


Рис. 2. Модель ЭКЦ на основе теории графов

Модель ЭКЦ на основе теории графов позволит наглядно увидеть отношения между вершинами.

Отношения вершин можно описать более подробно:

e_{12} — взаимодействие научно-методической подсистемы и технико-криминалистической путем разработки новых методик и применения их на практике;

e_{13} — разработанная методика должна быть нормативно подкреплена и официально оформлена;

e_{21} — современные виды криминалистических угроз требуют разработки новых методик;

e_{42} — оборудование, используемое экспертами, необходимо проверить на пригодность и исправность для эффективности и точности проверяемых доказательств;

e_{51} — функционирование научных лабораторий и приобретение нового оборудования;

e_{52} — обеспечивает бесперебойное электропитание сложных аналитических комплексов, поддерживает работу серверов для хранения цифровых доказательств;

e_{53} — обеспечивает работу защищенных каналов связи и систем хранения секретных документов;

e_{54} — создает необходимые помещения, где проводится поверка эталонного оборудования.

В этом аспекте исследование показало, что для эффективного управления ЭКЦ наиболее подходящим является метод декомпозиции. Этот метод позволяет разделить сложные и масштабные задачи на более мелкие, что упростит функционирование деятельности рассматриваемого центра.

Следующим этапом решения поставленной задачи является выбор показателей эффективности. Выбор конкретных показателей для оценки эффективности экспертно-криминалистического центра основывался на анализе существующих методик, применяемых в смежных областях управления сложными системами. В научной литературе представлены различные подходы к формированию систем показателей, каждый из которых адаптирован под специфику решаемых задач.

В контексте стратегического управления организациями предлагаются более сбалансированные системы. Исследование [11] посвящено совершенствованию таких систем для промышленных предприятий, где ключевыми показателями выступают финансы, клиенты, внутренние бизнес-процессы и обучение персонала. Этот подход ценен для формирования долгосрочной стратегии, однако его прямого применения к оперативной деятельности ЭКЦ может быть недостаточно из-за различия в целевых ориентирах.

Ближе к задачам оперативного управления организационно-техническими системами (ОТС) находится работа [12]. В ней для оценки сбалансированности ОТС предлагаются такие показатели, как время и стоимость принятия решения, а также вероятность его успешной реализации. Этот подход фокусируется на эффективности процесса принятия решений, что является важным аспектом для ЭКЦ, но не охватывает такие показатели, как качество результата или ресурсоемкость.

При оценке инновационной деятельности используются комплексные показатели, учитывающие как процесс, так и результат. В статье [13] рассматриваются показатели результативности (Output) и эффективности (Outcome) инновационных проектов, а также сбалансированные и интегральные индикаторы по фазам реализации. Данная методология полезна для оценки проектных инициатив внутри ЭКЦ, но требует адаптации для постоянной экспертной работы.

Наконец, для специализированных технических систем ключевыми зачастую являются показатели, характеризующие их работоспособность и производительность. Например, в исследовании сетей связи специального назначения [14] эффективность оценивается через отношение скорости передачи данных к пропускной способности канала, загрузку процессора и временные характеристики передачи информации. Подобные технические показатели критически важны для оценки подсистем ЭКЦ, таких как инженерно-эксплуатационная или технико-криминалистическая, но не отражают организационно-управленческую составляющую центра как целого.

Таким образом, анализ существующих подходов [11—14] показал, что для комплексной оценки эффективности ЭКЦ как организационно-технической системы необходим синтез и адаптация различных типов показателей, нами для качественной оценки

ЭКЦ предлагается использовать такие показатели, как время выполнения (T), качество (Q) и ресурсоемкость (R). Ни один из рассмотренных методов в отдельности не предоставляет готовой модели, что обосновывает необходимость разработки собственного интегрального алгоритма, объединяющего ключевые аспекты деятельности центра. Данное действие, соответственно, является третьим этапом решения поставленной задачи.

Алгоритм расчета показателей эффективности функционирования ЭКЦ.

Шаг 1. Выбор количества показателей для ЭКЦ — (n).

Шаг 2. Расчет показателя «Время выполнения» — (T). Шаг показывает, насколько быстро выполняются экспертизы. Вычисление производится следующим образом:

$$T = 1 - \frac{\bar{t}_{\text{факт}}}{t_{\text{норм}}} \text{ или } T = \frac{t_{\text{норм}} - \bar{t}_{\text{факт}}}{t_{\text{норм}}}, \quad (1)$$

где:

$\bar{t}_{\text{факт}}$ — среднее фактическое время выполнения экспертиз за период;

$t_{\text{норм}}$ — нормативное (допустимое) время выполнения (например, 5 рабочих дней).

Если

$\bar{t}_{\text{факт}} > t_{\text{норм}}$, то T может быть отрицательным, в таком случае приравниваем его к 0.

Шаг 3. Расчет показателя «Качество» — (Q). На данном шаге производится расчет показателя качества, насколько эффективна деятельность ЭКЦ. Критерии, по которым производится расчет, это количество ошибок, оспариваний и повторных экспертиз на этапе признания заключений в суде:

$$Q = 1 - \frac{N_{\text{ошибок}} + N_{\text{оспариваний}}}{N_{\text{всего}}}, \quad (2)$$

где:

$N_{\text{ошибок}}$ — количество экспертиз с ошибками;

$N_{\text{оспариваний}}$ — количество экспертиз, оспоренных в суде;

$N_{\text{всего}}$ — общее количество экспертиз, проводимых ЭКЦ.

Шаг 4. Расчет показателя «Ресурсоемкость» — (R). Шаг по расчету показателя R позволит оценить затраты на одну экспертизу. А именно такие затраты, как финансовые (закупка расходных материалов, обслуживание и калибровка оборудования), трудовые (основное время эксперта, повышение квалификации) и технические (амортизация оборудования (износ), вычислительные ресурсы). Вычисляется следующим образом:

$$R = \frac{1}{1 + \frac{C_{\text{ср}}}{C_{\text{эталон}}}}, \quad (3)$$

где: $C_{\text{ср}}$ — средняя стоимость одной экспертизы; $C_{\text{эталон}}$ — эталонная (оптимальная) стоимость.

Шаг 5. Расчет индекса эффективности (E). Данный показатель (количественный) отражает, насколько рассматриваемая система достигает поставленной цели. В нашем алгоритме будем интерпретировать данный показатель при помощи нормализации [0;1].

Расчет индекса эффективности позволит определить, как апробация выделенных показателей, может работать на основе представленного алгоритма и применительно к деятельности ЭКЦ.

$$E = w_1 \cdot T + w_2 \cdot Q + w_3 \cdot R, \quad (4)$$

где: T — нормализованная оценка времени выполнения (чем меньше время, тем выше показатель); Q — нормализованная оценка качества; R — нормализованная оценка ресурсоёмкости (чем меньше затрат, тем выше).

w_1, w_2, w_3 — весовые коэффициенты, $w_1 + w_2 + w_3 = 1$, определяемые по приоритетам центра. Определение весовых коэффициентов предлагается осуществлять на основе разработанного и апробированного алгоритма обработки экспертных оценок на основе взвешенной медианы [15]. Блок-схема разработанного алгоритма приведена рис. 3.

При этом алгоритм предполагает несколько вариантов развития в зависимости от рассчитанного индекса эффективности (E):

1. $0{,}8 \geq E \leq 1$ — система обладает высоким уровнем достижения поставленной цели.
2. $E \geq 6$ — система обладает средним уровнем достижения поставленной цели.
3. $E < 6$ — система обладает низким уровнем достижения поставленной цели, в данном случае требуется вернуться на шаг 2.

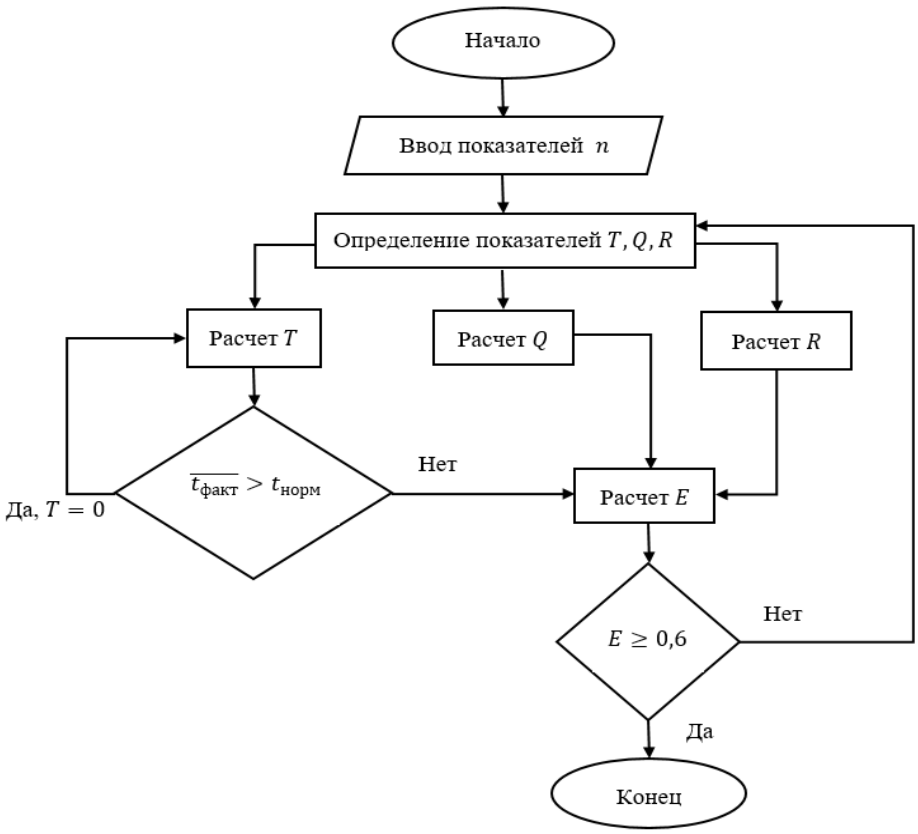


Рис. 3. Блок-схема алгоритма расчета показателей эффективности функционирования ЭКЦ

Вычислительный эксперимент. В целях апробации разработанного алгоритма расчёта индекса эффективности экспертно-криминалистического центра органов внутренних дел проведён вычислительный эксперимент. Эксперимент основан на имитационном моделировании деятельности центра с использованием нормативно-правовых и статистических данных, регламентирующих экспертную деятельность [16—19]. В качестве исходных приняты усреднённые показатели, характерные для типового регионального ЭКЦ.

Исходные данные.

Для расчёта частных критериев эффективности использованы следующие значения:

1. среднее фактическое время выполнения экспертизы: $\bar{t}_{\text{факт}}$ — 2 рабочих дня;
2. нормативное время выполнения экспертизы: $t_{\text{норм}}$ — 5 рабочих дней;
3. количество экспертиз, признанных ошибочными: $N_{\text{ошибок}}$ — 1;
4. количество экспертиз, оспоренных в суде: $N_{\text{оспариваний}}$ — 2;
5. общее количество проведённых экспертиз за период: $N_{\text{всего}}$ — 50;
6. средняя стоимость одной экспертизы: $C_{\text{ср}}$ — 50000 рублей;
7. эталонная (оптимальная) стоимость экспертизы: $C_{\text{эталон}}$ — 40000 рублей.

На основе формул (1) — (3), предложенных в основном алгоритме, произведены следующие вычисления.

Шаг 1. Расчет показателя «Время выполнения» — T.

$$T = 1 - \frac{2}{5},\ T = 0{,}6.$$

Полученное значение свидетельствует о том, что фактическая продолжительность экспертиз на 60 % ниже нормативной, что указывает на высокую оперативность работы подразделений ЭКЦ.

Шаг 2. Расчет показателя «Качество» — Q.

$$Q = 1 - \frac{1+2}{50},\ Q = 0{,}94.$$

Доля экспертиз, не вызывающих нареканий и не оспоренных в судебном порядке, составляет 94%, что характеризует высокий уровень профессиональной подготовки экспертов и методической обоснованности заключений.

Шаг 3. Расчет показателя «Ресурсоемкость» — R.

$$R = \frac{1}{1+\frac{50000}{40000}},\ R = 0{,}44.$$

Значение показателя $R = 0{,}44$ отражает умеренный уровень затрат на проведение экспертиз, однако указывает на наличие резервов для оптимизации ресурсного обеспечения.

Шаг 4. Расчет индекса эффективности (E). Для интегральной оценки эффективности функционирования ЭКЦ использован метод взвешенной суммы частных критериев (4). Весовые коэффициенты w_1, w_2, w_3 определены на основе алгоритма, опубликованного в работе [15].

Приоритеты распределены следующим образом:

1. Время выполнения (T) — $w_1 = 0{,}671$;
2. Качество экспертиз (Q) — $w_2 = 0{,}221$;
3. Ресурсоёмкость (R) — $w_3 = 0{,}108$.

$0{,}671 + 0{,}221 + 0{,}108 = 1$ — сумма коэффициентов равна единице, что обеспечивает корректность нормировки.

$$E = 0{,}671 \cdot \ 0{,}6 + 0{,}221 \cdot 0{,}94 + 0{,}108 \cdot 0{,}44 = 0{,}658.$$

Таким образом, согласно используем параметрам, исследуемая система обладает средним уровнем достижения поставленной цели. При помощи данного алгоритма возможно оценить функционирование ЭКЦ и при возможности внести корректировки при дальнейшей его работе.

Заключение. Полученное значение индекса эффективности $E = 0{,}658$ находится в средней области диапазона [0,1] и интерпретируется следующим образом: высокие показатели качества $Q = 0{,}94$ и времени выполнения $T = 0{,}6$ свидетельствуют о том, что ЭКЦ успешно справляется с основной функцией — своевременным и достоверным производством судебных экспертиз. Показатель ресурсоёмкости $R = 0{,}44$ ниже остальных, что указывает на необходимость оптимизации затратной части, например, за счёт внедрения более экономичных методик, автоматизации рутинных процессов или пересмотра нормативов материально-технического обеспечения.

Таким образом, разработанный алгоритм позволяет не только количественно оценить текущий уровень эффективности ЭКЦ, но и выявить направления для совершенствования его деятельности.

ЛИТЕРАТУРА

1. Баранников А. Л. Организационно-правовые основы деятельности экспертно-криминалистических подразделений. — М. : Щит-М, 2019. — 289 с.

2. О вопросах организации деятельности экспертно-криминалистических центров органов внутренних дел (ред. от 25.10.2023 № 799) : приказ МВД России от 30.05.2003 № 366 // СТРАСТ-ЮРИСТ (дата обращения: 05.03.2026).

3. Экспертно-криминалистический центр МВД России : официальный сайт. — URL: https://мвд.рф/mvd/structure1/Centri/JEkspertno_kriminalisticheskij_centr (дата обращения: 27.01.2026).

4. Терентьев А. А., Лукьянов А. С., Пославская В. Я. Исследование функционирования экспертно-криминалистического центра как организационно-технической системы на основе теории конфликта // Вестник Воронежского института МВД России. — 2025. — № 3. — С. 96—104.

5. Ерженин Р. В. Теоретические основы оценки эффективности сложной информационной системы // Вестник Астраханского государственного технического университета. Серия : Управление, вычислительная техника и информатика. — 2024. — № 2. — С. 105—110.

6. Спицын В. В. Методологический подход к оценке эффективности развития сложных социально-экономических систем // Экономика: вчера, сегодня, завтра. — 2017. — Т. 7. — № 4А. — С. 25—32.

7. Варнаков Д. В., Юденичев А. Н., Бугаев А. В. Разработка метода оценки эффективности функционирования сложных технических систем // Чтения академика В. Н. Болтинского : сборник статей, Москва, 25—26 января 2023 года. — М. : Сам Полиграфист, 2023. — С. 98—104.

8. Еримизина М. И., Волошина Е. И., Еримизина Е. Н. Теоретико-методические особенности и практические аспекты оценки функционирования сложных экономических систем (на примере административно-территориальных образований Республики Крым) // Научный вестник: Финансы, банки, инвестиции. — 2024. — № 4. — С. 60—75.

9. Меньших В. В., Пастушкова Е. А. Структурная модель функционально избыточного набора действий для принятия решений в органах внутренних дел // Вестник Воронежского института МВД России. — 2013. — № 4. — С. 226 — 235.

10. Пославская В. Я. Организационная структура экспертно-криминалистического центра МВД России // Актуальные проблемы деятельности подразделений уголовно-исполнительной системы : сборник материалов всероссийской научно-практической конференции. — Воронеж : Воронежский институт ФСИН России, 2025. — С. 449—453.

11. Белоусов И. Н., Белоусов Д. Н. Совершенствование системы сбалансированных показателей промышленных предприятий // Вестник Северо-Кавказского федерального университета. — 2015. — № 3(48). — С. 57—60.

12. Терентьев А. А., Пьянков О. В. Исследование сбалансированности организационно-технических систем при наличии нескольких показателей эффективности функционирования // Вестник Воронежского института МВД России. — 2023. — № 4. — С. 88—95.

13. Новикова О. В., Созонова Э. Э. Показатели оценки результативности и эффективности реализации инновационных проектов // Контроллинг. — 2021. — № 3(81). — С. 28—35.

14. Попов А. В., Пьянков О. В. Исследование взаимосвязи между конфликтными свойствами и показателями эффективности организационно-технических систем на примере сети связи специального назначения // Вестник НГУ. Серия : Информационные технологии. — 2022. — Т. 20. — № 4. — С. 39—60.

15. Терентьев А. А., Пославская В. Я. Разработка алгоритма обработки экспертных оценок на основе взвешенной медианы // Вестник Югорского государственного университета. — 2026. — Т. 22. — № 1. — С. 71—78.

16. Государственная судебно-экспертная деятельность в Российской Федерации : Федеральный закон от 31.05.2001 № 73-ФЗ (ред. от 22.07.2024). — URL: https://base.garant.ru/12123142/ (дата обращения: 15.02.2026).

17. Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации : приказ МВД России от 29.06.2005 № 511 (ред. от 27.09.2023) : зарегистрировано в Минюсте России 23.08.2005 № 6931. — URL: https://www.consultant.ru/document/cons_doc_LAW_55315/ (дата обращения: 15.02.2026).

18. Вопросы определения уровня профессиональной подготовки экспертов в системе МВД России : приказ МВД России от 09.01.2013 № 2 (ред. от 09.01.2017) : зарегистрировано в Минюсте России 19.04.2013 № 28236. — URL: https://base.garant.ru/70368458/ (дата обращения: 15.02.2026).

19. Об утверждении Наставления по организации экспертно-криминалистической деятельности в системе МВД России : приказ МВД России от 11.01.2009 № 7. — Доступ из справочно-правовой системы «КонсультантПлюс». — URL: https://www.consultant.ru/document/cons_doc_LAW_55315/ (дата обращения: 15.02.2026).

REFERENCES

1. Barannikov A. L. Organizatsionno-pravovye osnovy deyatel′nosti ekspertno-kriminalisticheskikh podrazdelenij. — M. : Shchit-M, 2019. — 289 s.

2. O voprosakh organizatsii deyatel′nosti ekspertno-kriminalisticheskikh tsentrov organov vnutrennikh del (red. ot 25.10.2023 № 799) : prikaz MVD Rossii ot 30.05.2003 № 366 // STRAST-YuRIST (data obrashcheniya: 05.03.2026).

3. Ekspertno-kriminalisticheskij tsentr MVD Rossii : ofitsial′nyj sajt. — URL: https://mvd.rf/mvd/structure1/Centri/JEkspertno_kriminalisticheskij_centr (data obrashcheniya: 27.01.2026).

4. Terent′ev A. A., Luk′yanov A. S., Poslavskaya V. Ya. Issledovanie funktsionirovaniya ekspertno-kriminalisticheskogo tsentra kak organizatsionno-tekhnicheskoj sistemy na osnove teorii konflikta // Vestnik Voronezhskogo instituta MVD Rossii. — 2025. — № 3. — S. 96—104.

5. Erzhenin R. V. Teoreticheskie osnovy otsenki effektivnosti slozhnoj informatsionnoj sistemy // Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya : Upravlenie, vychislitel′naya tekhnika i informatika. — 2024. — № 2. — S. 105—110.

6. Spitsyn V. V. Metodologicheskij podkhod k otsenke effektivnosti razvitiya slozhnykh sotsial′no-ekonomicheskikh sistem // Ekonomika: vchera, segodnya, zavtra. — 2017. — T. 7. — № 4A. — S. 25—32.

7. Varnakov D. V., Yudenichev A. N., Bugaev A. V. Razrabotka metoda otsenki effektivnosti funktsionirovaniya slozhnykh tekhnicheskikh sistem // Chteniya akademika V. N. Boltinskogo : sbornik statej, Moskva, 25—26 yanvarya 2023 goda. — M. : Sam Poligrafist, 2023. — S. 98—104.

8. Erimizina M. I., Voloshina E. I., Erimizina E. N. Teoretiko-metodicheskie osobennosti i prakticheskie aspekty otsenki funktsionirovaniya slozhnykh ekonomicheskikh sistem (na primere administrativno-territorial′nykh obrazovanij Respubliki Krym) // Nauchnyj vestnik: Finansy, banki, investitsii. — 2024. — № 4. — C. 60—75.

9. Men′shikh V. V., Pastushkova E. A. Strukturnaya model′ funktsional′no izbytochnogo nabora dejstvij dlya prinyatiya reshenij v organakh vnutrennikh del // Vestnik Voronezhskogo instituta MVD Rossii. — 2013. — № 4. — S. 226 — 235.

10. Poslavskaya V. Ya. Organizatsionnaya struktura ekspertno-kriminalisticheskogo tsentra MVD Rossii // Aktual′nye problemy deyatel′nosti podrazdelenij ugolovno-ispolnitel′noj sistemy : sbornik materialov vserossijskoj nauchno-prakticheskoj konferentsii. — Voronezh : Voronezhskij institut FSIN Rossii, 2025. — S. 449—453.

11. Belousov I. N., Belousov D. N. Sovershenstvovanie sistemy sbalansirovannykh pokazatelej promyshlennykh predpriyatij // Vestnik Severo-Kavkazskogo federal′nogo universiteta. — 2015. — № 3(48). — S. 57—60.

12. Terent′ev A. A., P′yankov O. V. Issledovanie sbalansirovannosti organizatsionno-tekhnicheskikh sistem pri nalichii neskol′kikh pokazatelej effektivnosti funktsionirovaniya // Vestnik Voronezhskogo instituta MVD Rossii. — 2023. — № 4. — S. 88—95.

13. Novikova O. V., Sozonova E. E. Pokazateli otsenki rezul′tativnosti i effektivnosti realizatsii innovatsionnykh proektov // Kontrolling. — 2021. — № 3(81). — S. 28—35.

14. Popov A. V., P′yankov O. V. Issledovanie vzaimosvyazi mezhdu konfliktnymi svojstvami i pokazatelyami effektivnosti organizatsionno-tekhnicheskikh sistem na primere seti svyazi spetsial′nogo naznacheniya // Vestnik NGU. Seriya : Informatsionnye tekhnologii. — 2022. — T. 20. — № 4. — S. 39—60.

15. Terent′ev A. A., Poslavskaya V. Ya. Razrabotka algoritma obrabotki ekspertnykh otsenok na osnove vzveshennoj mediany // Vestnik Yugorskogo gosudarstvennogo universiteta. — 2026. — T. 22. — № 1. — S. 71—78.

16. Gosudarstvennaya sudebno-ekspertnaya deyatel′nost′ v Rossijskoj Federatsii : Federal′nyj zakon ot 31.05.2001 № 73-FZ (red. ot 22.07.2024). — URL: https://base.garant.ru/12123142/ (data obrashcheniya: 15.02.2026).

17. Voprosy organizatsii proizvodstva sudebnykh ekspertiz v ekspertno-kriminalisticheskikh podrazdeleniyakh organov vnutrennikh del Rossijskoj Federatsii : prikaz MVD Rossii ot 29.06.2005 № 511 (red. ot 27.09.2023) : zaregistrirovano v Minyuste Rossii 23.08.2005 № 6931. — URL: https://www.consultant.ru/document/cons_doc_LAW_55315/ (data obrashcheniya: 15.02.2026).

18. Voprosy opredeleniya urovnya professional′noj podgotovki ekspertov v sisteme MVD Rossii : prikaz MVD Rossii ot 09.01.2013 № 2 (red. ot 09.01.2017) : zaregistrirovano v Minyuste Rossii 19.04.2013 № 28236. — URL: https://base.garant.ru/70368458/ (data obrashcheniya: 15.02.2026).

19. Ob utverzhdenii Nastavleniya po organizatsii ekspertno-kriminalisticheskoj deyatel′nosti v sisteme MVD Rossii : prikaz MVD Rossii ot 11.01.2009 № 7. — Dostup iz spravochno-pravovoj sistemy «Konsul′tantPlyus». — URL: https://www.consultant.ru/document/cons_doc_LAW_55315/ (data obrashcheniya: 15.02.2026).

СВЕДЕНИЯ ОБ АВТОРАХ

Терентьев Александр Андреевич. Старший преподаватель кафедры инфокоммуникационных систем и технологий. Кандидат технических наук.
Воронежский институт МВД России.
E-mail: Alextt02021993@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Пославская Виктория Яновна. Инженер отделения технического обеспечения отдела информационных технологий, связи и защиты информации.
Воронежский институт МВД России.
E-mail: vikka464@gmail.com
Россия, 394065, Воронеж, проспект Патриотов, 53.

Terentyev Alexander Andreevich. Senior lecturer of the chair of Infocommunication Systems and Technologies. Candidate of Technical Sciences.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: Alextt02021993@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Poslavskaya Victoria Yanovna. Engineer of the Department of Technical Support of the Department of Infocommunication Technologies, Communications and Information Security.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: vikka464@gmail.com
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: экспертно-криминалистический центр; организационно-техническая система; оценка эффективности; экспертные оценки; теория графов.

Key words: forensic center; organizational and technical system; efficiency assessment; expert assessments; graph theory.

УДК 519.6

РАДИОТЕХНИКА И СВЯЗЬ

Ю. С. Радченко, *доктор физико-математических наук, профессор*
Т. М. Овчинникова, *кандидат физико-математических наук, доцент*
В. П. Удалов, *кандидат физико-математических наук, доцент*

ОБРАБОТКА СЛОЖНЫХ СИГНАЛОВ С НЕИЗВЕСТНЫМ ЗАКОНОМ МОДУЛЯЦИИ В АНТЕННОЙ РЕШЕТКЕ НА ОСНОВЕ АНАЛИЗА СОБСТВЕННЫХ ЗНАЧЕНИЙ

PROCESSING COMPLEX SIGNALS WITH UNKNOWN MODULATION LAW IN AN ANTENNA ARRAY BASED ON EIGENVALUE ANALYSIS

В работе выполнен синтез и анализ алгоритмов обработки принимаемого поля и оценки угла прихода сложного сигнала при отсутствии сведений о его законе модуляции. Задача решена с использованием аппарата собственных значений и собственных векторов корреляционной матрицы поля в апертуре антенной решетки. Рассмотрены случаи, когда фронт волны является плоским и осуществляется только частотная обработка и когда волна формируется протяженным стохастическим источником. Получен логарифм функционала отношения правдоподобия, позволяющий решить задачи обнаружения сигнала, оценки среднего угла прихода волны и рассчитать величину углового рассеяния. Установлены условия, когда возможна оценка угла прихода волны.

The synthesis and analysis of algorithms for received field processing and the angle of arrival of a complex signal estimation in the absence of information about its modulation law have been performed. The problem was solved using the apparatus of eigenvalues and eigenvectors of the correlation matrix of the field in the aperture of an antenna array. The paper considers cases where the wavefront is flat and only frequency processing is performed, and where the wave is generated by an extended stochastic source. The logarithm of the likelihood ratio functional, which allows us to solve the problems of signal detection, estimation of the average arrival angle of the wave, and calculation of the angular scattering was obtain. The limits of applicability have been established for estimating the angle of wave arrival.

Введение. Вопросам оптимальной обработки стохастических сигналов с неизвестными параметрами посвящен ряд работ, например [1, 2]. Однако разработанные методы синтеза и анализа алгоритмов обработки сложных сигналов базируются на высокой априорной осведомлённости относительно принимаемых сигналов. В то же время такая задача, как мониторинг электромагнитной обстановки решается в условиях априорной неопределенности относительно параметров сложных сигналов и законов их модуляции.

Одним из способов построения алгоритмов и разработки методов анализа является переход к устойчивым статистикам поля. Продуктивным подходом к синтезу таких алгоритмов является использование аппарата собственных значений и собственных векторов корреляционной матрицы поля в апертуре антенной решетки (АР) [3, 4].

Следует отметить, что решение задачи зависит от того, является ли фронт волны плоским и осуществляется только частотная обработка, или же волна формируется протяженным стохастическим источником. Для этих случаев необходимы различные модели сигнала. В данной работе предложены и обоснованы такие модели. На их основе выполнен синтез и анализ алгоритмов обнаружения и оценки угла прихода сложного сигнала при отсутствии сведений о его законе модуляции.

Синтез алгоритма обработки квазидетерминированного сигнала. Рассмотрим способ обработки поля, основанный на анализе собственных значений сигнала в частотной области.

Пусть имеется N-элементная АР, которая обрабатывает сигналы

$$x_n(t) = s_n(t;\theta_0) + \xi_n(t), \quad t \in [0, T_H] \ , \ n = 1..N \ . \tag{1}$$

Здесь $\xi_n(t)$ — независимые гауссовские шумы на элементах АР, $s_n(t,\theta_0)$ — полезный сигнал, который в общем случае можно записать в виде

$$s_n(t,\theta_0) = A_0 F(t)\cos[\omega_0 t + \psi(t) - \Delta\varphi_n(\theta_0) - \varphi_0]. \tag{2}$$

$\Delta\varphi_n(\theta_0)$ — набег фазы на n-м элементе антенны. В данной модели полагается, что частотно-временная локализация сигнала выполнена, поэтому временное положение и положение спектра на частотной оси известны. Неизвестными являются угол прихода волны θ_0 и законы амплитудной и фазовой модуляции сигнала, соответственно $F(t), \psi(t)$. В процессе обработки смеси (1) необходимо оценить пеленг θ_0. Для дальнейшей работы целесообразно перейти к комплексной форме сигнала

$$\dot{s}_n(t,\theta_0) = \dot{\mu}_n \dot{F}(t) e^{i\omega_0 t},$$

где

$$\dot{\mu}_n(\theta_0) = A_0 e^{i\varphi_0} e^{i\Delta\varphi_n(\theta_0)},$$

$$\dot{F}(t) = F(t) e^{i\psi(t)}.$$

Тогда спектр, вычисленный с помощью ДПФ, по отсчетам $t_j = j\Delta t = j / F_d$, будет иметь вид

$$\begin{aligned} G_n(f_k) &= \sum_{j=0}^{J-1} \dot{s}_n(t_j)\exp(-i2\pi jk / J) = \dot{\mu}_n(\theta_0) G_0(f_k), \\ G_0(f_k) &= \sum_{j=0}^{J-1} \dot{F}(t_j)\exp(-i2\pi jk / J + i2\pi f_0 j / F_d). \end{aligned} \tag{3}$$

Причем локализация спектра $G_0(f_k)$ известна до обработки: $f_a \le f_k \le f_{a+Q-1}, \quad a \le k \le a + Q - 1.$

То есть размерность ненулевого спектрального вектора равна Q.

Выполняя ДПФ над принятой реализацией $\dot{x}_n(t_j)$, сигналом и шумом

$$\dot{X}_n(f_k) = \sum_{j=0}^{J-1} \dot{x}_n(t_j) \exp\left(-i\frac{2\pi kj}{J}\right),$$

$$\xi_{n,k} = \sum_{j=0}^{J-1} \xi_n(t_j) \exp(-i2\pi kj / J). \quad (4)$$

Можно записать с учетом (4)

$$\dot{X}_n(f_k) = \dot{\mu}_n(\theta_0)\dot{G}_0(f_k) + \xi_{n,k}. \quad (5)$$

Если $\xi_n(t)$ гауссовские процессы, то модель (5) приводит нас к задаче оценки комплексного сомножителя $\dot{\mu}_n(\theta_0)$ в аддитивной смеси сигнала и шума. Решение такой задачи известно [1]:

$$\dot{\mu}_n(\theta_0) = \frac{\sum_k \dot{X}_n(f_k) G_0^*(f_k)}{\sum_k |G_0(f_k)|^2}. \quad (6)$$

Выражение (6) определяет оптимальную фильтрацию в частотной области при известном спектре и оценку угла прихода волны θ_0. Данный способ представляет алгоритм, который является эталонным для обработки квазидетерминированного сигнала и с которым сравниваются другие алгоритмы.

В том случае, когда $G_0(f_k)$ неизвестно, алгоритм (6) неприменим.

Обработка неизвестного сигнала. Введем обозначения

$$\mathbf{X} = \begin{pmatrix} X_1(f_a) & \dots & X_1(f_{a+Q-1}) \\ \vdots & \dots & \vdots \\ X_N(f_a) & \dots & X_N(f_{a+Q-1}) \end{pmatrix}. \quad (7)$$

$\mathbf{X}$ — матрица, состоящая из N строк и Q столбцов. Строки содержат спектры ДПФ на каждом элементе АР, столбцы значения одинаковых спектральных компонент на разных элементах АР, $(a, Q-1)$ — граничные частоты спектра, $N \le Q$.

$$\mathbf{M} = \begin{pmatrix} \dot{\mu}_1(\theta_0) \\ \vdots \\ \dot{\mu}_N(\theta_0) \end{pmatrix}. \quad (8)$$

Вектор — столбец комплексных амплитуд размерностью N.

$$\mathbf{G}_0 = \begin{pmatrix} G_0(f_a) \\ \vdots \\ G_0(f_{a+Q-1}) \end{pmatrix}. \quad (9)$$

Вектор — столбец спектральных компонент размерностью Q.

Тогда с точностью до несущественного сомножителя выражение (6) можно переписать в виде

$$\mathbf{M} = \mathbf{X}\mathbf{G}_0, \tag{10}$$

где $\mathbf{G}_0$ неизвестно. Для нахождения оптимального фильтра необходимо максимизировать величину

$$\delta^2 = \mathbf{M}^+\mathbf{M} = \mathbf{G}^+\mathbf{X}^+\mathbf{X}\mathbf{G}. \tag{11}$$

Здесь $(\ )^+$ символ эрмитова сопряжения. Для нахождения нетривиального решения (11) наложим ограничение на $\mathbf{G}$:

$$\mathbf{G}^+\mathbf{G} = 1. \tag{12}$$

Оптимизация (11) с учетом ограничения (12) называется оптимизацией Лагранжа. Для этого составляется целевая функция [4]

$$L = \delta^2 + \lambda\left(1 - \mathbf{G}^+\mathbf{G}\right) = \left(\mathbf{G}^+\mathbf{X}^+\mathbf{X}\mathbf{G}\right) + \lambda\left(1 - \mathbf{G}^+\mathbf{G}\right), \tag{13}$$

где λ — множитель Лагранжа. Дифференцируя (13) по компонентам вектора $\mathbf{G}$, приходим к задаче нахождения собственных значений и собственных векторов:

$$\mathbf{X}^+\mathbf{X}\mathbf{G} = \lambda\mathbf{G} \tag{14}$$

или

$$\mathbf{K}\mathbf{G} = \lambda\mathbf{G}, \ \ \mathbf{K} = \mathbf{X}^+\mathbf{X}. \tag{15}$$

Корреляционная матрица $\mathbf{K}$ размерностью $Q \times Q$ является эрмитовой и положительно полуопределенной. Поэтому все ее собственные значения $\lambda = (\lambda_1..\lambda_N) = \{\lambda_n\}$ вещественные и неотрицательные. Если $N < Q$, то ранг матрицы $\mathbf{K}$ не превосходит N. Так что по крайней мере N собственных значений ненулевые. Выбирая $\lambda_n = \lambda_{\max}$ и соответствующий ему вектор $\mathbf{G} = \mathbf{G}_{\max}$, получаем искомые решения. Подставляя $\lambda = \lambda_{\max}$ и $\mathbf{G} = \mathbf{G}_{\max}$ в (13), получаем

$$L = \delta^2 = \lambda_{\max}. \tag{16}$$

Для пояснения физического смысла полученных решений положим $\xi_{n,k} = 0$. В случае отсутствия шумов матрица $\mathbf{K}$ вырождается, поскольку фронт волны в модели (2) полагается плоским. В этом случае отлично от нуля только одно собственное значение $\lambda_{\max} \approx N$ и существует только один собственный вектор:

$$\mathbf{G}_{\max} = \pm\mathbf{G}_0 / \sqrt{\mathbf{G}_0^+\mathbf{G}_0}. \tag{17}$$

То есть с точностью до несущественных сомножителей (17) совпадает с (6). Таким образом, задача поиска собственных значений и собственных векторов приводит в данном случае к оптимальной фильтрации сигнала в частотной области и последующей обработке. При отсутствии сигнала все собственные значения одинаковы и имеют значения $\lambda_n \approx 1$. Если получается спектр собственных значений $(\lambda_1,..\lambda_N)$, то необходимо сформировать решающую статистку и по ней принимать решения об обнаружении и оценке параметров волны.

Если ввести параметр

$$\chi = \frac{\lambda_{\max}}{N\sum\lambda_n},$$

то его величина лежит в пределах $(1/N) \le \chi \le 1$. Задаваясь определенным порогом h_χ, можно по собственным значениям осуществлять процедуру обнаружения сигнала. Алгоритмы, основанные на статистиках (13), (17), являются непараметрическими, не зависящими от формы сигнала. При уменьшении уровня шумов они сходятся к оптимальным алгоритмам согласованной фильтрации в частотной области (6).

Обработка поля протяженного источника. Рассмотрим ситуацию, когда спектр собственных значений говорит о протяженном характере источника сигнала. Для расчета необходима более полная статистическая информация о поле, принимаемом на антенную решетку (АР). Рассмотрим структуру принимаемого поля в виде [5]

$$\mathbf{x}(t) = \mathbf{S}(t) + \mathbf{n}(t) = S_0 s(t)\sum_{n=1}^{L}\gamma_n(t)\mathbf{U}(\theta_0+\alpha_n) + \mathbf{n}(t),$$

$$\mathbf{U}(\theta) = \left[G_1(\theta)a_1(\theta), G_2(\theta)a_2(\theta), ..G_m(\theta)a_m(\theta)\right]^T,\ \mathbf{n}(t) = \left[n_1(t)...n_m(t)\right]^T, \qquad (18)$$

$$a_k(\theta) = \exp(j2\pi\frac{\Delta}{\lambda_0}(k-1)\sin(\theta)),\quad k = 0..m-1.$$

Здесь $a_k(\theta)$ — комплексная амплитуда на k-м элементе АР, $G_k(\theta)$ — диаграмма направленности k-го элемента АР. L — случайное число плоских волн, приходящих на АР, каждая из которых характеризуется своим отклонением α_n от некоторого общего угла прихода θ_0 и случайной комплексной амплитудно-фазовой модуляцией $\gamma_n(t)$, которую будем считать гауссовской с характеристиками $\langle\gamma_n(t_1)\rangle = 0$, $\langle\gamma_n(t_1)\gamma_k(t_2)\rangle = 0$, $\langle\gamma_n(t_1)\gamma_k^*(t_2)\rangle = \sigma_\gamma^2\delta_{k,n}\rho(t_1-t_2)$. Длина волны несущей обозначена λ_0. Огибающую $s(t)$ и амплитудный множитель S_0 будем считать одинаковыми для всех лучей. Вектор $\mathbf{n}(t)$ представляет собой аддитивный белый гауссовский шум в каждом элементе АР с характеристиками $< n_k(t) >= 0$, $< n_k(t_1)n_i(t_2) >= \sigma_n^2\delta_{k,i}\delta(t_1-t_2)$. Следовательно, сигнал (18) является условным гауссовским случайным полем с нулевым средним, со случайными параметрами L, γ_n и α_n и неизвестным параметром θ_0.

Корреляционная матрица принятого поля согласно [5]

$$\mathbf{R}_\mathbf{X}(t_1,t_2) = \mathbf{R}_\mathbf{S}(t_1,t_2) + \mathbf{R}_\mathbf{n}(t_1,t_2) = \langle\mathbf{S}(t_1)\mathbf{S}^H(t_2)\rangle + \langle\mathbf{n}(t_1)\mathbf{n}^H(t_2)\rangle =$$
$$= S_0^2 s(t_1)s^*(t_2)\langle\sum_{n=1}^{L}\gamma_n(t_1)\gamma_n^*(t_2)\mathbf{U}(\theta_0+\alpha)\mathbf{U}^H(\theta_0+\alpha)\rangle_{L,\gamma,\alpha} + \sigma_n^2\delta(t_1-t_2)\mathbf{I}. \qquad (19)$$

Будем считать, что величины L, γ, α статистически независимы между собой, и их статистические характеристики не зависят от номера луча n. Пусть случайные величины α имеют распределение $P(\alpha)$. Вводя обозначение

$$R_{k,i}^{(a)} = \langle U_k(\theta_0+\alpha)U_i^*(\theta_0+\alpha)\rangle_\alpha,\ i,k = 1..m, \qquad (20)$$

получим следующее выражение для матрицы $\mathbf{R_S}(t_1-t_2)$:

$$\mathbf{R}_S(t_1,t_2) = P_S \rho(t_1 - t_2) s(t_1) s^*(t_2) \mathbf{R}^{(a)}, \tag{21}$$

где $P_S = S_0^2 \sigma_\gamma^2 < L >$ — средняя мощность поля, $< L >$ — среднее число лучей. В выражении (21) элементы матрицы выражаются как

$$R_{k,i}^{(a)} = \int_{-\infty}^{\infty} P(\alpha) G_k(\theta_0 + \alpha) G_i^*(\theta_0 + \alpha) \exp\left(j2\pi \frac{\Delta}{\lambda_0} (k-i) \sin(\theta_0 + \alpha) \right) d\alpha .$$

Сделаем допущение о малости флуктуаций α отклонений угла прихода. Тогда можно положить $G(\theta_0 + \alpha) \approx G(\theta_0)$. В итоге выражение для $R_{k,i}^{(a)}(\theta_0, \sigma_\alpha)$ примет вид

$$\begin{aligned} R_{k,i}^{(a)} &= \exp\left(j2\pi \frac{\Delta}{\lambda_0} (k-i) \sin(\theta_0) \right) G_k(\theta_0) G_i^*(\theta_0) \int_{-\infty}^{\infty} P(\alpha) \exp(j u_{k,i} \alpha) d\alpha = \\ &= a_k(\theta_0) G_k(\theta_0) a_i^*(\theta_0) G_i^*(\theta_0) B(u_{k,i}), \end{aligned} \tag{22}$$

где введено обозначение $u_{k,i} = 2\pi(\Delta / \lambda_0)(k-i)\cos(\theta_0)$, а $B(u)$ — характеристическая функция распределения $P(\alpha)$.

Из работ [6, 7] следует, что распределение $P(\alpha)$ может быть хорошо аппроксимировано либо распределением Гаусса (оценка угла прихода в вертикальной плоскости) с характеристической функцией

$$B(u) = \exp(-\sigma_\alpha^2 u^2 / 2),$$

либо распределением Лапласа (оценка угла прихода в горизонтальной плоскости) с характеристической функцией

$$B(u) = 1/(1 + 0.5\sigma_\alpha^2 u^2).$$

В этих случаях характеристическая функция $B(u)$ будет зависеть только от среднеквадратического отклонения σ_α. Так как величина σ_α характеризует дисперсию разброса углов прихода лучей от общего угла θ_0, то назовем эту величину угловым рассеянием принимаемого сигнала (18).

Корреляционная матрица (22) зависит от параметров принимаемого сигнала — общего угла прихода θ_0 и его углового рассеяния σ_α, которые необходимо оценить при приеме сигнала (18), и не зависит от модуляции сигнала. Обозначим $\Omega = \{\theta_0, \sigma_\alpha\}$, введем матрицу $\mathbf{B}(\Omega) = \left[B(u_{k,i} \mid \Omega) \right]$ и $\mathbf{F}(\theta_0) = diag(a_1(\theta_0) G_1(\theta_0), a_2(\theta_0) G_2(\theta_0) .. a_m(\theta_0) G_m(\theta_0))$. Тогда корреляционную матрицу $\mathbf{R}_S(t_1, t_2)$ (21) можно записать в виде

$$\mathbf{R}_S(t_1,t_2;\Omega) = P_S \rho(t_1 - t_2) s(t_1) s^*(t_2) \mathbf{F}(\theta_0) \mathbf{B}(\Omega) \mathbf{F}^H(\theta_0). \tag{23}$$

При таком допущении рассматриваемая модель сигнала имеет следующие особенности:

- временная и пространственная обработки разделяются,
- в пространственной области сигнал является стохастическим,
- во временной области сигнал является детерминированным.

Поскольку в данной задаче представляют интерес угловые характеристики поля, будем предполагать, что за время наблюдения среда остается замороженной и выполняется условие $\rho(t_1 - t_2) = 1$. Обозначим $\mathbf{K}(\Omega) = \mathbf{F}(\theta_0)\mathbf{B}(\Omega)\mathbf{F}^H(\theta_0)$ — нормированную корреляционную матрицу сигнала на приемной апертуре, где $\sigma_S^2 = P_S \int_0^T |s(t)|^2 \, dt$, $\sigma_N^2 = \sigma_n^2 \int_0^T |s(t)|^2 \, dt$, $\varepsilon = \sigma_N^2 / \sigma_S^2$.

Для анализа характеристик оценок угла прихода и углового рассеяния удобнее получить выражение для ЛФОП в терминах собственных значений λ_k, $k = 1..m$ матрицы $\mathbf{K}(\Omega)$. Введем матрицу $\mathbf{P} \equiv \mathbf{P}\{\Omega\}$ — матрицу собственных векторов $\mathbf{K}(\Omega)$. Тогда $\mathbf{K}(\Omega) = \mathbf{P}\mathbf{\Lambda}\mathbf{P}^H$, где $\mathbf{\Lambda} = diag\{\lambda_k\}$.

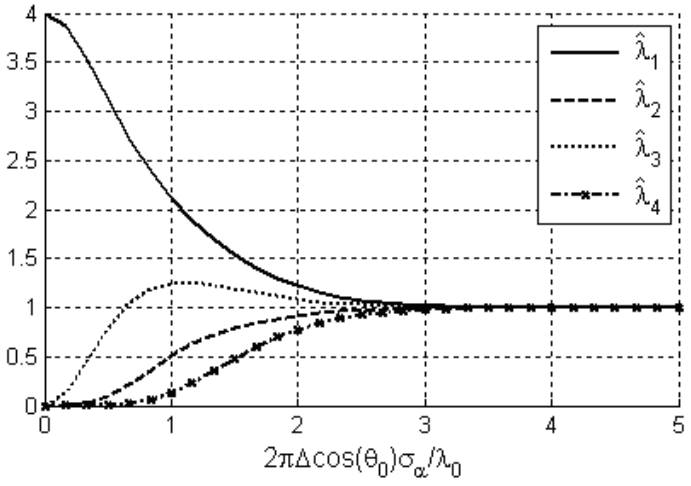


Рис. 1. Собственные числа матрицы $\mathbf{K}$ для 4-элементной АР

На рис. 1 приведены графики поведения собственных значений корреляционной матрицы $\mathbf{K}$ волнового поля, поступающего на линейную АР. Здесь Δ — шаг решетки, θ_0 — угол прихода волны, отсчитанный от нормали к АР, λ_0 — длина волны , соответствующая центральной частоте спектра сигнала, σ_α — дисперсия углов прихода волны на антенную решетку.

При приходе плоской квазидетерминированной волны на АР аргумент графика равен 0. Поэтому все собственные числа, кроме одного λ_1, стремятся к нулю. Увеличение аргумента на графике рис. 1 физически означает приближение отсчетов поля на АР к системе независимых отсчетов (белому изотропному шуму). В таком случае число собственных значений определяется числом элементов в АР N, а сами собственные значения стремятся к 1. В таком случае оценка θ_0 невозможна.

Логарифм функционала отношения правдоподобия (ЛФОП) по пространственным параметрам сигнала в форме собственных значений и собственных векторов матрицы $\mathbf{K}(\Omega)$ принятой волны имеет вид

$$M(\Omega)=\frac{1}{2}\sum_{k=1}^{m}\frac{\lambda_k(\Omega)/\varepsilon}{1+\lambda_k(\Omega)/\varepsilon}\frac{|Y_k|^2}{\sigma_N^2}-\frac{1}{2}\sum_{k=1}^{m}\ln\left(1+\lambda_k(\Omega)/\varepsilon\right). \qquad (24)$$

Здесь $\mathbf{Y}=\mathbf{X}^H\mathbf{P}$. Максимизируя (24) по информационным параметрам $\Omega=\{\theta_0,\sigma_\alpha\}$, можно получить оценки максимального правдоподобия (ОМП) этих параметров. Вид распределения ЛФОП $M(\Omega)$ существенно негауссовский, и его анализ производится путем статистического моделирования [8].

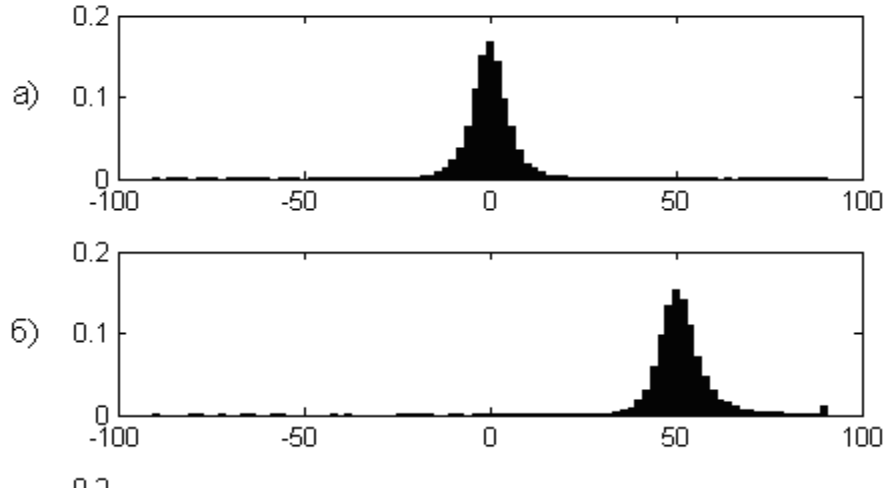


Рис 2. Гистограммы оценок углов прихода

На рис. 2 приведены полученные в результате моделирования гистограммы угла прихода волны от протяженного источника при σ_α=5°, $1/\varepsilon$=+25дб , числе элементов АР — $m=4$ при разных значениях параметра θ_0. Как следует из (23), (24), пространственная обработка в форме собственных значений не требует знания формы сигнала и закона модуляции. При этом алгоритм обработки поля имеет достаточно ясный физический смысл.

Выводы. В работе рассмотрены задачи обработки полей с неизвестным углом прихода и неизвестным законом модуляции в антенных решетках на основе анализа собственных значений корреляционных матриц этих полей. Алгоритмы обладают инвариантностью по отношению к закону модуляции. Рассмотрены два случая: обработка плоской волны от точечного источника и обработка поля, создаваемого протяженным источником.

В первом случае задача сводится к оптимизации частотной обработки с ограничениями Лагранжа, позволяющей найти спектр собственных значений и собственных векторов частотно-пространственной матрицы сигналов на элементах АР. Анализ собственных значений и собственных векторов позволяет синтезировать инвариантные к неизвестному закону модуляции алгоритмы обнаружения сигнала и оценки угла прихода квазидетерминированной волны.

Для обработки флуктуирующего поля от протяженного источника предложена его модель на раскрыве антенной решетки. Сформулированы условия разделения обработки на пространственную и временную. Найдены собственные вектора и собственные значения. Анализ собственных значений позволил установить условия, когда возможна оценка угла прихода волны. Получен логарифм функционала отношения правдоподобия, позволяющий решить задачи обнаружения сигнала, оценки среднего угла прихода волны и величины углового рассеяния.

ЛИТЕРАТУРА

1. Фалькович С. Е., Пономарев В. И., Шкварко Ю. В. Оптимальный прием пространственно-временных сигналов в радиоканалах с рассеянием / под ред. С. Е. Фалькович. — М. : Радио и связь, 1989. — 296 с.

2. Радченко Ю. С., Овчинникова Т. М., Удалов В. П. Сравнительный анализ алгоритмов пространственно-временного поиска сигнала с неизвестными параметрами // Вестник Воронежского института МВД России. — 2024. — № 1. — С. 151—160.

3. Тыртышников Е. Е. Матричный анализ и линейная алгебра. — М. : Физматлит, 2007. — 480 с.

4. Пистолькорс А. А., Литвинов О. С. Введение в теорию адаптивных антенн. — М. : Наука, 1991. — 200 с.

5. Радченко Ю. С., Титов Р. В. Модель поля, формируемого случайным кластером рассеивателей // Вестник ВГУ. Серия : Физика, математика. — 2010. — Вып. 2. — С. 271—275.

6. Bengtsson M., Ottersten B. Low-Complexity Estimators for Distributed Sources // IEEE Transactions on Signal Processing. — 2000. — Vol. 48. — № 8. — P. 2185—2193.

7. Stoica P., Babu P, Li J. Sparse Covariance-Based Estimation Method for Array Pro-cessing // IEEE Transactions on Signal Processing. — 2011. — Vol. 59. — № 2. — P. 629—638.

8. Плохотников К. Э. Вычислительные методы. Теория и практика в среде MATLAB : курс лекций. — М. : Горячая линия — Телеком, 2009. — 496 с.

REFERENCES

1. Fal′kovich S. E., Ponomarev V. I., Shkvarko Yu. V. Optimal′nyj priem prostranstvenno-vremennykh signalov v radiokanalakh s rasseyaniem / pod red. S. E. Fal′kovicha. — M. : Radio i svyaz′, 1989. — 296 s.

2. Radchenko Yu. S., Ovchinnikova T. M., Udalov V. P. Sravnitel′nyj analiz algoritmov prostranstvenno-vremennogo poiska signala s neizvestnymi parametrami // Vestnik Voronezhskogo instituta MVD Rossii. — 2024. — № 1. — S. 151—160.

3. Tyrtyshnikov E. E. Matrichnyj analiz i linejnaya algebra. — M. : Fizmatlit, 2007. — 480 s.

4. Pistol′kors A. A., Litvinov O. S. Vvedenie v teoriyu adaptivnykh antenn. — M. : Nauka, 1991. — 200 c.

5. Radchenko Yu. S., Titov R. V. Model′ polya, formiruemogo sluchajnym klasterom rasseivatelej // Vestnik VGU. Seriya : Fizika, matematika. — 2010. — Vyp. 2. — S. 271—275.

6. Bengtsson M., Ottersten V. Low-Complexity Estimators for Distributed Sources // IEEE Transactions on Signal Processing. — 2000. — Vol. 48. — № 8. — P. 2185—2193.

7. Stoica P., Babu R, Li J. Sparse Covariance-Based Estimation Method for Array Processing // IEEE Transactions on Signal Processing. — 2011. — Vol. 59. — № 2. — P. 629—638.

8. Plokhotnikov K. E. Vychislitel′nye metody. Teoriya i praktika v srede MATLAB : kurs lektsij. — M. : Goryachaya liniya — Telekom, 2009. — 496 s.

СВЕДЕНИЯ ОБ АВТОРАХ

Радченко Юрий Степанович. Профессор кафедры радиофизики. Доктор физико-математических наук, профессор.
Воронежский государственный университет.
E-mail: yuriy.radchenko@gmail.com
Россия, 394018, Воронеж, Университетская площадь, 1.

Овчинникова Татьяна Михайловна. Доцент кафедры электроники. Кандидат физико-математических наук, доцент.
Воронежский государственный университет.
E-mail: ya.otm2016@yandex.ru
Россия, 394018, Воронеж, Университетская площадь, 1.

Удалов Валерий Петрович. Доцент кафедры физики и радиоэлектроники. Кандидат физико-математических наук, доцент.
Воронежский институт МВД России.
E-mail: uvalery@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Radchenko Yury Stepanovich. Professor of the chair of Radiophysics. Doctor of Physical and Mathematical Sciences, Professor.
Voronezh State University.
E-mail: yuriy.radchenko@gmail.com
Work address: Russia, 394018, Voronezh, University Square, 1.

Ovchinnikova Tatyana Mikhailovna. Associate Professor of the chair of Electronics. Candidate of Physical and Mathematical Sciences, Associate Professor.
Voronezh State University.
E-mail: ya.otm2016@yandex.ru,
Work address: Russia, 394018, Voronezh, University Square, 1.

Udalov Valery Petrovich. Associate Professor of the chair of Physics and Radioelectronics. Candidate of Physical and Mathematical Sciences, Associate Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: uvalery@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: антенная решетка; корреляционная матрица поля; собственные значения и собственные вектора матрицы; точечный и протяженный источник; сигнал с неизвестным законом модуляции; оценка угла прихода волны.

Key words: antenna array; field correlation matrix; eigenvalues and eigenvectors of the matrix; point and extended source; signal with unknown modulation law; estimation of wave arrival angle.

УДК 621.391

А. Б. Антиликаторов, *кандидат технических наук, доцент*
С. П. Алексеенко, *кандидат физико-математических наук, доцент*
О. Н. Чирков

МЕТОДИКА СРАВНИТЕЛЬНОГО АНАЛИЗА ТОЧНОСТИ ВОССТАНОВЛЕНИЯ КАНАЛА СВЯЗИ В OFDM СИСТЕМАХ НА ОСНОВЕ АЛГОРИТМОВ ГЛУБОКОГО ОБУЧЕНИЯ

METHOD FOR COMPARATIVE ANALYSIS OF THE ACCURACY OF RECOVERY OF THE COMMUNICATION CHANNEL IN OFDM SYSTEMS BASED ON DEEP LEARNING ALGORITHMS

В работе рассматривается актуальная задача повышения точности восстановления частотной характеристики канала в современных системах беспроводной связи, использующих технологию ортогонального частотного разделения каналов (OFDM). Традиционные алгоритмы, такие как метод наименьших квадратов (LS) и метод минимальной среднеквадратической ошибки (MMSE), обладают существенными недостатками: низкой помехоустойчивостью в условиях малого отношения сигнал/шум (SNR) и необходимостью априорного знания статистических характеристик канала, что ограничивает их применение в нестационарных средах. Предложен новый алгоритм восстановления канала, основанный на методах глубокого обучения. Ключевой особенностью алгоритма является использование гибридной архитектуры нейронной сети, которая комбинирует свёрточные (CNN) и рекуррентные (LSTM) слои. CNN-модуль выполняет роль интеллектуального интерполятора в частотно-временной области, а LSTM-модуль учитывает временную корреляцию канала, вызванную доплеровскими эффектами, что позволяет эффективно подавлять шум и отслеживать быстрые замирания.

The paper addresses the pressing issue of improving the accuracy of channel frequency response estimation in modern wireless communication systems that use orthogonal frequency-division multiplexing (OFDM) technology. Traditional algorithms, such as the least squares (LS) method and the minimum mean-square error (MMSE) method, have significant drawbacks, including low noise immunity in low signal-to-noise ratio (SNR) environments and the need for a priori knowledge of the channel's statistical characteristics, which limits their applicability in non-stationary environments. To address these challenges, a new channel estimation algorithm based on deep learning techniques is proposed. The key feature of the algorithm is the use of a hybrid neural network architecture that combines convolutional (CNN) and recurrent (LSTM) layers. The CNN module acts as an intelligent interpolator in the frequency-time domain, while the LSTM module takes into account the temporal correlation of the channel caused by Doppler effects, which allows for effective noise suppression and fast fading tracking.

Введение. Ортогональное частотное разделение каналов (OFDM) зарекомендовало себя как ключевая технология физического уровня для построения эффективных

систем беспроводной связи [1]. OFDM используется как основа различных стандартов: сотовой связи 4G (LTE) и 5G (NR), а также Wi-Fi. Но эффективность данных систем существенно зависит от точности и оперативности восстановления состояния канала передачи данных.

Существует ряд традиционных методов восстановления канала: оценка пилот-сигналами, использование алгоритмов наименьших квадратов, использование минимальной среднеквадратичной ошибки [2—4]. Все они имеют ряд недостатков.

Например, использование алгоритмов наименьших квадратов очень простое в реализации, но существенно теряет точность в условиях низкого отношения сигнал/шум. Метод минимальной среднеквадратичной ошибки способен обеспечить достаточно высокую точность, но требует априорного знания статистических характеристик канала, а также связан с высокими вычислительными затратами, то есть в случае быстро меняющихся каналов данный метод является непригодным.

Сегодня для задачи точного восстановления канала связи широко применяют методы глубокого обучения (Deep Learning, DL) [5—7]. Такие методы позволяют отказаться от строгих статистических предположений о канале и обучаться его сложным, нелинейным моделям непосредственно на основе данных.

Нейронные сети способны выявлять скрытые зависимости и паттерны в принятых сигналах, обеспечивая более точную оценку по сравнению с классическими методами, особенно в сложных сценариях с нестационарными помехами и быстрыми замираниями. Именно поэтому разработка различных методик для восстановления канала для OFDM систем на основе глубокого обучения является актуальной научно-технической задачей.

Однако, хоть в последние годы изучение и разработка методик восстановления канала на основе глубокого обучения становится всё более актуальной, многие вопросы остаются открытыми и нерешёнными. Например, весьма важно сделать правильный выбор архитектуры нейронной сети для различных сценариев распространения сигнала, эффективно комбинировать пилотные символы и данные, а также анализировать вычислительную сложность и пригодность реализации в реальном времени.

Проблемой исследования является то, что существует потребность высокоточной, но при этом низкозатратной методики восстановления канала в условиях нестационарной помеховой обстановки и с ограниченными возможностями традиционных алгоритмических методов для решения этой задачи.

Основная часть. Разработка алгоритма. В OFDM системе передаваемый сигнал в частотной области X (известные пилот-символы) искажается каналом H и добавляется шум N. Принятый сигнал Y описывается как

$$Y = X \odot H + N, \quad (1)$$

где $\odot$ — поэлементное умножение.

Цель алгоритма: по принятому сигналу на пилотах Y_p и известным пилотам X_p восстановить полную матрицу канала H (как на пилотных, так и на данных поднесущих).

Данный алгоритм сочетает в себе свёрточные нейронные сети (CNN) для анализа локальных корреляций в частотно-временной области и рекуррентные сети (LSTM) для учёта временной зависимости канала.

Шаг 1: Сбор данных: генерируется большой датасет с различными сценариями канала. Каждый сэмпл данных представляет собой:

- `Y_pilot`: принятые пилот-символы в частотно-временной сетке OFDM (ресурсный блок);

- `H_ideal`: идеальная (эталонная) матрица коэффициентов канала, полученная, например, с помощью идеальных опорных сигналов.

На основе `Y_pilot` и известных `X_pilot` вычисляется наивная оценка канала на позициях пилотов: `H_naive_pilot = Y_pilot / X_pilot`.

Шаг 2: Архитектура состоит из двух основных блоков: CNN-модуль (рис. 1) (для частотно-временной интерполяции): этот модуль выполняет роль интеллектуального интерполятора, превосходящего линейные или полиномиальные методы.

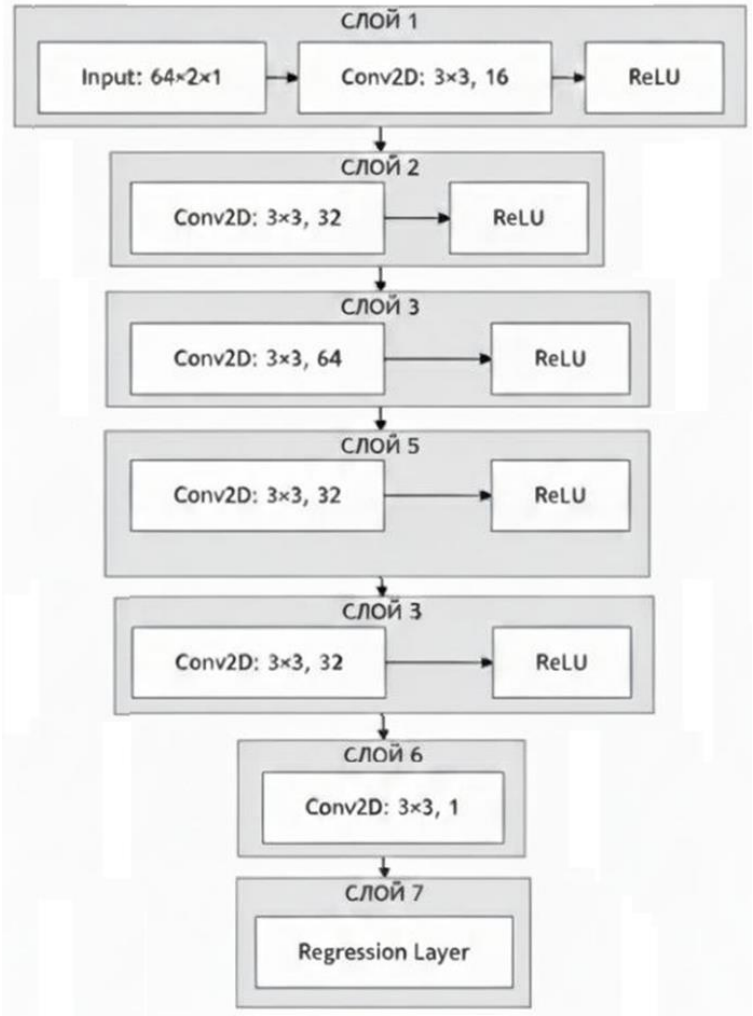


Рис. 1. Архитектура CNN

LSTM-модуль (для учёта временной когерентности): улавливает и запоминает временную динамику канала (доплеровские эффекты), что позволяет сглаживать оценку и уменьшать шум.

Шаг 3: Функция потерь: используется среднеквадратичная ошибка (MSE) между предсказанной нейросетью матрицей канала `H_est` и идеальной `H_ideal`.

Обучение: сеть обучается на большом наборе данных, пока функция потерь не перестанет уменьшаться на валидационной выборке.

Шаг 4: После обучения модель готова к работе:

1. Принимается OFDM символ (или блок символов).

2. Из него извлекаются пилот-символы `Y_pilot`.

3. Вычисляется `H_naive_pilot = Y_pilot / X_pilot`.

4. Эта разреженная матрица подаётся на вход обученной нейронной сети;

5. На выходе мгновенно получается полная, высококачественная оценка канала `H_est`.

Описание методики.

1) Блок инициализации параметров устанавливает основные параметры системы OFDM и процесса обучения нашей нейронной сети. Он определяет саму структуру OFDM системы (FFT и циклический префикс) и задает параметры модуляции и пилотных символов. Кроме этого, в нем мы устанавливаем параметры, влияющие на обучения нейронной сети, и определяем размеры datasets (набора данных для обучения и тестирования нейронной сети).

Создает структуру params со всеми необходимыми параметрами, задает позиции пилотных поднесущих для оценки канала и определяет диапазон SNR для анализа производительности.

2) Блок генерации dataset непосредственно генерирует набор данных для обучения и тестирования нашей нейронной сети. Он генерирует обучающие, валидационные и тестовые данные, которые подготавливаются для обучения и оценки выбранных моделей.

3) Функция генерации OFDM samples. В блоке происходит генерация отдельных OFDM символов, моделирование каналов связи с эффектом релеевского замирания и добавлением шума с различными SNR (отношением сигнал/шум). Также здесь происходит создание идеальной частотной характеристики канала.

Алгоритм работы следующий:

- генерация данных, а именно создание случайных битов и модуляция QPSK сигнала;

- формирование OFDM символа с распределением данных и пилотов по поднесущим;

- модуляция OFDM сигнала с использованием обратного быстрого преобразования Фурье (IFFT) и добавление циклического префикса;

- моделирование канала, генерируя импульсную характеристику канала Релея и добавляя гауссовский шум;

- демодуляция OFDM сигнала, удаляя циклический префикс и используя обратное быстрое преобразование Фурье.

4) Блок создания нейронных сетей.

Данный блок отвечает за создание архитектуры сверточной нейронной сети. Здесь мы настраиваем слои для задачи регрессии нашей сети и подготавливаем ее к последующему обучению.

5) Блок обучения моделей (рис. 2).

В данном блоке происходит обучение нейронной сети с использованием ранее сгенерированных и подготовленных данных. Также в данном коде реализован мониторинг процесса обучения нейронной сети, который позволяет следить за прогрессом и качеством усвоения данных за определенный промежуток времени. В конце происходит сохранение обученных моделей.



Рис. 2. Обучение CNN

За непосредственное обучение нейронной сети отвечает функция train_cnn_model. Для обучение используется алгоритм SGDM (Stochastic Gradient Descent with Momentum). Для предотвращения переобучения нейронной сети была предусмотрена валидация.

6) Блок оценки производительности.

Данный блок предназначен для сравнения между собой трех методов оценки канала: LS, MMSE и CNN. Здесь происходит расчет метрик MSE (среднеквадратичная ошибка) и BER (коэффициент битовых ошибок) для каждого метода.

За оценку метода LS отвечает функция evaluate_ls_simple. Вначале происходит извлечение пилотных поднесущих из принятого сообщения. Делением принятого пилотного символа на отправленный мы получаем оценку канала.

Далее происходит интерполяция на все поднесущие, благодаря которой из 12 пилотных оценок получается 64 оценки для всех поднесущих.

За оценку метода MMSE отвечает функция evaluate_mmse_simple. Вначале происходит получение LS оценок из предыдущего метода, в которые в последующем вносятся коррекции.

За оценку метода CNN отвечает функция evaluate_cnn_simple. Реализация данного метода основана на обработке входных данных и извлечении предсказаний сети.

Функция calculate_ber_simple предназначена для расчета BER после компенсации в канале. Далее происходит демодуляция QPSK сигнала и расчет самой BER.

7) Блок визуализации результатов.

За работоспособность этого блока отвечает функция plot_all_results_safe.

Данный блок предназначен для построения комплексных графиков, необходимых для анализа полученных результатов; сравнения методов по полученным значениям MSE и BER; визуализации характеристик канала; отображения процесса обучения.

Функциональная схема разработанной методики отражена на рисунке 3.

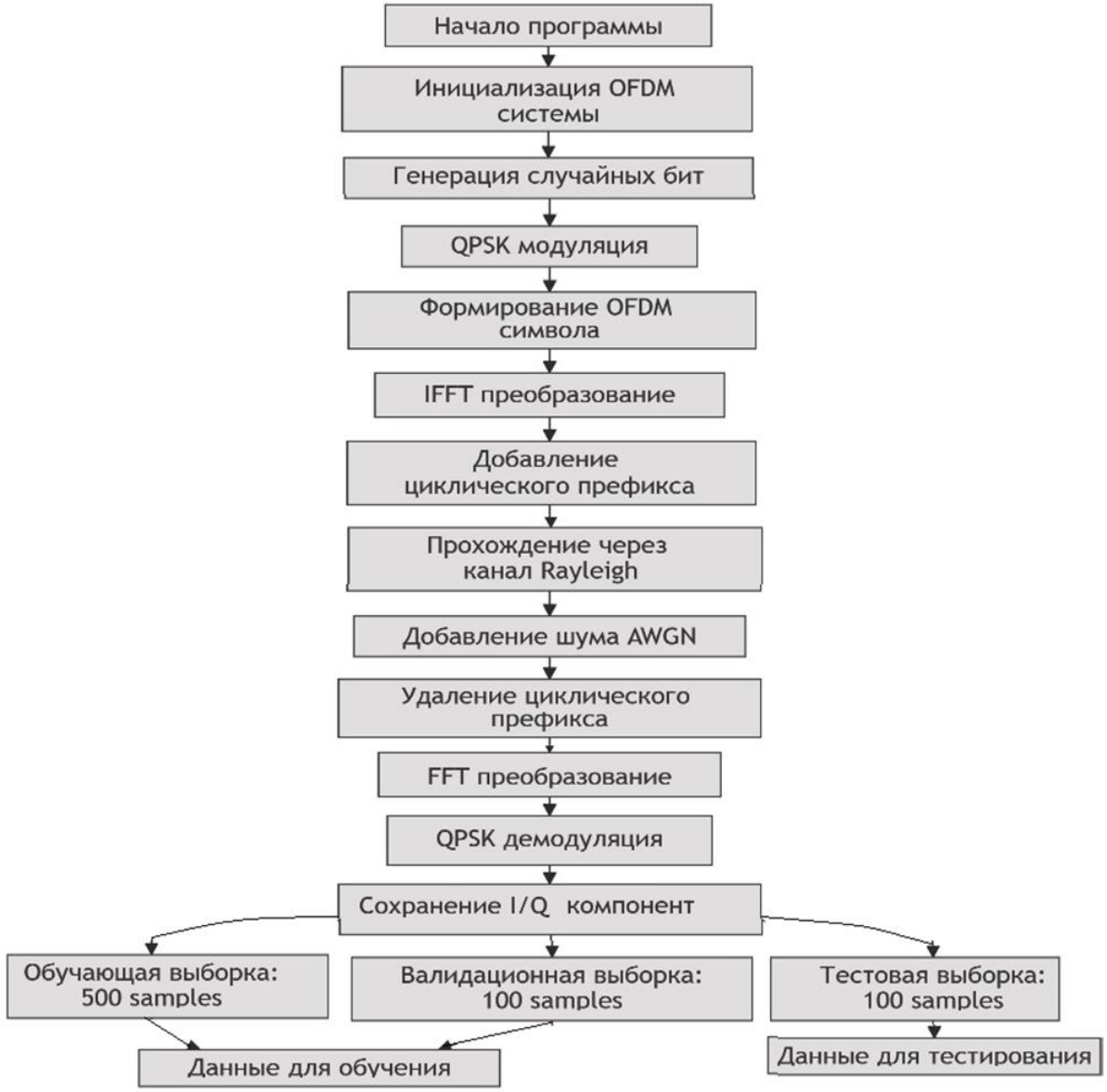


Рис. 3. Функциональная схема работы методики

Моделирование предложенного гибридного алгоритма оценки канала проводилось в среде MATLAB/Simulink для OFDM систем. Для всесторонней оценки производительности были сгенерированы наборы данных, имитирующие широкий диапазон условий распространения сигнала, включая различные профили замираний (Релея) и уровни отношения сигнал/шум (SNR). Производительность предложенного метода сравнивалась с классическими алгоритмами: методом наименьших квадратов (Least Squares, LS) и методом минимальной среднеквадратичной ошибки (Minimum Mean Square Error, MMSE).

Параметры OFDM системы соответствовали типичным конфигурациям: размер БПФ (FFT) — 64 поднесущих, из которых 12 использовались в качестве пилот-сигналов, циклический префикс длиной 16 отсчетов. Модуляция данных — QPSK. Нейронная сеть

обучалась на 50 000 OFDM символах, валидация проводилась на отдельной выборке из 10 000 символов. Оптимизатор — SGD с моментом (SGDM), функция потерь — среднеквадратичная ошибка (MSE). Кривая обучения (рис. 4) демонстрирует устойчивую сходимость модели: MSE на валидационной выборке монотонно уменьшалась, что указывает на отсутствие переобучения и способность сети обобщать скрытые зависимости в данных.

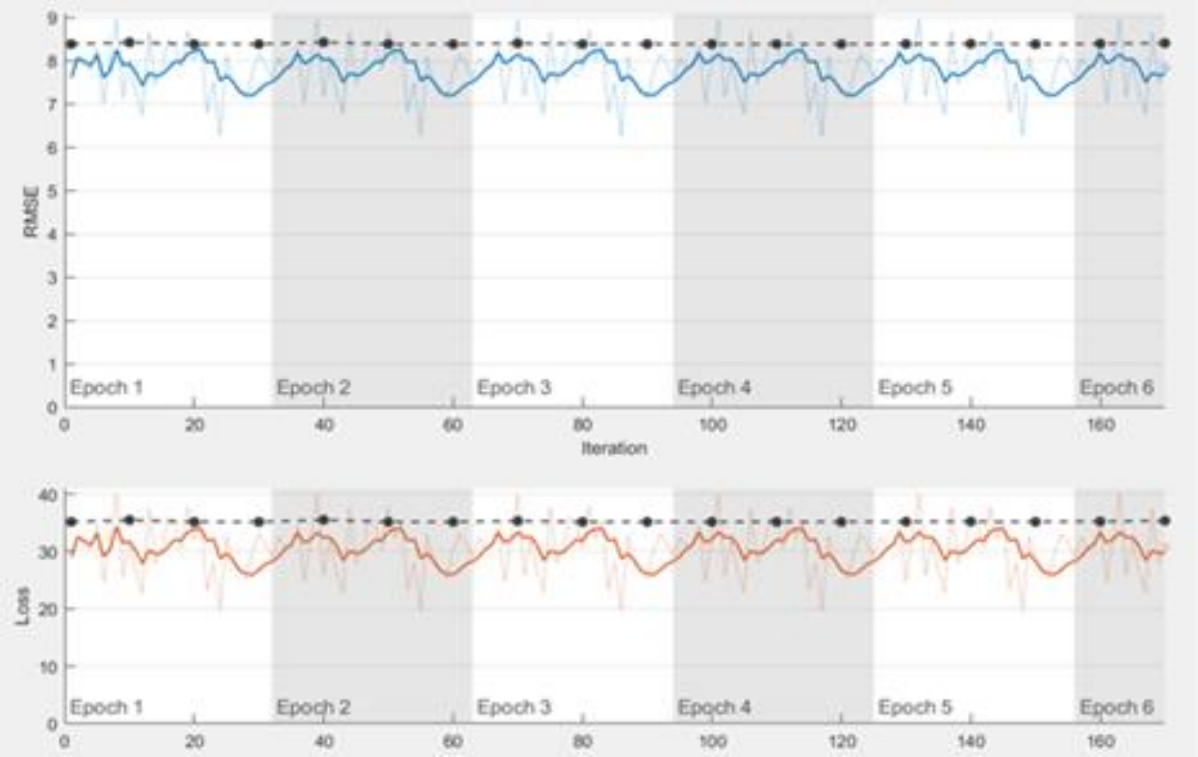


Рис. 4. Обучение CNN

На рисунке 5 приведены столбчатые диаграммы, показывающие сравнение методов LS, MMSE и CNN между собой по среднеквадратичной ошибке. Диаграммы дают визуальное представление, насколько хорошо различные методы могут восстановить искаженный шумом сигнал. Метод CNN имеет преимущество над MMSE в два раза и над LS в пять раз по эффективности восстановления искаженного сигнала.

На рисунке 6 отражены столбчатые диаграммы, показывающие сравнение методов LS, MMSE и CNN между собой по коэффициенту битовой ошибки. Диаграммы показывают, насколько часто различные методы принимают ошибочные биты. Предлагаемая методика, основанная на CNN, имеет преимущество над MMSE на 10% и над методом LS на 30% по правильности определения и восстановления ошибочных битов.

Результаты моделирования. Основной метрикой точности восстановления частотной характеристики канала (Channel Frequency Response, CFR) служила среднеквадратичная ошибка (MSE).

Сравнение методов по среднеквадратичной ошибке (рис. 5) наглядно демонстрирует преимущество предложенного метода. Алгоритм на основе CNN значительно ближе к эталонной (H_ideal), обеспечивая более гладкую и точную интерполяцию между пилот-

символами по сравнению с зашумленными результатами LS и даже сглаженной, но менее точной оценкой MMSE.

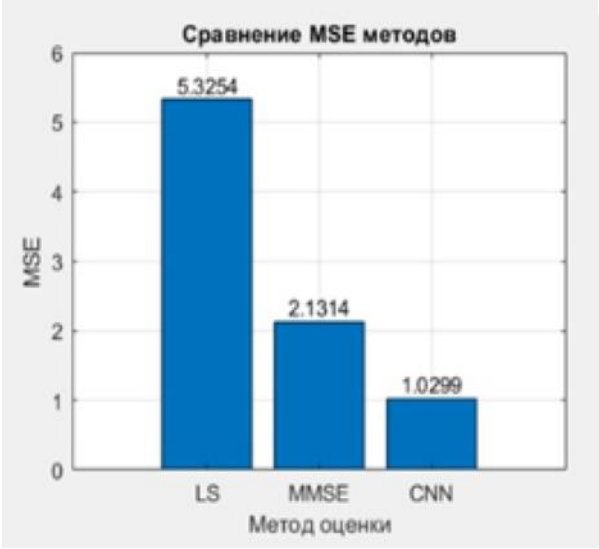


Рис. 5. Сравнение методов оценки по среднеквадратичной ошибке

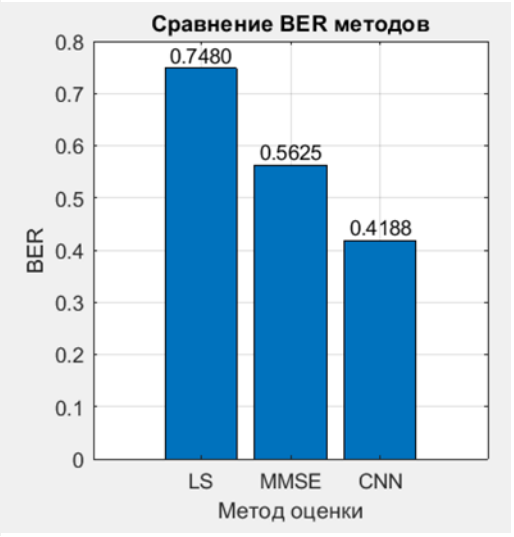


Рис. 6. Сравнение методов оценки по битовой ошибке

Результаты количественного сравнения MSE при фиксированном SNR = 20 дБ приведены на столбчатой диаграмме (рис. 6). Предложенный алгоритм на CNN превосходит метод MMSE в 2 раза, а метод LS — в 5 раз по точности оценки. Это подтверждает гипотезу о способности глубокой нейронной сети извлекать сложные пространственно-временные зависимости и эффективно подавлять шум, не требуя априорного знания статистики канала, необходимого для MMSE.

Для оценки влияния точности оценки канала на качество связи был рассчитан коэффициент битовых ошибок (Bit Error Rate, BER) после компенсации канала с использованием оценок, полученных разными методами.

Результаты (рис. 6) показывают, что использование CNN для оценки канала приводит к значительному снижению BER по сравнению с классическими методами. При том же уровне SNR (20 дБ) метод на основе глубокого обучения обеспечивает:

- снижение BER на 30% по сравнению с методом LS;
- снижение BER на 10% по сравнению с методом MMSE.

Это прямое следствие более точного восстановления коэффициентов канала, что позволяет приемнику корректнее демодулировать передаваемые символы данных.

В ходе тестирования было зафиксировано время, необходимое для оценки канала одного OFDM символа. Несмотря на то, что этап обучения CNN-LSTM является ресурсоемким, процесс инференции (вывода) выполняется за постоянное время и может быть эффективно оптимизирован. После развертывания обученной модели, затраты на получение оценки H_est сравнимы со сложностью прямого прохода через компактную нейросеть, что делает метод пригодным для систем квазиреального времени. В отличие от MMSE предложенный алгоритм не требует операций обращения матриц, зависящих от состояния канала в каждый момент времени.

Проведенное моделирование подтвердило высокую эффективность гибридного подхода CNN-LSTM для задачи оценки канала в OFDM системах. Основные результаты заключаются в следующем:

1. Алгоритм на основе глубокого обучения обеспечивает существенное (в 2—5 раз) снижение MSE оценки канала по сравнению с классическими методами LS и MMSE.

2. Более точная оценка напрямую улучшает показатель BER системы, снижая его на 10-30%.

3. Метод не требует априорного знания статистических характеристик канала (как MMSE) и демонстрирует устойчивость в условиях низкого SNR, где метод LS деградирует.

Практическая применимость: архитектура приведенной методики открывает путь к использованию глубокого обучения в задачах оценки канала для систем связи следующих поколений, работающих в нестационарных условиях с ограниченными пилот-сигналами.

Таким образом, предложенный подход успешно решает поставленную задачу повышения точности и эффективности оценки состояния канала в OFDM системах.

Заключение. В работе исследована актуальная задача повышения точности и эффективности оценки состояния канала в OFDM системах в условиях нестационарной помеховой обстановки и ограниченности традиционных алгоритмических методов. Для её решения был разработан и детально изучен гибридный алгоритм, основанный на методах глубокого обучения, который сочетает свёрточные (CNN) и рекуррентные (LSTM) нейронные сети.

Проведённое комплексное моделирование подтвердило ключевые преимущества предложенного подхода. В отличие от классического метода наименьших квадратов (LS), демонстрирующего высокую чувствительность к шуму, и метода минимальной среднеквадратичной ошибки (MMSE), требующего априорного знания статистики канала и обладающего высокой вычислительной сложностью, нейросетевой алгоритм обеспечивает принципиально иное качество работы.

Разработанный алгоритм оценки канала успешно решает поставленную проблему, предлагая высокоточную, адаптивную и практически реализуемую альтернативу традиционным методам. Полученные результаты открывают перспективы для дальнейших исследований, направленных на оптимизацию архитектуры сети для конкретных стандартов связи (например, массивный MIMO в 5G/6G), учёт более сложных видов помех и интеграцию алгоритма в аппаратные платформы программно-определяемых радиосистем (SDR). Внедрение подобных интеллектуальных методов оценки канала является важным шагом на пути к созданию более спектрально-эффективных и устойчивых систем беспроводной связи следующего поколения.

ЛИТЕРАТУРА

1. Чирков О. Н. Прямое формирование OFDM сигналов // Вестник Воронежского государственного технического университета. — 2012. — Т. 8. — № 5. — С. 54—56.

2. Пилотная оценка канала радиосвязи в MIMO-OFDM системах / О. Н. Чирков, М. А. Ромащенко, И. С. Бобылкин [и др.] // Труды международного симпозиума «Надежность и качество». — 2019. — Т. 2. — С. 87—90.

3. Методы помехоустойчивого обнаружения сигналов в многоантенных системах

MIMO с пространственным мультиплексированием / О. Н. Чирков, М. А. Ромащенко, И. С. Бобылкин [и др.] // Труды международного симпозиума «Надежность и качество». — 2019. — Т. 2. — С. 85—87.

4. Чирков О. Н. Актуальные подходы к оценке канала радиосвязи в системе подвижных абонентов с высокой скоростью перемещения // Вестник Воронежского государственного технического университета. — 2019. — Т. 15. — № 6. — С. 89—93. — DOI 10.25987/VSTU.2019.15.6.013.

5. Чирков О. Н., Пирогов А. А. Применение алгоритмов машинного обучения в задаче оценки беспроводного канала связи с OFDM // Вестник Воронежского государственного технического университета. — 2023. — Т. 19. — № 6. — С. 164—169. — DOI 10.36622/VSTU.2023.19.6.025.

6. Башкиров А. В., Чирков О. Н., Демихова А. С. Применение глубоких нейронных сетей для задачи оценки канала и обнаружения сигнала в системах с OFDM // Радиотехника. — 2025. — Т. 89. — № 7. — С. 10—14. — DOI 10.18127/j00338486-202507-02.

7. Чирков О. Н., Белецкая С. Ю. Повышение производительности приемника OFDM на основе сверточных нейронных сетей // Радиотехника. — 2025. — Т. 89. — № 7. — С. 73—77. — DOI 10.18127/j00338486-202507-14.

REFERENCES

1. Chirkov O. N. Pryamoe formirovanie OFDM signalov // Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. — 2012. — T. 8. — № 5. — S. 54—56.

2. Pilotnaya otsenka kanala radiosvyazi v MIMO-OFDM sistemakh / O. N. Chirkov, M. A. Romashchenko, I. S. Bobylkin [i dr.] // Trudy mezhdunarodnogo simpoziuma «Nadezhnost′ i kachestvo». — 2019. — T. 2. — S. 87—90.

3. Metody pomekhoustojchivogo obnaruzheniya signalov v mnogoantennykh sistemakh MIMO s prostranstvennym mul′tipleksirovaniem / O. N. Chirkov, M. A. Romashchenko, I. S. Bobylkin [i dr.] // Trudy mezhdunarodnogo simpoziuma «Nadezhnost′ i kachestvo». — 2019. — T. 2. — S. 85—87.

4. Chirkov O. N. Aktual′nye podkhody k otsenke kanala radiosvyazi v sisteme podvizhnykh abonentov s vysokoj skorost′yu peremeshcheniya // Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. — 2019. — T. 15. — № 6. — S. 89—93. — DOI 10.25987/VSTU.2019.15.6.013.

5. Chirkov O. N., Pirogov A. A. Primenenie algoritmov mashinnogo obucheniya v zadache otsenki besprovodnogo kanala svyazi s OFDM // Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. — 2023. — T. 19. — № 6. — S. 164—169. — DOI 10.36622/VSTU.2023.19.6.025.

6. Bashkirov A. V., Chirkov O. N., Demikhova A. S. Primenenie glubokikh nejronnykh setej dlya zadachi otsenki kanala i obnaruzheniya signala v sistemakh s OFDM // Radiotekhnika. — 2025. — T. 89. — № 7. — S. 10—14. — DOI 10.18127/j00338486-202507-02.

7. Chirkov O. N., Beletskaya S. Yu. Povyshenie proizvoditel′nosti priemnika OFDM na osnove svertochnykh nejronnykh setej // Radiotekhnika. — 2025. — T. 89. — № 7. — S. 73—77. — DOI 10.18127/j00338486-202507-14.

СВЕДЕНИЯ ОБ АВТОРАХ

Антиликаторов Александр Борисович. Доцент кафедры конструирования и производства радиоаппаратуры. Кандидат технических наук, доцент.

Воронежский государственный технический университет.
E-mail: antilikatorov63@mail.ru
Россия, 394026, Воронеж, Московский проспект, 14.

Алексеенко Сергей Павлович. Доцент кафедры информационной безопасности. Кандидат физико-математических наук, доцент.
Воронежский институт МВД России.
E-mail: aleks_serg@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Чирков Олег Николаевич. Старший преподаватель кафедры конструирования и производства радиоаппаратуры.
Воронежский государственный технический университет.
E-mail: chir_oleg@mail.ru
Россия, 394026, Воронеж, Московский проспект, 14.

Antilikatorov Aleksandr Borisovich. Associate Professor of the chair of Design and Production of Radio Equipment. Candidate of Technical Sciences, Associate Professor.
Voronezh State Technical University.
E-mail: antilikatorov63@mail.ru.
Work address: Russia, 394026, Voronezh, Moskovskiy Prospect, 14.

Alekseenko Sergey Pavlovich. Associate Professor of the chair of Information Security. Candidate of Sciences (Physics and Mathematics), Associate Professor.
Voronesh Institute of the Ministry of the Interior of Russia.
E-mail: aleks_serg@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Chirkov Oleg Nikolaevich. Senior lecturer of the chair Design and Production of Radio Equipment.
Voronezh State Technical University.
E-mail: chir_oleg@mail.ru
Work address: Russia, 394026, Voronezh, Moskovskiy Prospect, 14.

Ключевые слова: OFDM; оценка канала; глубокое обучение; беспроводные сети; битовая ошибка.

Key words: OFDM; channel estimation; deep learning; wireless networks; bit error.

УДК 621.396

ЮРИДИЧЕСКИЕ НАУКИ

В. В. Денисенко, *доктор юридических наук, профессор*

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ПУБЛИЧНОГО УПРАВЛЕНИЯ В СФЕРЕ МИГРАЦИИ: ПРАВОВЫЕ ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

DIGITAL TRANSFORMATION OF PUBLIC GOVERNANCE IN MIGRATION: LEGAL CHALLENGES AND PERSPECTIVES

В статье рассматриваются актуальные вопросы цифровой трансформации публичного управления в сфере миграции. Анализируется современное состояние правового регулирования цифровых миграционных процедур. Исследуются правовые проблемы использования биометрических данных в миграционном контроле, определяются основания и пределы сбора биометрической информации. Рассматриваются вопросы юридической силы решений, принимаемых автоматизированными системами, и гарантий защиты прав мигрантов при алгоритмическом управлении. Формулируются предложения по совершенствованию законодательства в сфере цифровизации миграционных процессов.

The article discusses topical issues of digital transformation of public administration in the field of migration. The current state of legal regulation of digital migration procedures is analyzed. The legal problems of using biometric data in migration control are investigated, the grounds and limits for collecting biometric information are determined. The issues of the legal force of decisions made by automated systems and guarantees of protecting the rights of migrants in algorithmic management are considered. Proposals are formulated to improve legislation in the field of digitalization of migration processes.

Введение. Современный этап развития российского государства характеризуется активным внедрением цифровых технологий в систему публичного управления [5. — С. 150—156; 6. — С. 4—16; 7. — С. 419—428]. Сфера миграции представляет собой один из наиболее динамично цифровизируемых сегментов государственного администрирования, что обусловлено ростом миграционных потоков, необходимостью повышения эффективности контроля и обеспечения национальной безопасности [8. — С. 118—129]. Однако стремительное технологическое развитие опережает формирование адекватной правовой базы, что порождает комплекс теоретических и практических проблем.

Актуальность исследования цифровой трансформации публичного управления в сфере миграции обусловлена противоречием между объективной потребностью в цифровизации миграционного управления и недостаточной разработанностью правовых механизмов, обеспечивающих баланс между эффективностью администрирования и защитой прав личности. Цифровая трансформация порождает новые правовые явления: электронные миграционные процедуры, автоматизированные системы принятия решений, биометрическую идентификацию, — которые требуют теоретического осмысления и нормативного закрепления.

Цифровизация миграционных процедур: правовое регулирование и проблемы. В рамках рассмотрения заявленной проблематики необходимо, на взгляд автора, проанализировать современное состояние правового регулирования цифровых миграционных процедур. Действующее законодательство Российской Федерации содержит ряд норм, регулирующих использование информационных технологий в сфере миграции. Базовыми актами являются Федеральный закон от 18.07.2006 № 109-ФЗ «О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации» [1], Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, инфор-

мационных технологиях и о защите информации» [2], Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [3].

Важным элементом цифровой инфраструктуры является Государственная информационная система миграционного учета (ГИСМУ) [1. — Ст. 10]. Данная система призвана обеспечить межведомственное взаимодействие, автоматизацию процедур миграционного учета, контроля за пребыванием иностранных граждан. Однако правовое регулирование функционирования ГИСМУ остается фрагментарным, отсутствуют детальные нормы, регламентирующие порядок обмена данными между ведомствами, ответственность за достоверность информации, процедуры исправления ошибок.

Существенной проблемой является терминологическая неопределенность. В законодательстве используются понятия «электронное заявление», «электронный документ», «автоматизированная обработка данных», однако их содержание применительно к миграционным процедурам не всегда раскрыто. Это создает риски разночтений в правоприменительной практике. Например, неясен правовой статус уведомлений, направленных через личные кабинеты: считаются ли они надлежащим образом доведенными до сведения мигранта, если он не имел технической возможности их получить.

Другой важной проблемой является доступность цифровых сервисов для различных категорий мигрантов. Не все иностранные граждане обладают необходимыми цифровыми компетенциями, доступом к интернету, техническими устройствами. Это создает риски дискриминации и нарушения принципа равенства перед законом. Законодательство должно предусматривать альтернативные способы получения государственных услуг, чтобы цифровизация не стала барьером для реализации прав.

Биометрическая идентификация в миграционном контроле: баланс безопасности и прав личности. Особое внимание в рамках исследования следует уделить правовым аспектам использования биометрических данных в миграционном управлении. Биометрическая идентификация (отпечатки пальцев, сканирование радужной оболочки глаза, распознавание лица) становится стандартом в международной практике миграционного контроля. В Российской Федерации использование биометрических данных регулируется положениями ст. 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Определено, что биометрические персональные данные — это «сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных…» (часть 1 статьи 11). При этом в части 2 статьи 11 закреплены исключения из общего правила, которыми определено, что «обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, обязательной государственной геномной регистрации, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму…, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации, о правовом положении иностранных граждан в Российской Федерации, о миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации…». Однако специальные нормы использования биометрических данных применительно к миграционной сфере отсутствуют.

Правовая проблема заключается в определении оснований и пределов сбора биометрических данных. С одной стороны — биометрия повышает эффективность контроля, способствует борьбе с незаконной миграцией, терроризмом. С другой — биометрические данные относятся к специальной категории персональных данных, их обработка требует повышенной защиты. Возникает вопрос о добровольности предоставления биометрических данных: может ли мигрант отказаться от дактилоскопической регистрации без негативных последствий для его правового статуса.

Действующее законодательство предусматривает обязательную дактилоскопическую регистрацию для отдельных категорий иностранных граждан, однако перечень таких категорий и правовые последствия отказа от регистрации определены недостаточно четко. Это создает риски произвольного применения мер принуждения.

Другой важной проблемой является хранение и защита биометрических данных. Неясны сроки хранения биометрической информации, порядок ее уничтожения после истечения срока пребывания мигранта, механизмы защиты от несанкционированного доступа. Утечка биометрических данных создает необратимые риски, так как биометрические параметры невозможно изменить, в отличие от пароля или пин-кода.

Сравнительно-правовой анализ показывает, что в Европейском союзе использование биомет-

рических данных в миграционной сфере регулируется Регламентом (ЕС) 2016/679 (General Data Protection Regulation) [4]. Для сравнения, в указанном регламенте под термином «биометрические данные» понимаются «персональные данные, возникающие в результате особой технической обработки, касающиеся физических, физиологических или поведенческих характеристик физического лица, которые предусматривают или подтверждают уникальную идентификацию указанного физического лица, например, изображение лица человека или дактилоскопические данные» (пункт 14 статьи 4).

Обратим внимание на положения, регламентирующие обработку особых категорий персональных данных, в соответствии с которыми «обработка персональных данных, раскрывающих расовое или этническое происхождение, политические взгляды, религиозные убеждения или философские воззрения, членство в профессиональном союзе, а также обработка генетических данных, биометрических данных для однозначной идентификации физического лица, данных, касающихся здоровья, половой жизни или сексуальной ориентации физического лица, должна быть запрещена» (пункт 1 статьи 9). В целом Регламент (ЕС) 2016/679 устанавливает строгие требования к обработке специальных категорий данных, включая биометрию. В Российской Федерации отсутствует аналогичный специализированный акт, регулирующий именно биометрические данные в миграционной сфере.

Автоматизированные системы принятия решений: правовые гарантии. В рамках изучения заявленной проблематики проанализируем правовые проблемы использования автоматизированных систем принятия решений в миграционном управлении. Искусственный интеллект и алгоритмические системы все чаще применяются для обработки заявлений, проверки документов, оценки рисков. Однако правовое регулирование данного процесса остается фрагментарным.

Ключевая проблема заключается в определении юридической силы решений, принятых автоматизированной системой. Может ли компьютерная программа самостоятельно отказать в выдаче разрешения, или решение всегда должно приниматься должностным лицом? Кто несет ответственность за ошибку алгоритма: разработчик системы, оператор данных или государственное ведомство?

Действующее законодательство не содержит четких ответов на эти вопросы. Административные регламенты предусматривают возможность использования информационных систем, однако не разграничивают функции системы и должностного лица. Это создает риски принятия необоснованных решений без человеческого контроля.

Другой важной проблемой является прозрачность алгоритмических решений. Мигрант, получивший отказ, имеет право на обжалование, но как он может оспорить решение, если не понимает, на каком основании алгоритм его принял? Принципы объяснимости и прозрачности искусственного интеллекта должны быть закреплены законодательно.

Сравнительный анализ показывает, что в Европейском союзе Регламент (ЕС) 2016/679 устанавливает право субъекта данных не подвергаться решению, основанному исключительно на автоматизированной обработке, включая профилирование. В Российской Федерации аналогичная норма отсутствует, что создает пробел в защите прав мигрантов.

Межведомственное электронное взаимодействие: проблемы координации. Важным аспектом цифровизации является межведомственное электронное взаимодействие. Эффективное миграционное управление требует координации действий МВД, МИД, ФСБ, Минцифры, Роспотребнадзора и других ведомств. Однако на практике возникают проблемы дублирования функций, несогласованности баз данных, технических несовместимостей информационных систем.

Правовая проблема заключается в отсутствии единого нормативного акта, регламентирующего межведомственное взаимодействие в цифровой среде. Каждое ведомство разрабатывает собственные регламенты, что приводит к фрагментарности регулирования. Необходима системная кодификация норм, устанавливающих порядок обмена данными, разграничение полномочий, ответственность за достоверность информации.

Другой проблемой является защита данных при межведомственной передаче. Не всегда ясно, какие именно данные могут передаваться между ведомствами, на каком основании, с какими гарантиями защиты. Это создает риски избыточного сбора информации и нарушения принципа минимизации персональных данных.

Перспективы гармонизации регулирования. Перспективы развития правового регулирования связаны с несколькими направлениями. Во-первых, необходима кодификация норм о цифровом миграционном управлении, возможно, в рамках специального федерального закона. Во-вторых, требуется детальное регулирование использования биометрических данных, включая основания сбора, сроки хранения, гарантии защиты. В-третьих, необходимо законодательное закрепление принципов использования искусственного интеллекта в миграционной сфере, включая требования к прозрачности, объяснимости, человеческому контролю. В-четвертых, требуется совершенствование норм о межведомственном взаимодействии, включая технические стандарты обмена данными.

Заключение. Проведенное исследование позволяет сформулировать следующие выводы, характеризующие состояние и перспективы правового регулирования цифровой трансформации публичного управления в сфере миграции.

Правовое регулирование цифровых миграционных процедур отличается значительной неопределённостью и фрагментарностью, что создает системные препятствия для эффективного функционирования информационных систем учета иностранных граждан. Отсутствие детальных норм, регламентирующих порядок электронного взаимодействия между ведомствами, правовой статус электронных документов и процедурные гарантии для участников миграционных процессов, приводит к разночтениям в правоприменительной практике и снижает предсказуемость административных процедур для мигрантов. Терминологическая неустойчивость в определении ключевых понятий цифровой среды («электронное заявление», «автоматизированная обработка», «цифровой профиль») препятствует формированию единого понятийного аппарата и затрудняет системное совершенствование законодательства.

Правовое регулирование использования биометрических данных в миграционном контроле характеризуется недостаточной специализацией и отсутствием четких оснований для сбора, хранения и уничтожения биометрической информации. Действующее законодательство не содержит дифференцированных норм, учитывающих специфику миграционной сферы, что создает риски избыточного сбора персональных данных и недостаточной защиты биометрической информации. Отсутствие законодательно закрепленных механизмов добровольного предоставления биометрических данных и чётких правовых последствий отказа от дактилоскопической регистрации порождает условия для произвольного применения мер принуждения и нарушает баланс между интересами безопасности и правами личности.

Юридическая сила решений, принимаемых автоматизированными системами в миграционной сфере, остается неопределенной, что создает правовую неопределенность в вопросах ответственности за ошибки алгоритмов и гарантий обжалования автоматизированных решений. Отсутствие законодательных требований к прозрачности, объяснимости и человеческому контролю за алгоритмическими процессами принятия решений снижает уровень процессуальных гарантий для мигрантов и создает риски принятия необоснованных административных актов без должного человеческого участия. Принципы «цифровой этики» и защиты прав личности в условиях алгоритмического управления требуют нормативного закрепления и имплементации в административные регламенты.

Межведомственное электронное взаимодействие в сфере миграционного управления осуществляется в условиях отсутствия единого нормативного акта, регламентирующего порядок обмена данными, разграничения полномочий и ответственности за достоверность информации. Фрагментарность регулирования, обусловленная ведомственной разрозненностью нормативных актов, приводит к дублированию функций, техническим несовместимостям информационных систем и рискам избыточного сбора персональных данных. Необходима системная кодификация норм, устанавливающих единые стандарты межведомственного взаимодействия в цифровой среде и обеспечивающих баланс между эффективностью управления и защитой прав личности.

Перспективы совершенствования правового регулирования цифровой трансформации миграционного управления связаны с разработкой комплексного нормативного акта о цифровом миграционном управлении, детальным регулированием использования биометрических данных, законодательным закреплением принципов использования искусственного интеллекта в миграционной сфере и совершенствованием норм о межведомственном электронном взаимодействии. Реализация данных направлений позволит обеспечить баланс между эффективностью государственного управления и защитой конституционных прав мигрантов в цифровой среде, создать правовую основу для дальнейшего технологического развития сферы миграции и повысить уровень доверия граждан к цифровым государственным сервисам.

ЛИТЕРАТУРА

1. О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации : Федеральный закон от 18.07.2006 № 109-ФЗ (с изменениями и дополнениями). — URL: https://base.garant.ru/12148419/

2. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (с изменениями и дополнениями). — URL: https://base.garant.ru/12148555/

3. О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (с изменениями и дополнениями). — URL: https://base.garant.ru/12148567/

4. Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении

таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных) (General Data Protection Regulation) (GDPR). — URL: https://base.garant.ru/71936226/

5. Ламзин Р. М. Цифровизация как приоритет трансформации публичного управления // Инновационная экономика: перспективы развития и совершенствования. — 2019. — № 5(39). — С. 150—156.

6. Василенко Л. А., Зотов В. В. Цифровизация публичного управления в России: риски, казусы, проблемы // Цифровая социология. — 2020. — Т. 3. — № 2. — С. 4—16.

7. Чаннов С. Е. Использование цифровых технологий в сфере публичного управления // Известия Саратовского университета. Новая серия. Серия : Экономика. Управление. Право. — 2021. — Т. 21. — Вып. 4. — С. 419—428.

8. Попова С. М. Цифровизация миграционной сферы в России: состояние и перспективы // Право и политика. — 2021. — № 9. — С. 118—129.

REFERENCES

1. O migratsionnom uchete inostrannykh grazhdan i lits bez grazhdanstva v Rossijskoj Federatsii : Federal′nyj zakon ot 18.07.2006 № 109-FZ (s izmeneniyami i dopolneniyami). — URL: https://base.garant.ru/12148419/

2. Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii : Federal′nyj zakon ot 27.07.2006 № 149-FZ (s izmeneniyami i dopolneniyami). — URL: https://base.garant.ru/12148555/

3. O personal′nykh dannykh : Federal′nyj zakon ot 27.07.2006 № 152-FZ (s izmeneniyami i dopolneniyami). — URL: https://base.garant.ru/12148567/

4. Reglament Evropejskogo Parlamenta i Soveta Evropejskogo Soyuza 2016/679 ot 27 aprelya 2016 g. o zashchite fizicheskikh lits pri obrabotke personal′nykh dannykh i o svobodnom obrashchenii takikh dannykh, a takzhe ob otmene Direktivy 95/46/ES (Obshchij Reglament o zashchite personal′nykh dannykh) (General Data Protection Regulation) (GDPR). — URL: https://base.garant.ru/71936226/

5. Lamzin R. M. Tsifrovizatsiya kak prioritet transformatsii publichnogo upravleniya // Innovatsionnaya ekonomika: perspektivy razvitiya i sovershenstvovaniya. — 2019. — № 5(39). — S. 150—156.

6. Vasilenko L. A., Zotov V. V. Tsifrovizatsiya publichnogo upravleniya v Rossii: riski, kazusy, problemy // Tsifrovaya sotsiologiya. — 2020. — T. 3. — № 2. — C. 4—16.

7. Channov S. E. Ispol′zovanie tsifrovykh tekhnologij v sfere publichnogo upravleniya // Izvestiya Saratovskogo universiteta. Novaya seriya. Seriya : Ekonomika. Upravlenie. Pravo. — 2021. — T. 21. — Vyp. 4. — C. 419—428.

8. Popova C. M. Tsifrovizatsiya migratsionnoj sfery v Rossii: sostoyanie i perspektivy // Pravo i politika. — 2021. — № 9. — S. 118—129.

СВЕДЕНИЯ ОБ АВТОРЕ

Денисенко Виктор Васильевич. Профессор кафедры конституционного, административного и гражданского права. Доктор юридических наук, профессор.

Краснодарский университет МВД России.

E-mail: profdenisenko@mail.ru

ORCID 0000-0003-4704-0774.

Россия, 350005, Краснодар, ул. Ярославская, 128.

Denisenko Viktor Vasilievich. Professor of the chair of Constitutional, Administrative and Civil Law. Doctor of Law, Professor.

Krasnodar University of the Ministry of the Interior of the Russia.

E-mail: profdenisenko@mail.ru

ORCID 0000-0003-4704-0774.

Work address: Russia, 350005, Krasnodar, Yaroslavskaya Str., 128.

Ключевые слова: цифровизация; публичное управление; миграция; электронное правительство; биометрические данные; административные процедуры; права человека; информационные системы.

Key words: digitalization; public administration; migration; e-government; biometric data; administrative procedures; human rights; information systems.

УДК 342.9:004

А. А. Насонов, *доктор юридических наук*

О ПЕРСПЕКТИВАХ РАЗВИТИЯ УГОЛОВНО-ПРОЦЕССУАЛЬНОГО ИНСТИТУТА СОГЛАСИЯ

ON THE PROSPECTS FOR THE DEVELOPMENT OF THE CRIMINAL PROCEDURE INSTITUTE OF CONSENT

В статье анализируется современное состояние уголовно-процессуального института согласия. Предлагаются пути его дальнейшего совершенствования. Обосновывается необходимость включения в указанный институт норм, регламентирующих общие вопросы согласования.

The article analyzes the current state of the criminal procedure institution of consent. It proposes ways to further improve this institution. The article substantiates the need to include norms regulating general issues of consent in this institution.

Согласие как правовое явление широко распространено в современном российском уголовном процессе, присутствуя во множестве его институтов в качестве средства, необходимого для их реализации. Пристальный интерес государства к вопросам согласия обусловлен стремлением к гармонизации уголовно-процессуальных отношений, обеспечению в них справедливого баланса между публичными и частными интересами, чего невозможно достигнуть без компромиссов [1. — С. 6—7; 2. — С. 75]. Именно согласование позволяет до разумного предела снизить конфликтность уголовно-процессуальных отношений.

К сожалению, далеко не всегда реализация уголовно-процессуального согласия является результативной. Несмотря на то что в определяемых законом ситуациях дача согласия юридически значима для уголовно-процессуальных отношений, правоприменитель указанное обстоятельство иногда игнорирует. Нередки также случаи, когда правоприменитель неправильно оценивает волеизъявление невластных участников уголовного судопроизводства, ошибочно воспринимая его за согласие.

Так, по одному из уголовных дел, рассматриваемых в г. Костроме, постановление приговора осуществлялось в особом порядке (гл. 40 УПК РФ). Выясняя отношение подсудимого И. к обвинению в совершении преступления, предусмотренного п. «в» ч. 3 ст. 158 УПК РФ, суд пришел к выводу о том, что И. соглашается с ним. При этом было проигнорировано заявление И. о несогласии с размером ущерба, причиненного совершением преступления. Вместе с тем именно это заявление смогло поколебать данное подсудимым согласие. Как указала кассационная инстанция, согласие лица с обвинением для перехода на особый порядок судебного разбирательства (гл. 40 УПК РФ) предполагает его согласие не только с фактическими обстоятельствами содеянного, формой вины, мотивами совершения деяния, юридической оценкой содеянного, но и с характером и размером вреда, причиненного деянием обвиняемого. Однако такого согласия получено не было. В результате приговор суда первой инстанции был отменен по жалобе осужденного И. [3], которая еще раз продемонстрировала несогласие заявителя с рассмотрением уголовного дела в порядке гл. 40 УПК РФ.

Несоблюдение требований согласования наблюдается не только в деятельности властных субъектов. Со стороны лиц, не обладающих властными полномочиями, также встречаются ошибки в указанной сфере. Особенно это касается адвокатов, которые не согласовывают свою позицию с позицией доверителя. В пользу сказанного свидетельствует следующий пример. Адвокат, оказывающий юридическую помощь К., осужденному приговором Ленинского районного суда г. Саранска Республики Мордовия от 07.04.2021 по п. «г» ч. 2 ст. 161, п. «г» ч. 3 ст. 158 УК РФ, не согласовал свою позицию с позицией К. Такая ситуация сложилась в суде апелляционной инстанции в результате изменения позиции К. Осужденный в суде вину признавал частично. Адвокат вопреки позиции осужденного просила лишь о смягчении наказания. Президиум Верховного Суда РФ пришел к выводу о том, что позиция адвоката прямо противоречила позиции защищаемого им лица. В результате апелляционное определение судебной коллегии по уголовным делам Верховного Суда Республики Мордовия от 24.06.2021 было отменено, а уголовное дело было передано на новое рассмотрение [4].

Ошибки в сфере согласования в приведенных случаях привели к серьезным последствиям — отмене приговоров. Эти последствия можно расценивать как уголовно-процессуальные санкции за допущенные в сфере согласования нарушения.

Однако негативное воздействие на правоприменительную деятельность оказывают не только ошибки, допускаемые на практике, но и невысокое качество правовой регламентации вопросов, относящихся к сфере согласования. И наоборот, высокое качество нормативной регламентации согласия и его реализации способно оказывать позитивное воздействие на эффективность правоприменительной деятельности. Иными словами, надлежащее состояние института согласия способно в определенной мере гарантировать качество правоприменения.

К сожалению, современное состояние указанного института далеко от идеального. Требуется принять ряд мер, позволяющих завершить его формирование. Наличие нормативного определения согласия и регулирование отдельных вопросов согласования на сегодняшний день не могут восполнить всех потребностей уголовно-процессуального института согласия. Необходим более надежный фундамент для данного правового образования. Он видится в создании правовых норм, регулирующих общие для всех видов согласия вопросы, и объединение этих норм в главу 17.1 «Согласие в уголовном судопроизводстве».

К числу таких вопросов следует отнести: круг субъектов, дающих согласие; правила дачи согласия; заявление обращения, содержащего просьбу дать согласие, и его рассмотрение; уведомление заинтересованных лиц о результатах рассмотрения обращения и разъяснение им права на их обжалование; обжалование решения, принятого в результате согласования.

Субъекты, уполномоченные давать согласие, в соответствии с действующим законодательством представлены как властными, так и невластными субъектами. Указанные субъекты могут быть как участниками уголовного судопроизводства, так и лицами, не являющимися таковыми. Например, к властным участникам уголовного судопроизводства, наделенным полномочием согласования, относятся руководители следственных органов, прокуроры. Руководитель следственного органа, например, дает согласие следователю на обращение в суд за избранием заключения под стражу. Аналогичное согласие дает прокурор дознавателю.

Согласие невластных субъектов также востребовано в уголовно-процессуальном пространстве. К данному виду согласия, например, относятся: согласие лиц, обладающих свидетельским иммунитетом, дать показания (ч. 2 ст. 11 УПК РФ); согласие проживающих в жилище лиц на его осмотр (ч. 1 ст. 12, п. 4 ч. 2 ст. 29, ч. 5 ст. 177 УПК РФ) и др.

В приведенных примерах согласие исходит от лиц, обладающих статусом участников уголовного судопроизводства. Однако уголовно-процессуальное значение может иметь и согласие, исходящее от лиц, не наделенных таким статусом. Например, согласие Государственной Думы, полученное на основании представления Генерального прокурора Российской Федерации, Председателю Следственного комитета Российской Федерации на возбуждение уголовного дела в отношении депутата Государственной Думы (п. 1 ч. 1 ст. 448 УПК РФ) и др.

Широкий круг лиц, наделенных правом согласовывать те или иные действия, решения, процедуры, нуждается в обобщении на уровне уголовно-процессуального закона. Для этого необходимо соответствующую информацию сосредоточить в отдельной статье, которую следует включить в гл. 17.1 УПК РФ.

Отдельного закрепления в указанной главе требуют и правила, предъявляемые к согласованию. Среди них такие очевидные правила, как добровольность, ясность и действительность согласия. Необходимость соблюдения первого признака согласия — добровольности — продиктована правилами, содержащимися в ст. 9 УПК РФ и выражающими суть принципа уважения чести и достоинства. Представляется, что унижениям не должны подвергаться не только участники уголовного судопроизводства, но и лица, не наделенные процессуальным статусом. Это значит, что принцип, предусмотренный в ст. 9 УПК РФ, должен толковаться расширительно и распространяться на всех, кто имеет касательство к уголовно-процессуальным отношениям.

Ясность согласия предполагает его четкое формулирование лицом, от которого оно исходит. Это позволяет избежать его двусмысленности и в определенной мере гарантировать правомерность согласия.

Действительность согласия означает его подлинность. Такое согласие не выдумано, оно настоящее.

Что касается оформления согласия, то в настоящее время для одних видов согласия допустима устная форма, для других — письменная. Думается, что приоритет должен отдаваться письменной форме согласия, поскольку с ее помощью доказать факт согласования гораздо легче. Учитывая постепенное проникновение цифровизации в уголовно-процессуальное пространство, расширение электронного документооборота, следует задуматься и над распространением согласия в

форме электронного документа, заверенного электронной подписью.

Соблюдение указанных форм (устной, письменной, электронной) в определенной мере гарантирует добровольность, ясность и действительность согласия. Кроме того, при таком подходе обоснованно исключается из числа согласия молчание.

Очевидно, что помощь в выборе формы выражения согласия невластному субъекту должен оказывать его адвокат, выполняющий различные роли в уголовном судопроизводстве (защитника, представителя, адвоката свидетеля). Адвокат также должен разъяснить невластному участнику уголовного судопроизводства как наличие у него права заявлять согласие в той или иной ситуации, его суть, так и последствия, к которым может привести реализация данного права. Такое участие адвоката в судьбе своего доверителя усилит защиту законных интересов последнего. В связи с этим было бы не лишним закрепление в главе 17.1 УПК РФ правила о том, что согласие лица, не являющегося должностным лицом, должно заявляться после проведения консультаций с адвокатом и в его присутствии.

Что касается властных участников уголовного судопроизводства, то их уголовно-процессуальная деятельность также подчиняется ряду общих правил, касающихся согласования. Представляется, что их обращение за получением согласия должно не только носить письменный характер, но и быть аргументированным. Заявитель из числа властных субъектов обязан обосновать необходимость выполнения процессуального действия, принятия решения, требующих согласования.

В главе 17.1 УПК РФ следует закрепить также следующие гарантии согласования у властного субъекта.

Поступившее обращение о согласовании действий, решений должно быть рассмотрено компетентным лицом в срок, указанный законом. Если такой срок в УПК РФ не предусмотрен, то руководствоваться следует разумным сроком.

По результатам рассмотрения обращения должно приниматься одно из следующих решений: 1) о даче согласия; 2) об отказе в даче согласия.

Лицо, принявшее по поступившему обращению решение, обязано уведомить о нем заявителя и разъяснить ему право обратиться за получением согласия повторно либо обжаловать принятое решение об отказе в даче согласия.

Если у заявителя возникнет желание обжаловать решение об отказе в даче ему согласия, например, на выполнение того или иного процессуального действия, то он вправе в течение суток после уведомления о таком отказе обратиться с жалобой к вышестоящему должностному лицу. Если заявителем выступал следователь, то ему необходимо предоставить возможность направить такую жалобу руководителю вышестоящего следственного органа. Последний обязан будет рассмотреть ее в течение трех дней со дня получения. Если для принятия решения данному лицу потребуется истребовать дополнительные материалы, то срок рассмотрения жалобы может быть увеличен до 10 суток. В любом случае о результатах рассмотрения жалобы должно быть сообщено следователю.

Описанные правила, детализирующие получение властными субъектами согласия у властных субъектов, в настоящее время в УПК РФ отсутствуют. Включение рекомендуемых новелл в УПК РФ и сосредоточение их в отдельной главе, посвященной согласию в уголовном судопроизводстве, позволит существенно укрепить фундамент уголовно-процессуального института согласия. По сути, существующий институт согласия будет достроен и приведен в полноценное состояние благодаря появлению в УПК РФ главы 17.1, сосредотачивающей в себе общие нормы получения согласия. Новый уровень правового регулирования уголовно-процессуального согласия создаст необходимые предпосылки для роста эффективности правоприменительной деятельности в соответствующей области.

ЛИТЕРАТУРА

1. Насонов А. А. Система частных интересов в российском уголовном процессе и роль категории «согласие» в обеспечении ее сбалансированности // Вестник Воронежского института МВД России. — 2022. — № 2. — С. 225—233.

2. Насонов А. А. Разумное соотношение публичных и частных интересов в уголовно-процессуальной сфере и роль категории «согласие» в его обеспечении // Общество и право. — 2022. — № 2(80). — С. 71—76.

3. Определение судебной коллегии по уголовным делам Второго кассационного суда общей юрисдикции от 19.11.2020 // Бюллетень Верховного Суда РФ. — 2023. — № 4. — С. 14—15.

4. Постановление Президиума Верховного Суда РФ от 26.042023 № 7-П23пр // Бюллетень Верховного Суда РФ. — 2024. — № 5. — С. 16—17.

REFERENCES

1. Nasonov A. A. Sistema chastnykh interesov v rossijskom ugolovnom protsesse i rol′ kategorii «soglasie» v obespechenii ee sbalansirovannosti // Vestnik Voronezhskogo instituta MVD Rossii. — 2022. — № 2. — S. 225—233.

2. Nasonov A. A. Razumnoe sootnoshenie publichnykh i chastnykh interesov v ugolovno-protsessual′noj sfere i rol′ kategorii «soglasie» v ego obespechenii // Obshchestvo i pravo. — 2022. — № 2(80). — S. 71—76.

3. Opredelenie sudebnoj kollegii po ugolovnym delam Vtorogo kassatsionnogo suda obshchej yurisdiktsii ot 19.11.2020 // Byulleten′ Verkhovnogo Suda RF. — 2023. — № 4. — S. 14—15.

4. Postanovlenie Prezidiuma Verkhovnogo Suda RF ot 26.042023 № 7-P23pr // Byulleten′ Verkhovnogo Suda RF. — 2024. — № 5. — S. 16—17.

СВЕДЕНИЯ ОБ АВТОРЕ

Насонов Александр Александрович. Старший преподаватель кафедры уголовного процесса. Доктор юридических наук.

Воронежский институт МВД России.

E-mail: tribalcrest@yandex.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Nasonov Alexander Alexandrovich. Senior lecturer of the chair of Criminal Proceeding. Doctor of Law.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: tribalcrest@yandex.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: уголовно-процессуальный институт согласия; участники уголовного судопроизводства; эффективность; добровольность; ясность.

Key words: criminal procedural institution of consent; participants in criminal proceedings; effectiveness; voluntariness; clarity.

УДК 343.1

И. А. Насонова, *доктор юридических наук, профессор*

ПРИНЦИП СВОБОДЫ ОЦЕНКИ ДОКАЗАТЕЛЬСТВ И ПРОБЛЕМЫ ЕГО ПРАВОВОЙ РЕГЛАМЕНТАЦИИ

THE PRINCIPLE OF FREEDOM OF EVIDENCE ASSESSMENT AND THE PROBLEMS OF ITS LEGAL REGULATION

В статье раскрывается сущность принципа свободы оценки доказательства, выявляются проблемы правовой регламентации, обосновываются меры, направленные на совершенствование действующего законодательства в соответствующей части. Приводятся аргументы в пользу расширения круга лиц, обязанных осуществлять собирание, проверку и оценку доказательств.

The article reveals the essence of the principle of freedom of evaluation of evidence, identifies the problems of legal regulation, and substantiates measures aimed at improving the current legislation in this area. The article also provides arguments in favor of expanding the range of individuals who are required to collect, verify, and evaluate evidence.

Свобода оценки доказательств в качестве принципа уголовного процесса впервые была закреплена в УПК РФ. Советское уголовно-процессуальное законодательство такого принципа не знало, несмотря на то что оценка доказательств занимала центральное место в доказательственной деятельности и той эпохи. Появление в уголовном судопроизводстве принципа свободы оценки доказательств подтверждало не только важность соответствующего участка доказывания, но и означало, что прохождение его должно подчиняться определенным правилам. Необходимость их соблюдения вызвана потребностью в создании надежных гарантий для качественного осуществления уголовно-процессуального доказывания, которая по праву относится к ключевым видам деятельности в уголовном судопроизводстве. Учитывая, что обязанность доказывания, в том числе и обязанность по осуществлению оценки доказательств, возлагается не на одного, а на ряд субъектов, она становится масштабной проблемой, на которую законодатель не мог не реагировать. Кроме того, нельзя также не учитывать существование определенного круга лиц, непосредственно не обязанных осуществлять оценку доказательств, но имеющих определенное касательство к данному виду деятельности. Речь идет о тех участниках уголовного судопроизводства, которые либо обязаны участвовать в доказывании в силу осуществляемой ими на профессиональной основе своей уголовно-процессуальной функции (например, адвокат-защитник, адвокат-представитель), либо вправе осуществлять доказывание по своему усмотрению (например, обвиняемый, подозреваемый, потерпевший и т. д.). При этом успешность участия этих лиц в доказывании напрямую зависит от соблюдения ими универсальных правил реализации данного вида деятельности. Данное обстоятельство повышает ценность оценки доказательств в отечественном уголовном судопроизводстве.

За претворение принципа свободы оценки доказательств в жизнь главным образом отвечают властные участники уголовного судопроизводства. Их ответственность полностью согласуется с возложенной на них обязанностью оценивать доказательства. Об этой обязанности говорится в ч. 1 ст. 17 УПК РФ. Согласно этой норме обязанность оценивать доказательства возлагается на следующих субъектов: судью, присяжных заседателей, прокурора, следователя, дознавателя. Представляется, что приведенный в ч. 1 ст. 17 УПК РФ перечень лиц, несущих соответствующую обязанность, нельзя признать полным. Учитывая, что полномочиями следователя может обладать руководитель следственного органа (ч. 2 ст. 39 УПК РФ), а полномочиями дознавателя — начальник подразделения дознания (ч. 2 ст. 40.1 УПК РФ), эти участники-руководители также должны быть включен в перечень субъектов оценки доказательств, содержащийся в ч. 1 ст. 17 УПК РФ.

Соответствующему дополнению подлежат также ч. 2 и ч. 3 ст. 88 УПК РФ, посвященной вопросам оценки доказательств. К числу лиц, признающих доказательство недопустимыми, наряду с теми, кто уже указан в нормах, содержащихся в ст. 88 УПК РФ, следует относить руководителя следственного органа и начальника подразделения дознания. В связи с этим указанная статья нуждается в дополнении.

Учитывая, что оценка доказательств лишь звено в общей цепи уголовно-процессуального доказывания, взаимодействующее с другими звеньями указанного процесса (собиранием и проверкой доказательств), необходимы также коррективы уголовно-процессуальных норм, закрепляющих вопросы собирания и проверки доказательств (ч. 1 ст. 86, ст. 87 УПК РФ). Эти коррективы должны быть связаны с включением руководителя следственного органа и начальника подразделения дознания в число субъектов собирания доказательств и субъектов проверки доказательств.

Руководитель следственного органа, начальник подразделения дознания, как и другие властные участники уголовного судопроизводства, указанные в упомянутых статьях, осуществляя доказывание по уголовному делу, руководствуются определенными критериями. Особенно четко они сформулированы законодателем применительно к оценке доказательств. Последняя осуществляется по внутреннему убеждению указанных субъектов, формируемому на основе совокупности имеющихся по уголовному делу доказательств, закона и совести (ч. 1 ст. 17 УПК РФ). Последний критерий, имеющий нравственное содержание, впервые включен в уголовно-процессуальное законодательство в 2001 году. Тем самым был взят курс на справедливость уголовного судопроизводства. И хотя принцип справедливости непосредственно в УПК РФ не был закреплен, многое указывает на его существование в уголовном судопроизводстве. Это не случайно, поскольку запрос на этот принцип формировался долгое время и в определенной мере был обусловлен противоречивостью проводимых в уголовно-процессуальной сфере реформ. Все это дает повод отдельным авторам не без основания считать справедливость составляющей системы принципов уголовного судопроизводства [1. — С. 8].

Совесть, наряду с другими критериями (совокупностью имеющихся по уголовному делу доказательств и законом), позволяет субъекту доказывания сформировать внутреннее убеждение относительно соответствия доказательств требованиям относимости, допустимости, достаточности и достоверности. Благодаря мыслительной деятельности соответствующие субъекты из имеющейся совокупности доказательств обнаруживают те, которые, во-первых, соответствуют действительности и в этом смысле являются достоверными; во-вторых, позволяют устанавливать значимые для дела обстоятельства, соответствующие требованиям закона (получены из источника, предусмотренного законом; способом, предусмотренным законом; имеют надлежащую фиксацию), то есть представляют собой допустимые доказательства. Допустимость — одно из важнейших свойств доказательств, которое начало постепенно формироваться в далеком историческом прошлом [2. — С. 98] и продолжает оставаться востребованным в наши дни.

В помощь субъектам доказывания законодатель проработал вопрос о допустимости доказательств на нормативном уровне. Был определен круг доказательств, не отвечающих требованию допустимости. Правда, сделано это в обобщенном варианте, допускающем возможность расширительно толковать перечень, содержащийся в ч. 2 ст. 75 УПК РФ. В литературе такой способ регулирования вопроса о недопустимых доказательствах нередко подвергается критике. Указывается на то, что приведенный перечень должен быть более подробным, в чем особенно нуждаются субъекты, применяющие соответствующие уголовно-процессуальные нормы [3. — С. 130—131; 4. — С. 182; 5. — с. 229].

К сожалению, признание доказательства недопустимым на практике встречается достаточно часто. В особенности такое признание имеет место со стороны суда. В связи с этим следует привести следующие примеры. Они показывают, что недопустимость доказательств нередко является следствием нарушения прав подозреваемого, обвиняемого, подсудимого на защиту. Причем нарушения допускаются властными субъектами, которые наоборот должны создавать условия для их реализации [6. — С. 237; 7. — С. 90].

В частности, первый кассационный суд общей юрисдикции признал недопустимым доказательством объяснения В., поскольку они были даны в отсутствие защитника. Кроме того, ему не только не было разъяснено право пользоваться услугами защитника, но и другие принадлежащие ему права. В результате приговор суда первой инстанции, в качестве которой выступил Промышленный районный суд г. Курска, и апелляционное определение Курского областного суда в отношении В. были изменены [8].

Седьмой кассационный суд общей юрисдикции изменил приговор Чебаркульского городского суда Челябинской области от 01.04.2024 и апелляционное определение Челябинского областного суда от 12.07.2024 в отношении К. И., осужденной по ч. 4 ст. 160 УК РФ. Кассационная инстанция установила, что показания обвиняемой были даны в ходе досудебного производства по уголовному делу в отсутствие защитника. Вследствие этого из приговора была исключена ссылка суда на показания осужденной, данные ею при осмотре места происшествия, в части хищения денежных средств в сумме около 1,2 миллиона руб-

лей (т. 1. — Л. д. 157—163). Эти пояснения осужденная давала в отсутствие адвоката и не подтвердила в судебном заседании, что в силу ст. 75 УПК РФ не может быть признано в этой части допустимым доказательством [9].

Приведенные примеры показывают, что необъективному подходу властного субъекта, обязанного в силу закона осуществлять оценку доказательств, в суде ставится надежная преграда. Это полностью согласуется с одним из правил, работающих в рамках принципа свободы оценки доказательства. Согласно этому правилу никакие доказательства не имеют заранее установленной силы (ч. 2 ст. 17 УПК РФ). Однако оно не всегда соблюдается. И речь идет не столько о допускаемых в ходе уголовно-процессуального доказывания нарушениях, сколько о предусмотренных законодателем исключениях из принципа, предусмотренного статьей 17 УПК РФ. Одно из таких исключений связано со снижением стандартов доказывания в ходе сокращенной формы дознания (например, возможность не проверять доказательства в определенных случаях) [10. — С. 49]. Другое исключение предусмотрено в ч. 5 ст. 316 УПК РФ. Из нормы, содержащейся в этой статье, видно, что судья не проводит в общем порядке исследование и оценку доказательств. Тем самым, отмечает Ф. Ф. Зарипов, законодатель игнорирует в производстве, предусмотренном главой 40 УПК РФ, доминантную норму, содержащуюся в ч. 5 ст. 316 УПК РФ [11. — С. 333]. Действительно, анализ указанных норм позволяет говорить о том, что принцип свободы оценки доказательств не работает в полную силу в особом порядке судебного разбирательства. Судья лишь вправе исследовать обстоятельства, характеризующие личность подсудимого, и обстоятельства, смягчающие и отягчающие наказание. Однако иное положение дел в оценке доказательств судом применительно к производству, предусмотренному главой 40 УПК РФ, сведет на нет преимущества упрощенного производства, позволяющего ускорить движение уголовного дела и обеспечить процессуальную экономию. Поэтому упомянутое выше исключение из принципа свободы оценки доказательств неизбежно.

Исключение из общего правила, сформулированного в рамках того или иного принципа уголовного судопроизводства, становится все более распространенным явлением, несмотря на предупреждение ученых о том, что отступление от принципа уголовного судопроизводства в конце концов способно привести к разрушению уголовно-процессуальной системы [1. — С. 8].

Связано это с тем, что с помощью исключений учитываются самые разнообразные факторы. Тем самым достигается соответствие между принципом и определенными процедурами, наполняющими уголовное судопроизводство и соответствующими современным реалиям.

В заключение следует отметить, что содержание принципа свободы оценки доказательств передается с помощью общего правила, из которого существует исключение. Правовая регламентация общего правила-принципа нуждается в коррекции. Последняя должна коснуться круга лиц, обязанных осуществлять оценку доказательств в уголовном судопроизводстве России. Круг таких лиц нуждается в расширении за счет руководителя следственного органа и начальника подразделения дознания.

ЛИТЕРАТУРА

1. Васильев О. Л. Теоретические аспекты действия принципа справедливости на досудебных стадиях российского уголовного процесса : автореф. дис. … д-ра юрид. наук. — М., 2018. — 45 с.

2. Колосович М. С. Зарождение процедуры розыска и формирования доказательств в праве Древней Руси // Вестник Волгоградской академии МВД России. — 2015. — № 3(34). — С. 95—99.

3. Кокорев Л. Д., Кузнецов Н. П. Уголовный процесс: доказательства и доказывание. — Воронеж : Издательство Воронежского университета, 1995. — 272 с.

4. Халимоненко С. С. Запрет в уголовно-процессуальном праве России : дис. … канд. юрид. наук. — Воронеж, 2021. — С. 368—369.

5. Насонов А. А. Применение согласования в ходе доказывания по уголовному делу на предварительном расследовании // Вестник Воронежского института МВД России. — 2023. — № 1. — С. 226—230.

6. Цинова М. В., Насонов А. А. О субъектах обеспечения подозреваемому и обвиняемому права на защиту и некоторых особенностях их процессуальных возможностей при производстве дознания в сокращенной форме // Общество и право. — 2015. — № 4(54). — С. 236—241.

7. Насонова И. А., Насонов А. А. Руководитель следственного органа и начальник подразделения дознания как субъекты обеспечения подозреваемому и обвиняемому права на защиту // Вестник Воронежского института ФСИН России. — 2012. — № 2. — С. 90—92.

8. Определение первого кассационного суда общей юрисдикции от 06.07.2021 по делу № 77-2299/2021 // СПС «КонсультантПлюс».

9. Кассационное определение седьмого кассационного суда общей юрисдикции от 31.03.2025 № 77-967/2025 // СПС «КонсультантПлюс».

10. Насонова И. А., Зотова М. В. Протокольная форма досудебной подготовки материалов как базовая модель для дознания в сокращенной форме // Вестник Воронежского института МВД России. — 2017. — № 2. — С. 47—53.

11. Зарипов Ф. Ф. Гуманистическое, человеколюбивое содержание принципов российского уголовного судопроизводства // Охрана прав и свобод человека и гражданина в сфере уголовного судопроизводства : материалы международной научно-практической конференции. — М. : Московская академия экономики и права ; Союз криминалистов и криминологов, 2016. — С. 328—334.

REFERENCES

1. Vasil′ev O. L. Teoreticheskie aspekty dejstviya printsipa spravedlivosti na dosudebnykh stadiyakh rossijskogo ugolovnogo protsessa : avtoref. dis. … d-ra yurid. nauk. — M., 2018. — 45 s.

2. Kolosovich M. S. Zarozhdenie protsedury rozyska i formirovaniya dokazatel′stv v prave Drevnej Rusi // Vestnik Volgogradskoj akademii MVD Rossii. — 2015. — № 3(34). — S. 95—99.

3. Kokorev L. D., Kuznetsov N. P. Ugolovnyj protsess: dokazatel′stva i dokazyvanie. — Voronezh : Izdatel′stvo Voronezhskogo universiteta, 1995. — 272 s.

4. Khalimonenko S. S. Zapret v ugolovno-protsessual′nom prave Rossii : dis. … kand. yurid. nauk. — Voronezh, 2021. — S. 368—369.

5. Nasonov A. A. Primenenie soglasovaniya v khode dokazyvaniya po ugolovnomu delu na predvaritel′nom rassledovanii // Vestnik Voronezhskogo instituta MVD Rossii. — 2023. — № 1. — S. 226—230.

6. Tsinova M. V., Nasonov A. A. O sub″ektakh obespecheniya podozrevaemomu i obvinyaemomu prava na zashchitu i nekotorykh osobennostyakh ikh protsessual′nykh vozmozhnostej pri proizvodstve doznaniya v sokrashchennoj forme // Obshchestvo i pravo. — 2015. — № 4(54). — S. 236—241.

7. Nasonova I. A., Nasonov A. A. Rukovoditel′ sledstvennogo organa i nachal′nik podrazdeleniya doznaniya kak sub″ekty obespecheniya podozrevaemomu i obvinyaemomu prava na zashchitu // Vestnik Voronezhskogo instituta FSIN Rossii. — 2012. — № 2. — S. 90—92.

8. Opredelenie pervogo kassatsionnogo suda obshchej yurisdiktsii ot 06.07.2021 po delu № 77-2299/2021 // SPS «Konsul′tantPlyus».

9. Kassatsionnoe opredelenie sed′mogo kassatsionnogo suda obshchej yurisdiktsii ot 31.03.2025 № 77-967/2025 // SPS «Konsul′tantPlyus».

10. Nasonova I. A., Zotova M. V. Protokol′naya forma dosudebnoj podgotovki materialov kak bazovaya model′ dlya doznaniya v sokrashchennoj forme // Vestnik Voronezhskogo instituta MVD Rossii. — 2017. — № 2. — S. 47—53.

11. Zaripov F. F. Gumanisticheskoe, chelovekolyubivoe soderzhanie printsipov rossijskogo ugolovnogo sudoproizvodstva // Okhrana prav i svobod cheloveka i grazhdanina v sfere ugolovnogo sudoproizvodstva : materialy mezhdunarodnoj nauchno-prakticheskoj konferentsii. — M. : Moskovskaya akademiya ekonomiki i prava ; Soyuz kriminalistov i kriminologov, 2016. — S. 328—334.

СВЕДЕНИЯ ОБ АВТОРЕ

Насонова Ирина Александровна. Профессор кафедры уголовного процесса. Доктор юридических наук, профессор.
Воронежский институт МВД России.
E-mail: nasonova-amelina@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Nasonova Irina Alexandrovna. Professor of the chair of Criminal Proceding. Doctor of Law, Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: nasonova-amelina@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: оценка доказательств; руководитель следственного органа; начальник подразделения дознания; следователь; дознаватель; суд.
Key words: evaluation of evidence; head of the investigative body; head of the investigation unit; investigator; interrogator; court.

УДК 343.1

У. Н. Ахмедов, *кандидат юридических наук, доцент*

ОСОБЕННОСТИ ПРИОБРЕТЕНИЯ НЕСОВЕРШЕННОЛЕТНИМИ УГОЛОВНО-ПРОЦЕССУАЛЬНОГО СТАТУСА, ЕГО ИЗМЕНЕНИЕ И ДИНАМИКА В РОССИЙСКОМ УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

PECULIARITIES OF GRANTING MINORS THE CRIMINAL PROCEDURAL STATUS, ITS CHANGE AND DYNAMICS IN RUSSIAN CRIMINAL PROCEEDINGS

В статье исследуются специфические особенности формирования и реализации уголовно-процессуального статуса несовершеннолетнего в российском уголовном судопроизводстве. Анализируются нормы Уголовно-процессуального кодекса РФ [1], закрепляющие дополнительные гарантии и права для несовершеннолетних подозреваемых, обвиняемых и потерпевших. Рассматривается влияние возрастного фактора на процессуальное положение несовершеннолетнего. Особое внимание уделяется дуализму статуса несовершеннолетних, сочетающего в себе черты общего процессуального статуса и специальных положений, призванных обеспечить их повышенную защиту. Исследуется также динамика уголовно-процессуального статуса несовершеннолетних, возникающая в связи с изменением его возраста в ходе уголовного судопроизводства. Анализируются правовые и практические проблемы, связанные с «переходом» лица из категории несовершеннолетнего в категорию совершеннолетнего после достижения 18-летнего возраста в досудебных и судебных стадиях.

The article examines the specific features of the formation and implementation of the criminal procedural status of minors in Russian criminal proceedings. The article analyzes the norms of the Criminal Procedure Code of the Russian Federation, which establish additional guarantees and rights for juvenile suspects, accused and victims. The influence of the age-related psychophysiological factor on the procedural situation is considered. Special attention is paid to the dualism of the status of a minor, which combines the features of a general procedural status and special provisions designed to provide increased protection. The article also examines the dynamics of the criminal procedural status of a minor, which arises in connection with a change in his age during criminal proceedings. The article analyzes the legal and practical problems associated with the «transition» of a person from the category of a minor to the category of an adult after reaching the age of 18 during the investigation or trial.

Правовой механизм осуществления правосудия в отношении несовершеннолетних представляет собой одну из наиболее социально-значимых и динамично развивающихся областей уголовно-процессуального права. Его формирование обусловлено признанием специфики детства и юношества, а также необходимости особого подхода к лицам, не достигшим восемнадцатилетнего возраста, в силу их психологической и социальной несформированности и потребности в повышенной правовой защите. Наделение несовершеннолетнего уголовно-процессуальным статусом — это не простое распространение общих норм на особую категорию субъектов, а сложный многоуровневый процесс, предполагающий предоставление дополнительных прав и установление повышенных гарантий их реализации.

Целью настоящей статьи является комплексный анализ особенностей наделения несовершеннолетних уголовно-процессуальным статусом в Российской Федерации, выявление системных характеристик данного процесса и его соответствия международным правовым стандартам. Для этого необходимо выделить и проанализировать особенности наделения уголовно-процессуальным статусом несовершеннолетнего. По нашему мнению, к ним, в первую очередь, могут быть отнесены следующие:

1. Дуализм уголовно-процессуального статуса несовершеннолетнего.

Несовершеннолетний, вовлекаемый в уголовное судопроизводство в качестве подозреваемого, обвиняемого (подсудимого), а также потерпевшего обладает «дуалистичным статусом». С одной стороны, он наделяется всеми основными

правами и обязанностями, присущими соответствующему участнику процесса (например, правом на защиту, правом давать показания). С другой стороны, в силу возраста к общему статусу добавляется комплекс специальных норм, образующих «особый процессуальный режим» (глава 50 УПК РФ).

Этот режим базируется на двух фундаментальных принципах:

- Принцип повышенной юридической охраны (протекционизма). Государство принимает на себя обязанность обеспечить несовершеннолетнему максимальную защиту его прав и законных интересов, компенсируя возрастную недееспособность или ограниченную дееспособность.

- Принцип индивидуализации производства по уголовному делу. Требуется обязательное установление условий жизни и воспитания, уровня психического развития и иных особенностей личности несовершеннолетнего, влияющих на степень осознания своих действий и способность к защите в ходе уголовного судопроизводства. Некоторые исследователи верно отмечают, что при производстве по делам о преступлениях в отношении несовершеннолетних особое значение приобретает индивидуализация уголовного процесса, которая наиболее выражена в особом порядке судопроизводства [2].

2. Специфические элементы статуса несовершеннолетнего подозреваемого или обвиняемого.

Особенности наделения процессуально-правовым статусом несовершеннолетнего проявляются в следующих ключевых элементах:

2.1. Обязательное участие защитника и законного представителя. Участие защитника является не правом, а обязательным условием производства с момента фактического задержания лица или предъявления ему обвинения (ст. 51 УПК РФ). Отказ от защитника не обязателен для следователя и суда. Параллельно в процесс привлекается законный представитель (родитель, опекун и др.), чьи права закреплены в ст. 428 УПК РФ. Он имеет право защищать интересы несовершеннолетнего, что создает систему «двойной защиты». Следует также отметить, что участие законного представителя и защитника в процессуальных действиях с несовершеннолетним на стадии возбуждения уголовного дела законодателем регламентируется недостаточно. Мы согласны с Е. Е. Босак, Е. Н. Холоповой, которые считают, что для соблюдения прав несовершеннолетних осужденных в период проверки сообщения о преступлении при проведении любых предусмотренных законом процессуальных действий в обязательном порядке следует обеспечивать допуск и присутствие не только законного представителя, но и защитника, а в случае необходимости также специалиста-педагога [3].

2.2. Специальный порядок вызова и допроса. Допрос несовершеннолетнего подозреваемого, обвиняемого не может продолжаться без перерыва более 2 часов, а в общей сложности — более 4 часов в день (ч. 1 ст. 425 УПК РФ). При допросе вправе присутствовать защитник, который может задавать вопросы, а также педагог или психолог, если несовершеннолетний не достиг 16 лет либо страдает психическим расстройством. Это направлено на минимизацию психологической травмы и давления. Мы согласны с Е. В. Цветковой, которая отмечает, что с точки зрения процессуального права ни педагог, ни психолог не являются полноценными участниками уголовного судопроизводства в силу того, что они не отнесены законодательно ни к одной квалификационной категории. Процессуальное положение педагога или психолога, их полномочия, права и обязанности не закреплены в Кодексе [4].

2.3. Расширенные основания для избрания меры пресечения. Наряду с общими основаниями заключение под стражу в отношении несовершеннолетнего может быть применено лишь в исключительных случаях, когда это связано с совершением им тяжкого или особо тяжкого преступления (ч. 2 ст. 108 УПК РФ). Приоритет отдается альтернативным, более мягким мерам. При решении вопроса о мере пресечения обязательно учитываются условия жизни, род занятий, состояние здоровья несовершеннолетнего. Н. А. Шатов справедливо предполагает, что в уголовно-процессуальных исследованиях, в которых поднимаются вопросы модернизации механизмов применения мер пресечения в отношении несовершеннолетних, следует делать основной акцент на совершенствовании процедуры заключения под стражу, а не на ее запретах и разработке специализированных мер принуждения [5].

2.4. Приоритет восстановительного подхода. Законодатель стимулирует применение процедур, направленных на примирение с потерпевшим и заглаживание причиненного вреда (ст. 25, 76 УК РФ, ст. 427 УПК РФ о прекращении уголовного дела с применением принудительной меры воспитательного воздействия). Это предполагает наделение несовершеннолетнего и его представителя правом на активное участие в восстановительных программах. Показательным примером применения принудительной меры воспитательного воздействия в отношении несовершеннолетнего является решение (постановление) Кузьминского районного суда города Москвы от 2 апреля 2021 года в отношении несовершеннолетнего М., который обвинялся в совершении преступления,

предусмотренного ч. 1 ст. 166 УК РФ, неправомерное завладение автомобилем без цели хищения (угон). Суд освободил от уголовной ответственности несовершеннолетнего и применил принудительную меру воспитательного воздействия на основании п.п. «б» и «г» ч. 2 ст. 90 УК РФ в виде передачи несовершеннолетнего под надзор родителей и установления особых требований к поведению несовершеннолетнего [6].

3. Особенности статуса несовершеннолетнего потерпевшего, свидетеля.

В современном уголовном процессе сформировался устойчивый «охранительный» уклон в отношении несовершеннолетних потерпевших и свидетелей. Законодатель, стремясь максимально оградить психику ребенка от травмирующего воздействия уголовного процесса, наделяет его особым статусом, который, приводит к «процессуальной недееспособности».

Основное противоречие заключается в следующем: с одной стороны, существует объективная необходимость в дополнительных гарантиях (участие педагога, психолога, законного представителя), так как несовершеннолетний в силу возраста не может в полной мере самостоятельно защищать свои интересы, а с другой — действующий механизм реализации этих гарантий (особенно для детей старшего подросткового возраста — 14—17 лет) фактически подменяет волю и позицию несовершеннолетнего мнением его законного представителя или представителя органа опеки.

Ключевыми аспектами проблемы являются следующие. Во-первых, конфликт интересов законного представителя и ребенка. На практике законным представителем часто является родитель. Однако существует высокая вероятность, что именно родитель может быть причастен к совершению преступления (например, насилие в семье) или, наоборот, халатно относиться к защите прав ребенка. В такой ситуации интересы представителя и представляемого диаметрально противоположны, а процессуальный закон не содержит действенного механизма оперативного отстранения такого представителя на ранних этапах расследования. Во-вторых, формальность учета мнения. Участие педагога или психолога зачастую сводится к формальному присутствию, а не к обеспечению психологического комфорта и помощи в формулировании показаний. Закон не регламентирует четко, как именно специалист должен помогать ребенку, что снижает качество получаемых доказательств. В-третьих, отсутствие «права на ошибку» и самостоятельности. Для несовершеннолетнего потерпевшего старшего возраста (например, 16 лет) действуют те же жесткие правила допроса, что и для младших лиц. Другими словами, подросток лишен права давать показания без «свидетелей» (например, педагога), что подрывает доверие к следствию и не способствует формированию у него чувства ответственности за даваемые показания.

Для устранения вышеуказанных проблем следует дифференцировать процессуальный статус несовершеннолетнего на основе возрастных подгрупп с наделением разным объемом процессуальных прав и обязанностей. Например, младшая группа (до11 лет): ребенок рассматривается как лицо, нуждающееся в полном представительстве. Его показания имеют доказательственное значение, но все процессуальные решения от его имени принимает законный представитель (при условии отсутствия конфликта интересов). Обязательно участие психолога; средняя группа (12—14 лет): частичная процессуальная дееспособность. Ребенок допрашивается в присутствии психолога (педагога), но его показания фиксируются как самостоятельный источник доказательств. Он должен быть официально уведомлен о своих правах в доступной форме. Согласие ребенка обязательно для проведения ряда следственных действий (например, освидетельствования), если это не терпит отлагательства; старшая группа (15—17 лет): расширенная процессуальная дееспособность. Предполагается, что подросток может самостоятельно давать показания и понимать их значение.

Защита прав несовершеннолетних потерпевших и свидетелей также имеет специфику. Наиболее полно такая специфика выражается при производстве допроса несовершеннолетнего потерпевшего или свидетеля.

Допрос потерпевшего или свидетеля в возрасте до 16 лет проводится обязательно с участием педагога или психолога (ст. 191, 280 УПК РФ).

С целью охраны психики несовершеннолетнего потерпевшего или свидетеля закон допускает проведение допроса в отсутствие подсудимого, с последующим предъявлением ему видеозаписи (ч. 6 ст. 281 УПК РФ).

Полагаем внедрение специализированных процедур допроса должно быть направлено на решение сразу несколько задач: снижение количества повторных допросов несовершеннолетнего потерпевшего и свидетеля, травмирующих психику; позволение суду в дальнейшем оценивать не только содержание, но и обстановку, в которой давались показания, а также реакцию ребенка, исключив обвинения в «наводящих вопросах» со стороны следствия.

Предложенные меры смещают акцент с тотальной опеки над несовершеннолетним на «индивидуализированную защиту». Это позволит повысить качество следствия, снизить риск оговора

или самооговора под давлением семьи и обеспечит реальное, а не декларативное соблюдение прав ребенка в уголовном процессе.

4. Соответствие международным стандартам.

Российская модель производства по уголовным делам в отношении несовершеннолетнего в целом соответствует ключевым положениям международного права, таким как:

- минимальные стандартные правила ООН, касающиеся отправления правосудия в отношении несовершеннолетних (Пекинские правила, 1985) [7]: принцип соразмерности, минимального вмешательства, приоритет благополучия несовершеннолетнего;

- конвенция о правах ребенка (1989) [8]: право не быть подвергнутым пыткам, жестокому обращению, право на свободу и личную неприкосновенность, рассмотрение дел с учетом возраста и желательности содействия реинтеграции (ст. 37, 40).

Однако на практике остаются проблемы: недостаточное использование восстановительных технологий, формализм в участии педагога или психолога, перегрузка и низкая специализация защитников и следователей и др.

Таким образом, наделение несовершеннолетнего уголовно-процессуальным статусом в российском законодательстве представляет собой дифференцированный процесс, основанный на идее повышенной правовой защиты. Он характеризуется дуализмом (общий статус плюс специальные гарантии), расширением субъектного состава (обязательное участие защитника, законного представителя, специалистов), ограничением карательного инструментария и ориентацией на воспитательно-восстановительные цели.

Дальнейшее совершенствование данного института видится в более глубокой имплементации международных стандартов, развитии сети ювенальных судов, внедрении междисциплинарного подхода с привлечением социальных работников и психологов на всех этапах процесса, а также в расширении применения медиативных и восстановительных практик, которые позволяют не просто определить процессуальный статус, но и наполнить его реальным, ориентированным на будущее несовершеннолетнего, содержанием.

Российское уголовно-процессуальное законодательство стремится к регулированию изменения уголовно-процессуального статуса несовершеннолетнего в ходе уголовного судопроизводства.

Уголовно-процессуальный статус несовершеннолетнего представляет собой особый правовой режим, характеризующийся комплексом специальных гарантий и процедур, предусмотренных как главой 50 УПК РФ «Производство по уголовным делам в отношении несовершеннолетних», так и иными нормами УПК РФ. Эти гарантии (обязательное участие защитника и законного представителя, возможность прекращения дела с применением принудительной меры воспитательного воздействия, особенности избрания меры пресечения, специальные условия допроса, приоритет воспитательных задач и др.) призваны компенсировать возрастную психофизическую и социальную незрелость лица, обеспечить его повышенную защиту в уголовном процессе.

Однако уголовное судопроизводство нередко носит протяженный во времени характер. В ситуации, когда лицо совершило преступление в несовершеннолетнем возрасте, но к моменту вынесения процессуального решения (окончания предварительного следствия, рассмотрения дела судом) достигло совершеннолетия, возникает правовая коллизия. Процессуальный статус такого лица становится неопределенным: следует ли продолжать применять к нему специальный режим, предназначенный для несовершеннолетних, или оно утрачивает право на соответствующие гарантии? Данная проблема обладает высокой теоретической и практической значимостью, поскольку непосредственно затрагивает принцип индивидуализации уголовной ответственности и процессуальных гарантий.

1. Правовая природа и момент фиксации статуса несовершеннолетнего.

В теории уголовно-процессуального права в целом утвердился подход, согласно которому возраст, определяющий специальный статус несовершеннолетнего в уголовном процессе, является «юридическим фактом, имеющим материально-правовое значение». Согласно п. 1 ст. 420 УПК РФ, производство по делам несовершеннолетних ведется в отношении лиц, «не достигших к моменту совершения преступления возраста восемнадцати лет». Таким образом, исходным базовым критерием является возраст на момент совершения инкриминируемого деяния. Этот факт определяет изначальную квалификацию дела как «дела в отношении несовершеннолетнего» и влечет применение соответствующих норм с самого начала производства.

Однако процессуальный статус — категория динамичная. Изменение возраста лица в ходе производства порождает сложные вопросы о том, «на какие процессуальные действия и решения распространяются специальные правила».

2. Основные проблемы и направления изменения процессуального статуса

2.1. Применение принудительных мер воспитательного воздействия (ПМВВ). Согласно

ст. ст. 90, 427 УПК РФ, прекращение уголовного преследования с применением ПМВВ возможно только в отношении несовершеннолетнего. Если к моменту принятия решения лицо уже достигло 18 лет, судебная практика (с учетом разъяснений Пленума Верховного Суда РФ [9]) исходит из того, что применение ст. 427 УПК РФ невозможно. Суд или следователь должен либо прекратить дело по иным основаниям (например, в связи с деятельным раскаянием), либо направить его в суд для рассмотрения по существу. Это связано с тем, что цель ПМВВ — воспитание, которое в отношении взрослого лица в рамках уголовного процесса не предусмотрено. Таким образом, в этой части статус несовершеннолетнего утрачивается полностью.

2.2. Особенности избрания меры пресечения. Часть 2 ст. 108 УПК РФ запрещает заключение под стражу несовершеннолетнего, подозреваемого или обвиняемого в совершении преступлений средней тяжести впервые. Если лицо достигло совершеннолетия в ходе следствия, возникает вопрос: сохраняется ли данный запрет? Позиция правоприменителя склоняется к тому, что «запрет перестает действовать», поскольку формально лицо более не является несовершеннолетним на момент рассмотрения ходатайства. Однако такой подход представляется спорным, так как игнорирует причину установления запрета — повышенную уязвимость лица «на момент совершения преступления». Более логичным было бы связывать применение этой нормы с возрастом на момент инкриминируемого деяния.

2.3. Подследственность и подсудность. Уголовные дела о преступлениях несовершеннолетних расследуются следователями Следственного комитета РФ (п. 2 ч. 2 ст. 151 УПК РФ) и рассматриваются судами с участием коллегий присяжных заседателей в ином порядке (ст. 420 УПК РФ). Достижение 18 лет не влечет изменения подследственности дела — оно продолжает расследоваться тем же органом. Подсудность также, как правило, не меняется, поскольку определяется на момент принятия дела к производству. Однако возможны сложности при решении вопроса о рассмотрении дела судом присяжных, если обвинение переквалифицировано на статью, не предусматривающую такой формы судопроизводства для несовершеннолетних.

2.4. Процессуальные гарантии участия защитника и законного представителя. Обязательное участие защитника (ст. 51 УПК РФ) сохраняет силу вне зависимости от изменения возраста. Что касается законного представителя, то его участие после достижения подсудимым 18 лет перестает быть обязательным (ч. 1 ст. 428 УПК РФ). Суд вправе, но не обязан, допустить к участию в судебном заседании бывшего законного представителя, если признает это целесообразным. На практике суды часто отказывают в таком участии, что может нарушать интересы лица, нуждающегося в психологической поддержке.

2.5. Особенности судебного разбирательства и назначения наказания. Согласно ст. 429 УПК РФ, суд вправе удалить несовершеннолетнего подсудимого из зала суда на время исследования обстоятельств, могущих оказать на него отрицательное воздействие. После достижения совершеннолетия эта норма формально применяться не может. При назначении наказания суд, руководствуясь ст. 96 УК РФ, «вправе применить положения главы 14 УК РФ об особенностях уголовной ответственности несовершеннолетних» к лицам, совершившим преступления в возрасте от 18 до 20 лет, но не обязан этого делать. Это дискреционное право суда, решение по которому принимается с учетом характера совершенного деяния и личности виновного. Таким образом, в вопросах наказания статус несовершеннолетнего может быть частично «продлен» по усмотрению суда.

С учетом вышесказанного можно утверждать, что изменение возраста несовершеннолетнего в ходе уголовного судопроизводства приводит к сложному, дифференцированному изменению его процессуального статуса. Законодатель не дает четких ответов на все возникающие вопросы, что порождает противоречивую судебную практику и правовую неопределенность.

Можно выделить несколько моделей изменения статуса:

1. Полная утрата специального статуса (в отношении ПМВВ).

2. Сохранение статуса на ключевые моменты (подследственность, подсудность).

3. Факультативное (зависимое от усмотрения суда) применение гарантий (участие законного представителя, применение норм о принудительных мерах воспитательного воздействия).

4. Неясность в применении гарантий, требующая толкования (избрание меры пресечения).

Для устранения пробелов и коллизий предлагается:

1. Внести изменения в ст. 420 УПК РФ, четко разграничив, какие из процессуальных гарантий применяются исключительно исходя из возраста на момент совершения преступления (например, запрет на заключение под стражу по преступлениям средней тяжести, подследственность), а какие утрачивают силу после достижения совершеннолетия (ПМВВ).

2. Конкретизировать в законе (ст. 428 УПКРФ) критерии допуска бывшего законного представителя к участию в судебном заседании, сместив акцент с формального возраста на необходимость обеспечения права на защиту и психологическую поддержку.

3. Закрепить в УПК РФ правило о том, что достижение совершеннолетия в ходе производства не является основанием для изменения подсудности уголовного дела.

Устранение правовой неопределенности в данной сфере будет способствовать реализации принципов справедливости, гуманизма и индивидуализации уголовного судопроизводства в отношении лиц, совершивших преступление в несовершеннолетнем возрасте.

ЛИТЕРАТУРА

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 27.10.2025) // Собрание законодательства РФ. — 2001. — № 52 (ч. I). — Ст. 4921.

2. Кутуев Э. К., Шувалова М. А. Проблемные аспекты участия защитника в процессе доказывания по уголовным делам в отношении несовершеннолетних // Российская юстиция. — 2021. — № 1. — С. 34—36.

3. Босак Е. Е., Холопова Е. Н. Проверка сообщения о преступлении, совершенном несовершеннолетним осужденным // Российский следователь. — 2021. — № 10. — С. 20—22.

4. Цветкова Е. В. Правовые проблемы участия педагога или психолога в уголовном судопроизводстве с участием несовершеннолетних // Современное право. — 2024. — № 4. — С. 120—123.

5. Шатов Н. А. Теоретические и нормативные аспекты избрания меры пресечения в виде заключения под стражу в отношении несовершеннолетних // Актуальные проблемы российского права. — 2025. — № 9. — С. 84—95.

6. Уголовное дело №1-392/2021 от 2 апреля 2021 года. — URL: https://mosgorsud.ru/rs/kuzminskij/cases/docs/content/872c6330-9397-11eb-8903-edec68ee2154 (дата обращения: 20.03.2026).

7. Минимальные стандартные правила Организации Объединенных Наций, касающиеся отправления правосудия в отношении несовершеннолетних (Пекинские правила) (приняты Резолюцией 40/33 Генеральной Ассамблеи ООН от 29 ноября 1985 года). — URL: https://www.un.org/ru/documents/decl_conv/conventions/beijing_rules.shtml (дата обращения: 29.12.2025).

8. Конвенция о правах ребенка (одобрена Генеральной Ассамблеей ООН 20.11.1989) (вступила в силу для СССР 15.09.1990). Документ ратифицирован Постановлением ВС СССР от 13.06.1990 № 1559-I // Сборник международных договоров СССР. Вып. XLVI. — М., 1993.

9. О судебной практике применения законодательства, регламентирующего особенности уголовной ответственности и наказания несовершеннолетних : постановление Пленума Верховного Суда РФ от 01.02.2011 № 1 (ред. от 09.12.2025) // Бюллетень Верховного Суда РФ. — 2011. — № 4.

REFERENCES

1. Ugolovno-protsessual′nyj kodeks Rossijskoj Federatsii ot 18.12.2001 № 174-FZ (red. ot 27.10.2025) // Sobranie zakonodatel′stva RF. — 2001. — № 52 (ch. I). — St. 4921.

2. Kutuev E. K., Shuvalova M. A. Problemnye aspekty uchastiya zashchitnika v protsesse dokazyvaniya po ugolovnym delam v otnoshenii nesovershennoletnikh // Rossijskaya yustitsiya. — 2021. — № 1. — S. 34—36.

3. Bosak E. E., Kholopova E. N. Proverka soobshcheniya o prestuplenii, sovershennom nesovershennoletnim osuzhdennym // Rossijskij sledovatel′. — 2021. — № 10. — S. 20—22.

4. Tsvetkova E. V. Pravovye problemy uchastiya pedagoga ili psikhologa v ugolovnom sudoproizvodstve s uchastiem nesovershennoletnikh // Sovremennoe pravo. — 2024. — № 4. — S. 120—123.

5. Shatov N. A. Teoreticheskie i normativnye aspekty izbraniya mery presecheniya v vide zaklyucheniya pod strazhu v otnoshenii nesovershennoletnikh // Aktual′nye problemy rossijskogo prava. — 2025. — № 9. — S. 84—95.

6. Ugolovnoe delo №1-392/2021 ot 2 aprelya 2021 goda. — URL: https://mosgorsud.ru/rs/kuzminskij/cases/docs/content/872c6330-9397-11eb-8903-edec68ee2154 (data obrashcheniya: 20.03.2026).

7. Minimal′nye standartnye pravila Organizatsii Ob″edinennykh Natsij, kasayushchiesya otpravleniya pravosudiya v otnoshenii nesovershennoletnikh (Pekinskie pravila) (prinyaty Rezolyutsiej 40/33 General′noj Assamblei OON ot 29 noyabrya 1985 goda). — URL: https://www.un.org/ru/documents/decl_conv/conventions/beijing_rules.shtml (data obrashcheniya: 29.12.2025).

8. Konventsiya o pravakh rebenka (odobrena General′noj Assambleej OON 20.11.1989) (vstupila v silu dlya SSSR 15.09.1990). Dokument ratifitsirovan Postanovleniem VS SSSR ot 13.06.1990 № 1559-I // Sbornik mezhdunarodnykh dogovorov SSSR. Vyp. XLVI. — M., 1993.

9. O sudebnoj praktike primeneniya zakonodatel′stva, reglamentiruyushchego osobennosti ugolovnoj otvetstvennosti i nakazaniya nesovershennoletnikh : postanovlenie Plenuma Verkhovnogo Suda RF ot 01.02.2011 № 1 (red. ot 09.12.2025) // Byulleten′ Verkhovnogo Suda RF. — 2011. — № 4.

СВЕДЕНИЯ ОБ АВТОРЕ

Ахмедов Ульви Низами оглы. Доцент кафедры уголовного процесса. Кандидат юридических наук, доцент.

Воронежский институт МВД России.

E-mail: Ulvi27@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Akhmedov Ulvi Nizami ogli. Associate Professor of the chair of Criminal Proceeding. Candidate of Law, Associate Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: Ulvi27@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: несовершеннолетний; уголовно-процессуальный статус; подозреваемый; обвиняемый; подсудимый; потерпевший; возраст; уголовно-процессуальные гарантии; достижение совершеннолетия; динамика правового статуса.

Key words: minor; criminal procedural status; suspect; accused; defendant; victim; age; criminal procedural guarantees; reaching the age of majority; dynamics of legal status.

УДК 343.131

А. Н. Белоусова, *кандидат юридических наук, доцент*
Е. А. Запорожцева

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТ-СЕРВИСОВ РАЗМЕЩЕНИЯ ОБЪЯВЛЕНИЙ ДЛЯ ВОВЛЕЧЕНИЯ НЕСОВЕРШЕННОЛЕТНИХ В МОШЕННИЧЕСКИЕ ДЕЙСТВИЯ

FEATURES OF USING INTERNET ADVERTISING SERVICES TO INVOLVE MINORS IN FRAUDULENT ACTIVITIES

Развитие современного общества происходит в условиях нарастающей цифровизации. Несовершеннолетние чаще других групп населения пользуются интернет-платформами, для которых они становятся не только средством обучения и социализации, но и средством удовлетворения потребностей в самореализации и финансовой самостоятельности. Повышенная внушаемость, доверчивость, яркость восприятия информации, эмоциональность и некритичность создают благоприятную почву для воздействия со стороны мошенников, которые эксплуатируют потребность подростков в признании, доверии и материальной выгоде. Цифровая активность, социальная уязвимость и психологическая восприимчивость к манипулятивным воздействиям при отсутствии жизненного опыта и правовых знаний позволяет втягивать несовершеннолетних в совершение отдельных операций в мошеннических схемах, совершаемых через интернет-сервисы размещения объявлений. В условиях дистанционного общения при использовании технических возможностей преступники целенаправленно формируют у подростков иллюзию дружеских либо партнерских отношений, манипулируют сознанием, постепенно формируя установку на допустимость нарушения закона, тем самым вовлекая в преступную деятельность на постоянной основе.

The development of modern society is taking place in the context of increasing digitalization. Minors are more likely than other population groups to use Internet platforms, which become not only a means of learning and socialization, but also a means of meeting the needs for self-realization and financial independence. Increased suggestibility, gullibility, vivid perception of information, emotionality, and lack of critical thinking create a favorable environment for the influence of fraudsters who exploit the need of adolescents for recognition, trust, and material benefits. Digital activity, social vulnerabilities, and psychological susceptibility to manipulative influences, combined with a lack of life experience and legal knowledge, make it possible to involve minors in fraudulent schemes conducted through online advertising services. In the context of remote communication, by using technical capabilities, criminals purposefully create the illusion of friendly or partnership relations among teenagers, manipulating their consciousness and gradually forming an attitude of permissibility towards breaking the law, thereby involving them in criminal activities on a regular basis.

Стремительное развитие цифровых технологий и повсеместное использование сети Интернет существенно трансформировали формы социального и экономического взаимодействия. Интернет-сервисы прочно вошли в повседневную жизнь граждан, обеспечивая доступность купли-продажи товаров и услуг, платежей и финансовых операций, трудовой деятельности и досуга, расширяя возможности для общения и сотрудничества. Вместе с тем эти цифровые платформы стали активно использоваться в противоправных целях, в первую очередь в мошеннических схемах.

Мошеннические действия, совершаемые с использованием интернет-сервисов размещения объявлений, представляют собой устойчивый и динамично развивающийся сегмент современной киберпреступности, обладающий рядом специфических криминологических признаков. Их распространенность обусловлена массовым характером использования цифровых платформ, относительной анонимностью сетевого взаимодействия, а также низким порогом вхождения в противоправную деятельность [1—3]. Ранее главная угроза заключалась в возможности стать жертвой мошеннических действий и потерять собственное имущество или накопления. В таких ситуациях наиболее уязвимыми были пенсионеры (обладающие собственными накоплениями) и несовершеннолетние (имеющие представления о накоплениях

родителей). В настоящее время злоумышленники применяют навыки дистанционной коммуникации в отношении виктимных категорий граждан для использования их в совершении преступлений как орудия или средства. И если старшее поколение относится с опаской к любым новшествам, критически подходит к своим возможностям и способностям дистанционного общения, то несовершеннолетние и молодежь, воспитанные в информационно-телекоммуникационной среде и постоянно общающиеся в ней, не задумываются о скрытых опасностях.

Защита несовершеннолетние как наиболее уязвимой группы населения, как ресурса общественного движения и государственного развития должна стать приоритетной задачей. По данным Сбербанка, за последние два года количество несовершеннолетних, пострадавших от мошеннических действий либо вовлеченных в их совершение, увеличилось более чем на 30% [4]. Особую обеспокоенность вызывает тенденция активного вовлечения несовершеннолетних в мошеннические схемы, реализуемые посредством онлайн-площадок объявлений. Подростки, обладая высокой цифровой активностью и зачастую недостаточным уровнем правовой и финансовой грамотности, становятся удобной мишенью для преступных групп. Они могут использоваться как исполнители отдельных операций (например, в качестве так называемых «дропперов») либо вовлекаться в соучастие в противоправной деятельности под видом «подработки», не осознавая в полной мере уголовно-правовых последствий своих действий [5]. Так, аналитиками компании в сфере кибербезопасности F6 за период с января по октябрь 2025 года было зафиксировано более 6 тысяч инцидентов, в рамках которых киберпреступники через онлайн-игры, социальные сети и мессенджеры манипулировали детьми в возрасте от 10 до 14 лет с целью хищения денежных средств со счетов их родителей [6]. Общий материальный ущерб от подобных схем превысил 850 млн рублей, что не только свидетельствует о высокой экономической и социальной значимости рассматриваемой проблемы, но и подтверждает системный характер проблемы.

В этой связи несовершеннолетних следует рассматривать как жертв вовлечения в мошеннические действия, несмотря на их статус пособника или соисполнителя в уголовном преследовании. На этом акцентировал внимание Президент РФ на расширенном заседании коллегии МВД 4 марта 2026 года, подчеркнув необходимость оперативного выявления и привлечения к ответственности лиц, использующих несовершеннолетних в преступных целях [7].

Эффективность вовлечения подростков в преступную деятельность обусловлена множеством факторов: социально-экономической обстановкой в стране, характером совершаемых посягательств (путем обмана или злоупотребления доверием), формой вовлечения (дистанционной), техническими и технологическими особенностями информационных ресурсов, индивидуальными психофизиологическими характеристиками детей.

Изо всех социальных групп несовершеннолетние — наиболее активные пользователи информационных ресурсов. Повышенный интерес к сетевым ресурсам связан с возможностью удовлетворить широкий спектр потребностей юных пользователей: в развлечениях, получении новой информации, привлечении к себе внимания, в социальном признании и одобрении и, главное, в общении. Интеренет-пространство рассматривается ими как наиболее удобный актив. Самореализация и самоидентификация через онлайн-ресурсы происходит с меньшими затратами: одновременно можно коммуницировать с неограниченным кругом людей/групп, не выходя из дома, не придерживаясь правил и норм поведения, не опасаясь осуждения или огласки [1]. Согласно данным «Лаборатории Касперского» за 2024 год, почти все дети России (92%) пользуются мессенджерами. При этом популярность выросла среди младших школьников (82% детей 7—10 лет, в 2022 г. таких было 72%, а в 2018 году — 60%). Дети в возрасте от 3—6 лет пользуются сетью Интернет в 83% [8]. По данным опроса, проведенного компанией МТС в 2025 г., 74% детей пользуются мессенджерами, 71% — соцсетями (в 2018 году их было 47%), 70% — мобильными играми и 66% — видеосервисами [9].

Условия современной действительности поставили детей в опасные рамки зависимости от интернета. И дело не в том, что киберпространство для них что-то новое и потому особенно притягательное, от соблазнов которого они не могут отказаться. Период пандемии заставил образовательные и досуговые организации перейти в дистанционный формат, обучиться современным технологиям и постоянно их применять. Образовательный процесс во всех его проявлениях и со всеми возможностями в значительной части перешел в виртуальное пространство. Необходимость и обязательность получения образования заставляет несовершеннолетних быть участниками киберпространства. Поэтому сами дети не могут отказаться от пользования сетью Интернет, а родители не могут им этого запретить. Более того, последние обязаны обеспечивать им постоянный и стабильный доступ к информационному пространству. Интернет для подростка перешел из

разряда «новое и интересное» в «нормальное и неизбежное».

При незаконченном интеллектуальном развитии, недостаточности знаний и жизненного опыта, несформированности нравственных ценностей и неопределенности жизненных целей большой поток неконтролируемой информации интернет-платформ скорее причинит вред интеллектуальному, нравственному или физическому здоровью, нежели облегчит социализацию. Во-первых, сама информация, размещаемая в сети, представляется ярко и интересно, а потому в подростковом сознании не может быть опасной. Во-вторых, отсутствуют критерии опасности информации. В-третьих, постоянство ее трансляции с учетом поисковых запросов несовершеннолетних с напором и динамизмом технических возможностей позволяет манипулировать их сознанием [2].

Привычность дистанционного общения, неизменность контента способствует формированию у несовершеннолетних завышенного уровня доверия к незнакомым пользователям и снижает барьеры при вступлении в сомнительные формы взаимодействия. Отсутствие устойчивых навыков критической оценки информации, получаемой через интернет, повышает восприимчивость к манипулятивным воздействиям. Ключевой особенностью мошенничеств с использованием сервисов объявлений является отсутствие непосредственного личного контакта между преступником и потерпевшим, что существенно снижает субъективное восприятие риска у потенциального потерпевшего, позволяет преступникам имитировать законную деятельность и одновременно затрудняет идентификацию злоумышленника [10].

Технические возможности интернет-площадок делают их доступными любым пользователям, в любое время, с возможностью подключения любого устройства. Отсутствие ограничений и запретов на предоставление и использование третьими лицами личной информации при доверчивом, неосмотрительном или некритичном поведении определяет эффективность вовлечения подростков в преступления. А излишняя самоуверенность последних делает их привлекательным и доступным ресурсом для использования в преступлениях. В этой связи криминогенные факторы мошеннических действий с использованием онлайн-сервисов объявлений в равной степени можно рассматривать как виктимогенные.

Криминогенное значение имеют и организационно-технологические факторы, присущие самим интернет-сервисам размещения объявлений. Это возможность анонимной регистрации, использование подставных или временных аккаунтов, отсутствие обязательной верификации личности, а также упрощенные механизмы электронных платежей. Эти особенности активно используются мошенниками для вовлечения несовершеннолетних в качестве формально «незаметных» исполнителей, уверяя последних в ненаказуемости деяний и невозможности их выявления и привлечения к ответственности. Понятность и простота цифровых технологий формируют ощущение безнаказанности, что способствует вовлечению новых участников [11]. Эти же особенности снижают риски разоблачения организаторов преступной деятельности, позволяют им оставаться вне закона и закрепляют уверенность во вседозволенности.

Благодаря техническим возможностям интеренет-платформ и невежественности несовершеннолетних преступники выбирают подростков, испытывающих финансовые затруднения (например, ищущих легкий заработок через использование услуги на маркетплейсах «отзывы за деньги», публикующих объявления о продаже товаров или оказании услуг и не имеющих достаточного опыта совершения онлайн-сделок). Активное использование цифровых сервисов, предлагающих инвестирование капитала или монетизацию активности в сети, позволяет выявить подростков, обладающих навыками коммуникации в интернет-пространстве. Сами же несовершеннолетние пользователи социальных сетей, мессенджеров и онлайн-площадок объявлений за счет привычности и постоянства виртуального взаимодействия становятся уверенными в его безопасности [12], провоцируя своим неосмотрительным, рискованным или легкомысленным поведением посягательства.

Безусловно, материальная нестабильность отдельных семей, завышенные потребности, транслируемые как базовые, оказывают существенное влияние. Однако доминирующим мотивом поведения подростков по-прежнему остается стремление к самореализации через раннюю финансовую самостоятельность. При всеобщей меркантилизации жизни и афишировании корыстно-потребительских тенденций формируется представление о возможности быстрого обогащения, а IT-технологии делают его доступным и реальным. При этом интернет-сервисы размещения объявлений воспринимаются ими как легитимное и безопасное пространство для экономической активности [13]. Желание получить быстрый доход без значительных трудовых затрат нередко используется мошенниками в качестве основного инструмента вербовки [14]. Предложения о «подработке» в виде размещения объявлений, приема денежных средств, регистрации аккаунтов или пересылки товаров маскируются под законную деятельность

и не воспринимаются несовершеннолетними как противоправные.

Стоит обратить внимание на то, что границы законного и противоправного в сознании несовершеннолетних размываются расширением объема дееспособности по достижении 14 лет, когда появляются законом установленные права на собственные счета в банках, собственные средства, на самостоятельное распоряжение отдельными видами семейных доходов с согласия родителей. Именно с достижением 14-летнего возраста подростки чаще всего вовлекаются в мошеннические схемы в роли посредников, исполнителей либо формальных участников сделок. В мошеннических схемах им отводится роль исполнителей вспомогательных функций, например, регистрация и администрирование аккаунтов, размещение объявлений, ведение переписки с потерпевшими, прием и перевод денежных средств [15].

Возрастная специфика личности несовершеннолетнего проявляется в недостаточной сформированности правосознания и неспособности в полной мере прогнозировать правовые последствия своих действий. Вовлекаемые подростки зачастую не осознают уголовно-правового характера совершаемых ими деяний, воспринимая участие в мошеннических схемах как «подработку», «помощь в продаже» либо техническое содействие третьим лицам [16]. А отсутствие системного понимания уголовно-правовых последствий участия в мошеннических схемах приводит к тому, что подростки нередко не осознают свою роль как соучастников преступления, полагая, что ответственность несут исключительно «организаторы» или «заказчики» их действий [17].

Высокая цифровая активность подростков и стремление к быстрому заработку облегчает преступный замысел организаторов. Для вовлекаемых подростков характерен высокий уровень цифровой компетентности в техническом смысле (умение пользоваться сервисами, платформами и инструментами веб-ресурсов, создавать и управлять аккаунтами), который, однако, не сопровождается адекватным уровнем правовой и финансовой грамотности. Это формирует иллюзию уверенности в своих знаниях и умениях и контроля над ситуацией, что активно используется мошенниками при вовлечении несовершеннолетних в противоправную деятельность. Подросткам предоставляют распространенные и типовые схемы обмана [18], когда специальных знаний в области интернет-технологий не требуется, достаточно только поверхностных пользовательских цифровых навыков и стремления заработать больше. По данным Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России, размещение объявлений о продаже несуществующих товаров или оказании фиктивных услуг с последующим получением предоплаты составляет около 46% всех выявленных эпизодов мошенничества на площадках бесплатных объявлений. Это свидетельствует о преобладании относительно простых, но высокоэффективных моделей преступного поведения, ориентированных на массового пользователя и не требующих от преступника высокой технической квалификации.

Высокий уровень цифровизации повседневной жизни выступает криминогенным фактором для вовлечения несовершеннолетних в мошеннические действия, совершаемые с использованием интернет-сервисов размещения объявлений. Комплексное воздействие совокупности взаимосвязанных социальных, психологических, экономических и организационно-технологических факторов формирует благоприятную криминогенную среду, в которой подростки выступают как объект целенаправленного преступного воздействия, а в ряде случаев — как активные участники противоправной деятельности.

ЛИТЕРАТУРА

1. Белоусова А. Н., Кулешова В. В. Виктимогенный механизм совершения преступлений в отношении несовершеннолетних с использованием социальных сетей и мессенджеров // Вестник Воронежского института МВД России. — 2024. — № 1. — С. 186—192.

2. Белоусова А. Н. Механизм деструктивного воздействия информационных ресурсов на поведение несовершеннолетних // Вестник Воронежского института МВД России. — 2025. — № 3. — С. 187—194.

3. Белоусова А. Н., Кулешова В. В., Лупырь М. В. Перспективы профилактики посягательств на интересы несовершеннолетних, совершаемых с использованием информационных технологий // Вестник Воронежского института МВД России. — 2024.— № 4. — С. 172—179.

4. Сбер фиксирует растущий тренд вовлечения детей и подростков в мошенничество // Вести Воронеж. — URL: https://vestivrn.ru/news/2025/11/17/ (дата обращения: 28.02.2026).

5. Карманные деньги, глупость и шантаж: почему подростки все чаще становятся соучастниками мошенников // Комсомольская правда. —

URL: https://www.kp.ru/daily/27756/5204472/ (дата обращения: 28.02.2026).

6. Рост мошенничества с участием детей // Коммерсант. — URL: https://www.kommersant.ru/doc/8209999 (дата обращения: 28.02.2026).

7. Расширенное заседание коллегии МВД // Кремлин. — URL: http://www.kremlin.ru/events/president/transcripts/comminity_meetings/79255 (дата обращения: 05.03.2026).

8. Сиденко А. Г. Взрослые и дети в интернете : аналитический отчет. — URL: https://kids.kaspersky.ru/files/13443_Brochure_Kids.pdf.

9. Треть детей сидит в интернете от трех до восьми часов ежедневно. — URL: https://tass.ru/obschestvo/24110383

10. Вакуленко Н. А. Мошенничество с использованием телекоммуникационных и компьютерных сетей: процессы детерминации и криминализации // Юристъ-Правоведъ. — 2024. — № 1(108). — С. 79.

11. Шаназарова Е. В. Мошенничество: криминологическая характеристика и предупреждение // Тенденции развития науки и образования. — 2024. — № 113-3. — С. 123.

12. Квасникова Т. В., Гасанов А. М. Особенности криминологической характеристики мошенничества // Colloquium-Journal. — 2019. — № 16-7(40). — С. 81.

13. Основы криминологии : учебник для студентов вузов, обучающихся по направлению «Юриспруденция» / А. В. Федоров, С. Я. Лебедев, Е. А. Антонян [и др.]. — 3-е изд., перераб. и доп. — М. : Юнити-Дана, 2024. — С. 58.

14. Вакуленко Н. А., Морозов А. П. Криминология : учебное наглядное пособие. — Ростов-на-Дону : Ростовский юридический институт МВД России, 2025. – С. 79.

15. Зотина Е. В. Мошенничество с использованием информационно-телекоммуникационных технологий и приемов социальной инженерии: криминологическое исследование : автореф. дис. … канд. юрид. наук / Зотина Елена Владимировна. — Казань, 2025. — С. 11.

16. Хайрусов Д. С. Криминология : учебное пособие. — М. : Юрайт, 2024. — С. 44.

17. Осипенко А. Л., Соловьев В. С. Киберугрозы в отношении несовершеннолетних и особенности противодействия им с применением информационных технологий // Общество и право. — 2019. — № 3(69). — С. 23—24.

18. Красев Д. В. Криминологические особенности организованного мошенничества в сфере информационных технологий // Вопросы российского и международного права. — 2025. — Т. 15. — № 3-1. — С. 571.

REFERENCES

1. Belousova A. N., Kuleshova V. V. Viktimogennyj mekhanizm sovershheniya prestuplenij v otnoshenii nesovershennoletnikh s ispol′zovaniem sotsial′nykh setej i messendzherov // Vestnik Voronezhskogo instituta MVD Rossii. — 2024. — № 1. — S. 186—192.

2. Belousova A. N. Mekhanizm destruktivnogo vozdejstviya informatsionnykh resursov na povedenie nesovershennoletnikh // Vestnik Voronezhskogo instituta MVD Rossii. — 2025. — № 3. — S. 187—194.

3. Belousova A. N., Kuleshova V. V., Lupyr′ M. V. Perspektivy profilaktiki posyagatel′stv na interesy nesovershennoletnikh, sovershaemykh s ispol′zovaniem informatsionnykh tekhnologij // Vestnik Voronezhskogo instituta MVD Rossii. — 2024.— № 4. — S. 172—179.

4. Sber fiksiruet rastushchij trend vovlecheniya detej i podrostkov v moshennichestvo // Vesti Voronezh. — URL: https://vestivrn.ru/news/2025/11/17/ (data obrashcheniya: 28.02.2026).

5. Karmannye den′gi, glupost′ i shantazh: pochemu podrostki vse chashche stanovyatsya souchastnikami moshennikov // Komsomol′skaya pravda. — URL: https://www.kp.ru/daily/27756/5204472/ (data obrashcheniya: 28.02.2026).

6. Rost moshennichestva s uchastiem detej // Kommersant. — URL: https://www.kommersant.ru/doc/8209999 (data obrashcheniya: 28.02.2026).

7. Rasshirennoe zasedanie kollegii MVD // Kremlin. — URL: http://www.kremlin.ru/events/president/transcripts/comminity_meetings/79255 (data obrashcheniya: 05.03.2026).

8. Sidenko A. G. Vzroslye i deti v internete : analiticheskij otchet. — URL: https://kids.kaspersky.ru/files/13443_Brochure_Kids.pdf.

9. Tret′ detej sidit v internete ot trekh do vos′mi chasov ezhednevno. — URL: https://tass.ru/obschestvo/24110383

10. Vakulenko N. A. Moshennichestvo s ispol′zovaniem telekommunikatsionnykh i komp′yuternykh setej: protsessy determinatsii i kriminalizatsii // Yurist″-Pravoved″. — 2024. — № 1(108). — S. 79.

11. Shanazarova E. V. Moshennichestvo: kriminologicheskaya kharakteristika i preduprezhdenie // Tendentsii razvitiya nauki i obrazovaniya. — 2024. — № 113-3. — S. 123.

12. Kvasnikova T. V., Gasanov A. M. Osobennosti kriminologicheskoj kharakteristiki moshennichestva // Colloquium-Journal. — 2019. — № 16-7(40). — S. 81.

13. Osnovy kriminologii : uchebnik dlya studentov vuzov, obuchayushchikhsya po napravleniyu «Yurisprudentsiya» / A. V. Fedorov, S. Ya. Lebedev, E. A. Antonyan [i dr.]. — 3-e izd., pererab. i dop. — M. : Yuniti-Dana, 2024. — S. 58.

14. Vakulenko N. A., Morozov A. P. Kriminologiya : uchebnoe naglyadnoe posobie. — Rostovna-Donu : Rostovskij yuridicheskij institut MVD Rossii, 2025. – S. 79.

15. Zotina E. V. Moshennichestvo s ispol′zovaniem informatsionno-telekommunikatsionnykh tekhnologij i priemov sotsial′noj inzhenerii: kriminologicheskoe issledovanie : avtoref. dis. … kand. yurid. nauk / Zotina Elena Vladimirovna. — Kazan′, 2025. — S. 11.

16. Khajrusov D. S. Kriminologiya : uchebnoe posobie. — M. : Yurajt, 2024. — S. 44.

17. Osipenko A. L., Solov′ev V. S. Kiberugrozy v otnoshenii nesovershennoletnikh i osobennosti protivodejstviya im s primeneniem informatsionnykh tekhnologij // Obshchestvo i pravo. — 2019. — № 3(69). — S. 23—24.

18. Krasev D. V. Kriminologicheskie osobennosti organizovannogo moshennichestva v sfere informatsionnykh tekhnologij // Voprosy rossijskogo i mezhdunarodnogo prava. — 2025. – T. 15. — № 3-1. — S. 571.

СВЕДЕНИЯ ОБ АВТОРАХ

Белоусова Анна Николаевна. Доцент кафедры уголовного права и криминологии. Кандидат юридических наук, доцент.
Воронежский институт МВД России.
E-mail: velanna22@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Запорожцева Евгения Андреевна. Курсант.
Воронежский институт МВД России.
Россия, 394065, Воронеж, проспект Патриотов, 53.

Belousova Anna Nikolaevna. Associate Professor of the chair of Criminal Law and Criminology. Candidate of Law, Associate Professor.
E-mail: velanna22@mail.ru
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Zaporozhtseva Evgeniya Andreevna. Cadet.
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: несовершеннолетние; виктимность; информационное пространство; интернет-ресурсы; интеренет-платформы, цифровизация; вовлечение в мошеннические действия, криминогенность информационного пространства; социальные сети.

Key words: minors; victimization; information space; Internet resources; Internet platforms, digitalization; involvement in fraudulent activities, criminality of the information space; social networks.

УДК 343.971

Е. А. Буданова, *кандидат юридических наук, доцент*
Э. Р. Шикалова

КРИМИНОЛОГИЧЕСКИЙ АНАЛИЗ СОВРЕМЕННОГО ЭКСТРЕМИЗМА: ТРАДИЦИОННЫЕ И ЦИФРОВЫЕ ФОРМЫ ПРОЯВЛЕНИЯ

CRIMINOLOGICAL ANALYSIS OF MODERN EXTREMISM: TRADITIONAL AND DIGITAL FORMS OF MANIFESTATION

В статье рассматриваются современные формы экстремизма, проявляющиеся как в традиционной, так и в цифровой среде. На основе криминологического анализа раскрываются подходы к пониманию экстремизма, его основные виды, особенности организованных и молодежных форм, а также роль сети Интернет в распространении радикальных установок и вовлечении уязвимых лиц, прежде всего несовершеннолетних. Особое внимание уделяется статистической динамике преступлений экстремистской направленности и вопросам профилактики. Обосновывается вывод о необходимости сочетания уголовно-правовых, организационных и воспитательно-профилактических мер противодействия экстремизму.

The article examines contemporary forms of extremism manifested in both traditional and digital environments. Based on a criminological analysis, it identifies approaches to understanding extremism, its main types, the specifics of organized and youth-related forms, and the role of the Internet in spreading radical attitudes and recruiting vulnerable persons, especially minors. Particular attention is paid to the statistical dynamics of extremist crimes and to prevention issues. The article substantiates the conclusion that countering extremism requires a combination of criminal-law, organizational, and educational preventive measures.

Экстремизм в современных условиях сохраняет статус одной из наиболее опасных угроз общественной безопасности, поскольку его проявления охватывают не только традиционные формы насилия, но и цифровое пространство [1]. Изучение данного явления требует комплексного криминологического подхода, позволяющего выявить его основные формы, тенденции развития и направления эффективного предупреждения.

Экстремизм является крайней формой интолерантности, соединенной с агрессией и насилием как методами выражения непримиримости к другому [2]. Актуальность исследования обусловлена не только традиционными формами радикальной деятельности, связанными с уличным насилием, деятельностью запрещенных объединений или распространением печатных материалов, но и распространением экстремизма в цифровой среде. Это сделало экстремистские практики более гибкими по способу распространения и повысило возможность быстрого вовлечения уязвимых участников, прежде всего молодежи. Подтверждается это официальной статистикой: в 2024 году в России зарегистрировано 1719 преступлений экстремистской направленности, а за январь — декабрь 2025 года — уже 2241, что показывает сохранение роста и высокой общественной опасности рассматриваемого явления [3].

Правоприменительная статистика субъектов учета также свидетельствует об активизации выявления преступлений экстремистской направленности. За январь — май 2025 года всего выявлено 941 такое преступление (+39,0%), из них сотрудниками Следственного комитета Российской Федерации — 37 (+85,0%), органов внутренних дел — 458 (+36,3%); удельный вес органов внутренних дел составил 48,7%, таможенных органов — 0. Эти показатели позволяют сделать вывод, что рост фиксируется не только на уровне регистрации и раскрытия, но и на уровне выявления соответствующих деяний, а значит, рассматриваемое явление требует не эпизодических, а системных профилактических и правоохранительных мер [3].

Кроме того, статистические данные свидетельствуют о том, что преступления террористического характера и экстремистской направленности остаются достаточно распространенными наравне с другими видами, в которых участвуют несовершеннолетние. Следует отметить, что применительно к рассматриваемой категории преступлений речь идет в основном о вовлечении

несовершеннолетних в их совершение. Это объясняется тем, что несовершеннолетние являются незащищенным слоем общества, отличающимся повышенной виктимностью, а также низким уровнем психологической и эмоциональной устойчивости. В социальной коммуникации подростков в разных ее видах открыто или завуалированно все чаще прослеживается влияние элементов идеологии экстремизма и терроризма. Внешние проявления этого явления нередко наблюдаются в трансляции идеи социального, расового, национального превосходства, угнетения своих социальных оппонентов. Указанные обстоятельства обусловливают необходимость обращения не только к социальным и криминологическим характеристикам экстремизма, но и к современным государственным механизмам его предупреждения и пресечения.

Так, утверждение новой Стратегии противодействия экстремизму в Российской Федерации Указом Президента РФ от 28 декабря 2024 г. № 1124 закрепило обновленные ориентиры государственной политики в этой сфере, включая профилактику, мониторинг и пресечение экстремистских проявлений, в том числе в сети Интернет [4]. В этой связи представляется необходимым обратиться к эволюции самого понятия экстремизма, поскольку именно изменение его содержания позволяет точнее определить пределы правового регулирования и направления практического противодействия.

Изначально в законодательстве различных стран под экстремизмом понимались действия, направленные на насильственное изменение конституционного строя, подрыв государственного единства и территориальной целостности. Однако со временем это определение расширилось, включив в себя широкий спектр деяний, объединенных общей целью — возбуждение ненависти или вражды, унижение человеческого достоинства по различным признакам (раса, национальность, вероисповедование, социальная принадлежность и т. д.), а также пропаганда исключительности и превосходства одних групп над другими.

На сегодняшний день отсутствует единое, универсальное определения экстремизма, принятого всеми странами [5]. Однако общим для большинства уголовных кодексов является акцент на противоправных действиях, направленных на подрыв общественного порядка и безопасности, дестабилизацию общества и создание атмосферы насилия и нетерпимости.

Развитие экстремизма как правового понятия можно условно разделить на этапы: от первоначального фокуса на насильственном изменении власти к включению в сферу уголовной ответственности различных форм пропаганды ненависти, дискриминации, насилия, а также организации и участия в экстремистских сообществах.

В научной литературе экстремизм традиционно связывается с приверженностью крайним взглядам и методам, а в дальнейшем — с политическими и идеологическими практиками, ориентированными на достижение власти и влияния посредством радикальных средств [6]. Отсутствие единого и четкого определения экстремизма порождает множество его интерпретаций, классифицируемых по различным параметрам: направленности, мотивации и целям. Эта вариативность затрудняет создание единой модели противодействия, что подчеркивает актуальность дальнейшего исследования данного феномена.

Наиболее распространенными видами экстремизма, выделяемыми по направленности, традиционно считаются религиозный и национальный экстремизм. К ним, исходя из мотивации, относится и политический экстремизм.

Религиозный экстремизм проявляется в форме нетерпимости к иным конфессиям или в ожесточенном противостоянии внутри одной религиозной структуры, используя религиозную догматику как инструмент оправдания насилия и дискриминации. Национальный экстремизм, зарождаясь в межнациональных отношениях, подпитывает враждебность между различными этническими группами, основываясь на идеологии превосходства одной нации над другими, что способно приводить к масштабным конфликтам. Политический экстремизм характеризуется применением радикальных методов в борьбе с властью; использование террористических актов как инструмента достижения политических целей является одним из наиболее опасных проявлений такого подхода.

Современные формы экстремизма, как правило, организованны и структурированы, свое отражение они находят в деятельности экстремистских организаций. Согласно действующему законодательству РФ экстремистской организацией признается общественное или религиозное объединение либо иная организация, чья деятельность признана судом незаконной и запрещенной вследствие осуществления экстремистской деятельности. Список таких организаций постоянно обновляется и доступен на официальном сайте Министерства юстиции РФ [7]. Динамичный характер списка подчеркивает эволюцию экстремистских угроз и необходимость постоянного мониторинга.

В зависимости от идеологической направленности условно можно выделить «левый» и «правый» экстремизм. «Левый экстремизм, опираясь

на идеи революционизма и анархизма, позиционирует себя как защитник интересов трудящихся и обездоленных слоев населения, критикуя социальное неравенство и подавление личности» [8]. Для достижения своих целей такие организации готовы прибегать к любым методам, в том числе к вооруженному восстанию. В качестве исторических примеров обычно приводятся «Фракция Красной Армии» в Германии и «Красные бригады» в Италии.

«Правый» экстремизм, включающий фашистские, неофашистские, националистические и расистские движения, критикует современное общество через идеи «деградации морали», «господства денег» и иные подобные конструкции. Для него также характерно использование насилия, а в современных условиях и активное применение сетевых каналов распространения идеологии, что усложняет своевременное выявление таких проявлений [9].

Отдельно стоит выделить молодежный экстремизм, отражающий культивирование насилия и агрессии в молодежной среде. В отличие от более организованных форм такой экстремизм часто характеризуется стихийностью, эмоциональностью и отсутствием глубоко разработанной идеологической доктрины. Это обусловлено, прежде всего, возрастными особенностями: несформированным мировоззрением, повышенной внушаемостью и сниженным чувством страха перед правовыми последствиями. Распространение молодежного экстремизма в последнее десятилетие проявлялось в игнорировании общественных норм и правил поведения, что, по сути, является симптомом грубого социального диссонанса [10].

Инициация вовлечения в экстремистские группировки нередко происходит через участие в асоциальных неформальных субкультурах (футбольные фанатские группировки, сатанистские организации и др.). При этом цифровые технологии играют значительную роль в распространении экстремистских идей среди молодежи [11]. Киберпространство стало удобной площадкой для совершения экстремистских преступлений и правонарушений, а также для вербовки, координации и идеологической обработки пользователей.

Для понимания идеологических основ и методов распространения экстремизма необходим анализ экстремистских материалов. Согласно законодательству РФ — это информация на любых носителях, призывающая к экстремистской деятельности, обосновывающая и оправдывающая ее необходимость. К таким материалам могут относиться не только современные публикации, но и тексты, оправдывающие нацистские преступления, геноцид, расовое или национальное превосходство. Учитывая быстрое развитие технологий и способов коммуникации в сети Интернет, проблема обнаружения и блокировки подобных материалов является одной из ключевых задач в противодействии экстремизму.

Существует и классификация экстремизма по методам воздействия, где выделяются три основные группы: экстремизм, основанный на физическом насилии (убийства, увечья, лишение свободы), экстремизм, связанный с уничтожением материальных объектов (поджоги, разрушение имущества), и экстремизм, использующий методы морально-психологического давления (угрозы, шантаж, распространение дезинформации) [12]. Практика показывает, что экстремистские акции редко ограничиваются одним методом, чаще всего наблюдается комплексное применение, приоритетность которого определяется конкретными обстоятельствами: ресурсами экстремисткой группировки, политическим контекстом и региональной спецификой.

Разделение экстремизма по используемым средствам позволяет выделить две основных формы: традиционный и технологический. Традиционный экстремизм использует классические средства: огнестрельное и холодное оружие, взрывчатые вещества и взрывные устройства. Указанные способы известны на протяжении длительного исторического периода и находили применение в различных проявлениях политически мотивированного насилия. Технологический экстремизм опирается на современные достижения науки и техники: информационные технологии, радиоэлектронику, а в перспективе — и более опасные технологии (ядерные материалы, генные модификации) [13]. Именно эта трансформация делает цифровое измерение экстремизма самостоятельным объектом криминологического анализа.

Сегодня экстремизм все также продолжает оказывать тяжелое влияние на общество, подрывая основы демократических ценностей и стабильности. Он приводит к социальной напряженности, дискриминации и разделению людей по различным признакам. При этом моральные нормы, традиции, общепринятые правила поведения и интересы окружающих не останавливают экстремистов: они исходят из установки, согласно которой цель оправдывает средства, и потому прибегают к запугиванию, насилию и иным крайним методам.

В настоящее время экстремизм является одной из наиболее сложных социально-политических проблем современного российского общества. Это обусловлено разнообразием его проявлений и разнородным составом организаций, имеющих экстремистскую направленность, а также

отказом от компромисса и использованием насилия для достижения целей. Сущность экстремизма заключается в глубоком убеждении его последователей в исключительной правоте собственной идеологии, что приводит к непринятию альтернативных точек зрения и к агрессивному отношению к тем, кто не разделяет их взгляды.

В условиях глобализации и распространения информации через сеть Интернет экстремистские идеи быстро тиражируются, способствуя радикализации отдельных лиц и групп, межэтническим конфликтам и вовлечению несовершеннолетних в противоправную деятельность. Именно поэтому законодательство и стратегические документы в рассматриваемой сфере ориентированы не только на пресечение, но и на предупреждение экстремистских проявлений [13].

В связи с этим необходимо сместить центр тяжести с исключительно запретительной модели на раннюю профилактику. Экстремизм не может эффективно сдерживаться только уголовным наказанием, поскольку наказание вступает в действие уже после того, как лицо радикализировано, вовлечено в деструктивную среду или совершило конкретное деяние. Более перспективен иной подход: работа с причинами и условиями. В литературе последних лет предлагается исходить из необходимости баланса между системой юридической ответственности и деятельностью общественных институтов. Иначе говоря, школа, семья, вуз, молодежные объединения, учреждения культуры, органы местного самоуправления, комиссии по делам несовершеннолетних и правоохранительные органы должны не дублировать друг друга, а действовать согласованно в одном направлении. Для этого нужны реальные, а не формальные программы правового просвещения, медиаграмотности, навыков распознавания манипуляции и дезинформации, а также создание легальных каналов для гражданской активности молодежи [14].

Проведенное исследование позволяет сделать вывод о том, что современный экстремизм представляет собой не просто совокупность отдельных противоправных проявлений, а сложное социально-правовое и криминологическое явление, способное адаптироваться к изменяющимся общественным и технологическим условиям. Его общественная опасность определяется не только направленностью на подрыв основ конституционного строя, общественной безопасности и межгруппового согласия, но и способностью формировать устойчивую среду нетерпимости, агрессии и радикального отрицания правовых и нравственных норм.

Анализ показал, что в настоящее время экстремизм развивается в двух взаимосвязанных измерениях — традиционном и цифровом. Если ранее экстремистская активность преимущественно выражалась в деятельности организаций, публичных призывах, насильственных акциях и распространении запрещенных материалов офлайн, то сегодня все большее значение приобретают информационно-коммуникационные технологии. Цифровая среда существенно расширяет возможности распространения радикального контента, обеспечивает анонимность участников, ускоряет вовлечение новых сторонников и облегчает координацию противоправной деятельности [15]. Особенно уязвимой категорией в таких условиях выступает молодежь, для которой интернет-пространство является естественной средой коммуникации, социализации и получения информации [16].

Статистические данные свидетельствуют о сохраняющейся высокой криминологической значимости преступлений экстремистской направленности и подтверждают необходимость дальнейшего совершенствования мер противодействия. Вместе с тем эффективная борьба с экстремизмом не может ограничиваться исключительно уголовно-правовым пресечением. Необходим комплексный подход, объединяющий правовые, организационные, информационные, воспитательные и профилактические механизмы.

В связи с этим приоритетным направлением следует признать раннее предупреждение экстремистских проявлений, основанное на межведомственном взаимодействии, развитии правового просвещения, формировании медиаграмотности и критического мышления, прежде всего в молодежной среде. Только сочетание криминологического анализа официальной статистики и системной профилактической работы позволяет адекватно оценить масштабы проблемы и определить наиболее результативные пути ее дальнейшего решения.

ЛИТЕРАТУРА

1. Игнатов А. Н. Современные трансформации экстремизма и терроризма // Актуальные проблемы противодействия экстремизму, русофобии и украинскому неонацизму : материалы всероссийской научно-практической конференции, Симферополь, 03 мая 2024 года. — Краснодар : Краснодарский университет МВД России, 2024. — С. 68—72.

2. Баева Л. В. Экстремизм: природа и формы проявления // Каспийский регион: политика, экономика, культура. — 2008. — № 3(16). — С. 21—25.

3. Данные ГИАЦ МВД РФ : официальный сайт. — URL: https://мвд.рф/reports/item/77848182/ (дата обращения: 15.04.2026).

4. Об утверждении Стратегии противодействия экстремизму в Российской Федерации : указ Президента Российской Федерации от 28.12.2024 № 1124 // Официальный интернет-портал правовой информации. — 2024.

5. Махмутова К. М. Проблемы определения понятия «экстремизм» // Меридиан : научный электронный журнал. — 2021. — № 9(62). — С. 123—125.

6. Плотников В. В. К вопросу о противодействии идеологии экстремизма // Военная мысль. — 2016. — № 2. — С. 3—10.

7. Перечень общественных и религиозных объединений, иных организаций, в отношении которых вступило в законную силу решение суда о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» // Официальный сайт Министерства юстиции Российской Федерации. — URL: https://minjust.gov.ru/ru/documents/7822/ (дата обращения: 15.04.2026).

8. Шарипов И. И. Левый экстремизм // Актуальные проблемы противодействия идеологии терроризма и экстремизма в современном обществе : материалы городской научно-практической конференции, Казань, 20 апреля 2018 года. — Казань : Казанский государственный технический университет им. А. Н. Туполева, 2018. — С. 226—228.

9. Кардашевская М. В. Уголовно-правовые и криминалистические проблемы расследования отдельных видов преступлений : монография : в 2 т. / под ред. А. Ф. Волынского, С. Л. Никоновича. — Тамбов — Липецк : Першина Р. В., 2011. — С. 158.

10. Никитина Т. А., Теретьева И. А. Противодействие распространению экстремистской идеологии в информационном пространстве России // Вестник Поволжского института управления. — 2019. — Т. 19. — № 3. — С. 101.

11. Игнатов А. Н. Виртуализация угрозы экстремизма и ее отражение в субкультуре несовершеннолетних // Судебная экспертиза и исследования. — 2025. — № 3. — С. 106—110.

12. Лапунова Ю. А. Распространение идеологии экстремизма и терроризма в киберпространстве: проблемы и пути их решения // Труды Академии управления МВД России. — 2017. — № 3(43). — С. 103.

13. Гаврилин Ю. В., Шмонин А. В. Использование информации, полученной из сети Интернет, в расследовании преступлений экстремистской направленности // Труды Академии МВД России. — 2019. — № 1(49). — С. 108.

14. Пучнина М. Ю. Способы вовлечения несовершеннолетних в совершение преступлений террористического характера и экстремистской направленности // Сборник научных трудов по итогам научно-представительских мероприятий, проводимых в Уфимском юридическом институте МВД России в 2024 году. — Уфа : Уфимский юридический институт МВД России, 2024. — С. 397—401.

15. Смыслова В. Н. Предупреждение преступлений экстремистской направленности в условиях радикализации и роста протестной активности населения с позиции интегративной концепции правопонимания: сдвиг парадигмы // Сибирский юридический вестник. — 2024. — № 2(105). — С. 94—102.

16. Пучнина М. Ю., Пучнин А. В. Факторы, способствующие вовлечению несовершеннолетних в совершение преступлений экстремистской направленности и террористического характера // Вестник Воронежского института МВД России. — 2024. — № 2. — С. 250—255.

REFERENCES

1. Ignatov A. N. Sovremennye transformatsii ekstremizma i terrorizma // Aktual′nye problemy protivodejstviya ekstremizmu, rusofobii i ukrainskomu neonatsizmu : materialy vserossijskoj nauchno-prakticheskoj konferentsii, Simferopol′, 03 maya 2024 goda. — Krasnodar : Krasnodarskij universitet MVD Rossii, 2024. — S. 68—72.

2. Baeva L. V. Ekstremizm: priroda i formy proyavleniya // Kaspijskij region: politika, ekonomika, kul′tura. — 2008. — № 3(16). — S. 21—25.

3. Dannye GIATs MVD RF : ofitsial′nyj sajt. — URL: https://mvd.rf/reports/item/77848182/ (data obrashcheniya: 15.04.2026).

4. Ob utverzhdenii Strategii protivodejstviya ekstremizmu v Rossijskoj Federatsii : ukaz Prezidenta Rossijskoj Federatsii ot 28.12.2024 № 1124 // Ofitsial′nyj internet-portal pravovoj informatsii. — 2024.

5. Makhmutova K. M. Problemy opredeleniya ponyatiya «ekstremizm» // Meridian : nauchnyj elektronnyj zhurnal. — 2021. — № 9(62). — S. 123—125.

6. Plotnikov V. V. K voprosu o protivodejstvii ideologii ekstremizma // Voennaya mysl′. — 2016. — № 2. — S. 3—10.

7. Perechen′ obshchestvennykh i religioznykh ob″edinenij, inykh organizatsij, v otnoshenii kotorykh vstupilo v zakonnuyu silu reshenie suda o likvidatsii ili zaprete deyatel′nosti po osnovaniyam, predusmotrennym Federal′nym zakonom ot 25.07.2002 № 114-FZ «O protivodejstvii ekstremistskoj deyatel′nosti» // Ofitsial′nyj sajt Ministerstva yustitsii Rossijskoj Federatsii. — URL: https://minjust.gov.ru/ru/documents/7822/ (data obrashcheniya: 15.04.2026).

8. Sharipov I. I. Levyj ekstremizm // Aktual′nye problemy protivodejstviya ideologii terrorizma i ekstremizma v sovremennom obshchestve : materialy gorodskoj nauchno-prakticheskoj konferentsii, Kazan′, 20 aprelya 2018 goda. — Kazan′ : Kazanskij gosudarstvennyj tekhnicheskij universitet im. A. N. Tupoleva, 2018. — S. 226—228.

9. Kardashevskaya M. V. Ugolovno-pravovye i kriminalisticheskie problemy rassledovaniya otdel′nykh vidov prestuplenij : monografiya : v 2 t. / pod red. A. F. Volynskogo, S. L. Nikonovicha. — Tambov — Lipetsk : Pershina R. V., 2011. — S. 158.

10. Nikitina T. A., Teret′eva I. A. Protivodejstvie rasprostraneniyu ekstremistskoj ideologii v informatsionnom prostranstve Rossii // Vestnik Povolzhskogo instituta upravleniya. — 2019. — T. 19. — № 3. — S. 101.

11. Ignatov A. N. Virtualizatsiya ugrozy ekstremizma i ee otrazhenie v subkul′ture nesovershennoletnikh // Sudebnaya ekspertiza i issledovaniya. — 2025. — № 3. — S. 106—110.

12. Lapunova Yu. A. Rasprostranenie ideologii ekstremizma i terrorizma v kiberprostranstve: problemy i puti ikh resheniya // Trudy Akademii upravleniya MVD Rossii. — 2017. — № 3(43). — S. 103.

13. Gavrilin Yu. V., Shmonin A. V. Ispol′zovanie informatsii, poluchennoj iz seti Internet, v rassledovanii prestuplenij ekstremistskoj napravlennosti // Trudy Akademii MVD Rossii. — 2019. — № 1(49). — S. 108.

14. Puchnina M. Yu. Sposoby vovlecheniya nesovershennoletnikh v sovershenie prestuplenij terroristicheskogo kharaktera i ekstremistskoj napravlennosti // Sbornik nauchnykh trudov po itogam nauchno-predstavitel′skikh meropriyatij, provodimykh v Ufimskom yuridicheskom institute MVD Rossii v 2024 godu. — Ufa : Ufimskij yuridicheskij institut MVD Rossii, 2024. — S. 397—401.

15. Smyslova V. N. Preduprezhdenie prestuplenij ekstremistskoj napravlennosti v usloviyakh radikalizatsii i rosta protestnoj aktivnosti naseleniya s pozitsii integrativnoj kontseptsii pravoponimaniya: sdvig paradigmy // Sibirskij yuridicheskij vestnik. — 2024. — № 2(105). — S. 94—102.

16. Puchnina M. Yu., Puchnin A. V. Faktory, sposobstvuyushchie vovlecheniyu nesovershennoletnikh v sovershenie prestuplenij ekstremistskoj napravlennosti i terroristicheskogo kharaktera // Vestnik Voronezhskogo instituta MVD Rossii. — 2024. — № 2. — S. 250—255.

СВЕДЕНИЯ ОБ АВТОРАХ

Буданова Елена Александровна. Начальник кафедры уголовного права и криминологии. Кандидат юридических наук, доцент.
Воронежский институт МВД России.
E-mail: budanovaelena@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Шикалова Эльмира Радиевна. Слушатель.
Воронежский институт МВД России.
E-mail: elmira.ziganshina.03@inbox.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Budanova Elena Aleksandrovna. Head of the chair of Criminal Law and Criminology. Candidate of Law, Associate Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: budanovaelena@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Shikalova Elmira Radiyevna. Listener.

Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: elmira.ziganshina.03@inbox.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: экстремизм; преступления экстремистской направленности; радикализация; цифровой экстремизм; молодежный экстремизм; сеть Интернет; экстремистские материалы; профилактика экстремизма; криминологический анализ; общественная безопасность.

Key words: extremism; extremist crimes; radicalization; digital extremism; youth extremism; Internet; extremist materials; prevention of extremism; criminological analysis; public safety.

УДК 343.85

Р. В. Колесников, *кандидат юридических наук, доцент*
Я. В. Юрьева

ПУБЛИЧНЫЕ ПРИЗЫВЫ К ОСУЩЕСТВЛЕНИЮ ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ СМИ ЛИБО ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, В ТОМ ЧИСЛЕ СЕТИ ИНТЕРНЕТ: ПОНЯТИЕ, ВОПРОСЫ КВАЛИФИКАЦИИ И СУДЕБНАЯ ПРАКТИКА

PUBLIC CALLS TO CARRY OUT EXTREMIST ACTIVITIES USING THE MEDIA OR INFORMATION AND TELECOMMUNICATION NETWORKS, INCLUDING THE INTERNET: CONCEPT, QUALIFICATION ISSUES, AND COURT PRACTICE

В работе реализован комплексный подход к исследованию категории «экстремистская деятельность», а также к анализу правовых и прикладных вопросов квалификации публичных призывов к ее осуществлению. Особое внимание уделено выявлению пробелов и противоречий в действующем законодательстве Российской Федерации. Проведено обобщение судебной практики, позволившее установить типичные правоприменительные ошибки, в том числе связанные с разграничением подстрекательства к экстремистской деятельности и публичных призывов к такой деятельности. С учетом полученных результатов предложена новая редакция абз. 3 п. 4 Постановления Пленума Верховного Суда РФ от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности», которая, по нашему мнению, способна повысить качество правоприменения в сфере противодействия экстремизму.

This paper implements a comprehensive approach to studying the category of "extremist activity," as well as to analyzing the legal and practical aspects of classifying public calls to engage in such activity. Particular attention is paid to identifying gaps and inconsistencies in current Russian legislation. A summary of judicial practice has been conducted, revealing typical law enforcement errors, including those related to the distinction between incitement to extremist activity and public calls to such activity. Based on these findings, a new version of paragraph 1 of Article 11 of the Criminal Code is proposed. 3 paragraph 4 of the Resolution of the Plenum of the Supreme Court of the Russian Federation of June 28, 2011 No. 11 "On judicial practice in criminal cases involving crimes of an extremist nature", which, in our opinion, can improve the quality of law enforcement in the area of countering extremism.

По официальным статистическим данным МВД России в 2021 году было зарегистрировано 1057 преступлений экстремистской направленности (+26,9%). В 2022 году 1566 преступлений (+48,2%). В 2023 году 1340 преступлений (-14,4%). В 2024 году 1719 преступлений (+28,3%). В 2025 году 2241 преступление (+30,4%). В январе—марте 2026 года зарегистрировано 708 преступлений экстремистской направленности (+28,3%) [1].

На основании статистики, представленной на официальном сайте МВД России, можно сделать вывод о том, что преступления экстремистской направленности имеют отрицательную тенденцию, то есть стабильно увеличивается их количество. В связи с этим необходимы исследования в области проблемных вопросов квалификации публичных призывов к осуществлению экстремистской деятельности.

Приступая к рассмотрению заявленной проблематики, целесообразно обратиться к этимологическому и содержательному анализу понятий «экстремизм» и «экстремистская идеология». Актуальность исследования экстремизма обусловлена современной геополитической ситуацией и необходимостью совершенствования механизмов противодействия преступлениям экстремистской направленности. Особое значение в данном контексте приобретает изучение вопросов квалификации публичных призывов к осуществлению экстремистской деятельности, что соответствует актуальным задачам, стоящим перед

МВД России. На заседании коллегии МВД России Президент Российской Федерации В. В. Путин акцентировал внимание на необходимости жесткого уголовно-правового реагирования на распространение экстремистских настроений, указав, что проявления национальной и религиозной нетерпимости, а также агрессивный радикализм представляют угрозу единству многонационального народа России, суверенитету и территориальной целостности государства. Для того чтобы всесторонне охарактеризовать современный экстремизм как противоправное деяние, необходимо рассмотреть отечественную правовую доктрину с применением достижений научного познания в области социальных, гуманитарных и политических наук.

А. А. Хоровинников с позиции философии считает, что сущность экстремизма заключается в отрицании, а впоследствии и разрушении устойчивой, регулярной идентичности и всегда сопровождается насилием, агрессией и изменением человеческого сознания через принятие определённых идей [2]. На наш взгляд, такой подход к пониманию термина «экстремизм» отражает всего лишь некоторые признаки современного экстремизма как противоправного деяния и не раскрывает его природу.

По мнению А. И. Веруш, экстремизм — это явление, которое выражается в наличии антиобщественных взглядов и поступков [3]. Такое определение представляется нам слишком расплывчатым и универсальным, то есть любое негативное явление либо общественно опасное деяние можно подвести под данную дефиницию.

По нашему мнению, наиболее содержательное философское определение экстремизма предложено Х. Ш. Килясхановым. Автор рассматривает экстремизм как форму радикальной активности субъектов, ориентированных на полное отрицание сложившейся социально-политической организации общества, правовой основы государства и на их насильственную трансформацию [4].

В политологии экстремизм представляется как радикальная деятельность субъектов, которые используют крайние способы и методы для достижения определённых целей в политике.

Ученые-политологи утверждают, что экстремизм носит ситуативный характер. Он используется, когда иные способы достижения целей в области политики становятся неэффективными или перестают действовать. Следовательно, специфика экстремизма с точки зрения политологии заключается не столько в идеях и целях, как в философии, сколько в методах и способах.

Е. Н. Гречкина характеризует экстремизм как совокупность идейных установок и практических методов, применяемых субъектами политической жизни, которые пропагандируют либо используют насилие и иные крайние средства для достижения политических целей [5].

Это определение отражает два наиболее важных признака экстремизма как противоправного деяния: способы, которые обязательно должны носить насильственный характер; идеи, то есть то, ради чего, собственно, и применяются те или иные методы.

С позиции права экстремизм рассматривается как агрессивное, наиболее разрушительное явление, которое выражается в антиобщественном настрое социальных групп. Как отмечает А. Г. Залужный, их цель заключается в демонстрации не только отдельно взятому государству, но и всему мировому сообществу, что поддержание правопорядка на принципах демократии не является верным вектором развития общества [6].

А. А. Можегова определяет исследуемое понятие как «многоаспектное социально-правовое явление, содержащие в себе не только определенную антисоциальную деятельность, но и одобряющую подобную деятельность идеологию, направленную на формирование в обществе состояния нетерпимости к представителям определенных социальных групп, выделенных на основе установленных законодателем либо определяемых правоприменителем с учётом конкретных обстоятельств уголовного дела критериев» [7]. На наш взгляд, предложенная дефиниция наиболее полно отражает идеологическую сторону экстремизма.

Приняв во внимание рассмотренные выше подходы к пониманию современного экстремизма как противоправного деяния с точки зрения социально-правовых наук, можно выделить следующие признаки.

Во-первых, экстремизм является противоправным и общественно опасным явлением, то есть совершение экстремистских действий приводит к нарушению правовых норм, которые находят свое отражение в отечественном законодательстве. Несоблюдение закона, в свою очередь, подвергает риску существование стабильности в обществе, нарушает общественный правопорядок и подрывает общественную безопасность государства.

Во-вторых, существенным признаком экстремизма как противоправного деяния выступает насильственный характер используемых методов. Именно посредством таких способов экстремисты идут к достижению поставленных целей.

В-третьих, экстремисты, осуществляющие противоправную деятельность, применяют методы, которые носят радикальный характер и затрагивают основы, принципы конституционного строя.

В-четвертых, экстремизм как противоправное деяние обладает выраженной идеологической направленностью. Это проявляется не только в отрицании иных взглядов, но и в активном распространении собственной системы идей, которая, как правило, ориентирована на подрыв основ конституционного строя Российской Федерации либо выражается в нетерпимости к отдельным социальным, религиозным или иным группам.

Особое значение имеет идеологический компонент экстремизма. Указом Президента Российской Федерации от 28 декабря 2024 г. № 1124 была утверждена Стратегия противодействия экстремизму в Российской Федерации, в которой закреплено понятие «экстремистская идеология».

Под экстремистской идеологией понимается совокупность взглядов и идей, обосновывающих или оправдывающих применение насилия для достижения политических, идеологических, религиозных и иных целей. Экстремистская идеология является инструментом вовлечения представителей различных социальных групп в экстремистскую деятельность.

Таким образом, экстремизм как противоправное деяние, на наш взгляд, представляет собой социально-правовое уголовно наказуемое и общественно опасное явление, основанное на экстремистской идеологии и выражающееся в крайних действиях либо приверженности радикальным взглядам физических или юридических лиц, социальных групп, политических партий и иных объединений. Такие субъекты используют насильственные либо ненасильственные радикальные методы для достижения определенных целей в сфере общественной и государственной жизнедеятельности.

Перейдем к рассмотрению основного вопроса заявленной темы научного исследования. Проанализировав уголовное законодательство Российской Федерации, мы пришли к выводу о том, что для верного определения объективных и субъективных признаков совершения публичных призывов к осуществлению экстремистской деятельности правоприменитель при квалификации противоправного деяния должен обращаться к Федеральному закону от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности» и Постановлению Пленума Верховного Суда РФ от 28 июня 2011 года № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» (далее — ППВС РФ № 11), поскольку ст. 280 УК РФ является бланкетной и не содержит в себе всех признаков состава преступления.

Согласно статистическим сведениям за 2025 г., 85% населения Российской Федерации пользуются сетью Интернет. Указанный показатель позволяет сделать вывод о повышенной общественной опасности публичных призывов к экстремистской деятельности, совершаемых посредством информационно-телекоммуникационных сетей, включая сеть Интернет. Расширение аудитории потенциального восприятия таких материалов увеличивает риск вовлечения лиц в совершение преступлений экстремистской направленности, ответственность за которые предусмотрена уголовным законодательством Российской Федерации.

Вместе с тем, несмотря на повышенную общественную опасность данного способа совершения преступлений экстремистской направленности, использование СМИ либо информационно-телекоммуникационных сетей, включая сеть Интернет, закреплено в качестве квалифицирующего признака только в ст. 280 и 280.1 УК РФ [8]. В ст. 282 УК РФ данный признак был включен в содержание объективной стороны основного состава преступления.

При исследовании квалифицированного состава преступления, предусмотренного ч. 2 ст. 280 УК РФ, необходимо учитывать разъяснения, содержащиеся в ППВС РФ № 11. В частности, в п. 6 указано, что при установлении факта использования СМИ либо информационно-телекоммуникационных сетей, включая сеть Интернет, правоприменителю следует обращаться к положениям Закона Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» и Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Изучив нормы Закона РФ № 2124-1, мы остановились на ст. 4, которая регламентирует недопустимость злоупотребления свободой СМИ. В правовой норме содержится запрет на использование СМИ в целях совершения деяний, ответственность за которые предусмотрена УК РФ. Запрет распространяется на все составы преступлений, которые предусмотрены Особенной частью УК РФ, в том числе и на ст. 280 УК РФ.

Данная ситуация может быть связана с тем, что Закон РФ № 2124-1 был принят в 1991 году с учетом складывающейся геополитической и социально-экономической обстановки того периода. Терроризм как негативное явление в 1990—2000 годах приобрел международный характер, в связи с этим уделялось особое внимание при составлении законодательной базы Российской Федерации международным договорам, направленным на противодействие терроризму [8]. Таким образом, при квалификации преступного деяния,

предусмотренного ч. 2 ст. 280 УК РФ, могут возникнуть противоречия и основания для оспаривания принятого решения.

Для устранения данного пробела предлагаем дополнить ст. 4 Закона РФ № 2124-1 в части запрета на распространение информации, которая содержит публичные призывы к осуществлению экстремистской деятельности или же публично оправдывает экстремизм.

Что касается правовых норм, содержащихся в Федеральном законе № 149-ФЗ, необходимо обратить внимание на ст. 15.3, которая регламентирует порядок ограничения доступа к информации, распространяемой с нарушением закона. В данном случае информация, распространяемая с нарушением закона, подлежит блокированию и ограничению доступа пользователей к ней.

Анализируемая норма Федерального закона № 149-ФЗ раскрывает содержание информации, распространяемой с нарушением закона. К такой информации, в частности, относятся материалы, содержащие призывы к осуществлению экстремистской деятельности, а также сведения, обосновывающие или оправдывающие необходимость ее совершения.

В теории уголовного права возникает справедливый вопрос о введении еще одного квалифицирующего признака в данную статью в виде специального субъекта. Так, А. А. Токбаев в своих научных работах говорит о недостатке ст. 280 УК РФ, который заключается в отсутствии специального субъекта и предлагает отнести к такому субъекту должностное лицо [10].

На наш взгляд, предложение о введении в ст. 280 УК РФ нового квалифицирующего признака является конструктивным, поскольку с учетом следственной и судебной практики имеются случаи, когда такие преступления совершены, в том числе и посредством сети Интернет, лицами, которые занимают определенные должности.

Проблематика квалификации публичных призывов к экстремистской деятельности во многом связана с разграничением смежных составов преступлений, а также с определением признака публичности соответствующего деяния, включая случаи его совершения посредством СМИ и информационно-телекоммуникационных сетей, в том числе сети Интернет [11].

Одним из значимых вопросов правоприменения является отграничение публичных призывов к экстремистской деятельности от подстрекательства к совершению преступлений экстремистского характера. Для этого необходимо обратиться к понятийному аппарату уголовного закона. В соответствии с ч. 4 ст. 33 УК РФ подстрекателем признается лицо, склонившее другое лицо к совершению преступления путем уговора, подкупа, угрозы либо иным способом [12].

Состав преступления, предусмотренный ст. 280 УК РФ, предполагает обязательное наличие публичности как признака объективной стороны. Следовательно, соответствующие призывы должны быть обращены к неопределенному кругу лиц [13]. При этом дискуссионным остается вопрос о численности лиц, которым могут быть адресованы публичные призывы к осуществлению экстремистской деятельности.

Представляется целесообразным при квалификации подобных деяний исходить из противопоставления указанных форм поведения: если при подстрекательстве к совершению преступлений экстремистской направленности воздействие обращено к конкретному лицу или определенному кругу лиц, то при публичных призывах адресаты, напротив, не индивидуализированы. Так, при квалификации считаем необходимым устанавливать, в каких именно взаимоотношениях находилось лицо, осуществляющее призывы или стремящееся к вовлечению в экстремистскую деятельность или же пытающееся вовлечь в совершение экстремистской деятельности, и те лица, на которых было направлено преступное деяние.

Например, решение Воркутинского городского суда Республики Коми в отношении гражданина К., который был осужден по ч. 1 ст. 280 УК РФ [14]. Из материалов уголовного дела, размещенных в открытых источниках, следует, что граждане К. и С. предпринимали действия по вовлечению группы лиц в создание экстремистского сообщества, разработав соответствующую схему его формирования и план дальнейшей деятельности. При этом существенным обстоятельством является то, что состав вовлекаемых лиц оставался постоянным и заранее определенным.

На наш взгляд, рассматриваемое судебное решение является примером существующих проблем в разграничении подстрекательства к совершению преступлений экстремистской направленности и публичных призывов к осуществлению такой деятельности, касающихся определения круга лиц, на который направлена преступная деятельность. С учетом проанализированных материалов уголовного дела можно сделать вывод о том, что у граждан К. и С. был умысел на вовлечение в преступную деятельность четко определенных знакомых им лиц.

Таким образом, полагаем, что при разграничении подстрекательства и публичных призывов к экстремистской деятельности необходимо исходить не столько из численности лиц, на которых направлен преступный умысел субъекта, сколько из личностных связей и отношений.

Подстрекательство к экстремистской деятельности необходимо квалифицировать согласно ст. 33 УК РФ в совокупности с соответствующей статьей Особенной части.

Например, ч. 1 ст. 280 УК РФ (если лицо побуждает к публичным призывам). Подстрекатель несет ответственность за соучастие в преступлении, даже если исполнителем оно не было совершено, если подстрекательство было доведено до конца (например, призывы были высказаны, но не привели к действиям).

В том случае, когда публичные призывы к экстремистской деятельности совершаются через подстрекательство, квалификация должна осуществляться следующим образом:

1) если лицо само совершает публичные призывы, оно несет ответственность как исполнитель по ч. 1 или ч. 2 ст. 280 УК РФ в зависимости от способа совершения;

2) если лицо побуждает другое лицо к совершению публичных призывов, оно привлекается как подстрекатель по ч. 4 ст. 33 УК РФ и ст. 280 УК РФ (например, лицо, организовавшее кампанию в интернете с целью побудить других публиковать экстремистские призывы, будет подстрекателем);

3) если подстрекательство направлено на совершение иных экстремистских действий (например, создание экстремистской организации), квалификация осуществляется по ч. 4 ст. 33 УК РФ в совокупности с соответствующими статьями (например, ст. 282.1 УК РФ).

На основании изложенного считаем необходимым изменить абз. 3 п. 4 ППВС РФ № 11, изложив его в следующей редакции: «При разрешении вопроса о публичном характере призывов судам необходимо учитывать место, обстановку и способ их выражения, характер личностных связей и отношения лица, совершающего призыв, а также иные обстоятельства конкретного дела. Публичными следует признавать призывы, выраженные в устной, письменной, визуальной, электронной или иной форме, если они адресованы неопределенному кругу лиц либо группе лиц в общественных местах, а равно распространены путем размещения печатной продукции, публикаций в СМИ, информационно-телекоммуникационных сетях, включая социальные сети, мессенджеры, видеохостинги и форумы, посредством массовой рассылки сообщений, в том числе электронных писем, push-уведомлений, сообщений в мобильных приложениях, либо иными способами, направленными на привлечение внимания широкой аудитории».

Что касается судебной практики привлечения лица, совершившего преступление, предусмотренное ч. 2 ст. 280 УК РФ, то заслуживает внимания приговор Хасавюртовского районного суда Республики Дагестан от 07 июня 2024 года по делу № 1-166/2024 [15].

Так, гражданин Б. совершил публичные призывы к осуществлению экстремистской деятельности путем размещения с личного аккаунта в приложении Telegram под наименованием «Абдурахман» под публикацией на странице открытого telegram-канала личного текстового комментария: «…нужна ваша помощь в Дагестане в Махачкале надо убить всех сотрудников…».

Свободный доступ к данному текстовому комментарию мог иметь неограниченный круг лиц из числа пользователей сети Интернет, в связи с чем сведения, содержащиеся в нем, стали общедоступными, то есть публичными.

Действия гражданина Б. обоснованно квалифицированы по ч. 2 ст. 280 УК РФ, так как: а) призывы к насилию в отношении сотрудников полиции были публичными, совершенными через интернет в открытом telegram-канале; б) разграничение с подстрекательством проведено верно, поскольку призывы адресованы неопределенному кругу лиц, а не конкретным исполнителям.

Подобное уголовное дело было рассмотрено Пугачевским районным судом Саратовской области 11 октября 2022 года № 1-160/2022 [16]. Из материалов приговора следует, что гражданин А. воспользовался своим мобильным устройством, ознакомился в социальной сети «ВКонтакте» с публикацией о языческом боге Велесе, имеющей негативное отношение к национальной группе евреев.

С целью реализации преступного умысла гражданин А., понимая, что размещенная им информация станет доступна неограниченному кругу пользователей интернет-ресурса, используя персональную страницу в социальной сети «ВКонтакте», разместил свой комментарий в виде текстового сообщения, содержащего нецензурную брань и побуждения (призывы) к изгнанию евреев, то есть побуждения (призывы) к совершению насильственных и дискриминационных действий в отношении представителей национальной группы евреев.

Суд постановил признать виновным гражданина А. в совершении преступления, предусмотренного ч. 1 ст. 282 УК РФ, и назначить лишение свободы с лишением права заниматься деятельностью, связанной с размещением обращений и иных материалов в информационно-телекоммуникационных сетях общего пользования, включая сеть Интернет.

На основе проанализированной судебной практики по уголовным делам гражданина Б. и

гражданина А. и с учетом изученной научной литературы по рассматриваемому вопросу мы пришли к выводу о том, что существуют проблемы разграничения составов преступлений, предусмотренных ч. 2 ст. 280 УК РФ и ч. 1 ст. 282 УК РФ.

Считаем необходимым наиболее детально проанализировать и сопоставить отдельные аспекты правового характера рассмотренного примера судебной практики с возможностью квалификации содеянного согласно ст. 282 УК РФ.

Изученные материалы уголовного дела в отношении гражданина А. у нас вызвали ряд вопросов. Призывы к «изгнанию» могут быть интерпретированы двояко: а) как призыв к насильственным действиям (ст. 280 УК РФ), если изгнание предполагает физическое принуждение; б) как возбуждение ненависти или вражды (ст. 282 УК РФ), если акцент ставится на формировании негативного отношения к евреям.

На наш взгляд, заслуживает внимания факт использования гражданином А. нецензурной брани и антисемитский контекст ее применения. Данные обстоятельства усиливают вероятность квалификации преступления в соответствии с ч. 1 ст. 282 УК РФ, особенно если призывы не содержат конкретных указаний на насилие.

Аналогичным примером будет выступать приговор Советского районного суда г. Воронежа от 21 февраля 2022 г. по делу № 1- 252/2022 [17], где гражданин Г., ранее привлеченный к административной ответственности по ст. 20.3.1 КоАП РФ, используя свою страницу «ВКонтакте», при помощи своего мобильного телефона марки «Xiaomi A2 Lite» под публикацией в сообществе «Я русский» разместил комментарий, унижающий человеческое достоинство лиц еврейской национальности.

В действиях гражданина Г. предусматривается умысел на унижение человеческого достоинства представителей еврейской национальности с использованием сети Интернет. Рассмотрев материалы уголовного дела, суд квалифицировал действия гражданина Г. по ч. 1 ст. 282 УК РФ и назначил наказание в виде лишения свободы.

Мы выделили наиболее значимые причины, на наш взгляд, которые создают правовые коллизии:

1) наличие неточностей в формулировке терминов, что при квалификации деяния может привести к нарушению принципов уголовного права. Понятие «экстремистская деятельность» (указанное в ст. 280 УК РФ) включает широкий круг действий, в том числе и те, которые могут пересекаться с диспозицией ст. 282 УК РФ;

2) субъективность интерпретации совершенных действий. Лингвистические экспертизы, используемые для квалификации, могут по-разному оценивать одно и то же высказывание (например, «изгнание» как насилие или как дискриминация);

3) пересечение в интернет-среде. Высказывания, сделанные в сети Интернет, зачастую содержат элементы и призывов, и возбуждения ненависти, что затрудняет процесс квалификации.

Анализируемая правовая ситуация может быть квалифицирована как конкуренция специальных норм Особенной части УК РФ. В подобных случаях с учетом положений уголовного закона, судебно-следственной практики и доктринальных подходов подлежит применению только одна уголовно-правовая норма. Такой вывод согласуется с ч. 1 ст. 50 Конституции РФ, согласно которой никто не может быть повторно осужден за одно и то же преступление, а также с ч. 2 ст. 6 УК РФ, закрепляющей недопустимость двойной уголовной ответственности за одно и то же деяние.

Вместе с тем ППВС РФ № 11 обращает внимание судов на то, что в ст. 280 УК РФ предусмотрена ответственность лишь за публичные призывы к осуществлению экстремистской деятельности. Публичное распространение информации, в которой обосновывается необходимость совершения противоправных действий в отношении лиц по признаку расы, национальности, религиозной принадлежности и т. д., либо информации, оправдывающей такую деятельность, следует квалифицировать по ст. 282 УК РФ при наличии иных признаков этого состава преступления.

В научной литературе представлена позиция, согласно которой при наличии в одном деянии признаков составов преступлений, предусмотренных обеими рассматриваемыми статьями, содеянное должно квалифицироваться по ст. 282 УК РФ [18]. Однако, по нашему мнению, такой подход не в полной мере соответствует условиям применения указанной нормы и не всегда позволяет корректно отразить уголовно-правовую сущность совершенного деяния.

В результате рассмотрения дискуссионных вопросов можно сделать следующие выводы:

1. Общественная опасность совершения публичных призывов к осуществлению экстремистской деятельности заключается в том, что общественно опасные последствия от совершенных преступных действий способны существенно дестабилизировать социально-политическую обстановку в государстве, нарушить общественный порядок, а также вызвать угрозу национальной безопасности.

2. Судам следует учитывать характер взаимодействия лица, совершающего призыв, с аудиторией, включая наличие умысла на побуждение к действиям, степень влияния на аудиторию (например, использование авторитета, доверия, эмоционального воздействия или иных форм убеждения), а также восприимчивость аудитории с учётом её состава, уровня организации или спонтанности собрания и иных факторов, способствующих реализации призыва.

3. Для разграничения публичных призывов и подстрекательства к их совершению судам необходимо учитывать, что публичные призывы характеризуются прямым обращением к неопределенному кругу лиц или группе лиц с целью побуждения к совершению противоправных действий.

4. Подстрекательство отличается направленностью на формирование у другого лица умысла совершить публичный призыв, а не непосредственное обращение к широкой аудитории. При квалификации судам следует анализировать, было ли деяние направлено на создание условий для последующих публичных призывов (подстрекательство) или на прямое побуждение аудитории к противоправным действиям (публичный призыв).

5. В ходе анализа судебной практики мы выявили проблемы при разграничении преступлений, предусмотренных ст. ст. 280 и 282 УК РФ. Для целей наиболее точного применения названных статей мы предлагаем внести изменения в отечественное уголовное законодательство, уточняющие правовую сущность терминов для целей применения ст. ст. 280, 282 УК РФ. Данная мера позволит минимизировать противоречия в части определения меры дозволенного поведения человека, а также поспособствует четкому установлению пределов криминализации. В качестве такого примера уточнения анализируемых уголовно-правовых норм стоит акцентировать внимание на конкретных действиях для целей применения ст. 280 УК РФ, а в ст. 282 УК РФ указать на формирование негативного отношения.

6. Мы выявили проблемы, связанные с разграничением подстрекательства к осуществлению экстремистской деятельности и публичных призывов к осуществлению такой деятельности. Соответственно, при квалификации деяний, где лицо подстрекает к совершению преступлений экстремистского характера, необходимо квалифицировать деяние, ссылаясь на Общую часть УК РФ. Однако, как показывает судебная практика, существуют ошибки при квалификации. В соответствии с названными обстоятельствами мы считаем, что необходимо внести в постановление Пленума Верховного Суда РФ от 28 июня 2011 года № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности», а именно в абз. 3. п. 4, изменения и изложить его в следующей редакции:

«При разрешении вопроса о публичном характере призывов судам необходимо учитывать место, обстановку и способ их выражения, характер личностных связей и отношения лица, совершающего призыв, а также иные обстоятельства конкретного дела. Публичными следует признавать призывы, выраженные в устной, письменной, визуальной, электронной или иной форме, если они адресованы неопределенному кругу лиц либо группе лиц в общественных местах, а равно распространены путем размещения печатной продукции, публикаций в СМИ, информационно-телекоммуникационных сетях, включая социальные сети, мессенджеры, видеохостинги и форумы, посредством массовой рассылки сообщений, в том числе электронных писем, push-уведомлений, сообщений в мобильных приложениях либо иными способами, направленными на привлечение внимания широкой аудитории».

ЛИТЕРАТУРА

1. Состояние преступности в России за 2021—2026 годы : статистика и аналитика // Официальный сайт МВД России. — URL: https://мвд.рф/folder/101762 (дата обращения: 25.04.2026).

2. Хоровинников А. А. Экстремизм как социальное явление: философский анализ : дис. ... канд. филос. наук. — Саратов, 2007. — 201 с.

3. Веруш А. И. Экстремизм как понятие и явление // Актуальные проблемы гуманитарных и социально-экономических наук. — 2019. — Т. 13. — № 4. — С. 34—37.

4. Килясханов Х. Ш. Современная деятельность ОБСЕ в сфере борьбы с терроризмом // Вестник Нижегородской академии МВД России. — 2012. — № 19. — С. 37.

5. Гречкина Е. Н. Молодежный политический экстремизм в условиях трансформирующейся российской действительности : дис. ... канд. полит. наук. — Ставрополь, 2006. — 174 с.

6. Залужный А. Г. Правовые гарантии противодействия экстремистской деятельности в политической, религиозной и других сферах общественной жизни // Закон и право. — 2002. — № 9. — С. 29—32.

7. Можегова А. А. Экстремистские преступления и преступления экстремистской направленности по уголовному праву Российской Федерации : дис. ... канд. юрид. наук. — М., 2015. — 169 с.

8. Узембаева Г. И. Общественная опасность преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных сетей // Вестник Волгоградской академии МВД России. — 2020. — № 1. — С. 91.

9. Хумаров М. С. Социально-правовая характеристика терроризма в России в 1990-х гг. и формирование государственной концепции по его предупреждению // Общество и право. — 2008. — № 2. — С. 12.

10. Токбаев А. А. Современные тенденции развития экстремизма в социальных сетях // Пробелы в российском законодательстве. — 2020. — № 4. — С. 109.

11. Пучнина М. Ю., Прохонов В. С. О проблеме вовлечения несовершеннолетних в экстремистскую деятельность с использованием информационно-коммуникационных технологий // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. — 2024. — № 10. — С. 104—109.

12. Будкова А. А., Устинова Е. П. Подстрекательство как вид соучастия в совершении преступления: основные проблемы и перспективы // Сфера науки. — 2025. — № 1. — С. 1—12.

13. Ахъядов Э. С. Анализ состава публичных призывов к осуществлению экстремистской деятельности (ст. 280 УК РФ) // Евразийский научный журнал. — 2021. — № 3. — С. 14.

14. Материалы уголовного дела № 1-10/2020. — URL: https://sudact.ru/regular/doc (дата обращения: 30.04.2026).

15. Материалы уголовного дела № 1-166/2024. — URL: https://sudact.ru/regular/doc (дата обращения: 30.04.2026).

16. Материалы уголовного дела № 1-160/2022. — URL: https://sudact.ru/regular/doc (дата обращения: 30.04.2026).

17. Материалы уголовного дела № 1-252/2022. — URL: https://sudact.ru/regular/doc (дата обращения: 30.04.2026).

18. Степанов В. В., Струков А. В. Проблемы разрешения конкуренции составов преступлений экстремистской направленности // Вестник Пермского университета. — 2015. — № 1 — С. 67.

REFERENCES

1. Sostoyanie prestupnosti v Rossii za 2021—2026 gody : statistika i analitika // Ofitsial′nyj sajt MVD Rossii. — URL: https://mvd.rf/folder/101762 (data obrashcheniya: 25.04.2026).

2. Khorovinnikov A. A. Ekstremizm kak sotsial′noe yavlenie: filosofskij analiz : dis. ... kand. filos. nauk. — Saratov, 2007. — 201 s.

3. Verush A. I. Ekstremizm kak ponyatie i yavlenie // Aktual′nye problemy gumanitarnykh i sotsial′no-ekonomicheskikh nauk. — 2019. — T. 13. — № 4. — S. 34—37.

4. Kilyaskhanov Kh. Sh. Sovremennaya deyatel′nost′ OBSE v sfere bor′by s terrorizmom // Vestnik Nizhegorodskoj akademii MVD Rossii. — 2012. — № 19. — S. 37.

5. Grechkina E. N. Molodezhnyj politicheskij ekstremizm v usloviyakh transformiruyushchejsya rossijskoj dejstvitel′nosti : dis. ... kand. polit. nauk. — Stavropol′, 2006. — 174 s.

6. Zaluzhnyj A. G. Pravovye garantii protivodejstviya ekstremistskoj deyatel′nosti v politicheskoj, religioznoj i drugikh sferakh obshchestvennoj zhizni // Zakon i pravo. — 2002. — № 9. — S. 29—32.

7. Mozhegova A. A. Ekstremistskie prestupleniya i prestupleniya ekstremistskoj napravlennosti po ugolovnomu pravu Rossijskoj Federatsii: dis. ... kand. yurid. nauk. — M., 2015. — 169 s.

8. Uzembaeva G. I. Obshchestvennaya opasnost′ prestuplenij ekstremistskoj napravlennosti, sovershaemykh s ispol′zovaniem informatsionno-telekommunikatsionnykh setej // Vestnik Volgogradskoj akademii MVD Rossii. — 2020. — № 1. — S. 91.

9. Khumarov M. S. Sotsial′no-pravovaya kharakteristika terrorizma v Rossii v 1990-kh gg. i formirovanie gosudarstvennoj kontseptsii po ego preduprezhdeniyu // Obshchestvo i pravo. — 2008. — № 2. — S. 12.

10. Tokbaev A. A. Sovremennye tendentsii razvitiya ekstremizma v sotsial′nykh setyakh // Probely v rossijskom zakonodatel′stve. — 2020. — № 4. — S. 109.

11. Puchnina M. Yu., Prokhonov V. S. O probleme vovlecheniya nesovershennoletnikh v ekstremistskuyu deyatel′nost′ s ispol′zovaniem informatsionno-kommunikatsionnykh tekhnologij // Prestupnost′ v sfere informatsionnykh i telekommunikatsionnykh tekhnologij: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestuplenij. — 2024. — № 10. — S. 104—109.

12. Budkova A. A., Ustinova E. P. Podstrekatel′stvo kak vid souchastiya v sovershenii prestupleniya: osnovnye problemy i perspektivy // Sfera nauki. — 2025. — № 1. — S. 1—12.

13. Akh″yadov E. S. Analiz sostava publichnykh prizyvov k osushchestvleniyu ekstremistskoj deyatel′nosti (st. 280 UK RF) // Evrazijskij nauchnyj zhurnal. — 2021. — № 3. — S. 14.

14. Materialy ugolovnogo dela № 1-10/2020. — URL: https://sudact.ru/regular/doc (data obrashcheniya: 30.04.2026).

15. Materialy ugolovnogo dela № 1-166/2024. — URL: https://sudact.ru/regular/doc (data obrashcheniya: 30.04.2026).

16. Materialy ugolovnogo dela № 1-160/2022. — URL: https://sudact.ru/regular/doc (data obrashcheniya: 30.04.2026).

17. Materialy ugolovnogo dela № 1-252/2022. — URL: https://sudact.ru/regular/doc (data obrashcheniya: 30.04.2026).

18. Stepanov V. V., Strukov A. V. Problemy razresheniya konkurentsii sostavov prestuplenij ekstremistskoj napravlennosti // Vestnik Permskogo universiteta. — 2015. — № 1 — S. 67.

СВЕДЕНИЯ ОБ АВТОРАХ

Колесников Роман Викторович. Доцент кафедры уголовного права и криминологии. Кандидат юридических наук, доцент.
Воронежский институт МВД России.
E-mail: rkolesnikow@mail.ru
Россия, 394065, Воронеж, проспект. Патриотов, 53.

Юрьева Яна Владимировна. Следователь следственного отдела Следственного управления.
Отдел полиции № 2 УМВД России по городу Тамбову.
E-mail: yanayreva_24_2002@mail.ru
Россия, 392001, Тамбов, ул. Ново-Стремянная, 8А.

Kolesnikov Roman Viktorovich. Associate Professor of the chair of Criminal Law and Criminology. Candidate of Law, Associate Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: rkolesnikow@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Yuryeva Yana Vladimirovna. Investigator of the Investigative Department of Investigative Directorate.
Police Department No. 2 of the Ministry of Internal Affairs of Russia for the city of Tambov.
E-mail: yanayreva_24_2002@mail.ru
Work address: Russia, 392001, Tambov, Novo-Stremyannaya Str., 8A.

Ключевые слова: экстремизм; экстремистская деятельность; экстремистская идеология; публичность; призыв; квалификация; судебная практика.

Key words: extremism; extremist activity; extremist ideology; publicity; appeal; qualification; judicial practice.

УДК 343.326

А. А. Коник, *кандидат педагогических наук, доцент*

АДМИНИСТРАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ И ИННОВАЦИОННЫЕ ПОДХОДЫ К ПРИМЕНЕНИЮ БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ADMINISTRATIVE AND LEGAL REGULATION AND INNOVATIVE APPROACHES TO THE USE OF UNMANNED AERIAL VEHICLES IN THE ACTIVITIES OF THE INTERNAL AFFAIRS AGENCIES OF THE RUSSIAN FEDERATION

В статье исследуются административно-правовые основы применения беспилотных воздушных судов (БВС) в деятельности органов внутренних дел Российской Федерации. Рассматривается нормативное регулирование эксплуатации БВС: государственный учет и регистрация, порядок получения разрешений на использование воздушного пространства, полномочия и обязанности внешних пилотов и специализированных подразделений. Анализируются законодательные акты, регулирующие использование БВС в оперативно-розыскной, следственной и профилактической деятельности, а также административная ответственность за нарушения правил использования воздушного пространства. Выявлены проблемы действующей нормативной базы: недостаточная централизация управления подразделениями, ограниченная техническая оснащенность и дефицит специализированной подготовки персонала. Предлагаются направления совершенствования законодательства и практики применения БВС, включая внедрение цифрового мониторинга полетов, автоматизированных систем управления, использование данных БВС в качестве доказательств, развитие кадровых структур и подготовку внешних пилотов. Автором подчеркивается значение интеграции правового регулирования и современных технологий для повышения эффективности деятельности МВД и обеспечения общественной безопасности.

The article examines the administrative and legal framework for the use of unmanned aerial vehicles (UAVs) by the internal affairs agencies of the Russian Federation. It examines the regulatory framework for UAV operation, including state registration and accounting, the procedure for obtaining airspace permits, and the powers and responsibilities of remote pilots and specialized units. It also analyzes legislative acts regulating the use of UAVs in investigative, investigative, and preventive activities, as well as administrative liability for violating airspace regulations. Problems with the current regulatory framework are identified, including insufficient centralization of unit management, limited technical equipment, and a lack of specialized personnel training. The article proposes areas for improving legislation and the practice of UAV use, including the implementation of digital flight monitoring, automated control systems, the use of UAV data as evidence, the development of personnel structures, and the training of remote pilots. The author emphasizes the importance of integrating legal regulation and modern technologies to improve the effectiveness of the Ministry of Internal Affairs and ensure public safety.

Стремительное развитие цифровых технологий и внедрение робототехнических систем в публичное управление обусловили качественную трансформацию механизмов реализации правоохранительных функций государства. Одним из наиболее динамично развивающихся направлений в указанной сфере выступает использование беспилотных воздушных судов (далее — БВС) в деятельности органов внутренних дел Российской Федерации. Их применение охватывает широкий спектр задач: от обеспечения общественного порядка при проведении массовых мероприятий до фиксации административных правонарушений, проведения оперативно-розыскных мероприятий и участия в раскрытии преступлений.

Административно-правовое регулирование применения БВС сотрудниками МВД России формируется на стыке воздушного, административного

и ведомственного законодательства [1]. Нормативную основу составляют положения Воздушного кодекса Российской Федерации, определяющие правовой режим воздушных судов, Федеральный закон «О полиции», закрепляющий полномочия сотрудников полиции по использованию технических средств, а также подзаконные акты, регламентирующие порядок эксплуатации БВС и пресечения их функционирования. Существенное значение имеют и положения Кодекса Российской Федерации об административных правонарушениях, устанавливающие ответственность за нарушение правил использования воздушного пространства.

Вместе с тем действующее нормативное регулирование носит фрагментарный характер и формировалось преимущественно исходя из потребностей гражданской авиации и обеспечения безопасности полетов [2]. Специфика правоохранительной деятельности органов внутренних дел (оперативность принятия решений, необходимость применения мер административного пресечения, обеспечение доказательственной базы по делам об административных правонарушениях) требует более детальной и системной регламентации статуса БВС как специального технического средства публичной власти.

Особую актуальность проблематика приобретает в условиях расширения полномочий правоохранительных органов по пресечению функционирования беспилотных аппаратов, установления региональных ограничений их использования, а также активного вовлечения БВС в процесс доказывания по делам об административных правонарушениях. Возникает необходимость доктринального осмысления правовой природы БВС в системе публично-правовых средств обеспечения безопасности, определения границ дискреционных полномочий должностных лиц, а также выработки предложений по совершенствованию административного законодательства.

БВС представляют собой уникальный правовой феномен на пересечении авиационного, административного и ведомственного законодательства. С одной стороны, БВС являются объектами воздушного права и подчиняются общим правилам эксплуатации воздушных судов, закрепленным в Воздушном кодексе Российской Федерации и соответствующих подзаконных актах [3]. С другой стороны, использование БВС в деятельности органов внутренних дел наделяет их особенностями публичного регулирования и обуславливает необходимость отдельного административно-правового регулирования.

Правовая природа БВС определяется сочетанием двух аспектов: материально-технического и юридического. С материально-технической стороны беспилотные авиационные системы (далее — БАС) представляют собой аппаратно-программный комплекс, включающий БВС, средства дистанционного управления, системы навигации, видеосъемки и обработки данных. С юридической точки зрения БВС является объектом правового регулирования, что проявляется в необходимости регистрации, учета, сертификации, назначения экипажа, а также соблюдения правил использования воздушного пространства.

В контексте административного права БВС выступает как средство, применяемое сотрудниками органов внутренних дел Российской Федерации в рамках реализации публичных полномочий. Использование БВС сотрудниками МВД России осуществляется в рамках реализации функций государства по обеспечению общественного порядка, безопасности граждан, охране имущества и предупреждению административных правонарушений. Указанное обстоятельство определяет специфику административно-правового регулирования, поскольку нормы должны обеспечивать сочетание оперативности, безопасности полетов и защиты прав и законных интересов граждан.

В соответствии со ст. 11 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции» (далее — Закон о полиции) сотрудники наделены правом использования достижений науки и техники, современных технологий и информационных систем в служебной деятельности в целях документирования правонарушений и обеспечения безопасности. П. 40 ч. 1 ст. 13 Закона о полиции регламентирует также возможность контролировать правомерность применения БВС в воздушном пространстве, пресекая его незаконное функционирование. В ст. 21 Закона о полиции регламентировано применение спецсредств и огнестрельного оружия для пресечения функционирования БВС, если они создают угрозу жизни, здоровью, имуществу или используются для совершения тяжких преступлений. Отдельно необходимо отметить положения приказа МВД России от 16.11.2023 № 865, регламентирующего порядок принятия решения о пресечении нахождения беспилотных воздушных судов в воздушном пространстве в целях защиты жизни, здоровья и имущества граждан над местом проведения публичного (массового) мероприятия и прилегающей к нему территории, проведения неотложных следственных действий и оперативно-розыскных мероприятий. В этом нормативном акте утвержден перечень должностных лиц, уполномоченных на принятие такого решения о пресечении функционирования БВС, в том числе с использованием огнестрельного оружия.

Административно-правовое регулирование применения БВС строится на принципах законности, целесообразности и пропорциональности [4]. Принцип законности предполагает, что любое использование БВС должно соответствовать нормам федерального законодательства, подзаконных актов и ведомственных приказов. Принцип целесообразности обуславливает применение БВС исключительно в целях, прямо предусмотренных правовыми нормами: обеспечение безопасности, контроль за соблюдением административного законодательства, проведение оперативно-розыскных мероприятий и фиксация доказательственной информации. Принцип пропорциональности выражается в соотношении цели применения БВС и степени ограничения прав и свобод граждан, например, при осуществлении видеоконтроля за участниками дорожного движения.

Важным элементом правового режима БВС является их регистрация и учет. Согласно положениям Воздушного кодекса РФ, БВС с максимальной взлетной массой от 0,15 кг до 30 кг подлежат государственному учету, а более 30 кг — государственной регистрации (Воздушный кодекс РФ, ст. 33, пп. 1 п. 1, п. 3.2). Такой подход позволяет обеспечить контроль за использованием БВС, идентификацию аппарата и его владельца, а также формирование базы данных для органов, отвечающих за транспортную безопасность и надзор за использованием воздушного пространства.

Административная ответственность за нарушение правил использования БВС закреплена в КоАП РФ (КоАП РФ, ст. 11.4, ч. 5 ст. 11.5) и охватывает как несоблюдение правил полетов и эксплуатации, так и действия, совершенные лицами, не наделенными полномочиями на использование воздушного пространства. Например, ч. 1 ст. 11.4 КоАП РФ предусматривает штрафы для граждан (20—50 тыс. руб.), должностных лиц (100—150 тыс. руб.) и юридических лиц (250—300 тыс. руб.), а также административное приостановление деятельности на срок до 90 суток. Ч. 2 ст. 11.4 КоАП РФ расширяет санкции в отношении лиц, не имеющих полномочий на использование воздушного пространства. Установленные меры создают систему контроля и стимулируют соблюдение правил эксплуатации БВС, что демонстрирует привязку правового режима БВС к принципу ответственности за нарушение правил общественной безопасности.

Можно отметить, что БВС как объект административно-правового регулирования обладает двойственной природой, одновременно технического средства и юридического объекта, использование которого подчинено публичным правовым нормам. Системное регулирование применения БВС в деятельности МВД России требует комплексного подхода, учитывающего правовой статус аппарата, компетенции должностных лиц, порядок эксплуатации и контроля, а также меры административной ответственности.

Регулирование полетов БВС также охватывает вопросы использования воздушного пространства. В целях соблюдения безопасности полетов и координации с другими воздушными судами необходимо получать разрешения от региональных и зональных центров Единой системы организации воздушного движения Российской Федерации (ЕС ОрВД), органов местного самоуправления и лиц, в интересах которых установлены зоны с ограничением полетов. Правила включают требования к представлению плана полета, указанию аэродрома, маршрута, диапазона высот и расчетного времени. Полеты БВС на высотах до 150 м для целей гражданских, спортивных и образовательных организаций регулируются упрощенно, что обеспечивает баланс между оперативными задачами и безопасностью граждан.

Рассмотрев БВС сквозь призму административно-правового регулирования, обратимся к эмпирической составляющей — практике их применения. Практика использования БВС сотрудниками МВД России охватывает несколько ключевых направлений:

- охрана общественного порядка и массовых мероприятий — БВС используются для видеонаблюдения, мониторинга территорий, предотвращения столкновений участников массовых мероприятий и своевременного реагирования на правонарушения. Информация с видеокамер БВС позволяет руководителям подразделений своевременно выявлять нарушения и принимать оперативные решения в режиме реального времени;

- контроль за дорожной безопасностью — использование БВС в ГИБДД позволяет фиксировать административные правонарушения, включая выезд на полосу встречного движения, нарушение правил остановки и стоянки. По данным за 2022—2023 годы, с использованием БВС в деятельности ГИБДД было выявлено около 35 тысяч нарушений ПДД в 29 регионах России. Чаще всего фиксировались выезд на полосу встречного движения и нарушения расположения автомобилей на проезжей части (например, движение по обочине). В Курганской области с помощью БВС также выявляли проезд на красный свет. Использование видеоматериалов в протоколах об административных правонарушениях требует соблюдения процедурной законности, включая лицензирование камер, хранение видео на оптических

носителях и соответствующую фиксацию данных:

- поиск и розыск лиц — БВС позволяют обследовать труднодоступные территории, вести мониторинг в условиях ограниченной видимости и оперативно выявлять местонахождение потерявшихся или подозреваемых лиц;

- документирование и сбор доказательств — видеозаписи и фотоматериалы, полученные с БВС, могут использоваться как доказательная база при рассмотрении административных и уголовных дел. Законность таких доказательств обеспечивается соблюдением правил эксплуатации, точной фиксацией времени и места съемки, хранением оригиналов записей и их последующим приобщением к материалам дела.

С целью организации функционирования БВС в деятельности территориальных органов МВД России созданы отделения применения и эксплуатации робототехнических комплексов и беспилотных воздушных судов (далее — ОПиЭРКиБВС), включающие в штат сотрудников внешних пилотов и операторов.

Как правило, сотрудники отделений ОПиЭРКиБВС привлекаются иными службами по отдельному запросу для оказания практической помощи, что существенно снижает оперативность их деятельности в неотложных ситуациях.

Отдельно следует отметить, что в подобных подразделениях отсутствует должность специалиста по противодействию БВС, который отвечает за выявление и нейтрализацию несанкционированных аппаратов, предотвращение угроз и поддержание безопасности воздушного пространства.

Несмотря на существующую нормативно-правовую базу, ряд проблем препятствует эффективному и безопасному использованию БВС в оперативно-розыскной деятельности, охране общественного порядка, дорожной безопасности и других сферах служебной деятельности МВД России [5].

Во-первых, наблюдается разрозненность и фрагментарность норм, регулирующих использование БВС. Федеральное законодательство, ведомственные приказы и региональные акты не всегда согласованы между собой, что порождает правовую неопределенность для сотрудников МВД России. Например, требования к регистрации и учету БВС устанавливаются Воздушным кодексом, в то время как правила эксплуатации, получения разрешений на полеты и использования воздушного пространства закреплены в приказах Минтранса и Росавиации. В условиях оперативной деятельности это может приводить к задержкам при получении разрешений и формировать риски нарушения закона.

Во-вторых, законодательство в значительной мере ориентировано на массовое гражданское использование БВС, в то время как потребности МВД России включают оперативные и специфические задачи: пресечение противоправной деятельности, контроль массовых мероприятий, поиск и спасение лиц. Например, ч. 1 и 2 ст. 11.4 КоАП РФ устанавливают административную ответственность за нарушение правил использования воздушного пространства, но не уточняют особенности применения этих норм сотрудниками МВД России при исполнении служебных обязанностей, что создает правовую неопределенность при документировании нарушений с использованием БВС и при представлении видеоматериалов в качестве доказательств.

В-третьих, недостаточно урегулированы вопросы признания данных, полученных с БВС, доказательствами в административных и уголовных производствах. Практика демонстрирует необходимость лицензирования камер, хранения оригиналов видеозаписей и их надлежащего приобщения к материалам дела. В отсутствие единых правил возможны споры о допустимости и юридической значимости таких доказательств, что снижает эффективность применения БВС в правоохранительной деятельности.

Также на практике выявляются следующие основные организационные трудности:

- недостаточный уровень оснащения подразделений беспилотными комплексами. Существующая авиационная техника, находящаяся на снабжении МВД России, не всегда соответствует современным требованиям к оперативным задачам, что ограничивает возможности контроля за массовыми мероприятиями и дорожной обстановкой;

- недостаточная подготовка специалистов. Обучение внешних пилотов проводится фрагментарно, без системного подхода к подготовке кадров, способных действовать в условиях оперативной обстановки;

- после получения квалификации специалиста по эксплуатации беспилотных авиационных систем и удостоверения о повышении квалификации установленного образца сотрудник полиции, проходящий службу не в профильном подразделении, вынужден дублировать функции, что повышает нагрузку на него, с одной стороны и снижает возможность эффективного выполнения служебных задач — с другой;

- отсутствие четких правил признания данных с БВС доказательствами. Для обеспечения законности использования информации в производстве по административным и уголовным делам необходимо разработать ведомственные стандарты видеозаписи, хранения, маркировки и передачи материалов, полученных с БВС;

- необходимость внедрения современных технологий в эксплуатацию БВС. Использование систем дистанционного контроля, автоматизированного планирования полетов и анализа данных позволит оптимизировать работу подразделений, повысить эффективность мониторинга и снизить риск ошибок.

В результате совершенствование административно-правового регулирования использования БВС в деятельности МВД России предполагает комплексный подход, включающий разработку унифицированной нормативной базы, модернизацию деятельности специализированных подразделений, обучение персонала, внедрение технологий и уточнение норм административной ответственности. Только при условии сочетания правового, организационного и технического регулирования возможно максимально эффективное использование возможностей БВС в интересах общественной безопасности и охраны правопорядка.

При наличии надлежащего уровня организационного и нормативно-правового обеспечения представляется обоснованным внедрение концепции «цифрового внешнего пилота», предполагающей осуществление дистанционного контроля за эксплуатацией БВС. Вместе с тем главным условием реализации указанной концепции является законодательное закрепление четкого распределения ответственности между всеми субъектами, вовлеченными в процесс эксплуатации беспилотных воздушных судов, что позволит обеспечить правовую определенность и минимизировать риски правоприменительной неопределенности.

Правовое закрепление указанных функций обусловливает необходимость системного обновления действующего нормативного массива, прежде всего, посредством внесения изменений в Воздушный кодекс Российской Федерации и федеральные авиационные правила. Соответствующие изменения должны быть направлены на институционализацию статуса «цифрового внешнего пилота» как самостоятельного субъекта правоотношений и, в частности, на признание его субъектом административной ответственности, сопоставимой по своему содержанию и объему с ответственностью физического внешнего пилота.

Отдельного внимания в данном контексте требует регламентация деятельности, связанной с применением средств радиоэлектронной борьбы (РЭБ), что предполагает установление четких правовых механизмов контроля за кругом субъектов, уполномоченных осуществлять функции противодействия беспилотным воздушным судам [6]. Указанное направление правового регулирования призвано обеспечить баланс между необходимостью обеспечения общественной безопасности и недопущением неправомерного вмешательства в функционирование воздушного пространства, а также минимизировать риски злоупотреблений при использовании соответствующих технологий.

Расширение системы административной ответственности. В контексте инновационного регулирования необходимо разработать новые виды административной ответственности для лиц, участвующих в эксплуатации БВС, которые выходят за пределы классических нарушений правил полетов. Среди них можно выделить ненадлежащее использование интеллектуальных систем контроля БВС, включая отключение автоматического ограничения зоны полета или вмешательство в работу сенсоров; эксплуатацию БВС с нарушением требований к кибербезопасности, создающую угрозу утечки данных; предоставление доступа к управлению БВС лицам, не прошедшим специальную подготовку и не имеющим необходимой квалификации.

Особое внимание следует уделить ситуациям, создающим угрозу тяжкого вреда здоровью или крупного имущественного ущерба [7]. В таких случаях административная ответственность должна сочетаться с возможностью уголовного преследования, что обеспечит пропорциональность меры наказания и повышенную безопасность граждан.

Правовые механизмы дистанционного вмешательства. Еще одним инновационным инструментом является использование технологий подавления или перехвата несанкционированных БВС, осуществляющих противоправные действия в воздушном пространстве. Законодательное закрепление возможности применения таких мер предполагает определение компетенции органов внутренних дел на применение средств подавления, установление процедур уведомления и отчетности о каждом случае дистанционного вмешательства, разработку критериев законности и пропорциональности воздействия на БВС. Применение дистанционных средств контроля и подавления должно сопровождаться строгим административным надзором и регламентироваться отдельными нормативными актами, что исключает произвольное использование указанных технологий.

Анализ административно-правового регулирования применения беспилотных воздушных судов в деятельности органов внутренних дел Российской Федерации демонстрирует, что современная правовая система уже создала основу для легального и безопасного использования БВС в правоохранительной практике. Однако практика применения БВС в оперативной деятельности выявляет ряд значимых пробелов. Нормы права фрагментарны и частично ориентированы на гражданское использование БВС, что порождает

правовую неопределенность для сотрудников МВД России при осуществлении служебных функций. Отсутствует централизованная система управления подразделениями, использующими БВС, что снижает эффективность координации и оперативное взаимодействие с другими органами. Не в полной мере урегулированы вопросы правомерного использования данных, полученных с помощью БВС, в качестве доказательств по делам об административных правонарушениях и уголовным делам.

Перспективы совершенствования административного регулирования включают комплекс мер, направленных на интеграцию правового, организационного и технического аспектов. Важно также усовершенствовать административную ответственность, закрепив особенности применения норм КоАП РФ для сотрудников МВД при выполнении служебных задач с использованием БВС. Совершенствование административно-правового регулирования применения БВС в деятельности МВД России является неотъемлемой частью модернизации правоохранительных органов и внедрения высоких технологий в практику обеспечения безопасности.

ЛИТЕРАТУРА

1. Бегишев И. Р. Правовое регулирование беспилотных транспортных средств // Транспортное право. — 2021. — № 3. — С. 7—10.

2. Владимиров И. А. Правовое регулирование использования беспилотных воздушных судов в сельском хозяйстве // Информационное общество. — 2025. — № 3. — С. 78—87.

3. Зарапина Л. В. Правовое регулирование полетов беспилотных летательных аппаратов: перспективы, новации, проблемы // Юридический вестник Кубанского государственного университета. — 2021. — № 4. — С. 29—37.

4. Королева Е. Г. Правовое регулирование использования беспилотных транспортных средств в Российской Федерации // NB : Административное право и практика администрирования. — 2024. — № 1. — С. 13—22.

5. Фролов А. А. Правовое регулирование и противодействие незаконному использованию беспилотных воздушных судов в деятельности МВД России // Право и управление. — 2025. — № 9. — С. 133—136.

6. Курысев К. Н. Противодействие беспилотным летательным аппаратам в условиях уголовно-исполнительной системы: проблемы и пути их решения // Вестник Владимирского юридического института. — 2021. — № 1(58). — С. 56—61.

7. Плотников Г. Г. Противодействие беспилотным летальным аппаратам для обеспечения задач общественной безопасности // Современная наука: актуальные проблемы теории и практики. Серия : Естественные и технические науки. — 2025. — № 9. — С. 80—85.

REFERENCES

1. Begishev I. R. Pravovoe regulirovanie bespilotnykh transportnykh sredstv // Transportnoe pravo. — 2021. — № 3. — S. 7—10.

2. Vladimirov I. A. Pravovoe regulirovanie ispol′zovaniya bespilotnykh vozdushnykh sudov v sel′skom khozyajstve // Informatsionnoe obshchestvo. — 2025. — № 3. — S. 78—87.

3. Zarapina L. V. Pravovoe regulirovanie poletov bespilotnykh letatel′nykh apparatov: perspektivy, novatsii, problemy // Yuridicheskij vestnik Kubanskogo gosudarstvennogo universiteta. — 2021. — № 4. — S. 29—37.

4. Koroleva E. G. Pravovoe regulirovanie ispol′zovaniya bespilotnykh transportnykh sredstv v Rossijskoj Federatsii // NB : Administrativnoe pravo i praktika administrirovaniya. — 2024. — № 1. — S. 13—22.

5. Frolov A. A. Pravovoe regulirovanie i protivodejstvie nezakonnomu ispol′zovaniyu bespilotnykh vozdushnykh sudov v deyatel′nosti MVD Rossii // Pravo i upravlenie. — 2025. — № 9. — S. 133—136.

6. Kurysev K. N. Protivodejstvie bespilotnym letatel′nym apparatam v usloviyakh ugolovno-ispolnitel′noj sistemy: problemy i puti ikh resheniya // Vestnik Vladimirskogo yuridicheskogo instituta. — 2021. — № 1(58). — S. 56—61.

7. Plotnikov G. G. Protivodejstvie bespilotnym letal′nym apparatam dlya obespecheniya zadach obshchestvennoj bezopasnosti // Sovremennaya nauka: aktual′nye problemy teorii i praktiki. Seriya : Estestvennye i tekhnicheskie nauki. — 2025. — № 9. — S. 80—85.

СВЕДЕНИЯ ОБ АВТОРЕ

Коник Алексей Алексеевич. Заместитель начальника кафедры тактико-специальной подготовки. Кандидат педагогических наук, доцент.
Белгородский юридический институт МВД России имени И. Д. Путилина.
E-mail: 89205666067@mail.ru
Россия, 308024, Белгород, ул. Горького, 71.

Konik Alexey Alekseevich. Deputy head of the chair of Tactical and Special Training. Candidate of Pedagogical Sciences, Associate Professor.
Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I. D. Putilin.
E-mail: 89205666067@mail.ru
Work address: Russia, 308024, Belgorod, Gorky Str., 71.

Ключевые слова: беспилотные воздушные суда; административное право; органы внутренних дел; внешние пилоты; государственный учет; разрешение на использование воздушного пространства; административная ответственность; инновационные технологии; противодействие БВС; нормативно-правовое регулирование.

Key words: unmanned aerial vehicles; administrative law; law enforcement agencies; remote pilots; state registration; airspace use permits; administrative liability; innovative technologies; countering UAVs; legal regulation.

УДК 342.9

С. Ю. Можаева, *кандидат юридических наук*
Н. В. Полякова, *кандидат юридических наук, доцент*

О НЕКОТОРЫХ ОСОБЕННОСТЯХ ПРОВЕДЕНИЯ ДОСЛЕДСТВЕННЫХ ПРОВЕРОК ПО СООБЩЕНИЯМ О ПРЕСТУПЛЕНИЯХ, ПРЕДУСМОТРЕННЫХ СТАТЬЕЙ 314.1 УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ

ABOUT SOME OF THE FEATURES OF THE EVENT PRE-INVESTIGATION CHECKS BASED ON REPORTS ON CRIMES PROVIDED FOR IN ARTICLE 314.1 THE CRIMINAL CODE OF THE RUSSIAN FEDERATION

В статье анализируются отдельные проблемы правоприменительного характера, возникающие у сотрудников органов внутренних дел Российской Федерации при осуществлении доследственных проверок по сообщениям о преступлениях, предусмотренных статьей 314.1 Уголовного кодекса Российской Федерации. В работе предложен примерный алгоритм сбора материалов процессуальных проверок до принятия решения о возбуждении уголовного дела, определен порядок осуществления запросов необходимых сведений, предложен перечень вопросов, которые необходимо выяснять при проведении опросов лиц. В качестве мер совершенствования норм уголовного законодательства авторами предложены изменения части 2 статьи 314.1 УК РФ.

The article analyzes certain problems of a law enforcement nature that arise for employees of the internal affairs bodies of the Russian Federation when conducting preinvestigative checks on reports of crimes under Article 314.1 of the Criminal Code of the Russian Federation. The paper proposes an approximate algorithm for collecting materials of procedural checks before making a decision to initiate a criminal case, defines the procedure for requesting necessary information, and provides a list of questions that should be clarified during interviews with individuals. As measures to improve the norms of criminal legislation, the authors propose changes to Part 2 of Article 314.1 of the Criminal Code of the Russian Federation.

Актуальность темы научной статьи обусловлена необходимостью совершенствования уголовного законодательства в части квалификации преступлений, связанных с несоблюдением ограничений лицами, в отношении которых установлен административный надзор. Административный надзор выступает мерой правового контроля, которая направлена на исправление лица, осужденного за совершение преступлений, а также в целях его воспитания. Установление административного надзора на практике показывает его эффективность в большинстве случаев, но вместе с тем доказывание фактов несоблюдения ограничений, введенных в процессе установления административного надзора, вызывает отдельные правоприменительные проблемы. Кроме того, совершенствование процессуальных особенностей проведения доследственных проверок в случае выявления фактов нарушений поднадзорными лицами норм законодательства будет способствовать и совершенствованию правоприменительной деятельности органов внутренних дел. Тема установления административного надзора и соблюдения его требований неоднократно рассматривалась в трудах таких ученых, как А. О. Астахова, О. М. Калинина, Н. Д. Данилова, О. В. Петрова, и других.

Анализ деятельности территориальных органов внутренних дел свидетельствует о том, что за последние 5 лет рост деяний, связанных с уклонением от административного надзора (статья 314.1 УК РФ), составил 2,2% [1], то есть за указанный период количество преступлений по части первой статьи 314.1 УК РФ («неприбытие без уважительных причин лица, в отношении которого установлен административный надзор, к выбранному им месту жительства») возросло на 7,1% (с 5454 до 5869). При этом незначительно снизилось число преступлений по части второй статьи 314.1 УК РФ («неоднократное несоблюдение лицом, в отношении которого установлен административный надзор, административных ограничений») —

на 3,2% (с 5506 до 5335). Приведенные статистические данные свидетельствуют о формировании на территории страны обширной практики выявления в отношении поднадзорных лиц состава преступления, предусмотренного статьей 314.1 УК РФ.

Важным фактом привлечения к ответственности по рассматриваемой статье является необходимость определения временных промежутков отсутствия поднадзорного лица по месту жительства или прибытия к нему, которые не установлены законодательно. Диспозиция части 1 статьи 314.1 УК РФ, а также положения Постановления Пленума Верховного Суда РФ от 24 мая 2016 г. № 21 «О судебной практике по делам о преступлениях, предусмотренных статьей 314.1 Уголовного кодекса Российской Федерации» (далее — ППВС РФ № 21) не устанавливают конкретный временной промежуток (часы, сутки, месяцы и т. д.), в течение которого поднадзорное лицо может отсутствовать по своему месту жительства или пребывания без риска образования состава преступления.

По смыслу положений статьи 11 Федерального закона от 6 апреля 2011 года № 64-ФЗ «Об административном надзоре за лицами, освобожденными из мест лишения свободы» (далее — ФЗ № 64) поднадзорное лицо обязано в установленные законом сроки уведомить орган внутренних дел (далее — ОВД РФ) о любых изменениях места своего жительства или пребывания. Нарушение указанных сроков может рассматриваться как противоправное деяние, может быть квалифицировано по статье 314.1 УК РФ. Таким образом, временной интервал, в течение которого поднадзорное лицо находится вне избранного места жительства или пребывания без уведомления ОВД РФ, является важным элементом, который подлежит тщательному анализу при установлении признаков состава преступления.

По факту неявки поднадзорного лица к месту жительства (пребывания) или его несанкционированного ухода проводится доследственная проверка, в процессе которой необходимо осуществить детальный анализ всех релевантных обстоятельств данного происшествия. Во-первых, следует выяснить мотив и цель, побудившие субъекта правонарушения к уклонению от исполнения запретов, установленных судом. Кроме того, сотрудник ОВД РФ, в производстве которого находится материал процессуальной проверки, приобщает к материалам следующие документы: судебное решение об установлении административного надзора (с заверенной отметкой суда о вступлении в законную силу); материалы, поступившие из исправительного учреждения ФСИН России (уведомление территориального органа МВД России, предписание о выезде поднадзорного лица к указанному месту жительства (пребывания), а также другие материалы, такие как социально-психологические характеристики от администрации исправительного учреждения, рапорты (справки) сотрудников ФСИН России о проведенной в период исполнения наказания работе, копия справки об освобождении из исправительного учреждения ФСИН России).

Наряду с этим необходимо приобщать характеристики участкового уполномоченного полиции, ТСЖ или управляющей компании (администрации сельского поселения) по месту жительства, копии обвинительных приговоров, постановлений о привлечении к административной ответственности и справки о диспансерном наблюдении у врача-психиатра-нарколога [2].

В рамках процессуальной проверки целесообразно проводить осмотр места происшествия (по адресу проживания с согласия проживающих в нем лиц) с приложением фототаблицы к нему с указанием информации о наличии (отсутствии) в квартире (доме, территории) поднадзорного лица необходимых условий для проживания (например, отопления, электричества, водоснабжения и т. д.), а также следов его недавнего пребывания (свежие продукты питания и т. п.), личных вещей и предметов, принадлежащих поднадзорному.

По результатам рассмотрения сообщения о преступлении принимается решение, предусмотренное статьей 145 Уголовно-процессуального кодекса Российской Федерации.

Необходимо отметить, что предлагаемый нами перечень мероприятий при проведении доследственной проверки не может быть исчерпывающим и должен определяться исходя из обстоятельств происшествия, а также с учетом сложившейся правоприменительной практики в отдельно взятом регионе и уровня развития самого региона в различных сферах жизни.

Например, в ряде регионов России уже активно используются системы биометрического контроля лиц, и, соответственно, результаты фиксации на них противоправных деяний поднадзорных также могут приобщаться к материалам процессуальных проверок (подтверждение фактов нахождения поднадзорных длительное время за пределами границ субъекта РФ при наличии соответствующего запрета и т. д.).

К другим материалам, имеющим впоследствии доказательственное значение, могут относиться документально подтвержденные факты нахождения в связи с осуждением за совершение преступлений поднадзорных в исправительных центрах ФСИН, сеть которых в настоящее время активно расширяется в большинстве регионов страны. Аналогичной доказательственной базой

может являться подтверждение фактов нахождения в период уклонения от надзора подучетных лиц в различных социальных центрах и приютах.

Помимо этого стоит учитывать и факт совершения иного состава преступления поднадзорным в период его уклонения от надзора (например, кражи, разбоя), что будет доказывать, что он не стал на путь исправления. В данном случае надлежит приобщать к материалам процессуальных проверок документы, подтверждающие факт возбуждения уголовного дела и избрания поднадзорному лицу меры пресечения в порядке, предусмотренном уголовно-процессуальным законодательством.

В настоящее время для состава преступления по ч. 2 ст. 314.1 УК РФ требуется не менее трех нарушений административных ограничений в течение года, последнее из которых должно быть сопряжено с правонарушением против порядка управления или посягающим на общественный порядок, здоровье, санитарно-эпидемиологическое благополучие населения и общественную нравственность, либо предусмотренным частью 7 статьи 11.5, либо статьей 11.9, либо статьей 12.8, либо статьей 12.26 КоАП РФ.

При этом для квалификации деяния по части 2 статьи 314.1 УК РФ указанные правонарушения должны быть совершены одновременно с нарушением ограничений. Например, это могут быть нарушения, связанные с нахождением поднадзорного в запрещенных для пребывания местах, посещением массовых мероприятий при наличии запрета, пребыванием вне жилого помещения в запрещенное время суток.

Описанный выше механизм образования состава преступления определен ППВС РФ № 21.

Таким образом, при описанных условиях, значительная часть поднадзорных, нарушающих ограничения без сопряжения с этими правонарушениями, уголовной ответственности не подлежат.

К материалам проверки приобщаются копии постановлений о привлечении к административной ответственности, решение суда об установлении надзора и материалы дела административного надзора. Важно наличие действующих постановлений о назначении административного наказания. В случае пересмотра постановлений и принятия по ним последующих решений такие материалы не учитываются.

Обращает на себя внимание тот факт, что сопряжение должно происходить с правонарушением, совершаемым по отдельным статьям КоАП РФ (например, ст. ст. 6.1.1, 12.8 КоАП РФ), а не с составами преюдиционных преступлений, например, со статьями 116.1, 264.1 УК РФ. Этот запрет прямо вытекает из диспозиции части 2 статьи 314.1 УК РФ.

Из смысла пункта 11 ППВС РФ № 21 следует, что местом совершения преступления, предусмотренного статьей 314.1 УК РФ, является место, где органом внутренних дел осуществляется административный надзор. То есть в случае задержания сотрудниками полиции поднадзорного лица, состоящего на учете в Воронежской области, на факте сопряжения с определенным составом правонарушения, например, на территории Приморского края, уголовное дело подлежит возбуждению по части 2 статьи 314.1 УК РФ в Воронежской области, то есть по месту осуществления административного надзора.

На наш взгляд, в ППВС РФ № 21 не нашли своего отражения разъяснения, касающиеся понятия дополнительного эпизода преступной деятельности, когда поднадзорное лицо, в отношение которого уже возбуждено уголовное дело по части 2 статьи 314.1 УК РФ, продолжает многократно совершать правонарушения по части 3 статьи 19.24 КоАП РФ, в том числе ввиду их сопряженности, формально образующие однородный состав преступления.

Осознание поднадзорным лицом безнаказанности своих проступков нередко приводит к совершению им преступлений, в том числе тяжких и особо тяжких.

Характерным примером является совершение на территории одного из районов Воронежской области в июне 2019 года осужденным Ш., состоявшим под административным надзором, убийства родного брата.

Судом поднадзорному Ш. было установлено максимальное количество административных ограничений, предусмотренных ФЗ № 64. Регулярным проведением с ним профилактических бесед в целях разъяснения последствий несоблюдения таких запретов и неоднократным (4 раза) привлечением к административной ответственности за их нарушение, должного эффекта не было достигнуто. Отсутствие у органов внутренних дел иных действенных средств профилактического воздействия явилось одной из причин совершения Ш. особо тяжкого преступления [3].

Не являются исключением случаи совершения на территории Воронежской области серийных тяжких преступлений поднадзорными в период их уклонения от осуществления административного надзора.

Так, в период с 21 июня по 28 июля 2020 года скрывающийся от административного надзора, осуществляемого отделом МВД России по Семилукскому району, поднадзорный Я. на территории г. Воронежа совершил 8 грабежей имущества

граждан. В указанный период времени поднадзорный скрывался, по месту жительства не проживал и связь ни с кем из родственников не поддерживал. Соответственно, уголовное дело по части 1 статьи 314.1 УК РФ в отношении него было возбуждено только после его задержания и опроса, позволившего выяснить его прямой умысел, направленный на уклонение от надзора [4].

В обоснование данной позиции необходимо привести мнение О. М. Калининой, которая указывает, что рецидив преступлений рассматривается как элемент состава преступления, предусмотренного статьей 314.1 УК РФ, при этом минимальный срок лишения свободы составляет не менее одной трети максимального наказания, предусмотренного наиболее строгой санкцией, то есть в соответствии с частью 2 статьи 68 УК РФ [5]. Автор приводит в своей научной работе сведения о судебных приговорах, в которых рецидив преступлений учитывается дважды. В практической деятельности имеются также случаи, когда рецидив преступлений учитывается исключительно как квалифицирующий признак состава преступления и наказание назначается в пределах санкций, предусмотренных частью 1 или частью 2 статьи 314.1 УК РФ, без применения положений части 2 статьи 68 УК РФ. Тем самым рецидив преступлений влияет и на квалификацию, и на наказание: он учитывается как отягчающее обстоятельство и как квалифицирующий признак состава преступления

Позиция А. О. Астаховой, сформулированная на основе анализа существующего законодательства, позволяет сделать вывод о том, что рецидив преступлений может быть признан отягчающим обстоятельством при определении наказания для лица, совершившего деяние, предусмотренное статьей 314.1 УК РФ [6]. Ссылаясь на п. 1.4 постановления Конституционного Суда Российской Федерации от 19 марта 2003 года № 3-П, она считает, что двойной учет одних и тех же обстоятельств как при квалификации преступлений, так и при назначении наказания не допускается. Такая позиция правоприменителя противоречит, в первую очередь, Конституции РФ в части закрепления принципа равенства всех перед законом и судом в сфере уголовно-правовых отношений, а также ч. 2 ст. 63 УК РФ, которая устанавливает, что отягчающее обстоятельство, предусмотренное статьей Особенной части как признак преступления, не может повторно учитываться при назначении наказания.

Соглашаясь с позицией А. О. Астаховой, мы не соглашаемся с мнением, высказанным в юридической литературе, согласно которому непогашенная или неснятая судимость является обязательным признаком состава преступления, предусмотренного ст. 314.1 УК РФ, так как является обязательным признаком субъекта преступления. Действительно, непогашенная или неснятая судимость является обязательным условием, правовой основой назначения административного надзора, и действовать данная мера правового воздействия (административный надзор) может только в пределах судимости. Однако судимость является важным, но не единственным обстоятельством, влекущим возможность установления административного надзора. Кроме нее к числу обязательных признаков состава преступления, предусмотренного ст. 314.1 УК РФ, относится сам административный надзор, факт его установления судом, а не судимость как его основа.

Судимость представляет собой лишь одно из ключевых обстоятельств, которые могут послужить основанием для установления административного надзора. Таким образом, обязательным элементом состава преступления по указанной статье является не только наличие судимости, но и сам процесс судебного установления административного надзора, что требует более глубокого и всестороннего рассмотрения данной правовой категории. Это обусловлено тем, что административный надзор является мерой государственного контроля, направленной на обеспечение общественной безопасности и предотвращение рецидива преступлений [7].

На наш взгляд, приведенные примеры и мнения ученых свидетельствуют о необходимости уточнения законодательства.

Кроме того, полагаем, что в целях обеспечения надлежащего уровня защиты граждан от правонарушений против личности, собственности существует объективная необходимость исключения из части второй статьи 314.1 УК РФ признака сопряженности составов административных правонарушений.

Такой подход обусловлен тем, что УК РФ содержит нормы с административной преюдицией, которые образуются без какой-либо сопряженности с иными правонарушениями, то есть относятся к деяниям с простой повторностью. В их число входят статьи 116.1 «Нанесение побоев лицом, подвергнутым административному наказанию или имеющим судимость», 158.1 «Мелкое хищение, совершенное лицом, подвергнутым административному наказанию».

Такую позицию подтверждает Г. Р. Баркаев, который указывает на то, что нормы, включающие административную преюдицию, имеют различную конструкцию в уголовном законодательстве. По мнению автора, законодательная формулировка части 2 статьи 314.1 УК РФ нарушает принцип равенства граждан перед законом и не

полностью соответствует понятию «административная преюдиция», разработанному наукой уголовного права. Во всех преступлениях, содержащих административную преюдицию (за исключением статьи 314.1 УК РФ), не требуется совершения какого-либо иного деяния, кроме того, за которое лицо привлекалось к административной ответственности дважды (неоднократно) [8].

Проведенный нами анализ зарубежного опыта в указанной сфере деятельности показывает, что государствами — членами СНГ успешно реализуются законодательные нормы, предусматривающие уголовную ответственность за несоблюдение ограничения или ограничений лицом, в отношении которого установлен административный надзор, без дополнительных условий. Так, статья 421 «Несоблюдение требований превентивного надзора» Уголовного кодекса Республики Беларусь закрепляет ответственность за несоблюдение требований превентивного надзора без уважительных причин, совершенное лицом, за которым установлен превентивный надзор и которое дважды в течение года подвергалось административному взысканию за такие же нарушения [9]. В равной мере законодательством Туркменистана установлена уголовная ответственность за несоблюдение обязанностей и ограничений, установленных при административном надзоре [13]. Схожая по аналогии норма (часть первая статьи 198.2 «Злостное нарушение правил административного надзора» Уголовного кодекса РСФСР) ранее применялась в отечественном уголовном законодательстве [10].

На основании вышеизложенного представляется возможным внесение следующих изменений в законодательство:

1. Исключение признака сопряженности правонарушений из диспозиции части второй статьи 314.1 УК РФ с одновременной заменой понятия «неоднократное», например, на «многократное», определяющее число нарушений ограничений. При таком подходе состав преступления может образовываться после трехкратного совершения в течение года поднадзорным лицом административных правонарушений (в настоящее время в действующей редакции — два раза). Обозначенный признак будет более выраженно подчеркивать направленность выявленных нарушений именно в сфере административного надзора и устойчивость противоправного поведения поднадзорных. Полагаем, альтернативой может служить замена признака сопряженности на «сочетание» нарушений административных ограничений с другими составами, если не истекли сроки административного наказания по статье 19.24 КоАП РФ. Или, возможно, значительное сокращение времени, в течение которого допущенные правонарушения переходят в категорию уголовно наказуемых деяний. Например, можно установить срок в 180 дней, аналогичный статье 212.1 УК РФ «Неоднократное нарушение установленного порядка организации либо проведения собрания, митинга, демонстрации, шествия или пикетирования». В случае изменения диспозиции рассматриваемого состава преступления превентивной направленности прогнозируемо ожидается сокращение числа иных преступных деяний, совершаемых поднадзорными лицами.

2. Считаем целесообразным дополнение статьи 63 УК РФ таким отягчающим обстоятельством, как совершение преступления лицом, в отношении которого установлен надзор. На наш взгляд, внесение такой поправки может способствовать снижению уровня рецидивной преступности в стране и в целом явиться дополнительным инструментом в предупреждении преступлений различной степени тяжести.

3. В целях своевременного и качественного выполнения сотрудниками полиции своих обязанностей по пресечению противоправных действий со стороны поднадзорных имеется потребность в актуализации положений Постановления Пленума Верховного Суда Российской Федерации № 21 либо получения соответствующих разъяснений или рекомендаций.

ЛИТЕРАТУРА

1. Статистические сведения по Российской Федерации за 2020—2025 годы // Сайт Сервиса ведомственной правовой статистики единой системы информационно-аналитического обеспечения деятельности МВД России.

2. Балмочных С. Ю., Можаев С. А. О некоторых вопросах производства процессуальных проверок и возбуждения уголовных дел, предусмотренных статьей 314.1 УК РФ (на примере Воронежской области) // Вестник Воронежского института МВД России. — 2023. — № 2. — С. 249—254.

3. Приговор Грибановского районного суда Воронежской области (дело № 1-т 47/2019). — URL: https://gribanovsky--vrn.sudrf.ru/ (дата обращения: 22.03.2026).

4. Приговор Железнодорожного районного суда г. Воронежа (дело № 1-23/2021). — URL: https://zheleznodorozhny--vrn.sudrf.ru/ (дата обращения: 22.03.2026).

5. Калинина О. М. Проблемы назначения наказания по ст. 314.1 УК РФ // Уголовное право. — 2024. — № 3. — С. 26—33.

6. Астахова А. О. Уголовная ответственность за уклонение от административного надзора: проблемы применения и пути решения : монография. — Красноярск : СибЮИ МВД России, 2018.

7. Баркаев Г. Р. Нормы с административной преюдицией и место среди них уклонения от административного надзора // Право и государство: теория и практика. — 2022. — № 12(216). — С. 277—279.

8. Уголовный кодекс Республики Беларусь от 09.07.1999 № 275-З (ред. от 17.02.2025). — URL: https://bsmp.by/o-bolnitse/rabota-po-protivodejstviyu (дата обращения: 22.03.2026).

9. Уголовный кодекс Туркменистана от 12.06.1997 № 222-I (с изменениями и дополнениями по состоянию на 12.04.2025). — URL: https://continent-online.com/Document/?doc_id=31295286 (дата обращения: 22.03.2026).

10. Уголовный кодекс РСФСР (утв. ВС РСФСР 27.10.1960) // СПС «КонсультантПлюс».

REFERENCES

1. Statisticheskie svedeniya po Rossijskoj Federatsii za 2020—2025 gody // Sajt Servisa vedomstvennoj pravovoj statistiki edinoj sistemy informatsionno-analiticheskogo obespecheniya deyatel′nosti MVD Rossii.

2. Balmochnykh S. Yu., Mozhaev S. A. O nekotorykh voprosakh proizvodstva protsessual′nykh proverok i vozbuzhdeniya ugolovnykh del, predusmotrennykh stat′ej 314.1 UK RF (na primere Voronezhskoj oblasti) // Vestnik Voronezhskogo instituta MVD Rossii. — 2023. — № 2. — S. 249—254.

3. Prigovor Gribanovskogo rajonnogo suda Voronezhskoj oblasti (delo № 1-t 47/2019). — URL: https://gribanovsky--vrn.sudrf.ru/ (data obrashcheniya: 22.03.2026).

4. Prigovor Zheleznodorozhnogo rajonnogo suda g. Voronezha (delo № 1-23/2021). — URL: https://zheleznodorozhny--vrn.sudrf.ru/ (data obrashcheniya: 22.03.2026).

5. Kalinina O. M. Problemy naznacheniya nakazaniya po st. 314.1 UK RF // Ugolovnoe pravo. — 2024. — № 3. — S. 26—33.

6. Astakhova A. O. Ugolovnaya otvetstvennost′ za uklonenie ot administrativnogo nadzora: problemy primeneniya i puti resheniya : monografiya. — Krasnoyarsk : SibYuI MVD Rossii, 2018.

7. Barkaev G. R. Normy s administrativnoj preyuditsiej i mesto sredi nikh ukloneniya ot administrativnogo nadzora // Pravo i gosudarstvo: teoriya i praktika. — 2022. — № 12(216). — S. 277—279.

8. Ugolovnyj kodeks Respubliki Belarus′ ot 09.07.1999 № 275-Z (red. ot 17.02.2025). — URL: https://bsmp.by/obolnitse/rabota-po-protivodejstviyu (data obrashcheniya: 22.03.2026).

9. Ugolovnyj kodeks Turkmenistana ot 12.06.1997 № 222-I (s izmeneniyami i dopolneniyami po sostoyaniyu na 12.04.2025). — URL: https://continent-online.com/Document/?doc_id=31295286 (data obrashcheniya: 22.03.2026).

10. Ugolovnyj kodeks RSFSR (utv. VS RSFSR 27.10.1960) // SPS «Konsul′tantPlyus».

СВЕДЕНИЯ ОБ АВТОРАХ

Можаева Светлана Юрьевна. Доцент кафедры административного права. Кандидат юридических наук.

Воронежский институт МВД России.

E-mail: svetlana0710@internet.ru

Россия, 39065, Воронеж, проспект Патриотов, 53.

Полякова Наталья Викторовна. Начальник кафедры административного права. Кандидат юридических наук, доцент.

Воронежский институт МВД России.

E-mail: n.v.poliyakova@list.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Mozhaeva Svetlana Yuryevna. Associate Professor of the chair of Administrative Law. Candidate of Law.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: svetlana0710@internet.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Polyakova Natalia Viktorovna. Associate Professor of the chair of Administrative Law. Candidate of Law, Associate Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: n.v.poliyakova@list.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: административный надзор; поднадзорный; процессуальная проверка; ограничения; сопряжение; место жительства; территориальный орган.

Key words: administrative supervision; supervised person; procedural review; restrictions; conjugation; place of residence; territorial body.

УДК 343.8

Е. П. Новикова, *кандидат юридических наук, доцент*
Л. А. Гетманова

РАССТРЕЛЫ В ШКОЛЕ (СКУЛШУТИНГ): ИСТОРИЯ, ПРИЧИНЫ, ПРОФИЛАКТИКА

SCHOOL SHOOTINGS: HISTORY, CAUSES, PREVENTION

В статье проводится анализ появления такого преступления, как скулшутинг, анализируется причинный комплекс и основные меры профилактики расстрелов в школах.

The article analyzes the emergence of such a crime as school shooting, analyzes the causal complex and the main measures for the prevention of school shootings.

К сожалению, текущий период характеризуется участившимися в России и в мире случаями массовых расстрелов в школах. Только за 2 месяца 2026 года в мире зафиксированы уже 4 подобных случая (3 — в США, 1 — в Канаде). В частности, 10 февраля в Tumber Ridge Secondary School в Канаде в результате акта скулшутинга со стороны Джесси Ван Рутселаар (18 лет) были убиты 8 и ранены 27 человек, а сама она совершила самоубийство [12].

В РФ за 2 месяца текущего года «полноценных» фактов школьных расстрелов не выявлено, однако, по данным МВД России, произошло 5 нападений подростков в школах с огнестрельным, травматическим и холодным оружием и предметами, похожими на него, не приведших к массовым жертвам: 22 января — школа г. Нижнекамска (нападение с ножом и сигнальным устройством на одноклассников); 3 февраля — гимназия № 16 г. Уфы (нападение на учителя ученика 9 класса с пневматическим оружием и петардой); в этот же день в школе г. Кодинска Красноярского края школьница напала с ножом на учителя и одноклассницу; 4 февраля в школе № 153 г. Красноярска ученица 8 класса напала с молотком и причинила увечья разной степени тяжести 7 своим одноклассникам; 11 февраля в индустриальном техникуме г. Анапы студентом 17 лет был убит охранник и ранено 2 учащихся техникума. Кроме того, было предотвращено 21 потенциальное нападение в 15 российских регионах [11].

Скулшутинг (англ. — school shooting) является видом делинквентного антисоциального поведения. История появления данного термина связана с массовым убийством, произошедшим в 1999 году в школе «Колумбайн» штата Колорадо (США). 20 апреля 1999 года в школе «Колумбайн» округа Джефферсон в штате Колорадо США двое школьников совершили массовое нападение на образовательную организацию, в результате которого было убито 13 и ранено 23 человека, а сами преступники совершили самоубийство. Название школы вскоре стало нарицательным и сформировало одноименную субкультуру крайне радикального антисоциального поведения среди подростков [9].

В настоящее время скулшутинг — это совершение массовых убийств учащихся и персонала образовательных организаций, которые проводятся учащимися или посторонними лицами, проникшими в школу с оружием [3].

Если обратиться к дословному переводу этого понятия, то оно означает «стрельбу в школе», то есть преступление в образовательной организации с применением оружия. Скулшутинг возникает вследствие ряда внешних (семья, школа, буллинг, духовно-нравственное развитие, воздействие цифровых зависимостей и агрессивной внешней интерактивной среды) и внутренних (повышенное чувство справедливости, приверженность идеалам «Колумбайна») причин, провоцирующих стрелка на его совершение. Он представляет собой социальный феномен, при котором подросток по личным мотивам планирует и совершает массовый расстрел в образовательном учреждении, где потерпевшими являются одноклассники, одногруппники, учителя и другие лица, которые работают или обучаются в конкретном образовательном учреждении.

Наиболее часто преступники при совершении данного преступного деяния применяют огнестрельное оружие, чтобы убить максимально большое количество людей Агрессор во время скулшутинга разрушает в себе навыки саморегуляции, ведь, продолжая стрелять, виновный все более «разжигается» эмоционально и не способен

управлять своими действиями, не чувствует границ. Неспособный к регуляции и управлению своими эмоциями стрелок под влиянием фактора стресса, если не находит в себе сил для сопротивления, нередко может совершить самоубийство [6].

В России благодаря запрету в стране на ношение огнестрельного орудия и традиционным российским духовным ценностям субкультура «Колумбайн» распространилась значительно позднее, чем в США и странах Западной Европы. Более 4 лет назад Верховным Судом РФ неформальное движение «Колумбайн» официально признано террористическим. Вместе с тем, запрет не смог устранить основные причины скулшутинга, к которым в России относятся как внешние, так и внутренние факторы [12].

К основным внешним факторам скулшуттинга могут быть отнесены:

- проблемы в семье (злоупотребление родителей спиртными напитками и наркотиками; факты насилия в семье; частый уход подростка из дома; полное отсутствие семейного воспитания, выработки и закрепления надлежащих духовно-нравственных и моральных ценностей у подростка; отсутствие удовлетворения нормальных потребностей ребенка (сон, еда, одежда и т. д.); наличие дома огнестрельного или охотничьего оружия, взрывчатых веществ, взрывных устройств и боеприпасов в свободном доступе для подростка).

- проблемы в школе (недостаточная антитеррористическая укрепленность и обеспечение безопасности учащихся, отсутствие пунктов отражения атаки, убежищ и незнание школьниками и учителями алгоритма действий при эвакуации учащихся в случае возникновения экстренных ситуаций и т. д.);

- проблемы, связанные с регулярными фактами травли со стороны сверстников («буллинга») подростка в школе;

- проблемы, связанные с развитием зависимостей от агрессивных компьютерных игр и экстремистских интернет-сообществ [8].

Основными внутренним факторами скулшутинга являются: состояние озлобленности на школьное сообщество, чувство обиды, отложенная месть в целях восстановления справедливости; отсутствие твердых навыков социальной коммуникации и саморегуляции; необходимость в самоутверждении в школе, даже за счет лишения жизни других людей.

Постоянное состояние угнетения, страх, низкая самооценка, изоляция, ухудшение успеваемости, потеря аппетита, возникновение соматических болезней, эмоциональное напряжение, стресс, депрессия, бессонница способствуют возникновению ненависти к людям. Наравне с указанными факторами совершение насильственных действий при скулшутинге провоцируется эгоизмом преступника. Причиной стрельбы может стать попытка компенсировать определенные неудачи; высокая самооценка при очень низкой успеваемости или социальном признании. В таких случаях жертвами скулшутинга являются учащиеся, которые лучше учатся, имеют высокий рейтинг в коллективе и выше оцениваются педагогами. Но встречаются случаи, когда личности, гордящиеся своим интеллектом, переоценивают свои возможности и, расстреливая более слабых, демонстрируют свое превосходство над ними [7].

Общие черты и свойства личности субъекта скулшутинга надо искать не только в самом факте совершения преступления, а преимущественно в тех особенностях формирования личности, которые отличают этих людей от законопослушных граждан и которые детерминируют общественно опасное деяние и предопределяют потенциальную склонность к его совершению в будущем.

Следует согласиться с Т. С. Волчецкой, что одной из причин скулшутинга выступает чувство возмездия или протеста против регулярного физического или психического насилия [5].

В этой связи следует отметить такое распространенное антисоциальное явление, как буллинг — школьная травля, которое нередко предшествует скулшутингу. Период, когда будущего «школьного стрелка» буллят в школе, может длиться от нескольких дней до нескольких лет. Все зависит от нанесенной обиды, характера, темперамента и «степени терпения» жертвы буллинга, одновременно выступающей преступником при ее решении отомстить своим обидчикам с применением огнестрельного оружия. Так, по темпераменту один ребенок может хорошо учиться, отличаться флегматизмом, выдержанным характером, быть тихоней. Другой, наоборот, быть излишне импульсивным, ярким, подвижным, склонным к гиперактивному поведению. В первом случае весьма вероятна ситуация, когда акт скулшутинга совершается в качестве ответной реакции на постоянный буллинг со стороны сверстников, во втором — как реакция на постоянные «придирки» учителей [5].

Соответственно, и предотвращение причин скулшуттинга в конкретном учебном заведении может быть основано на модели противодействия «школьной травле» конкретных учащихся «группы риска», разработанной с учетом: уровня организации образования; возраста обучающихся и связанных с ним особенностей психологического и эмоционального развития; уровня физического и психического развития, способности понимать сущность антибуллинговых норм; мнения учащихся, их родителей (законных представителей), администрации и коллектива организации

образования) [5]. В этой связи необходимо отметить, например, что у «школьных стрелков» — жертв буллинга, как правило, нет настоящих друзей. Они практически всегда недовольны тем местом, которое занимают в реальной жизни. Последствия для участников буллинга в любой роли могут иметь катастрофический характер.

Ряд авторов (например, В. Е. Хазова и другие) отмечают и то, что у жертв травли, совершающих вооруженные нападения на обидчиков в школьных заведениях, снижается иммунитет, а также они страдают от соматических болезней, нервно-психических расстройств, бессонницы и потери аппетита, провоцирующих возникновение проблем со здоровьем; постоянный страх нахождения в учебном заведении мешает концентрироваться на обучении, снижается познавательная способность. В ряде случаев скулшутинг обусловлен тем фактом, что в школу переводятся новые ученики, имеющие большее влияние, чем стрелок, ранее бывший лидером класса. Для самого стрелка это может быть серьезным психологическим ударом, поскольку приходится отступать с высшей позиции в школьной иерархии [13].

Вместе с тем каждый случай скулшутинга индивидуален, и в ряде случаев у «школьных стрелков» выявляют слишком завышенную самооценку и нетерпимость к своим потенциальным жертвам. Школьные стрелки, нередко ведомые в детстве, как правило, не являются гиперактивными людьми, однако бывают исключения. Они склонны в порыве гнева терять контроль, испытывать крайне негативные эмоции и даже становиться одержимыми идеей отомстить тем, кто причинил им зло, становясь на тропу мести. В процессе планирования преступления им нужна жертва. Поэтому преступники делят окружающих их людей на две категории — «свой» и «чужой» и, хотя находятся в сильнейшей стрессовой ситуации, стараются действовать максимально хладнокровно. Нередко у них имеется четко выверенный план предполагаемого нападения [13].

В целом, ввиду серьезных угроз внутренней (общественной) безопасности РФ, которую представляют факты школьных расстрелов с использованием огнестрельного оружия, важным направлением борьбы с таким расстрелами выступает грамотно организованная профилактика скулшутинга.

Одним из решающих факторов является наличие у школьника первоначальных навыков стрельбы из огнестрельного оружия, которые могут быть сформированы, например, при неоднократном участии в охоте вместе с отцом или дедом, профессиональным занятием спортивной практической пулевой стрельбой из огнестрельного оружия, стрельбой в специальном тире и т. д. В ряде случаев стрелок-жертва воспитывался в благополучной семье, где отец (дед) занимается охотой либо работает в правоохранительных органах или охранных структурах, что позволяет ему иметь разрешение на хранение огнестрельного или травматического оружия в доме, где живет будущий «стрелок», либо в доме, куда у него имеется неограниченный доступ (например, в квартире дедушки и бабушки). Данную информацию тоже можно использовать для выявления лиц, склонных к скулшутингу или задумавших и планирующих проведение расстрела в школе.

Необходимо помнить, что в процессе совершения преступления, т. е. самого расстрела, перед одноклассниками и сотрудниками образовательных организаций появляется уже не ученик, а преступник и хладнокровный убийца с сознанием, измененным настолько, что все моральные установки отходят на второй план.

В настоящее время в России можно выделить два направления профилактических мер по купированию негативного влияния данного феномена: социальные (общие) и криминологические (специальные) меры.

В числе социальных мер профилактики скулшутинга видится:

1. Проведение работы с семьями учащихся (предупреждение безнадзорности; контроль и предупреждение фактов жестокого обращения со стороны родственников, сверстников, старшеклассников и педагогов; организация и проведение различных тренингов с родителями по выбору стилей воспитания, тактики предотвращения и разрешения семейных конфликтов; концентрация родителей на раннем выявлении и диагностике аддикций (зависимостей) различного рода и психологических маркеров скулшутинга и т. п.).

К сожалению, процесс выявления несовершеннолетнего, готовящегося к совершению преступления, чрезвычайно затруднен, и чаще всего сотрудникам правоохранительных органов приходится заниматься расследованием уже совершенного преступления. Однако при выявлении готовящегося преступления на ранней стадии, помимо недопущения совершения преступления, можно было бы успеть скорректировать поведение подростка с вовлечением в процесс его близких. Порядок действий с семьей предполагаемого скулшутера, планирующего расстрел, должен включать несколько вариантов. Например, во избежание паники, непонимания и поспешных действий со стороны родителей и самого ребёнка для пресечения готовящегося преступления и профилактической работы необходимо помимо сотрудников ПДН привлекать педагога-психолога. Подобный визит должен включать беседу с родителями ребёнка и самим подозреваемым с целью

информирования и психолого-педагогического консультирования как родителей, так и самого ребёнка. Цель такой беседы — в корректной форме донести информацию о предстоящих действиях правоохранительных органов по поводу выявленного готовящегося преступления и побудить семью к сотрудничеству.

Подобная беседа должна включать социально-психологический анализ личности подростка и его родителей, во-первых, для понимания психологического состояния ребёнка, во-вторых, для создания последующей стратегии взаимодействия с подозреваемым. В данном случае в зависимости от состояния подозреваемого выбираются дальнейшие методы работы с ним, к которым, в частности, относятся: задержание, арест, обыск, допрос, помещение в медицинское учреждение и т. п.

2. Проведение работы с образовательными учреждениями (раннее выявление фактов школьной травли отдельных учащихся, формирование группы специального психолого-педагогического сопровождения, проведение индивидуальных бесед классного руководителя, завуча или директора образовательного учреждения с родителями и законными представителями детей — зачинщиков буллинга или школьной травли и детей, которые подвергались травле; повышение требований к обеспечению безопасности территории образовательного учреждения, ужесточение контрольно-пропускного режима и т. д.) [2].

3. Противодействие школьному буллингу как одной из важнейших причин скулшутинга. Необходима разъяснительная работа как с родителями школьников — жертв травли, так и с родителями школьников — зачинщиков школьной травли. Также важно организовать работу с подростками педагога или специалиста-психолога с целью корректировки их модели поведения и снижения агрессии и недопущения развития иных моделей общеопасного аддиктивного поведения, способного привести к скулшутингу [5].

4. Противодействие цифровым зависимостям, а также негативному влиянию интернета, агрессивных компьютерных игр и экстремистских интернет-сообществ типа «Колумбайн». В данном направлении, например, в качестве действенных мер можно предложить:

а) закрепление в законе запрета доступа подросткам определенного возраста и состоящим, например, в школьной «группе риска» ввиду имеющихся аддиктивных особенностей или склонности к деструктивному поведению к таким категориям компьютерных игр, как «хорроры» и «шутеры»; создание в России эффективной системы контроля за этим со стороны государства, контроль со стороны родителей учащихся;

б) применение систем контентной фильтрации при доступе к интернету (например, по аналогии с кинофильмами, ввести в практику вырезание из сюжетов компьютерных игр наиболее агрессивных сцен либо сцен, которые могут склонить подростка к неконтролируемой вооруженной агрессии);

в) формирование в учебном заведении ежегодных программ по профилактике интернет-зависимости, включающих уроки по разъяснению учащимся наказуемых последствий их участия в экстремистских сообществах или деструктивных молодежных движениях (например, ЧВК «Редан» и т. п.), закрепляющие тренинги и ролевые игры по данному вопросу;

г) проведение постоянной разъяснительной работы с родителями, включающей проведение совместных досуговых мероприятий родителей и учеников одного класса (походы, выезды на природу, походы в театр и т. п.). Создание администрацией школы специальных информативных памяток по преодолению конфликтов в семье, школе и т. п. Конечная цель данной разъяснительной работы видится в создании привлекательного для школьников, а также интересного и безопасного «контента» с активным привлечением к нему подростков, учащихся о одном классе, а также налаживание положительных коммуникативных связей между одноклассниками или школьниками — сторонниками единых интересов и увлечений для образования групп и дальнейшего личного устного или письменного общения в этих группах. Школьник получит возможность реализовать себя как личность, завести новых друзей, пообщаться с психологом, что устранит его «зацикленность» на негативе и убережет от наиболее радикального разрешения конфликтных ситуаций со сверстниками и учителями, которым, безусловно, выступает скулшутинг [13].

5. Формирование модели воспитания подростка, основанного на привитии положительных духовно-нравственных ценностей и принципов («Не убий», «Возлюби ближнего своего как самого себя» и т. д.) [2].

Вторым направлением профилактики скулшутинга, или массовых расстрелов в школах, выступают специальные криминологические меры, в числе которых можно предложить:

1. Меры по совершенствованию действующего уголовного законодательства РФ (например, в вопросах криминализации буллинга как основной причины расстрелов в школах путем внесения отдельного состава преступления в Уголовный кодекс РФ и т. п.) [5].

2. Применение в РФ ряда специальных программ и модульных систем противодействия

скулшутингу в рамках образовательных учреждений.

3. Раннюю диагностику атипичного поведения ребенка и деятельность по предупреждению фактов скулшутинга с его участием (тесное взаимодействие и совместная работа педагогов, родителей и сотрудников правоохранительных органов по выявлению опасных отклонений в поведении подростка, комплекса факторов, побуждающих ребенка к массовому расстрелу в учебном заведении, и купированию противоправного вооруженного протеста) [1].

Необходимо подчеркнуть, что значимым фактором профилактики скулшутинга может стать ужесточение контроля за интернет-сообществами радикальной направленности и экстремистскими группами в молодежных социальных сетях, которые оправдывают и массово распространяют антиобщественную идеологию, культивирующую идею массовых убийств в учебных заведениях. Борьбу в данном направлении также необходимо активизировать в России, так как подростки являются легко внушаемым, эмоционально нестабильным объектом и благодаря этому подпадают под влияние подобных групп и становятся основой всякого рода экстремистских организаций и радикальных течений. В данном направлении обязательна совместная работа педагогов, родителей и сотрудников правоохранительных органов по выявлению опасных отклонений в поведении подростка и предупреждению совершения скулшутинга как акта вооруженного протеста с человеческими жертвами.

Наряду с вышеизложенным существенным потенциалом в России для профилактики скулшутинга обладает профессиональная психологическая работа в учебных заведениях, направленная на формирование у учащихся устойчивого механизма саморегуляции собственного поведения, который позволит обеспечить подростку в трудных ситуациях возможность активизировать самоконтроль, проявить твердость характера, самодисциплину и скоординировать собственное поведение при возникновении в процессе учебы разного рода стрессовых ситуаций.

ЛИТЕРАТУРА

1. Березнев А. В. Организация и управление системой предотвращения инцидентов скулшутинга в России : автореф. дис. ... канд. соц. наук. — Новочеркасск, 2025. — 27 с.

2. Борисова Н. Ф. Скулшутинг — новая криминальная угроза обществу // Российский правовой журнал. — 2021. — № 1. — С. 125—129.

3. Волчецкая Т. С. Криминологическая характеристика и профилактика скулшутинга и кибербулиинга в России и зарубежных странах // Всероссийский криминологический журнал. — 2021. — № 15. — С. 584—560.

4. Жмуров Д. В. Жертвы кибербуллинга: состояние проблемы // Российский следователь. — 2023. — № 1. — С. 45—50.

5. Коновалова А. А., Савчишкина О. Г. Скулшутинг или причины массовых убийств школьниками // Международный журнал гуманитарных и естественных наук. — 2023. — № 10. — С. 104—106.

6. Лангман П. Почему дети убивают. Что происходит в голове у школьного стрелка. — М. : Эксмо, 2022. — 304 с.

7. Лукашкова И. Л., Ященко А. А. Феномен скулшутинга: причины и профилактика // Ученые записки Казанского юридического института МВД России. — 2023. — № 2. – С. 337—341.

8. Наумов А. «Я ненавижу тупых людей». Жестокая бойня в школе сделала двух садистов героями Америки. — URL: https://lenta.ru/articles/2018/01/20/columbine/(дата обращения: 26.02.2026).

9. Орлова М. С. Криминогенные факторы, обусловливающие вооруженные нападения обучающихся (выпускников) в образовательных организациях // Российский следователь. — 2023. — № 8. — С. 58—61.

10. С начала 2026 года МВД России предотвратило 21 нападение на учащихся и педагогов. — URL: https://www.rbc.ru/ rbcfreenews/6996e71c9a7947df0d7ec6f8 (дата обращения: 26.02.2026).

11. Стрельбу в школе в Канаде совершил 18-летний трансгендер с расстройством психики. — URL: https://rtvi.com/news/strelbu-v-shkole-v-kanade-sovershil-18-letnij-transgender-s-rasstrojstvom-psihiki/?ysclid=mm1y1touvf829152824 (дата обращения: 26.02.2026).

12. Хазова В. Е. Предупреждение скулшутингов органами внутренних дел: современное состояние и социальные аспекты // Уголовное судопроизводство: проблемы теории и практики. — 2024. — № 2. — С. 44.

REFERENCES

1. Bereznev A. V. Organizatsiya i upravlenie sistemoj predotvrashcheniya intsidentov skulshutinga v Rossii : avtoref. dis. ... kand. sots. nauk. — Novocherkassk, 2025. — 27 s.

2. Borisova N. F. Skulshuting — novaya kriminal′naya ugroza obshchestvu // Rossijskij pravovoj zhurnal. — 2021. — № 1. — S. 125—129.

3. Volchetskaya T. S. Kriminologicheskaya kharakteristika i profilaktika skulshutinga i kiberbulinga v Rossii i zarubezhnykh stranakh // Vserossijskij kriminologicheskij zhurnal. — 2021. — № 15. — S. 584—560.

4. Zhmurov D. V. Zhertvy kiberbullinga: sostoyanie problemy // Rossijskij sledovatel′. — 2023. — № 1. — S. 45—50.

5. Konovalova A. A., Savchishkina O. G. Skulshuting ili prichiny massovykh ubijstv shkol′nikami // Mezhdunarodnyj zhurnal gumanitarnykh i estestvennykh nauk. — 2023. — № 10. — S. 104—106.

6. Langman P. Pochemu deti ubivayut. Chto proiskhodit v golove u shkol′nogo strelka. — M. : Eksmo, 2022. — 304 s.

7. Lukashkova I. L., Yashchenko A. A. Fenomen skulshutinga: prichiny i profilaktika // Uchenye zapiski Kazanskogo yuridicheskogo instituta MVD Rossii. — 2023. — № 2. – S. 337—341.

8. Naumov A. «Ya nenavizhu tupykh lyudej». Zhestokaya bojnya v shkole sdelala dvukh sadistov geroyami Ameriki. — URL: https://lenta.ru/articles/2018/01/20/columbine/(data obrashcheniya: 26.02.2026).

9. Orlova M. S. Kriminogennye faktory, obuslovlivayushchie vooruzhennye napadeniya obuchayushchikhsya (vypusknikov) v obrazovatel′nykh organizatsiyakh // Rossijskij sledovatel′. — 2023. — № 8. — S. 58—61.

10. S nachala 2026 goda MVD Rossii predotvratilo 21 napadenie na uchashchikhsya i pedagogov. — URL: https://www.rbc.ru/ rbcfreenews/6996e71c9a7947df0d7ec6f8 (data obrashcheniya: 26.02.2026).

11. Strel′bu v shkole v Kanade sovershil 18-letnij transgender s rasstrojstvom psikhiki. — URL: https://rtvi.com/news/strelbu-v-shkole-v-kanade-sovershil-18-letnij-transgender-s-rasstrojstvom-psihiki/?ysclid=mm1y1touvf829152824 (data obrashcheniya: 26.02.2026).

12. Khazova V. E. Preduprezhdenie skulshutingov organami vnutrennikh del: sovremennoe sostoyanie i sotsial′nye aspekty // Ugolovnoe sudoproizvodstvo: problemy teorii i praktiki. — 2024. — № 2. — S. 44.

СВЕДЕНИЯ ОБ АВТОРАХ

Новикова Елена Павловна. Доцент кафедры уголовного права и криминологии. Кандидат юридических наук, доцент.
Воронежский институт МВД России.
E-mail: epasyaeva@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Гетманова Лия Александровна. Курсант.
Воронежский институт МВД России.
E-mail: getmanovaliya10@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Novikova Elena Pavlovna. Associate Professor of the chair of Criminal Law and Criminology. Candidate of Law, Associate Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: epasyaeva@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Getmanova Liya Aleksandrovna. Cadet.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: getmanovaliya10@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: скулшутинг; преступление; буллинг; «Колумбайн»; причины скулшутинга; профилактика скулшутинга.

Key words: school shooting; crime; bullying; Columbine subculture; causes of school shooting; prevention of school shooting.

УДК 343.9

Е. А. Пидусов, *кандидат юридических наук, доцент*

ФАКТОРЫ, СПОСОБСТВУЮЩИЕ СОВЕРШЕНИЮ МОШЕННИЧЕСТВ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ТЕЛЕКОММУНИКАЦИИ

FACTORS CONTRIBUTING TO THE COMMISSION OF FRAUDULENT ACTS USING TELECOMMUNICATIONS

В статье рассматриваются некоторые факторы, которые объективно предопределяют возможности совершения мошеннических действий с использованием средств телекоммуникации.

The article discusses some factors that objectively determine the possibility of committing fraudulent acts using telecommunications.

Противоправные действия в любом социуме не являются новым и неизвестным явлением. Данные поведенческие мотивации демонстрируются индивидами на протяжении всей истории развития человечества. Естественно, что с развитием общества и протекающих в нем социальных, экономических, правовых и иных процессов происходит трансформация преступных посягательств (поведения). Преступность формирует новые вызовы общественному порядку и безопасности, при этом посягательства происходят в наименее защищенных (урегулированных) сферах либо в новых, «революционных» направлениях. Переход к информационно-телекоммуникационному образу взаимодействия в данном случае не является исключением.

Преступность организуется, формирует технические и информационные приемы противоправной деятельности, получает новые знания и оборудование, рассматривает пробелы и коллизии в действующем законодательстве, формирует региональные и международные связи. В некоторых случаях начало и окончание противоправного деяния по территориальности может распространяться на несколько государств.

Если типологизировать противоправную деятельность относительно ее целевой установки, то в данной сфере все неизменно. Мошенничество с использованием средств телекоммуникации по своим целям ориентировано на завладение имуществом или благом, как и несколько десятилетий назад. Но применение новых приемов и способов (сеть Интернет, информационно-телекоммуникационное оборудование) позволяет реализовывать данные противоправные замыслы с повышенной результативностью и безопасностью для правонарушителя.

Увеличивается количественный показатель совершенных мошеннических действий, повышается их латентность, способы обмана приобретают новые (не классические) формы подачи. К примеру, в 1980—1990 гг. мошеннические схемы выглядели достаточно заурядно, это привлечение инвестиций под баснословные процентные ставки, вложение в новые предприятия, займы (невозвратные), получение государственного финансирования под невыполняющиеся проекты и др. Зачастую общий посыл мошенника при обмане (завладении доверием) в данном контексте — это обещание выполнить что-либо в определенные сроки и на обоюдовыгодных условиях.

Привлечение средств телекоммуникации позволяет изменить саму процедуру введения в заблуждение, нет необходимости подготавливать документальные пакеты, готовиться и присутствовать на деловых (личных) встречах с жертвой обмана и, главное, возможно представлять человеку иную личность (должностное лицо, организацию и др.), при этом не фигурируя перед ним фактически. У мошенников появилась возможность представляться правоохранителями (сотрудниками МВД России, ФСБ России, Прокуратуры), выдавать себя за сотрудников служб безопасности и технической поддержки банков, изображать близких родственников и знакомых, попавших в сложные жизненные обстоятельства.

В некоторых случаях мошенничество реализуется даже не в личной (телефонной) беседе, а с использованием мессенджеров. По нашему мнению, главной причиной возможности совершения данных действий является развитие электронных банковских переводов и операций, мобильного банка, личных (интерактивных) кабинетов, ди-

станционного кредитования, круглосуточной работы электронных банковских операций (систем, банков).

Формально мошеннические действия, совершаемые с использованием современных средств телекоммуникации, возможно разделить на несколько направлений [1].

1. Использование банковских карт потенциальной жертвы с прямым воздействием на них. К данному виду мошенничества можно отнести такие приемы, как изготовление поддельных банковских карт, АТМ-мошенничество (реализуется с использованием банкоматов) [2].

Рассуждая достаточно кратко о данном направлении мошенничества, можно сказать следующее:

- это достаточно затратный в техническом плане способ завладения платежными данными карты;

- требуется значительная подготовка и последующее техническое взаимодействие с устройствами, позволяющими реализовать мошенническую схему (необходимо получить информацию со сканера, установленного на банкомате, требуется размещение сканера на нескольких устройствах для увеличения количества просканированных карт и др.);

- необходим доступ к электронной системе банковских операций, для получения возможности вывода (перевода) денежных средств на иные счета;

- необходимо привлечение нескольких участников в преступную группу для реализации противоправных действий.

2. Фишинг-атаки, вирусное программное обеспечение, установленное на устройство потенциальной жертвы мошенника, обеспечение удаленного доступа.

Относительно указанного мошеннического механизма можно отметить следующее:

- сложность реализации в контексте установки программы «шпиона» в софт электронного устройства лица, в отношении которого направлено посягательство;

- дорогое оборудование, а также необходимость наличия серьезных технических навыков для реализации обманной схемы;

- необходимость заблаговременной проверки остатка денежных средств на счетах жертвы (чтобы после реализации посягательства возможно было вернуть свои вложенные средства), а это подразумевает проведение трудоемкой технической и информационной разведывательной подготовки.

3. Взаимодействие с жертвой в рамках интернет-торговли. Данный способ мошенничества может сочетать в себе несколько элементов. Во-первых, представляется возможным завладеть набором банковских персональных данных самого покупателя. Во-вторых, после получения оплаты (товара или услуги) возможно не предоставлять заявленное в объявлении потенциальному покупателю, ссылаясь на проблемы с доставкой и др.

По данному виду мошенничества можно отметить:

- широкий охват аудитории, в случае размещения объявления о продаже дорогостоящей продукции по цене ниже рыночной на известных торговых интернет-площадках (Авито, Авто.ру, Алиэкспресс, Вайлдберис и др.);

- сложность убеждения покупателя оплатить потенциальный товар без использования платежного терминала площадки, путем задатка или полной оплаты покупки на отдельный счет продавца (зачастую данный счет привязан к карте банка другого государства либо оформлен на третье лицо);

- необходимость прохождения «условной» идентификации для размещения объявления на интернет-площадке.

4. Мошенничество с утерянными, украденными, неполученными банковскими картами. Данный вид мошеннических действий подразумевает наличие легитимной (оригинальной) банковской карты у злоумышленников.

Отметим следующее:

- наличествует необходимость прямого контакта, в отдельных случаях, с законным владельцем карты;

- реализация мошеннической схемы осложняется возможностью блокировки карты банком либо владельцем;

- наиболее часто подобные карты используются для реализации покупок с отложенным платежом либо при оплате на территории другого государства (мошенники пользуются временной задержкой при обмене информацией между банками на территории разных стран).

5. Похищение банковских данных о клиентах непосредственно из банка [3]. Данный вид мошенничества можно рассматривать как отдельный элемент либо как подготовительный этап для «телефонного» мошенничества.

Отметим, что он:

- представляется достаточно сложным с позиции реализации в техническом плане;

- требует (достаточно часто) личного внедрения сотрудника в штат банка (либо подкуп действующего сотрудника) для получения информации о клиентах;

- осложняется необходимостью проверки полученных результатов (баз данных о клиентах) на актуальность.

6. Телефонное (иное информационно-коммуникационное) мошенничество. Представляется наиболее распространенным в настоящее время, поскольку может комбинировать в себе несколько подвидов мошенничества. Ориентировано на доверчивость потенциальной жертвы и наличие навыков убеждения у правонарушителя.

По данному виду отметим следующее:

- это наименее затратное мошенничество, если не комбинируется с иными видами, не включает в себя подготовительного этапа (в части завладения информацией о клиентах банка, либо иными сведениями, хранящимися в электронных банках данных различных организаций);

- оно может быть ориентировано на различную тематику (помощь близким, друзьям; банковские операции, доступ на различные порталы (Госуслуги, личная почта, аккаунты социальных сетей); «холодный» обзвон);

- необходима высокая ораторско-психологическая подготовка звонящего, наличие убедительно построенной речи, грамотность, вежливость, умение поддерживать официально-деловой стиль общения;

- необходима подготовка речевой карты (скрипта) для мошенника, если он будет работать в группе.

Безусловно, представленный перечень разновидностей мошеннических манипуляций не является исчерпывающим и может быть дополнен. Это связано с тем, что технологические процессы, лежащие в основе киберпреступлений, носят исключительно динамический характер, системно развиваются, а в некоторых случаях по своей оснащенности, финансированию и технической укомплектованности на несколько шагов опережают возможности правоохранительных органов.

Необходимо отметить стабильные составляющие мошенничества с использованием технических средств:

- недобросовестное (некомпетентное) отношение владельца карты к конфиденциальной информации о нем;

- вовлечение в совершение деяния инсайда (информации либо лица, ею владеющего);

- международный (трансграничный) характер преступления;

- появление новых потенциально опасных угроз, основанных на прогрессе в данной сфере общественных отношений;

- наличие у преступников высокой технической (информационной) квалификации (навыков);

- влияние киберпреступности на состояние общественной безопасности.

Заметим, что прогресс, приносящий положительный результат, невозможно остановить из соображений безопасности. Люди достаточно быстро привыкают к удобным банковским сервисам и услугам. Зачастую многие исключают бумажный денежный оборот в своем бюджете по различным причинам: наличие карточки, платежи с использованием мобильного устройства, оплата через биометрические данные (например, «Плати улыбкой»), возможность онлайн переводов, магазины повсеместно устанавливают технические устройства, позволяющие безналичный расчет. Отметим, что речь в данном контексте не идет исключительно о покупках. Люди отправляют денежные средства внутри семьи, поддерживают (материально) детей, помогают друзьям и близким, и все это происходит за доли секунд. А какова прибыльность данной деятельности в сфере торгово-закупочной деятельности, невозможно себе представить.

Как дополнительный плюс для государства необходимо отметить выход из «темного» наличного оборота значительной части социального сегмента (простота и удобство налогообложения, прозрачность фискальных проводок, системный мониторинг денежной массы, отсутствие необходимости частого обновления денежных билетов Банка России).

Следовательно, говорить о том, что общество и государство откажутся от электронных платежных сервисов и услуг в угоду противодействию киберпреступлениям, в настоящее время не приходится. Таким образом, на правоохранительные органы возлагается повышенная ответственность по обеспечению комплекса мер экономической безопасности, основанных на достижениях науки и техники. И конечно же, данную работу необходимо проводить в тесном взаимодействии с финансовыми и кредитными организациями, учреждениями и гражданами, что в настоящее время и реализуется.

Кроме того, в качестве факторов, способствующих совершению мошеннических действий с использованием средств телекоммуникации, можно отметить:

1. Наличие значительной временной задержки между совершением противоправного деяния и сообщением о данном происшествии в правоохранительные органы. Поскольку правонарушители после совершения преступления понимают ограниченность латентного временного периода, они прикладывают все усилия к реализации способов сокрытия своих действий.

2. Возможность сложносоставного мошенничества с использованием информационно-телекоммуникационных средств. К примеру, скриминг карты будет первичным этапом (в части получения данных и подготовки), а уже телефонное

мошенничество с получением удаленного доступа к личному (онлайн) кабинету в банке жертвы — заключительным.

3. Высокая организованность преступных групп [4]. В данных социальных образованиях (несмотря на их противоправные устремления) присутствует достаточно четкое разделение обязанностей, система руководства, доступ к материальным и иным ресурсам, консультационная и иная помощь.

4. Высокий уровень технической подготовки преступников. Мошенники в своей деятельность используют различные приборы и оборудование, требующие профессионализма (эмбоссер необходим для нанесения объемных надписей на карты банка, тайпер впаивает магнитную пленку на карту, скриммер позволяет считывать данные с карты банка, энкодер записывает полученную информацию на новую карту и др.) [5].

5. Международный (трансграничный) характер обозначенной деятельности. Бесспорно, что безопаснее для преступников получать информацию (активы, данные и др.) в одном государстве, а использовать ее в другом. Дистанционный характер максимально осложняет процесс раскрытия, расследования, доказывания, предупреждения и пресечения противоправной деятельности.

ЛИТЕРАТУРА

1. Лукьянов С. О. Мошенничество с использованием банковских карт в России: современное состояние и виды защиты // Вестник ТГЭУ. — 2012. — № 2. — С. 201.

2. Нагорный В. А. Криминологические особенности некоторых преступлений, совершаемых в сфере оборота платежных карт // Права и свободы человека и эффективные механизмы их реализации в мире, России и Татарстане : материалы международной научно–практической конференции. — Казань, 2014. — С. 493—498.

3. Репин М. Е., Афанасьев А. Ю. Преступления в сфере компьютерной информации: проблемы выявления и раскрытия // Молодой ученый. — 2015. — № 15. — С. 460—463.

4. Данилова Н. А., Кушниренко С. П., Саржин А. Н. Преступления в сфере банковской деятельности как высокотехнологичные преступные посягательства международного характера // Вестник Санкт-Петербургского университета МВД России. — 2016. — № 2. — С. 329—333.

5. Гайдин А. И. Криминалистическое сопровождение проверочной деятельности по сообщениям о неправомерном доступе к компьютерной информации // Вестник Воронежского института МВД России. — 2025. — № 4. — С. 241—250.

REFERENCES

1. Luk′yanov S. O. Moshennichestvo s ispol′zovaniem bankovskikh kart v Rossii: sovremennoe sostoyanie i vidy zashchity // Vestnik TGEU. — 2012. — № 2. — S. 201.

2. Nagornyj V. A. Kriminologicheskie osobennosti nekotorykh prestuplenij, sovershaemykh v sfere oborota platezhnykh kart // Prava i svobody cheloveka i effektivnye mekhanizmy ikh realizatsii v mire, Rossii i Tatarstane : materialy mezhdunarodnoj nauchno–prakticheskoj konferentsii, 28–29 noyabrya 2013 g. — Kazan′, 2014. — S. 493—498.

3. Repin M. E., Afanas′ev A. Yu. Prestupleniya v sfere komp′yuternoj informatsii: problemy vyyavleniya i raskrytiya // Molodoj uchenyj. — 2015. — № 15. — S. 460—463.

4. Danilova N. A., Kushnirenko S. P., Sarzhin A. N. Prestupleniya v sfere bankovskoj deyatel′nosti kak vysokotekhnologichnye prestupnye posyagatel′stva mezhdunarodnogo kharaktera // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. — 2016. — № 2. — C. 329—333.

5. Gajdin A. I. Kriminalisticheskoe sopravozhdenie proverochnoj deyatel′nosti po soobshcheniyam o nepravomernom dostupe k komp′yuternoj informatsii // Vestnik Voronezhskogo instituta MVD Rossii. — 2025. — № 4. — S. 241—250.

СВЕДЕНИЯ ОБ АВТОРЕ

Пидусов Евгений Александрович. Начальник кафедры криминалистики. Кандидат юридических наук, доцент.

Воронежский институт МВД России.

E-mail: pidusov.vrn@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Pidusov Evgeny Alexandrovich. Head of the chair of Criminalistics. Candidate of Law, Associate Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: pidusov.vrn@mail.ru
Wok address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: мошенничество; средства коммуникации; расследование преступлений; информационные технологии.

Keywords: fraud; means of communication; crime investigation; information technology.

УДК 343.9

А. В. Пучнин, *кандидат юридических наук, доцент*
А. В. Польшиков, *кандидат юридических наук, доцент*
О. В. Демидова, *кандидат юридических наук, доцент*

КОМПЛЕКСНЫЙ ПОДХОД К РАННЕЙ ПРОФИЛАКТИКЕ ВОВЛЕЧЕНИЯ НЕСОВЕРШЕННОЛЕТНИХ В ДИВЕРСИОННУЮ И ТЕРРОРИСТИЧЕСКУЮ ДЕЯТЕЛЬНОСТЬ

A COMPREHENSIVE APPROACH TO EARLY PREVENTION OF INVOLVEMENT OF MINORS IN SUBVERSION AND TERRORIST ACTIVITIES

В статье рассматриваются меры повышения эффективности ранней профилактики вовлечения несовершеннолетних в диверсионную и террористическую деятельность. Авторы анализируют современные способы сетевой вербовки подростков и факторы риска. Рассматривают роль семьи, педагогов, сотрудников по делам несовершеннолетних органов внутренних дел (далее — ПДН ОВД) и иных субъектов профилактики по вопросу вовлечения несовершеннолетних в противоправную деятельность. Обосновывается необходимость комплексного подхода, включающего правовое просвещение, патриотическое воспитание, цифровую безопасность и межведомственное взаимодействие.

The article discusses measures to improve the effectiveness of early prevention of minors' involvement in sabotage and terrorist activities. The authors analyze modern methods of online recruitment of teenagers and risk factors. They examine the role of families, teachers, police officers, and other prevention agencies in preventing minors' involvement in illegal activities. The article emphasizes the need for a comprehensive approach that includes legal education, patriotic upbringing, digital security, and interagency cooperation.

Криминогенная обстановка с участием несовершеннолетних резко ухудшилась в 2023-м, к началу 2024-го частично стабилизировалась, но остается тревожной; силовые структуры подчеркивают критичность профилактики для безопасности общества и обороноспособности. В 2025—2026 гг. возможна резкая эскалация на фоне фактического перехода украинских и западных спецслужб к разведывательно-диверсионной деятельности в РФ (в новых регионах — к партизанским тактикам), при этом вовлечение детей растет.

Показателен приговор от 5 июня 2024 г.: Второй Западный окружной военный суд назначил организаторам сообщества, шантажом привлекавшим подростков и обещавшим 90 тыс. руб. за поджоги релейных шкафов на киевском направлении МЖД, наказания до 17—22 лет лишения свободы [1]. Подобные примеры свидетельствуют о том, что несовершеннолетние все чаще становятся объектом целенаправленного воздействия со стороны дистанционных кураторов, использующих их возрастные и психологические особенности в преступных целях. В этой связи особую значимость приобретают своевременные и адресные меры ранней профилактики, учитывающие региональную специфику, каналы сетевого вовлечения и совокупность факторов риска.

Ранняя профилактика противоправного вовлечения несовершеннолетних в деструктивную и преступную деятельность в сети Интернет должна носить комплексный характер и объединять просветительские, организационные и информационно-защитные меры. К числу приоритетных направлений следует отнести систематическое проведение в образовательных организациях лекториев и профилактических занятий с обучающимися, педагогами и родителями с участием психологов, сотрудников правоохранительных органов и иных профильных специалистов; повышение профессиональной готовности сотрудников ПДН ОВД посредством изучения действующих ведомственных и межведомственных методических материалов; а также развитие практик цифровой защиты несовершеннолетних, включая популяризацию средств родительского контроля.

Ключевым условием эффективности такой работы выступает активное участие семьи, поскольку обеспечение информационной безопасности ребенка невозможно без повышения циф-

ровой грамотности родителей. Практика профилактической деятельности показывает, что значительная часть родителей и педагогических работников не обладает необходимым минимумом знаний о способах онлайн-вовлечения подростков в противоправную деятельность, причинах и условиях ее распространения, а также о специфике функционирования криминогенных сегментов интернет-среды [2. — С. 33—34]. Между тем часть самих несовершеннолетних уже знакома с подобными ресурсами и рисками цифрового пространства.

В современных условиях особую актуальность приобретает информирование несовершеннолетних, их родителей и педагогов о технологиях дистанционного вовлечения в противоправную деятельность, реализуемых через мессенджеры, социальные сети и иные цифровые каналы коммуникации. В связи с этим целесообразно проведение регулярных неформальных и содержательно выверенных занятий по вопросам кибербезопасности для обучающихся, родителей и педагогов не реже одного раза в полугодие. Особое значение имеет разъяснение несовершеннолетним правовых последствий их действий и алгоритмов безопасного поведения при попытках вовлечения.

Алгоритм обеспечения личной безопасности подростков в подобных ситуациях должен быть четким, понятным и практически ориентированным. Прежде всего, несовершеннолетним необходимо разъяснять недопустимость вступления в диалог с неизвестными или сомнительными контактами в мессенджерах, социальных сетях, при телефонных звонках и иных формах цифрового общения. Любое обращение, содержащее навязчивый интерес, предложения быстрого заработка, просьбы о конфиденциальном взаимодействии либо попытки перевести общение в закрытый формат, должно рассматриваться как потенциально опасное. При выявлении подозрительного контакта рекомендуется незамедлительно прекратить общение, заблокировать пользователя или бот-аккаунт, а также ограничить возможности дальнейшего взаимодействия посредством изменения настроек приватности учетной записи. В случае массированных обращений целесообразно дополнительно скорректировать параметры конфиденциальности, изменить имя пользователя и минимизировать объем открыто размещенной персональной информации.

Особо следует подчеркнуть недопустимость так называемого «игрового» взаимодействия с сетевыми вербовщиками. Попытки вступить в переписку ради шутки, провокации или мнимого контроля ситуации способны создать условия для последующего психологического давления, шантажа и манипулирования. По этой причине подросток не должен пытаться самостоятельно «разоблачать» таких лиц.

Оптимальным алгоритмом реагирования является немедленное информирование родителей, педагогов, психолога либо сотрудников ПДН ОВД. При необходимости возможно обращение на телефон доверия или иные официальные каналы помощи. Главная задача профилактики состоит в формировании у несовершеннолетних устойчивой установки: любой подозрительный цифровой контакт требует не ответных действий, а своевременного обращения за помощью к взрослым и компетентным специалистам.

Тактика противника понятна — идет ежедневное «сражение» на информационном поле за живых людей, за каждого человека — и юного, и взрослого. Важно предупредить, когда дети и подростки отказываются сотрудничать — им всегда начинают открыто угрожать сетевые вербовщики, бояться этого не надо (стресс ребенка, паника и отчаяние играет на руку врагам). Цитата из опубликованной переписки ребенка с вербовщиком: «Если не согласишься, я тебя лично убью!». Идет массовая рассылка одинаковых сообщений, где неизвестный, например, спрашивает: «Слышали ли Вы что-то о теракте в Крокусе?» и т. п., а затем сетевой вербовщик предлагает снабдить несовершеннолетних необходимым, чтобы они сами заминировали или подожгли, например, крупный торгово-развлекательный центр за деньги (сумма варьирует от 400 до 700 тыс. рублей). Директор Лиги безопасного интернета, член Общественной палаты России Е. М. Мизулина по данному поводу неоднократно подчеркивала, чтобы дети и подростки не вступали в переписку и сразу блокировали такие сообщения и аккаунты.

Сотрудникам ПДН ОВД рекомендуется повторять ранее озвученный тезис и акцентировать внимание и педагогов, и родителей, и подростков, что о каждой без исключения попытке вербовки нужно сразу сообщать в ФСБ или МВД России. Важно объяснить, что в некоторых случаях это нелегко, но поступить нужно именно так. Можно привести реальный пример про несовершеннолетнею девочку — дочку российского военного, которого удерживали на Украине в плену. С его мобильного телефона девочке позвонили сотрудники СБУ и предложили, чтобы «с отцом все было хорошо, и он был просто жив», передать данные обо всех одноклассниках и их родителях. Девочка состояла во Всероссийском детско-юношеском военно-патриотическом общественном движении «Юнармия». Она вспомнила, что отец с раннего возраста всегда ей говорил, что «Родина всегда на первом месте»,

и она сразу сообщила по горячей линии ФСБ России для обращения граждан. Вот пример смелости и решительности в самой сложной и, казалось бы, даже безвыходной ситуации.

Повторим, что психотип подростков очень неуравновешен, часть из них имеет психические отклонения и расстройства. Такие молодые люди легко поддаются манипуляциям опытных сетевых вербовщиков. Типичный цифровой вовлекатель действует поэтапно: устанавливает контакт, проверяет готовность несовершеннолетнего к подчинению через незначительные поручения, а затем склоняет к противоправным действиям. В этой связи профилактическая работа с родителями должна быть ориентирована на раннее выявление подозрительных контактов, поддержание доверительных отношений с ребенком и пресечение вовлечения уже на стадии первичного онлайн-общения.

Инспекторам ПДН ОВД следует мобилизовать профилактический потенциал родителей и иных законных представителей несовершеннолетних, постоянно акцентируя внимание на том, что роль родителя в обеспечении безопасности своего ребенка трудно переоценить: так же, как в раннем возрасте мы учим ребенка ходить, огибать препятствия и внимательно смотреть под ноги, нам необходимо научить его «ходить» и по сети Интернет — уверенно и спокойно, понимая и осознавая все риски. Иными словами, приложить максимальные усилия для того, что-бы научить его осознанному выбору и технике безопасности так же, как и в реальной жизни [3].

Еще один немаловажный и специфический аспект в организации профилактической деятельности — сотрудникам территориальных ПДН ОВД, закрепленным за образовательными организациями, следует рекомендовать педагогическим работникам проводить работу по своевременному выявлению круга лиц среди учеников и несовершеннолетних студентов, а также их ближайшего окружения (друзей-сверстников и старших товарищей, родителей, если об этом стало известно), которые открыто не поддерживают СВО, ведут обособленный (скрытый) образ жизни (в частности, не идут на контакт ни с педагогами, ни с одноклассниками и однокурсниками, имеют странные и подозрительные хобби и увлечения, проявляют на уроках и вне учебных занятий немотивированную излишнюю жестокость и агрессию (например, высказывали намерения отомстить или причинить увечья другим подросткам, учителям и представителям администрации, сотрудникам правоохранительных органов, своим родителям или другим лицам) или, наоборот, подвергаются буллингу со стороны других учеников или подростков по месту учебы или жительства, а также носят с собой постоянно холодное и (или) пневматическое оружие и другие опасные (в том числе запрещенные к ношению) предметы (отвертки, кастеты, газовые баллончики, таблетки, заточки и т. д.). Такие лица могут проявить себя и в онлайн-играх, форумах, чатах, в принципе, везде (в магазине, на детской площадке, в поликлинике, на улице, в спортзале и т. д.).

Несовершеннолетним следует объяснить важность того, что о таких людях следует по возможности сразу сообщать родителям, педагогам или сотрудникам ПДН ОВД, а они, в свою очередь, передадут информацию (после ее предварительного анализа и принятия решения о целесообразности) сотрудникам ФСБ России. Показателен в этом смысле пример, который привели при интервьюировании социальные педагоги и психологи: 13-летний подросток в одном из городов ЦФО — типичная потенциальная жертва сетевого вербовщика с его Яндекс-картами и зацикленностью на постоянном повышении своего рейтинга «знатока города» (замкнутый ребенок, но в то же время идет на контакты со взрослыми). Для него не составит труда сфотографировать любой объект даже без денег, для него важен статус «знаток города высшего уровня», поэтому таких детей могут легко вслепую использовать для фото- и видеосъемок важных объектов, людей или использовать их аккаунты с фотографиями для изучения местности и системы охраны по геолокации, которая прикрепляется к таким «отчетам юного путешественника». Такой, казалось бы, весьма странный и одновременно достаточно интеллектуально развитый ребенок требует особого внимания и индивидуального подхода не только со стороны педагогических работников, родителей, но и сотрудника ПДН ОВД, который может авторитетно объяснить опасность подобного увлечения, не обидев его.

Особое значение при этом имеет не только информирование о самих каналах обращения, но и разъяснение конкретного алгоритма действий несовершеннолетних, родителей и педагогов в случае выявления признаков возможной вербовки или иной подозрительной активности. С учетом высокой латентности рассматриваемых деяний необходимо также расширять информированность о доступных механизмах анонимного обращения за помощью, включая детский телефон доверия, и укреплять доверие к таким каналам поддержки. При этом аналогичным образом следует поступить с номером горячей линии УФСБ России в конкретном регионе РФ для обеспечения быстрой возможности анонимного обращения граждан в случае попытки вербовки или наличия оперативно-значимой информации по таким преступлениям, а также довести телефоны горячей

линии других субъектов профилактики (как альтернативы) [4. — С. 430]. В этой связи инспекторам следует довести информацию педагогами, родителям и несовершеннолетним (по возможности под запись в дневник и мобильный телефон, разъяснить суть такой формы обращения граждан, порядок и ответственность за сообщение недостоверных сведений), что в целях профилактики, своевременного выявления и пресечения противоправных действий в отношении детей и оперативного реагирования на обращения по вопросам защиты прав и законных интересов несовершеннолетних в круглосуточном режиме можно обратиться по телефонам горячей линии [5].

Сотрудникам ПДН ОВД при активном взаимодействии с педагогами особое внимание следует уделить такому важному и востребованному направлению нравственно-патриотического воспитания подростков, как привлечение для проведения лекториев с несовершеннолетними и их родителями участников СВО (цели и задачи такой деятельности определены на самом высоком государственном уровне Президентом России как часть реализуемой общероссийской программы «Время Героев»). Цитата Президента РФ В. В. Путина из послания Федеральному Собранию России (29 февраля 2024 г.): «Подлинная, настоящая элита — это все, кто служит России, труженики и воины, надежные, проверенные, делом доказавшие свою преданность России, достойные люди» [6]).

При этом сотрудникам ПДН ОВД нужно взвешенно подходить к решению данной задачи. Подбор кандидатур целесообразно осуществлять с учетом тематики лектория, характеристик аудитории, а также целей и формата конкретного профилактического мероприятия. В качестве приоритетных следует рассматривать представителей системы МВД России, Росгвардии и Министерства обороны Российской Федерации, отвечающих требованиям безупречной репутации, в том числе не имеющих судимости и фактов привлечения к уголовной ответственности. Такой человек может довести информацию несовершеннолетним аккуратно и профессионально, учитывая свой опыт служебной деятельности, и главное, не идеализируя образ бывшего преступника.

Как показывает практика, бывшие сотрудники правоохранительных органов (пенсионеры и ветераны) охотно пойдут в школы и другие образовательные организации, знают цели и задачи ранних профилактических мероприятий, многие из них имеют огромный опыт профессиональной деятельности в этом направлении, в том числе в должности участковых уполномоченных полиции и сотрудников ПДН ОВД. Они могут расставить приоритеты в групповом занятии или индивидуальной беседе со школьниками или несовершеннолетними студентами, рассказав о подвигах наших защитников в период СВО по защите жителей Донбасса и других регионов России, об угрозах и новых формах вербовочной и разведывательно-диверсионной деятельности иностранных спецслужб, вовлекающих подростков в сети Интернет.

Для своевременного раскрытия рассматриваемых деяний с участием несовершеннолетних кроме использования данных с камер видеонаблюдения и биллинга мобильной связи применяются исследования и экспертизы, в том числе проводится изучение оставленных на месте преступления следов, которые имеют генетическую информацию (например, ДНК на оставленной одежде или на предметах на месте преступления). Несовершеннолетним нужно последовательно довести данную ключевую мысль, используя выборочную информацию резонансные и показательные примеры из СМИ и других масс-медиа, которым несовершеннолетние и родители в подавляющем большинстве полностью доверяют как официальным источникам, и акцентируя внимание на том обстоятельстве, что цифровым кураторам абсолютно безразлична судьба ребенка, вовлеченного в совершение преступления.

Отдельно стоит отметить, что подросткам необходимо разъяснять не только уголовно-правовые, но и имущественные последствия даже внешне незначительных противоправных действий. Повреждение объектов транспортной инфраструктуры, поджоги релейных шкафов, военной техники и иные аналогичные деяния способны повлечь не только дезорганизацию движения и создание угрозы жизни и здоровью граждан, но и причинение ущерба, исчисляемого десятками и сотнями миллионов рублей. В этой связи в профилактических беседах целесообразно использовать конкретные примеры крупных гражданских исков, заявляемых в рамках уголовных дел.

Одновременно родителям и педагогам следует рекомендовать проявлять повышенную бдительность к косвенным признакам возможного вовлечения несовершеннолетнего в противоправную деятельность: появлению у него легковоспламеняющихся веществ, подозрительных предметов, чужой одежды, следов копоти, специфических файлов и переписки на цифровых устройствах. Практика показывает, что значительным профилактическим потенциалом обладают краткие аудио- и видеосообщения, распространяемые в родительских чатах, поскольку они обеспечивают одновременно широкий охват аудитории и высокий уровень доверия к информации.

Причем по вопросу повышения эффективности организации ранней профилактики совершения несовершеннолетними рассматриваемых деяний за счет обеспечения безопасности образовательной среды сотрудникам ПДН ОВД рекомендуется активизировать системную работу не только с представителями администрации образовательной организации, но и с представителями частно-охранных предприятий (далее — ЧОП) и сотрудниками Росгвардии, которые осуществляют контроль за ними. При этом по вопросу организации контрольно-пропускного режима и в целом безопасности образовательного пространства, включая трактовку норм действующего законодательства и Устава образовательной организации (в частности, понимания целесообразности соблюдения условий и порядка личного досмотра учеников и студентов, определения перечня запрещенных к проносу предметов, внешнего вида ребенка и т. д.), нужен консенсус педагогов (при консультации с сотрудниками ПДН ОВД и Росгвардии), детей и родителей, когда в результате будет понятно, что «можно» и что «нельзя».

И самое главное — несовершеннолетним важно довести информацию о том, что в структуре центров информационно-психологических операций Сил специальных операций ВСУ (ЦИПСО) есть специальные группы сотрудников, объектом внимания которых являются, в основном, подростки, те, кто «засветился» в социальных сетях своими высказываниями, активным поведением (например, постоянно выкладывая провокационные и вызывающие фото и видеофайлы), подражая известным блоггерам, и т. д. Выявить и доказать подлинный источник происхождения таких сообщений сетевых вербовщиков сейчас практически невозможно. Это обстоятельство важно учитывать при проведении профилактических бесед, объясняя подросткам необходимость соблюдения элементарных правил личной безопасности в сети Интернет, прежде всего, путем максимально корректного поведения в виртуальном пространстве, а также удаления или минимизации информации о себе, родных и близких, месте учебы, жительства, проведения досуга и отдыха, которая, как правило, размещается с автоматической привязкой к геолокации.

Для обеспечения безопасности и здорового онлайн-пространства для детей существует несколько методов контроля доступа к интернету. Один из них «родительский контроль» в операционных системах. Это позволяет ограничить по времени использование устройства, блокировать определенные приложения и сайты. Также существует расширение функции родительского контроля в браузерах и антивирусных системах. С помощью последних можно блокировать определенные сайты и приложения, отслеживать активность ребенка в сети, ставить запреты на звонки, блокировать спам и многое другое. На практике значительная часть родителей не использует возможности родительского контроля либо применяет их фрагментарно, недооценивая профилактический потенциал таких цифровых инструментов. Сотруднику ПДН ОВД нужно объяснить им важность таких приложений и настроек мобильного телефона. Можно дать ребенку обычный телефон, что все чаще практикуют родители и учителя в провинции и не только.

Важным техническим направлением ранней профилактики является разъяснение несовершеннолетним рисков, связанных с использованием VPN-сервисов и онлайн-игровых коммуникаций. Подросткам следует объяснять, что загрузка как бесплатных, так и платных VPN-приложений может создавать дополнительные угрозы информационной безопасности, поскольку подобные программы нередко используются для сбора пользовательских данных, распространения вредоносного программного обеспечения, мошеннических схем и установления скрытого контроля над устройством. В отдельных случаях такие цифровые инструменты могут использоваться и лицами, осуществляющими противоправное вовлечение несовершеннолетних. В связи с этим родителям рекомендуется контролировать установку подобных приложений на устройствах детей и своевременно разъяснять им возможные последствия их использования. Аналогичный подход необходим и применительно к онлайн-играм, где игровые чаты нередко становятся каналом установления подозрительных контактов [7. — С. 17]. С профилактической точки зрения наиболее безопасной является минимизация участия несовершеннолетних в подобных коммуникациях либо полный отказ от переписки с незнакомыми пользователями в игровых сервисах.

Таким образом, исходя из вышеизложенного, необходимо сделать вывод о том, что оптимизация мер ранней профилактики диверсий и террористических актов, совершаемых подростками, требует комплексного подхода, который включает в себя образовательные, психологические, и социальные меры, а также активного взаимодействия между субъектами профилактики с учетом необходимости непрерывного мониторинга криминогенной ситуации в этой сфере [8, 9]. И главное, «волшебных способов, чтобы уберечь наших детей от вербовки неизвестных из социальных сетей и мессенджеров, нет, здесь необходим только контроль родителей, воздействие друзей, близких и профилактическая работа правоохранительных

органов и спецслужб, больше в этом случае ничего не придумаешь» [10].

В итоге сотрудникам ПДН ОВД можно предложить следующую последовательность действий в стенах образовательных организаций (оптимальный формат для работы в рамках профилактики):

1) Организовать для педагогических работников образовательной организации инструктивное совещание, посвященное современным способам вовлечения несовершеннолетних в противоправную деятельность, порядку взаимодействия с сотрудниками ПДН ОВД при выявлении таких фактов, а также рискам несвоевременного информирования правоохранительных органов.

2) Провести цикл профилактических лекций и индивидуальных бесед с несовершеннолетними, их родителями и студентами с учетом возраста и конкретных проблем. При необходимости к такой работе целесообразно привлекать психологов, социальных педагогов, а также представителей силовых структур, обладающих практическим опытом профилактической и патриотико-воспитательной деятельности (участников СВО, ветеранов боевых действий, действующих сотрудников и пенсионеров «силового блока» и т. д.).

3) При выявлении факта осуществления попытки вовлечения несовершеннолетнего в противоправные действия со стороны сетевых вербовщиков или иных лиц провести проверку поступившей информации (в том числе выяснив возможность группового или повторного совершения таких действий) и передать при необходимости материал для дальнейшего принятия решения по компетенции должностным лицам, а также провести подробное обсуждение происшествия с педагогическими работниками и при необходимости с учениками, несовершеннолетними студентами, их родителями (и иными законными представителями).

ЛИТЕРАТУРА

1. Принуждавшие детей к поджогам диверсанты получили сроки от 17 до 22 лет. — URL: https://ren.tv/news/ (дата обращения: 30.03.2026).

2. Абрамян С. К., Нескородова И. С., Соловьев В. С. Противодействие вовлечению молодежи в экстремистскую и террористическую деятельность через информационно-коммуникационную сеть Интернет : учебное пособие. — Краснодар : Краснодарский университет МВД России, 2022. — 60 с.

3. Артамонова Е. Г., Бородина А. С., Мелентьева О. С. Методические рекомендации для несовершеннолетних, родителей (законных представителей) несовершеннолетних, наглядные информационные материалы по безопасному использованию сети Интернет в целях предотвращения преступлений, совершаемых с ее использованием как самими несовершеннолетними, так и в отношении них. — М. : Центр защиты прав и интересов детей, 2021 — 35 с. // Банк документов Министерства просвещения РФ. — URL: https://docs.edu.gov.ru/document/f9f90ed22419ee2738e66ea467bf52ae/download/4403/ (дата обращения: 30.03.2026).

4. Диваева И. Р., Колесников Р. В., Любимов Л. В. О предупреждении вовлечения несовершеннолетних в экстремистскую деятельность с использованием информационно-телекоммуникационных технологий // Образование и право. — 2024. — № 8. — С. 428—432.

5. Телефон Горячей линии. — URL: https://telefon-doveria.ru/questions/ (дата обращения: 30.03.2026).

6. Программа развития для участников специальной военной операции реализуется по поручению Президента России Владимира Владимировича Путина Высшей школой государственного управления РАНХиГС на базе Мастерской управления «Сенеж». — URL: https://времягероев.рф/ (дата обращения: 30.03.2026).

7. Ильницкий А. С. Противодействие криминальной идеологии в сети Интернет : автореф. дис. … канд. юрид. наук / Ильницкий Александр Сергеевич. — Краснодар, 2022. — 31 с.

8. Игнатов А. Н. Современные трансформации экстремизма и терроризма // Актуальные проблемы противодействия экстремизму, русофобии и украинскому неонацизму : материалы всероссийской научно-практической конференции, Симферополь, 03 мая 2024 года. — Краснодар : Краснодарский университет МВД России, 2024. — С. 68—72.

9. Буданова Е. А., Буданов С. А., Кушнарева А. В. Особенности детерминации и предупреждения фактов вовлечения несовершеннолетних в совершение преступлений посредством сети Интернет // Вестник Воронежского института МВД России. — 2023. — № 4. — С. 211—218.

10. Как украинские спецслужбы вербуют российских детей. — URL: https://vz.ru/news/2023/1/30/1197194.html (дата обращения: 30.03.2026).

REFERENCES

1. Prinuzhdavshie detej k podzhogam diversanty poluchili sroki ot 17 do 22 let. — URL: https://ren.tv/news/ (data obrashcheniya: 30.03.2026).

2. Abramyan S. K., Neskorodova I. S., Solov′ev V. S. Protivodejstvie vovlecheniyu molodezhi v ekstremistskuyu i terroristicheskuyu deyatel′nost′ cherez informatsionno-kommunikatsionnuyu set′ Internet : uchebnoe posobie. — Krasnodar : Krasnodarskij universitet MVD Rossii, 2022. — 60 s.

3. Artamonova E. G., Borodina A. S., Melent′eva O. S. Metodicheskie rekomendatsii dlya nesovershennoletnikh, roditelej (zakonnykh predstavitelej) nesovershennoletnikh, naglyadnye informatsionnye materialy po bezopasnomu ispol′zovaniyu seti Internet v tselyakh predotvrashcheniya prestuplenij, sovershaemykh s ee ispol′zovaniem kak samimi nesovershennoletnimi, tak i v otnoshenii nikh. — M. : Tsentr zashchity prav i interesov detej, 2021 — 35 s. // Bank dokumentov Ministerstva prosveshcheniya RF. — URL: https://docs.edu.gov.ru/document/f9f90ed22419ee2738e66ea467bf52ae/download/4403/ (data obrashcheniya: 30.03.2026).

4. Divaeva I. R., Kolesnikov R. V., Lyubimov L. V. O preduprezhdenii vovlecheniya nesovershennoletnikh v ekstremistskuyu deyatel′nost′ s ispol′zovaniem informatsionno-telekommunikatsionnykh tekhnologij // Obrazovanie i pravo. — 2024. — № 8. — S. 428—432.

5. Telefon Goryachej linii. — URL: https://telefon-doveria.ru/questions/ (data obrashcheniya: 30.03.2026).

6. Programma razvitiya dlya uchastnikov spetsial′noj voennoj operatsii realizuetsya po porucheniyu Prezidenta Rossii Vladimira Vladimirovicha Putina Vysshej shkoloj gosudarstvennogo upravleniya RANKhiGS na baze Masterskoj upravleniya «Senezh». — URL: https://vremyageroev.rf/ (data obrashcheniya: 30.03.2026).

7. Il′nitskij A. S. Protivodejstvie kriminal′noj ideologii v seti Internet : avtoref. dis. … kand. yurid. nauk / Il′nitskij Aleksandr Sergeevich. — Krasnodar, 2022. — 31 s.

8. Ignatov A. N. Sovremennye transformatsii ekstremizma i terrorizma // Aktual′nye problemy protivodejstviya ekstremizmu, rusofobii i ukrainskomu neonatsizmu : materialy vserossijskoj nauchno-prakticheskoj konferentsii, Simferopol′, 03 maya 2024 goda. — Krasnodar : Krasnodarskij universitet MVD Rossii, 2024. — S. 68—72.

9. Budanova E. A., Budanov S. A., Kushnareva A. V. Osobennosti determinatsii i preduprezhdeniya faktov vovlecheniya nesovershennoletnikh v sovershenie prestuplenij posredstvom seti Internet // Vestnik Voronezhskogo instituta MVD Rossii. — 2023. — № 4. — S. 211—218.

10. Kak ukrainskie spetssluzhby verbuyut rossijskikh detej. — URL: https://vz.ru/news/2023/1/30/1197194.html (data obrashcheniya: 30.03.2026).

СВЕДЕНИЯ ОБ АВТОРАХ

Пучнин Александр Васильевич. Начальник кафедры оперативно-разыскной деятельности. Кандидат юридических наук, доцент.
Воронежский институт МВД России.
E-mail: lex-puch@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Польшиков Александр Васильевич. Доцент кафедры уголовного права и криминологии. Кандидат юридических наук, доцент.
Воронежский институт МВД России.
E-mail: polschikow@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Демидова Оксана Васильевна. Профессор кафедры уголовно-исполнительного и уголовного права. Кандидат юридических наук, доцент.
Воронежский институт ФСИН России.
E-mail: oks-dem.78@mail.ru
Россия, 394072, Воронеж, ул. Иркутская, 1а.

Puchnin Alexander Vasilievich. Head of the chair of Operational and Investigation Activities. Candidate of Law, Associate Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: lex-puch@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Polshikov Alexander Vasilievich. Associate Professor of the chair of Criminal Law and Criminology. Candidate of Law, Associate Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: polschikow@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Demidova Oksana Vasilievna. Professor of the chair of Criminal-Executive and Criminal Law. Candidate of Law, Associate Professor.
Voronezh Institute of the Federal Penitentiary Service of Russia.
E-mail: oks-dem.78@mail.ru
Work address: Russia, 394072, Voronezh, Irkutskaya Str., 1a.

Ключевые слова: несовершеннолетние; ранняя профилактика; сетевая вербовка; противоправная деятельность; диверсии; террористические акты; цифровая безопасность; инспектор по делам несовершеннолетних, образовательные организации; межведомственное взаимодействие.

Key words: minors; early prevention; network recruitment; illegal activities; sabotage; terrorist acts; digital security; juvenile inspector; educational organizations; interagency cooperation.

УДК 343.85

М. Ю. Пучнина, *кандидат юридических наук*
У. В. Безуглая

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА СОВРЕМЕННОГО ТЕРРОРИЗМА: ВООРУЖЕННОЕ НАСИЛИЕ, СКУЛШУТИНГ, ЦИФРОВАЯ ВЕРБОВКА

CRIMINOLOGICAL CHARACTERISTICS OF MODERN TERRORISM: ARMED VIOLENCE, SCHOOL SHOOTING, DIGITAL RECRUITMENT

В статье рассматриваются современные проявления терроризма и вооруженного насилия в условиях цифровой радикализации, роста сетевой вербовки несовершеннолетних и трансформации способов совершения насильственных преступлений. Цель исследования состоит в уточнении криминологической характеристики современного терроризма через анализ его правовых признаков, статистической динамики, особенностей личности преступника, роли скулшутинга как формы подражательного и идеологически опосредованного насилия, а также цифровых механизмов вовлечения несовершеннолетних.

The article examines the current manifestations of terrorism and armed violence in the context of digital radicalization, the growth of online recruitment of minors, and the transformation of methods of committing violent crimes. The purpose of the study is to clarify the criminological characteristics of modern terrorism through an analysis of its legal features, statistical dynamics, the characteristics of the criminal's personality, the role of school shooting as a form of imitative and ideologically mediated violence, and the digital mechanisms of involving minors.

В условиях нарастающей нестабильности, цифровой радикализации и расширения форм вооруженного насилия особую актуальность приобретает криминологическое осмысление терроризма как одной из наиболее опасных угроз общественной и государственной безопасности. Противодействие насильственным преступлениям, которые совершаются с использованием огнестрельного оружия, бесспорно является одной из насущных потребностей общества. Это обусловлено тем, что такие преступления наносят непоправимый вред жизни или здоровью граждан: приводят к гибели большого количества людей, в частности публичных личностей, политиков, государственных деятелей, журналистов, бизнесменов и т. д.; устрашают население и внушают безнадежность и невозможность борьбы с вооруженными преступниками, которые поставили себя выше закона и совести [1. — С. 134].

Нашествие терроризма, ставящее под угрозу нормальное существование мироустройства, в течение последних десятилетий остается предметом интенсивного международного и национального правового осмысления [2. — С. 145]. Международное сообщество неоднократно предпринимало попытки выработать эффективные меры противодействия терроризму, однако до сих пор не выработано даже единого мирового определения понятия «терроризм». Полагаем, что последнее связано с политическими разногласиями, многогранностью феномена и стремлением государств использовать собственные трактовки в национальных интересах. Разные страны часто квалифицируют действия террористов как «повстанческие» или «национально-освободительные» движения, что затрудняет создание универсального международного правового документа [3. — С. 8].

В соответствии со ст. 3 Федерального закона от 06.03.2006 № 35-ФЗ терроризм в российском праве понимается как идеология насилия и практика воздействия на принятие решений органами власти и международными организациями, связанные с устрашением населения и иными формами противоправных насильственных действий [4].

В этих условиях особое значение приобретает не только практическая деятельность правоохранительных органов, но и теоретическая проработка вопросов, связанных с предупреждением и пресечением подобного рода преступлений, в том числе и криминологическая характеристика терроризма и вооруженного насилия [5].

Вооруженное насилие рассматривается в настоящем исследовании как одна из содержательных форм проявления терроризма, поскольку именно через применение оружия, взрывных устройств и иных средств повышенной поражающей способности наиболее наглядно реализуются его ключевые признаки — устрашение населения, причинение массового вреда и демонстративное воздействие на общество и государственные институты. При этом не всякое вооруженное насилие имеет террористическую природу, однако в случаях, когда оно совершается ради запугивания, дестабилизации общественной безопасности, идеологического давления или принуждения к принятию определенных решений, оно приобретает криминологические признаки терроризма и должно анализироваться в едином исследовательском контексте.

Ситуации, которые влияют на определение лица относительно совершения им вооруженного нападения, бывают разной продолжительности, могут отличаться по интенсивности, имеют разные источники: стихийное бедствие, военные действия, политические кризисы, финансовые нужды конкретной семьи, поведение родных, что морально травмирует или вызывает насильственные действия в отношении них, и тому подобное. Значительную роль среди ситуаций, которые могут способствовать совершению преступлений, играет поведение жертвы преступления (так называемый виктимный фактор): иногда жертва сама (сознательно или нет) провоцирует агрессию по отношению к себе. Внутренние причины и условия преступлений, совершаемых с применением оружия или предметов, используемых в качестве оружия, тесно связаны с особенностями личности преступника, наличием определенного отклонения в его поведении. С психологической точки зрения девиантное (отклоняющееся) поведение возникает там, где личностные нормы вступают в конфликт с общепринятыми социальными нормами [6]. Агрессивность рассматривается как одна из возможных стратегий человеческого поведения, и на ее проявление влияют разные черты характера, в том числе демонстративность, уровень самоконтроля, склонность к соперничеству и т. д.

Криминологический портрет террориста показывает, что большинство членов террористических групп — мужчины. Это объясняется тем, что сама по себе преступная террористическая деятельность предъявляет повышенные требования к своим субъектам — как физические (необходимость переносить лишения, скрываться, участвовать в боевых столкновениях), так и психологические (решимость применить насилие, готовность пожертвовать жизнью и т. д.). Тем не менее современная практика требует отказаться от чрезмерно упрощенного «типового портрета» террориста: судебная статистика за 2024 г. показывает, что по террористическим статьям в России были осуждены 870 человек, среди них 77 женщин и 48 несовершеннолетних; по ст. 205.2 УК РФ были осуждены 410 лиц как по основному обвинению.

В 2025 году было зарегистрировано 2241 преступлений экстремистской направленности, что на 30,4% больше, чем за аналогичный период прошлого года (1719 преступлений). Доля преступлений, совершенных с использованием сети Интернет, составляет за период 2025 года — 31% (705 преступлений), что на 63,4% больше, чем в 2024 году — 447 преступлений [7].

Следовательно, криминологически значимы не только пол и возраст, но и социальный статус, уровень включенности в цифровые коммуникации, отсутствие устойчивого дохода, образовательная траектория и стадия радикализации личности. В современных условиях формирование личности террориста все чаще происходит под воздействием гибридного комплекса факторов, в котором офлайн-среда сочетается с интенсивным цифровым влиянием, способным ускорять усвоение идеологии насилия и снижать психологические барьеры перед совершением преступления. Поэтому криминологический анализ должен быть ориентирован на выявление не только социальных, но и информационно-поведенческих маркеров радикализации, особенно у молодежи и лиц, находящихся в состоянии социальной дезадаптации.

Следует также отметить и то, что портрет террориста меняется в соответствии с современными социальными и политическими реалиями.

В качестве негативных тенденций следует отметить следующие [8. — С. 98]:

- снижение в целом возраста лиц, принимающих участие в террористической деятельности — «омоложение» терроризма;

- стирание границ и идеологии — наличие псевдорелигиозных мотивов и навязывание искаженных взглядов;

- повышение количества наемных лиц с боевым опытом;

- эмоциональная неустойчивость;

- рост числа осужденных за преступления террористического характера.

С практической точки зрения это означает необходимость раннего выявления интернет-радикализации и более адресной профилактики в отношении подростков и молодых взрослых.

Современная литература подчеркивает повышенную уязвимость подросткового возраста к радикализации, поскольку именно в этот период особенно интенсивно протекают поиск идентичности, потребность в признании и стремление к

принадлежности группе [9]. Это особенно важно для анализа скулшутинга и цифровой вербовки: в этих случаях радикализация часто развивается не в классических иерархических организациях, а в сетевых субкультурах, где сочетаются идеология насилия, меметизация[1] преступника и символическое поощрение подражания.

В условиях кризисных социальных процессов вооруженное насилие усиливается под воздействием целого комплекса факторов — личностных, групповых, ситуационных и инфраструктурных. Более корректно связывать этот блок не с единичной цифрой за 2022 год (когда с началом специальной военной операции отмечался рост преступлений, связанных с применением оружия), а с устойчиво значимой проблемой незаконного оборота оружия. В 2025 году МВД выявило более 16 тысяч преступлений, связанных с незаконным оборотом оружия, изъято около 7,5 тысяч средств вооружения, 100 тысяч боеприпасов и 150 кг взрывчатых веществ [10]. Такие данные подтверждают, что контроль за доступностью оружия и взрывчатых средств остается существенным элементом предупреждения террористических и иных насильственных преступлений.

В условиях вооруженных конфликтов и тюремной идеологизации расширяется и укрепляется субкультура преступной среды, что особо заметно в террористических организациях: вырабатываются неформальные нормы поведения, формируется особая иерархия и дифференциация ролей. Большим «авторитетом» среди террористов (как и в криминальном мире в целом) пользуются лица, прошедшие через тюрьмы и лагеря — своеобразная «преступная элита».

Устойчивая преступная группа, включая террористическую, обычно имеет четкое распределение ролей — лидеры, идеологи, финансисты, исполнители, пособники — и соблюдает внутренние «понятия», заимствованные из воровского мира. Все это затрудняет внедрение в такие группы и требует от правоохранителей специальных знаний о криминальной субкультуре.

Для успешного раскрытия и расследования преступлений необходимо производить дифференциацию ролей и отношений внутри террористических структур, знать и понимать психологические особенности каждого конкретного участника группы, а также разделяемые ими нормы поведения и жизненные ценности. Эффективное противодействие законспирированным террористическим организациям требует от субъекта расследования комплексного междисциплинарного подхода, сочетающего в том числе психологический и социологический анализ.

Современный этап развития террористической преступности показывает колоссальное влияние цифровых технологий на эволюцию терроризма. Особенно заметно воздействие информационно-телекоммуникационной сети Интернет на молодых граждан, наиболее подверженных внушению в силу неопытности и возрастного максимализма. В сети идет открытая героизация террористов, их образы романтизируются, создаются своего рода культы. Возникают целые субкультуры с собственным жаргоном, символикой (специфические жесты, аватары, мемы), где преступники преподносятся как «мстители» за унижения и призываются последователи к повторению их «подвигов» [6 — С. 40]. Например, идеология скулшутинга («колумбайна»), зародившаяся после бойни, устроенной двумя учениками старших классов 20 апреля 1999 года в школе «Колумбайн» (округ Джефферсон, штат Колорадо, США). Они убили 13 человек (12 учеников и один учитель) и ранили ещё 23 человека, после чего покончили жизнь самоубийством. С приходом онлайн-СМИ образовался фэндом (субкультура, состоящая из поклонников/фанатов) массовых убийств в образовательных учреждениях, и данный феномен получил распространение, в том числе и в России. Отмечается, что т. н. движение «колумбайнеров» представляет экстремистскую и террористическую угрозу национальной безопасности: по сути, оно насаждает культ массового убийства и может рассматриваться как разновидность терроризма, направленного против общества [11].

В России идеология «колумбайна» уже привела к нескольким трагическим инцидентам — так, самым громким актом школьного насилия стал расстрел в Керченском политехническом колледже 17 октября 2018 года, в результате которого погиб 21 человек, а свыше 60 были ранены [12]. Данное преступление стало крупнейшим массовым убийством в учебном заведении за всю историю России. К сожалению, за ним последовали и другие: волну скулшутинга продолжили трагические события в Казани (май 2021 г., нападение на гимназию, 9 убитых) и Перми (сентябрь 2021 г., стрельба в университете, 6 погибших).

Давно известна закономерность: как только случается громкое, вопиющее, необычное убийство или самоубийство, тут же начинается волна точно таких же — подражательных (т. н. эффект Вертера). Подростки наиболее подвержены влиянию, поэтому зачастую они совершают поступки,

[1] Распространение мемов — единиц культурной информации, которые передаются от одного человека к другому путем коммуникации.

аналогичные тем, о которых узнали из сети Интернет. Именно по этой причине идеология «колумбайна» так быстро набрала обороты и получила немалое количество последователей.

Российские власти отреагировали на эти вызовы комплексом мер — была ужесточена ответственность за незаконный оборот оружия и усилены требования к его продаже (в 2021 г. повышен возраст приобретения охотничьего и длинноствольного оружия с 18 до 21 года, введены более строгие наказания за переделку и сбыт оружия). Кроме того, Верховный Суд РФ 2 февраля 2022 года признал международное молодежное движение «Колумбайн» террористической организацией и запретил его деятельность на территории России [13]. Этот беспрецедентный шаг — приравнивание разрозненных интернет-сообществ поклонников «шутингов» к террористам — свидетельствует о серьезности, с которой государство восприняло новую угрозу.

Заслуживает внимания и то, что террористы активно вербуют несовершеннолетних через интернет не только для массовых убийств в школах, но и для совершения диверсий, поджогов, иных преступлений экстремистского характера и террористической направленности. Исследование показало, что в настоящее время на совершение террористических актов и диверсий юных россиян толкают не только обещаниями денег, обманом, уговорами, но и все чаще прямыми угрозами жизни и здоровью, шантажом. Механизм вовлечения российских подростков в террористическую деятельность через онлайн-игры довольно прост [14. — С. 203]. Указанные обстоятельства свидетельствуют о трансформации способов террористической вербовки, при которой цифровая среда используется не только как канал коммуникации, но и как инструмент психологического воздействия, постепенного вовлечения и дистанционного контроля за поведением несовершеннолетних. Эта оценка подтверждается актуальными правоохранительными данными: в 2025 году за диверсии и поджоги на объектах транспорта задержано более 300 человек, причем более 150 из них были несовершеннолетними; в марте 2026 года начальник ГУТ МВД России отметил, что примерно 99% выявленных лиц были завербованы через социальные сети [15]. Особую опасность представляет то, что объектами вербовки становятся не только социально неблагополучные подростки, но и несовершеннолетние из внешне благополучной среды, обладающие устойчивым доступом к цифровым платформам и не находящиеся под должным вниманием взрослых [16]. Главное — работа сетевых кураторов из-за рубежа ведется по всем направлениям, основная задача — вовлечь как можно больше российских детей и подростков, которыми в силу возрастных, психофизиологических и иных личностных особенностей сравнительно легко и максимально безопасно можно манипулировать на расстоянии для совершения абсолютно любого преступления в ущерб безопасности государства.

В 2022—2023 гг. в российских регионах были выявлены первые случаи вовлечения несовершеннолетних через цифровые каналы связи в подготовку диверсий, поджогов и иных преступлений террористической направленности. Указанная тенденция обусловила как совершенствование уголовно-правовых средств противодействия, выразившееся в снижении возраста уголовной ответственности за диверсионные преступления, усилении санкций за вовлечение несовершеннолетних в террористическую и диверсионную деятельность, так и активизацию криминологических мер предупреждения, включая профилактическую работу с молодежью, информационно-разъяснительные мероприятия и усиление мониторинга социальных сетей. Отметим, что несмотря на принимаемые меры, в 2025 году в России кратно возросло число подростков, вовлеченных в преступления террористической направленности, которые приобретают все более агрессивные формы (поджоги, порча и уничтожение военного имущества, объектов транспортной инфраструктуры) [17]. В этих условиях деятельность государства, направленная на снижение уровня вовлечения несовершеннолетних в террористическую и экстремистскую деятельность, приобретает системный и превентивный характер. Одним из значимых направлений такой политики выступает ограничение доступа к цифровым коммуникационным платформам, используемым для анонимной вербовки, координации противоправных действий и распространения деструктивного контента. В данном контексте блокирование отдельных мессенджеров и сетевых сервисов следует рассматривать прежде всего как меру обеспечения информационной безопасности, ориентированную на защиту несовершеннолетних от криминогенного и радикализирующего воздействия. Соответственно, развитие и использование отечественных цифровых платформ, находящихся в национальной юрисдикции и подлежащих более эффективному правовому и технологическому контролю, может рассматриваться как один из инструментов минимизации рисков вовлечения молодежи в преступления террористической направленности.

Рост масштабов цифровой вербовки несовершеннолетних и усложнение способов их вовлече-

ния в преступления террористической направленности закономерно ставят вопрос об эффективности деятельности правоохранительных органов по своевременному выявлению, пресечению и предупреждению подобных угроз, которая складывается из противоречивых факторов. С одной стороны, цель — оперативно восстановить порядок и защитить общество от насилия, с другой — важно соблюдать принципы пропорциональности, не допуская чрезмерного применения силы и массового нарушения прав человека. Особенно важно, чтобы силовое реагирование сопровождалось последующим криминологическим анализом причин и условий конкретного инцидента, поскольку без этого невозможно перейти от разового пресечения к системному предупреждению повторных атак. Практика показывает, что результативность противодействия определяется не только быстротой нейтрализации непосредственной угрозы, но и качеством межведомственного взаимодействия, своевременностью обмена информацией и способностью выявлять признаки радикализации на ранней стадии. В 2025 году Национальный антитеррористический комитет сообщил о предотвращении 374 террористических преступлений, в том числе 273 терактов, а также об удалении из сети более 37 тыс. материалов террористического содержания [18].

Существенное значение имеет и соблюдение баланса между мерами безопасности и гарантиями прав граждан в цифровой среде, где профилактика не должна подменяться произвольным ограничением законной активности. Следовательно, оценка деятельности правоохранительных органов должна строиться по совокупности критериев: предотвращение теракта, минимизация вреда, законность примененных мер и эффективность последующей профилактической работы.

Таким образом, современный терроризм представляет собой сложный криминологический феномен, в котором традиционные формы вооруженного насилия сочетаются с цифровыми механизмами радикализации, вербовки и координации преступной деятельности. Его развитие обусловлено совокупностью кризисных социальных факторов, проблемами контроля за оборотом оружия, влиянием криминальной субкультуры и деструктивного интернет-контента, а особую опасность представляет вовлечение в такую деятельность несовершеннолетних [19]. Для российского контекста 2024—2026 гг. характерны: статистический рост террористических и экстремистских составов, усиление интернет-компонента, институциональное признание идеологии «колумбайна» террористической угрозой, а также увеличение случаев вовлечения несовершеннолетних в диверсионно-террористические практики. В этих условиях эффективное противодействие терроризму возможно лишь при сочетании уголовно-правовых, оперативно-розыскных, информационно-профилактических и криминологических мер, направленных на раннее выявление радикализации, защиту молодежи в цифровой среде и предупреждение вооруженных нападений.

ЛИТЕРАТУРА

1. Безлюдная Д. Ю. Обеспечение антитеррористической безопасности подразделениями ОВД на современном этапе // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений. — Воронеж, 2025. — С. 134—137.

2. Шагланов А. Н. Терроризм и экстремизм в условиях глобализации // Законность и правопорядок в современном обществе. — 2014. — № 19. — С. 145—150.

3. Остроухов В. В. Актуальные вопросы борьбы с международным терроризмом на современном этапе // Право и безопасность. — 2003. — № 3-4. — С. 8—9.

4. О противодействии терроризму : Федеральный закон от 06.03.2006 № 35-ФЗ // СПС «КонсультантПлюс».

5. Башлуева Н. Н., Карташов И. А. Терроризм как одна из главных угроз национальной безопасности // Лоббирование в законодательстве. — 2024. — Т. 3. — № 2. — С. 63— 66.

6. Пучнин А. В., Пучнина М. Ю. Тенденции и факторы вовлечения несовершеннолетних в совершение преступлений террористического характера и экстремистской направленности // Вестник Краснодарского университета МВД России. — 2024. — № 2(64). — С. 13—18.

7. Состояние преступности в Российской Федерации за январь—декабрь 2025 года. — URL: https://media.mvd.ru/files/application/16902466 (дата обращения: 16.04.2026).

8. Зарина А. М. Портрет современного террориста: криминологический аспект // Евразийская адвокатура. — 2024. — № 3(68). — С. 96—99.

9. Колесников Р. В. Зарубежный опыт профилактики преступности несовершеннолетних // Вестник Воронежского института ФСИН России. — 2020. — № 4 — С. 143—150.

10. МВД выявило более 16 тысяч фактов незаконного оборота оружия в 2024 году. — URL: https://tass.ru/proisshestviya/23315391?utm_source=chatgpt.com (дата обращения: 16.04.2026).

11. Ежегодный доклад Уполномоченного по правам ребенка в Пермском крае «О соблюдении и защите прав и законных интересов ребенка и деятельности уполномоченного по правам ребенка в Пермском крае в 2024 году». — URL: http://ivo.garant.ru/#/document/412307562 (дата обращения: 16.04.2026).

12. Пименов Н. А., Пименов Н. Н. Социальные вызовы современности в общем контексте безопасности личности, общества и государства : монография. — М. : Русайнс, 2020. — 212 с.

13. Верховный Суд признал «Колумбайн» террористическим движением. — URL: https://www.rbc.ru/society/02/02/2022/61fa80e89a7947fc73792fb5 (дата обращения: 16.04.2026).

14. Польшиков А. В., Демидова О. В., Кулешов А. А. Основные проблемы предупреждения террористических актов и диверсий, совершаемых несовершеннолетними и при их соучастии // Вестник Воронежского института ФСИН России. — 2025. — № 1 — С. 195—206.

15. В России за год задержали более 300 человек за диверсии на объектах транспорта. — URL: https://squarenews.ru/news/v-strane/ (дата обращения: 16.04.2026).

16. Колесников Р. В. Противодействие вербовочной деятельности экстремистских и террористических организаций в сети Интернет в контексте обеспечения информационно-психологической безопасности несовершеннолетних // Ученые записки Казанского юридического института МВД России. — 2023. — Т. 8. — № 1(15). — С. 36—41.

17. Число вовлеченных в терроризм подростков кратно возросло, заявил Гуцан. — URL: https://ria.ru/20260319/gutsan-2081749617.html (дата обращения: 26.03.2026).

18. НАК сообщил о предотвращении 273 терактов с начала года в РФ. — URL: https://interfax.ru](https://www.interfax.ru/russia/1062183?utm_source=chatgpt.com (дата обращения: 26.03.2026).

19. Пучнина М. Ю., Пучнин А. В. Факторы, способствующие вовлечению несовершеннолетних в совершение преступлений экстремистской направленности и террористического характера // Вестник Воронежского института МВД России. — 2024. — № 2. — С. 250—255.

REFERENCES

1. Bezlyudnaya D. Yu. Obespechenie antiterroristicheskoj bezopasnosti podrazdeleniyami OVD na sovremennom etape // Prestupnostʹ v SNG: problemy preduprezhdeniya i raskrytiya prestuplenij. — Voronezh, 2025. — S. 134—137.

2. Shaglanov A. N. Terrorizm i ekstremizm v usloviyakh globalizatsii // Zakonnostʹ i pravoporyadok v sovremennom obshchestve. — 2014. — № 19. — S. 145—150.

3. Ostroukhov V. V. Aktualʹnye voprosy borʹby s mezhdunarodnym terrorizmom na sovremennom etape // Pravo i bezopasnostʹ. — 2003. — № 3-4. — S. 8—9.

4. O protivodejstvii terrorizmu : Federalʹnyj zakon ot 06.03.2006 № 35-FZ // SPS «KonsulʹtantPlyus».

5. Bashlueva N. N., Kartashov I. A. Terrorizm kak odna iz glavnykh ugroz natsionalʹnoj bezopasnosti // Lobbirovanie v zakonodatelʹstve. — 2024. — T. 3. — № 2. — S. 63— 66.

6. Puchnin A. V., Puchnina M. Yu. Tendentsii i faktory vovlecheniya nesovershennoletnikh v sovershenie prestuplenij terroristicheskogo kharaktera i ekstremistskoj napravlennosti // Vestnik Krasnodarskogo universiteta MVD Rossii. — 2024. — № 2(64). — S. 13—18.

7. Sostoyanie prestupnosti v Rossijskoj Federatsii za yanvarʹ—dekabrʹ 2025 goda. — URL: https://media.mvd.ru/files/application/16902466 (data obrashcheniya: 16.04.2026).

8. Zarina A. M. Portret sovremennogo terrorista: kriminologicheskij aspekt // Evrazijskaya advokatura. — 2024. — № 3(68). — S. 96—99.

9. Kolesnikov R. V. Zarubezhnyj opyt profilaktiki prestupnosti nesovershennoletnikh // Vestnik Voronezhskogo instituta FSIN Rossii. — 2020. — № 4 — S. 143—150.

10. MVD vyyavilo bolee 16 tysyach faktov nezakonnogo oborota oruzhiya v 2024 godu. — URL: https://tass.ru/proisshestviya/23315391?utm_source=chatgpt.com (data obrashcheniya: 16.04.2026).

11. Ezhegodnyj doklad Upolnomochennogo po pravam rebenka v Permskom krae «O soblyudenii i zashchite prav i zakonnykh interesov rebenka i deyatelʹnosti upolnomochennogo po pravam rebenka v Permskom krae v 2024 godu». — URL: http://ivo.garant.ru/#/document/412307562 (data obrashcheniya: 16.04.2026).

12. Pimenov N. A., Pimenov N. N. Sotsialʹnye vyzovy sovremennosti v obshchem kontekste bezopasnosti lichnosti, obshchestva i gosudarstva : monografiya. — M. : Rusajns, 2020. — 212 s.

13. Verkhovnyj Sud priznal «Kolumbajn» terroristicheskim dvizheniem. — URL: https://www.rbc.ru/society/02/02/2022/61fa80e89a7947fc73792fb5 (data obrashcheniya: 16.04.2026).

14. Pol′shikov A. V., Demidova O. V., Kuleshov A. A. Osnovnye problemy preduprezhdeniya terroristicheskikh aktov i diversij, sovershaemykh nesovershennoletnimi i pri ikh souchastii // Vestnik Voronezhskogo instituta FSIN Rossii. — 2025. — № 1 — S. 195—206.

15. V Rossii za god zaderzhali bolee 300 chelovek za diversii na ob″ektakh transporta. — URL: https://squarenews.ru/news/v-strane/ (data obrashcheniya: 16.04.2026).

16. Kolesnikov R. V. Protivodejstvie verbovochnoj deyatel′nosti ekstremistskikh i terroristicheskikh organizatsij v seti Internet v kontekste obespecheniya informatsionno-psikhologicheskoj bezopasnosti nesovershennoletnikh // Uchenye zapiski Kazanskogo yuridicheskogo instituta MVD Rossii. — 2023. — T. 8. — № 1(15). — S. 36—41.

17. Chislo vovlechennykh v terrorizm podrostkov kratno vozroslo, zayavil Gutsan. — URL: https://ria.ru/20260319/gutsan-2081749617.html (data obrashcheniya: 26.03.2026).

18. NAK soobshchil o predotvrashchenii 273 teraktov s nachala goda v RF. — URL: https://interfax.ru](https://www.interfax.ru/russia/1062183?utm_source=chatgpt.com (data obrashcheniya: 26.03.2026).

19. Puchnina M. Yu., Puchnin A. V. Faktory, sposobstvuyushchie vovlecheniyu nesovershennoletnikh v sovershenie prestuplenij ekstremistskoj napravlennosti i terroristicheskogo kharaktera // Vestnik Voronezhskogo instituta MVD Rossii. — 2024. — № 2. — S. 250—255.

СВЕДЕНИЯ ОБ АВТОРАХ

Пучнина Маргарита Юрьевна. Старший преподаватель кафедры уголовного права и криминологии. Кандидат юридических наук.
Воронежский институт МВД России.
E-mail: masloy100@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Безуглая Ульяна Владимировна. Курсант.
Воронежский институт МВД России.
E-mail: ulyanabezuglaya@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Puchnina Margarita Yuryevna. Senior lecturer of the chair of Criminal Law and Criminology. Candidate of Law.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: masloy100@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Bezuglaya Ulyana Vladimirovna. Cadet.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: ulyanabezuglaya@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: терроризм; вооруженное насилие; цифровая радикализация; криминологическая характеристика; скулшутинг; несовершеннолетние; интернет-вербовка; предупреждение преступности; национальная безопасность.

Key words: terrorism; armed violence; digital radicalization; criminological characteristics; school shooting; minors; online recruitment; crime prevention; national security.

УДК 343.85

И. В. Азарова

КРИМИНОЛОГИЧЕСКИЙ ПОРТРЕТ ЛИЦА, СОВЕРШИВШЕГО МОШЕННИЧЕСТВО ПРИ ПОЛУЧЕНИИ ВЫПЛАТ

CRIMINOLOGICAL PORTRAIT OF A PERSON WHO COMMITTED FRAUDULENT ACTS IN ORDER TO RECEIVE PAYMENTS

В статье проводится комплексное криминологическое исследование личности преступника, совершающего мошенничество при получении социальных выплат (ст. 159^2 УК РФ). Актуальность темы обусловлена значительным ущербом, причиняемым данными преступлениями бюджетной системе, и необходимостью разработки адресных мер предупреждения. В работе автором сформирован обобщенный портрет мошенника при получении выплат на основе анализа статистических данных МВД России и судебной практики за период 2012—2024 гг., а также материалов уголовных дел. Особое внимание уделено нравственно-психологическим особенностям, включающим внешнюю социальную адаптацию, доминирование материальных ценностей, расчетливость и способность к длительному планированию противоправных действий.

The article provides a comprehensive criminological study of the personality of a criminal who commits fraud in obtaining social benefits (Article 159^2 of the Criminal Code of the Russian Federation). The relevance of the topic is due to the significant damage caused by these crimes to the budget system and the need to develop targeted prevention measures. The author has created a generalized portrait of a fraudster who receives benefits based on an analysis of statistical data from the Ministry of Internal Affairs and judicial practice for the period 2012—2024, as well as criminal case materials. Special attention is paid to moral and psychological characteristics, including external social adaptation, the dominance of material values, prudence, and the ability to plan illegal actions for a long time.

В криминологии исследование личности преступника занимает центральное место, выступая необходимым связующим звеном между анализом причин преступности и разработкой мер по ее предупреждению. По сути, невозможно эффективно противодействовать противоправным деяниям, не понимая, кто их совершает, под влиянием каких факторов формируется готовность к преступному поведению и какие специфические черты характеризуют нарушителя закона. Этот подход является фундаментальным, поскольку переносит фокус с абстрактного «преступления» на конкретного «преступника», рассматривая его не как изолированный феномен, а как продукт сложного взаимодействия социальной среды, индивидуальных особенностей и конкретной жизненной ситуации.

Таким образом, значение криминологического исследования личности трудно переоценить. Оно служит основой для дифференциации и индивидуализации как уголовной политики в целом, так и конкретных профилактических усилий. Изучая устойчивые сочетания свойств и характеристик, присущих определённым категориям правонарушителей, наука формирует теоретическую базу для прогнозирования поведения, выявления групп риска и адресного вмешательства.

Изучение личности преступника позволяет более эффективно предупреждать любое преступление, в том числе и мошенничество при получении выплат. Важно понимать, что основной задачей профилактики является в первую очередь изменение у людей вредных установок, которые толкают на преступление, а также разъяснение и правильная интерпретация норм права, как следствие — формирование положительного правосознания. Непосредственный инструментарий предупредительной работы определяется в зависимости от характеристик личности и видов противоправного поведения, запрещенного уголовным законом. Некоторые ученые изучение личности преступника связывают с исследованием ее структуры, рассматривая ее как комплекс социально-типологических, социально-ролевых и нравственно-психологических ее характеристик [1—3]. Другие ученые придерживаются схожей, в целом, структуры. Л. С. Кузина предлагает изучать личность преступника путем проведения анализа ее социально-демографических, правовых и нравственно-психологические признаков [4].

Под личностью преступника А. Б. Марданов предлагает понимать целостную систему социальных и психиатрических черт, свойств и качеств участника и носителя общественных отношений. Структурно личность преступника ученый предлагает рассматривать как совокупность трех основных компонентов:

- социальный статус личности — принадлежность лица к определенному социальному слою, социальной группе, включая его социально-демографические характеристики;

- социальные роли, то есть набор функций, которые личность исполняет в обществе;

- нравственно-психологические характеристики человека [5].

В криминологической науке в общем понимании личность преступника представляет собой совокупность свойств и качеств, которые при определенных ситуативных обстоятельствах приводят к совершению преступления.

Под личностью преступника в криминологии понимается системное единство объективных и субъективных качеств индивида, включающее его социально-демографический статус, социально-психологические черты, нравственные ориентиры и правовые представления. Именно эта совокупность свойств и внутренних взаимосвязей не только описывает правонарушителя, но и служит причинным фактором, определяющим выбор им преступной модели поведения.

Исследовав различные подходы относительно восприятия понятия «личность преступника», представляется возможным констатировать, что преступная личность отличается от правосознательной личности антиобщественными установками, отрицательным отношением к общественным интересам, выбранными средствами достижения целей и средствами взаимодействия с обществом.

При формировании портрета личности преступника, совершающего незаконное получение социальных выплат, следует выделять следующие группы свойств:

1) социально-демографические;

2) уголовно-правовые;

3) нравственно-психологические.

К социально-демографическим признакам в криминологии принято относить пол, возраст, гражданство, образование, социальное положение, профессиональную принадлежность, наличие судимости, место проживания и др.

Под уголовно-правовыми признаками личности преступника среди ученых устоялось мнение понимать квалификацию совершенного преступления, степень его тяжести, форму вины, одиночный или групповой характер преступления, роль в его совершении, форму множественности и т. д.

К нравственно-психологическим особенностям принято относить интеллект, волевые и эмоциональные свойства, потребности и интересы, мотивацию, установки, ценностные ориентации и взгляды, способности, навыки, привычки, а также наличие психических расстройств [6].

В рамках проводимого исследования стоит отметить, что за исследуемый период было выявлено 78 826 лиц, совершивших мошенничество при получении выплат. Так, в 2012 году было выявлено 162 мошенника (отметим, что уголовная ответственность за данное деяние была введена Федеральным законом РФ почти в конце календарного года (29.11.2012) [7]), в 2013 г. — 6012 мошенника при получении выплат, в 2014 г. — 6988; в 2015 г. — 6851; в 2016 г. — 5788; в 2017 г. — 6205; в 2018 г. — 5029; в 2019 г. — 7085; в 2020 г. — 7441; в 2021 г. — 9580; в 2022 г. — 5666; в 2023 г. — 5400; в 2024 г. — 6419 [8].

Рассмотрение социально-демографического портрета лица, совершившего мошенничество при получении выплат, логично начать с такого признака, как пол. Анализ статистических данных выявил, что в абсолютном большинстве случаев (56%) мошенничество при получении выплат, предусмотренное ст. 159^2 Уголовного кодекса Российской Федерации (далее — УК РФ) [9] совершают женщины. В общей структуре преступности количество лиц женского пола традиционно остается невысоким и, как правило, не превышает 15% от общего числа правонарушителей. На протяжении истории разделение социальных ролей по признаку пола определялось комплексом традиционных и семейных факторов, которые с детства формировали поведенческие стереотипы и очерчивали пределы допустимого поведения для каждого пола [10]. В контексте нашего исследования ключевым оказывается иной, прагматический фактор. Так, значительное преобладание женщин среди осуждённых по ст. 159^2 УК РФ обусловлено спецификой предмета преступления — социальных выплат. Поскольку такие выплаты (например, по беременности и родам, ежемесячное пособие по уходу за ребенком) в основном предназначены женщинам, именно они составляют основной круг их законных получателей, а следовательно, и потенциальных нарушителей. Исследование показывает, что мужчины, составляющие 46% осужденных по ст. 159^2 УК РФ, чаще совершают его в отношении специфических видов выплат: пенсий, компенсаций и субсидий, и в большинстве случаев свои поступки они совершают под влиянием женщины.

Обратим внимание, что основополагающим фактором, детерминирующим становление личности на разных этапах ее развития, выступают возрастные особенности индивида. Возрастная

стадия непосредственно обуславливает физическое и психическое состояние человека, характер поведенческих паттернов, спектр интересов и форм досуга, возможности получения образования, перспективы профессиональной реализации на высокооплачиваемых позициях, а также создание семьи и достижение материальной стабильности. В рамках криминологической науки возрастной критерий служит одним из базовых оснований для анализа криминальной активности различных социально-демографических групп и специфики их противоправного поведения. Изучение возрастных особенностей поведения в преступной среде имеет существенное значение для разработки и реализации эффективных мер профилактического воздействия среди населения.

Согласно данным уголовной статистики исследуемых преступлений (ст. 159^2 УК РФ), основной процент мошенничеств при получении выплат приходится на граждан в возрасте от 30 до 49 лет. На эту группу приходится более половины всех зафиксированных случаев — около 52%. Доля остальных возрастных категорий постепенно снижается: лица старше 50 лет — 21%, в возрасте 18—24 лет — 14%, возрастная группа 25—29 лет — 12%, несовершеннолетние 16—17 лет — менее 1%. Такое распределение связано с особенностями самого преступления. Поскольку речь идёт о преднамеренном обмане, часто требующем подготовки документов или использования специальных знаний, преступнику необходимы определённые навыки, жизненный и профессиональный опыт. Это объясняет, почему подобные схемы редко реализуются несовершеннолетними — их участие в таких деяниях, согласно статистике, носит единичный характер и не связано с системным вовлечением в мошеннические операции.

Способствуют повышенной криминальной активности в указанном возрасте и растущие потребности, которые в свою очередь провоцируют нехватку денежных средств. Такого рода нехватка в дуэте с отсутствием финансовой поддержки, экономической стабильности в стране подталкивают данную категорию лиц к поиску дополнительных источников дохода. Также стоит отметить, что социальные изменения, происходящие с личностью, связанные с возрастом, позволяют ей выбирать наиболее рациональные способы разрешения финансовых проблем, в том числе и с помощью совершения преступления [11].

С учетом выявленных гендерных особенностей личности преступника, совершившего мошенничество при получении выплат, стоит вспомнить высказывание Ю. М. Антоняна, который отмечает, что именно в этом возрасте наблюдается высокая социальная активность со стороны женщин [6].

Специфика механизма совершения мошенничества с выплатами детерминирует и образовательный уровень потенциального преступника. Проведенное исследование позволило выявить тот факт, что более половины правонарушителей обладали высшим (26%) или средним профессиональным (34%) образованием. Вместе с тем значительная доля — 40% — имели уровень образования не выше среднего общего. Согласно нашей гипотезе, данный образовательный статус мог выступать одним из факторов, способствовавших выбору криминальной стратегии поведения, что обусловлено ограниченностью легальных возможностей для достижения материального благополучия, а в ряде случаев — антисоциальным образом жизни, включая злоупотребление алкоголем. Структура этой группы по уровням образования распределяется следующим образом: основное общее образование имели 9% лиц, среднее общее — 28%. Минимальная доля (3%) приходится на лиц, не имеющих какого-либо образования.

Представляется, что показатель уровня образования может служить основанием для условной дифференциации правонарушителей. С одной стороны, существуют рядовые исполнители — лица, формально соответствующие законодательным критериям для назначения выплат. С другой — организаторы и инициаторы, которые благодаря своему образованию, профессиональным компетенциям и жизненному опыту способны вовлекать первых в противоправную деятельность, выступая в роли подстрекателей или пособников. Выполнение такой организующей роли объективно предполагает наличие у индивида достаточно высокого уровня образования и специальных познаний. Образование способствует определенному уровню развития личности, осмыслению цели, задачи, формированию и выбору оптимального пути и объема средств совершения противоправного деяния.

Одним из социально-демографических признаков является семейное положение преступника. По данным изучения 206 уголовных дел, возбужденных по признакам преступления, предусмотренного ст. 159^2 УК РФ, 59% преступников на момент совершения преступления состояли в браке. Большинство преступников (81%) имели детей (одного — 25%, двоих — 35%, трех и более — 40%). В свою очередь, наличие детей обуславливает повышенные финансовых трат, а следовательно, и существование затруднений экономического характера у потенциального преступника.

Обратим внимание, что для участия в совершении мошенничества при получении выплат необходимо занимать высокое служебное положение, а также обладать определенным уровнем образования как обязательным квалификационным условием для его занятия. Особенно это актуально для органов государственной власти, где существуют квалификационные требования для замещения должностей гражданской службы [12].

Анализируя трудовую занятость лиц, привлеченных к ответственности, важно отметить, что характер данного правонарушения предопределил специфику их социального статуса. Согласно статистике, чуть более половины (51%) не имели постоянного легального заработка на момент совершения деяния. Среди трудозанятых, составляющих 48%, наибольшую долю занимали наемные работники (33%), за которыми следовали служащие (8%), индивидуальные предприниматели (5%), сотрудники государственных органов (1%) и работники агропромышленного сектора (1%). Доля учащихся и студентов в общей структуре была минимальной, не превышая 1%. Что касается таких признаков, как гражданство и связь места жительства с местом совершения преступления, статистические данные указывают на явное преобладание граждан Российской Федерации, чья доля достигала 91% в исследуемый период.

Ко второй группе признаков личности преступника относятся уголовно-правовые. К ним принято относить сведения об устойчивости преступной направленности личности. Такого рода сведения связаны с категорией тяжести содеянного, наличием или отсутствием соучастия, судимости, рецидива.

Данные судебной статистика за период с 2012 по 2024 год позволяют констатировать, что наиболее часто в исследуемом периоде осуждались лица за совершение преступления, предусмотренного ч. 3 ст. 159^2 УК РФ, т. е. за совершение преступления с использованием своего служебного положения или в крупном размере.

О повышенной степени опасности свидетельствует и оценка содеянного со стороны законодателя в призме категории преступления и санкции за его совершение. В исследуемом периоде чаще осуждались лица (60%), совершившие мошенничество при получении выплат, отнесенное к категории тяжких преступлений. Почти в половину меньше (36%) было осужденных за совершение анализируемого вида мошенничества, отнесенного к преступлениям небольшой тяжести. И только 4% осужденных совершили преступление, отнесенное к категории средней тяжести. Проведенные данные свидетельствуют о том, что преступников не останавливает достаточно суровый репрессивный характер санкций, они надеются быть неразоблаченными. А сам размер выплаты только стимулирует их на принятие решения о выборе криминальной линии поведения для разрешения каких-либо затруднений финансового характера.

Анализ данных уголовной статистики позволяет сделать следующие выводы относительно соучастия в мошенничествах, связанных с получением выплат. Подавляющее большинство выявленных преступников (87%) действовали в одиночку, тогда как лишь 13% совершили преступления в соучастии. При этом наиболее распространённой формой групповой преступной деятельности являлась группа лиц по предварительному сговору (12% от общего числа преступников), в то время как совершение мошенничества в составе организованной группы зафиксировано лишь у 1% правонарушителей. Относительно низкие показатели рецидивной преступности, по нашему мнению, связаны со спецификой данного противоправного деяния, включая сферу его совершения, социально-демографический профиль типичного преступника, а также особенности механизма получения выплат и реализации преступного умысла.

Далее предлагаем перейти к рассмотрению нравственно психологических особенностей личности преступника, совершившего мошенничество при получении выплат. Изучение различных точек зрения ученых в области криминологии и материалов уголовных дел позволило выделить некоторые его специфические черты.

Проведенный анализ материалов уголовных дел свидетельствует о в целом законопослушном характере социального поведения исследуемой категории лиц до момента совершения преступления. С места жительства 62% обвиняемых были охарактеризованы положительно, в то время как отрицательные характеристики были зафиксированы лишь в 9% случаев. Аналогичная тенденция доминирования положительных оценок (76%) наблюдалась и в производственных характеристиках с места работы; при этом все фигуранты исследований характеризовались исключительно положительно или удовлетворительно. Возникающие криминогенные ситуации носят разнородный характер — от семейно-бытовых до хозяйственно-производственных обстоятельств. Для личности данного типа характерна выраженная иерархия ценностей с доминированием материальных благ над духовными, где четко проявляется утилитарно-потребительская направленность мотивационной сферы.

В подтверждение высказанного хотелось бы отметить, что на совершение преступления изучаемая личность шла осознанно, четко понимая, что совершает противоправное, незаконное деяние, и

осознавая, что в случае разоблачения будет привлечена к уголовной ответственности. Не осознавать противоправность своего деяния преступник не может в силу существующего алгоритма получения выплат, в котором четко прописаны условия для их получения, которые необходимо обязательно соблюдать.

Изучаемый преступник обладает выдержкой, самообладанием, расчетлив, при этом способен переступить через многие моральные принципы.

В качестве подтверждения высказанной точки зрения приведем примеры из судебно-следственной практики.

О самообладании изучаемой личности и способности не считаться с моральными принципами может свидетельствовать приговор Мценского районного суда (Орловская область) в отношении ФИО1, которая, действуя из корыстных побуждений, умышленно сообщила заведомо ложные и недостоверные сведения, указав, что ее скончавшийся отец является отцом ее детей. На основании представленных заведомо ложных и недостоверных сведений ФИО1 была назначена социальная пенсия по случаю потери кормильца с федеральной социальной доплатой и единовременной денежной выплатой, при этом ФИО1 достоверно знала, что социальная пенсия по случаю потери кормильца ей на ее несовершеннолетних детей не положена. ФИО1 путем обмана совершила хищение денежных средств в виде федеральной социальной доплаты и единовременной денежной выплаты на ее несовершеннолетних детей, перечисленных из федерального бюджета в сумме 868 769 рублей 87 копеек [13].

Следует отметить, что виновное лицо осуществляло свои противоправные действия систематически, на протяжении продолжительного периода скрывая обстоятельства, лишавшие его законных оснований для получения средств. Такое поведение, мотивированное корыстным интересом к регулярному незаконному обогащению, свидетельствует о выраженной способности к длительному планированию, внутренней дисциплине и сознательному контролю над своими действиями.

Изучение личности преступника, выделение ее характерных особенностей позволяет разработать типологию личности конкретного преступника.

Следует подчеркнуть, что понимание типологии личности преступника должно способствовать выработке эффективных мер борьбы с преступностью и, конечно же, разработке программ исправления и реабилитации преступников.

Личность преступника — проблема междисциплинарная, в ходе разработки типологии лиц, совершивших преступления, можно использовать различные основания и критерии [14].

Существует типологизация, например, по объекту посягательства, форме вины либо по степени общественной опасности личности преступника [15].

В первом случае ученые традиционно выделяют насильственный, корыстный и корыстно-насильственный типы преступников. Первые более импульсивны, явно пренебрежительно относятся к социальным нормам, агрессивны, обладают низким интеллектом и контролем собственной воли, постоянно демонстрируют враждебность к окружающему миру.

Вторые полностью социально адаптированы, менее импульсивны. Отличаются гибкостью линии поведения в соответствии с происходящим вокруг. Предрасположены к общению и налаживанию межличностных контактов. Менее агрессивны, умеют контролировать свое поведение.

Для третьего типа преступников характерно применение насилия для удовлетворения своих материальных потребностей. Им свойственны замкнутость, неконтактность, в какой-то степени агрессивность, неудовлетворенность своим положением в обществе.

Типология преступников, базирующаяся на форме вины, предполагает существование двух типов преступников: умышленных и неосторожных.

Умышленные преступники обладают импульсивностью, агрессивностью, преобладающе придерживаются асоциальной манеры поведения, характеризуются гиперчувствительностью, склонны во всем происходящем, в том числе и в своих личных неприятностях, винить окружающих.

Типология личности преступника, в качестве критерия берущая степень общественной опасности личности, выделяет следующие типы:

- случайный (с общей положительной направленностью);
- неустойчивый;
- злостный (с антиобщественной направленностью);
- особо злостный (с установкой на преступную деятельность).

Проведенное исследование позволило выделить по степени общественной опасности следующие типы личности мошенника при получении выплат: неустойчивый; злостный (с антиобщественной направленностью); особо злостный (с установкой на преступную деятельность).

Случайного типа преступника при совершении мошенничества при получении выплат, по нашему мнению, существовать не может, т. к. сам

механизм совершения преступления предусматривает осознание виновным своей противоправной деятельности, определенную предварительную подготовку к ее реализации в форме сбора необходимых документов, справок для получения выплаты и продолжительный период проверки представленных им сведений компетентными органами, принимающими решение об осуществлении выплаты. Мошенничество при получении выплаты не относится к скоротечным преступлениям, во многих случаях является продолжаемым преступлением, выплаты виновным получаются не однократно, а на протяжении определенного периода времени.

В качестве примера последнего можно привести приговор Хивского районного суда Республики Дагестан в отношении ФИО3, признанного виновным в совершении мошенничества при получении выплат в крупном размере. ФИО3 в декабре 2013 года не представил сведения в органы регистрации актов гражданского состояния администрации о факте смерти своего отца ФИО1 и, имея в пользовании банковскую карту ОАО «Россельхозбанк» с лицевым счетом 40817-№, открытую на имя ФИО1, путем обналичивания в банкоматах ОАО «Россельхозбанк» в период времени с января 2014 года по декабрь 2015 года осуществил хищение денежных средств, поступавших из Управления Пенсионного фонда РФ по Республике Дагестан на сумму 466902,76 руб., тем самым причинив Управлению Пенсионного фонда РФ по Республике Дагестан материальный ущерб в крупном размере [16].

К неустойчивому типу преступников, совершивших мошенничество при получении выплат, на основании проведенного анализа уголовных дел и опроса практических сотрудников МВД России необходимо относить лиц, которые при стечении определенных обстоятельствах допускают возможным выбор криминальной, преступной линии поведения. Изучение материалов уголовных дел позволило определить их долю среди остальных мошенников при получении выплат, которая составила 55%.

Основным обстоятельством выступает сам факт возможного претендования на выплату в силу пола, возраста, медицинского состояния, необходимости ухода за больными.

Этот тип преступников и ранее позволял себе для достижения личных целей или разрешения проблем либо из сострадания незначительное отступление от закона.

Проведенное исследование позволило среди мошенников при получении выплат *неустойчивого типа* (55%) выделить следующие подтипы:

- семейно-позитивный подтип, преступник данного типа совершает противоправное деяние для целей позитивного характера, например улучшить свое жилищное положение, расширив жилплощадь или приобретя дом (4%);

- семейно-негативный подтип, преступники данного типа совершают преступления для получения материальной выгоды, которая в дальнейшем идет на приобретение алкоголя, наркотиков (51%).

Следующим типом, выделенным в ходе исследования, является *злостный* (с антиобщественной направленностью). К таким мошенникам при получении выплат следует относить тех, которые совершают преступления с использованием своего служебного положения. Сами по себе они не могут претендовать на получение выплат, но, используя свое положение, как коррупционеры, способствуют на различных этапах получению выплаты. Их доля среди мошенников при получении выплат, по результатам изучения материалов уголовных дел, составляет 11%.

Наиболее общественно опасным мошенником при получении выплат является преступник *особо злостного* (с установкой на преступную деятельность) типа. К такому типу относятся мошенники при получении выплат, которые свою преступную деятельность воспринимают как основной, источник дохода. Они разрабатывают специальные схемы совершения преступления, осуществляют поиск и подбор лиц, которые могут претендовать на какие-либо выплаты либо желают эти выплаты использовать по нецелевому назначению. К такому типу преступников относится, по результатам проведенного исследования, 34% лиц, совершивших мошенничество при получении выплат.

Таким образом, проведенное криминологическое исследование позволило сформировать комплексный социально-демографический и нравственно-психологический портрет личности, совершающей мошенничество при получении выплат. Типичный преступник (мошенник при получении выплат) представляет собой женщину в возрасте 30—49 лет, обладающую высшим или средним профессиональным образованием, состоящую в браке и имеющую трех и более детей. Социально-экономический статус характеризуется формальным соответствием критериям для получения выплат при отсутствии постоянного источника дохода. Уголовно-правовой анализ выявил преобладание одиночного способа совершения преступления (87%) с доминированием квалифицированных составов тяжких преступлений (60%). Нравственно-психологические особенности включают внешне законопослушное социальное поведение, сочетающееся с доминированием материальных ценностей, расчетливостью и способностью к длительному

планированию противоправных действий. На основе критерия общественной опасности разработана типология, включающая неустойчивый (55%), злостный (11%) и особо злостный (34%) типы преступников, где последние характеризуются системной ориентацией на преступную деятельность. Специфика механизма преступления, требующего осознанного оформления документов и соответствия формальным критериям, исключает возможность отнесения данных деяний к категории случайных преступлений. Полученные результаты имеют практическую значимость для разработки дифференцированных мер криминологической профилактики, направленных на конкретные социально-демографические группы и типологические категории правонарушителей.

ЛИТЕРАТУРА

1. Клейменов М. П. Криминология : учебник. — 3-е изд., перераб. и доп. — М., 2023. — С. 87—92.

2. Прозументов Л. М., Шеслер А. В. Уголовно-правовые и криминологические аспекты преступлений против собственности. — Новосибирск, 2014. — С. 93—97.

3. Писаревская Е. А., Дворжицкая М. А. Криминология : учебное пособие. — Казань, 2023. — С. 33.

4. Кузина Л. С. Предупреждение вовлечения несовершеннолетних в незаконный оборот наркотических средств, психотропных веществ или их аналогов : дис. … канд. юрид. наук. — Воронеж, 2019. — С.114.

5. Марданов А. Б. Личность современного экономического преступника : дис. … канд. юрид. наук. — Сургут, 2010. — С. 67.

6. Антонян Ю. М., Кудрявцев В. Н., Эминов В. Е. Личность преступника : монография. — СПб., 2004. — 366 с.

7. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации : Федеральный закон от 29 ноября 2012 г. № 207-ФЗ // Собрание законодательства РФ. — 2012. — № 49. — Ст. 6752.

8. Официальные данные ГИАЦ МВД РФ (форма отчетности № 491 и № 493).

9. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 21.04.2025) // Собрание законодательства РФ. — 1996. — № 25. — Ст. 2954.

10. Антонян Ю. М. Преступность женщин. — М., 1992. — С. 67.

11. Кравцов И. А., Польшиков А. В., Буслов М. М. Мошенничество при получении выплат: специфика детерминации и направления повышения эффективности мер предупреждения // Вестник Воронежского института МВД России. — 2024. — № 3. — С. 182—188.

12. О государственной гражданской службе Российской Федерации : Федеральный закон от 27.07.2004 № 79-ФЗ (ред. от 14.02.2024 ; с изм. и доп., вступ. в силу с 12.03.2024) // Собрание законодательства РФ. — 2004. — № 31. — Ст. 3215.

13. Приговор № 1-1-153/2020 от 16 ноября 2020 г. по делу № 1-1-153/2020 // Судебные и нормативные акты РФ. — URL: https://sudact.ru/ (дата обращения: 28.06.2025).

14. Кириллов С. И. Личность преступника: проблемы типологии. — Курск, 1998. — С. 123.

15. Улезько С. И., Ганаева Е. Э. Личность преступника: понятие, структура и типология // Вестник Чеченского государственного университета им. А. А. Кадырова. — 2021. — № 3 (43). — С. 85—102.

16. Архив Хивского районного суда Республики Дагестан. Уголовное дело № 27/2017 // Судебные и нормативные акты РФ. — URL: https://sudact.ru/ (дата обращения: 28.06.2024).

REFERENCES

1. Klejmenov M. P. Kriminologiya : uchebnik. — 3-e izd., pererab. i dop. — M., 2023. — S. 87—92.

2. Prozumentov L. M., Shesler A. V. Ugolovno-pravovye i kriminologicheskie aspekty prestuplenij protiv sobstvennosti. — Novosibirsk, 2014. — S. 93—97.

3. Pisarevskaya E. A., Dvorzhitskaya M. A. Kriminologiya : uchebnoe posobie. — Kazan′, 2023. — S. 33.

4. Kuzina L. S. Preduprezhdenie vovlecheniya nesovershennoletnikh v nezakonnyj oborot narkoticheskikh sredstv, psikhotropnykh veshchestv ili ikh analogov : dis. … kand. yurid. nauk. — Voronezh, 2019. — S.114.

5. Mardanov A. B. Lichnost′ sovremennogo ekonomicheskogo prestupnika : dis. … kand. yurid. nauk. — Surgut, 2010. — S. 67.

6. Antonyan Yu. M., Kudryavtsev V. N., Eminov V. E. Lichnost′ prestupnika : monografiya. — SPb., 2004. — 366 s.

7. O vnesenii izmenenij v Ugolovnyj kodeks Rossijskoj Federatsii i otdel′nye zakonodatel′nye akty Rossijskoj Federatsii : Federal′nyj zakon ot

29 noyabrya 2012 g. № 207-FZ // Sobranie zakonodatel′stva RF. — 2012. — № 49. — St. 6752.

8. Ofitsial′nye dannye GIATs MVD RF (forma otchetnosti № 491 i № 493).

9. Ugolovnyj kodeks Rossijskoj Federatsii ot 13 iyunya 1996 g. № 63-FZ (red. ot 21.04.2025) // Sobranie zakonodatel′stva RF. — 1996. — № 25. — St. 2954.

10. Antonyan Yu. M. Prestupnost′ zhenshchin. — M., 1992. — S. 67.

11. Kravtsov I. A., Pol′shikov A. V., Buslov M. M. Moshennichestvo pri poluchenii vyplat: spetsifika determinatsii i napravleniya povysheniya effektivnosti mer preduprezhdeniya // Vestnik Voronezhskogo instituta MVD Rossii. — 2024. — № 3. — S. 182—188.

12. O gosudarstvennoj grazhdanskoj sluzhbe Rossijskoj Federatsii : Federal′nyj zakon ot 27.07.2004 № 79-FZ (red. ot 14.02.2024 ; s izm. i dop., vstup. v silu s 12.03.2024) // Sobranie zakonodatel′stva RF. — 2004. — № 31. — St. 3215.

13. Prigovor № 1-1-153/2020 ot 16 noyabrya 2020 g. po delu № 1-1-153/2020 // Sudebnye i normativnye akty RF. — URL: https://sudact.ru/ (data obrashcheniya: 28.06.2025).

14. Kirillov S. I. Lichnost′ prestupnika: problemy tipologii. — Kursk, 1998. — S. 123.

15. Ulez′ko S. I., Ganaeva E. E. Lichnost′ prestupnika: ponyatie, struktura i tipologiya // Vestnik Chechenskogo gosudarstvennogo universiteta im. A. A. Kadyrova. — 2021. — № 3 (43). — S. 85—102.

16. Arkhiv Khivskogo rajonnogo suda Respubliki Dagestan. Ugolovnoe delo № 27/2017 // Sudebnye i normativnye akty RF. — URL: https://sudact.ru/ (data obrashcheniya: 28.06.2024).

СВЕДЕНИЯ ОБ АВТОРЕ

Азарова Ирина Владимировна. Старший преподаватель кафедры социально-гуманитарных, экономических и правовых дисциплин.

Воронежский институт МВД России.

E-mail: aziravlad@rambler.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Azarova Irina Vladimirovna. Senior lecturer of the chair of Social and Humanitarian, Economic and Legal Disciplines.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: aziravlad@rambler.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: криминологический портрет; мошенничество при получении выплат; личность преступника; криминологическая характеристика; социально-демографические признаки; нравственно-психологические особенности; уголовно-правовые признаки; ст. 159^2 УК РФ; криминологическая типология; неустойчивый тип преступника; злостный тип преступника; особо злостный тип преступника; корыстная мотивация; предупреждение преступлений; криминологическая профилактика.

Key words: criminological portrait; fraud in receiving payments; criminal personality; criminological characteristics; socio-demographic features; moral and psychological features; criminal law features; Article 159^2 of the Criminal Code of the Russian Federation; criminological typology; unstable criminal type; malicious criminal type; particularly malicious criminal type; mercenary motivation; crime prevention; criminological prevention.

УДК 343.72

Г. Н. Волкодавова, *адъюнкт*

ИНСТИТУТ РУКОВОДИТЕЛЯ В СИСТЕМЕ МВД РОССИИ: НРАВСТВЕННЫЙ АСПЕКТ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

THE INSTITUTE OF LEADERSHIP IN THE SYSTEM OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA: THE MORAL ASPECT OF PROFESSIONAL ACTIVITIES

В статье рассматривается институт руководителя органов внутренних дел через призму нравственных требований, предъявляемых к сотрудникам, наделенным административно-властными полномочиями. Анализируется эволюция нравственного идеала руководителя милиции/полиции, соотношение правовых и моральных норм в управленческой деятельности. Особое внимание уделено проблеме профессионально-нравственной деформации, этике взаимодействия с подчиненными и гражданами, а также роли нравственного аспекта в обеспечении законности и авторитета полиции. Сделан вывод о том, что нравственная состоятельность руководителя является ключевым условием эффективности всей системы МВД России.

The article examines the institution of the head of the internal affairs bodies through the prism of moral requirements for employees with authority and managerial powers. It analyzes the evolution of the moral ideal of the head of the militia/police, the relationship between legal and moral norms in managerial activities. Special attention is paid to the problem of professional and moral deformation, the ethics of interaction with subordinates and citizens, and the role of the moral factor in ensuring the legality and authority of the police. The article concludes that the moral integrity of the head is a key condition for the effectiveness of the entire system of the Russian Ministry of Internal Affairs.

Реформирование системы МВД России, продолжающееся на протяжении последних лет, актуализировало вопрос не только о правовой компетенции, но и о нравственном облике сотрудников органов внутренних дел. В центре внимания находится институт руководителя. Руководитель органа внутренних дел (далее — руководитель ОВД) является ключевой фигурой, демонстрирующей подчиненным не только служебные задачи, но и нравственные ориентиры. Как отмечает А. В. Губанов, «руководитель в полиции — это не просто администратор, это носитель государственной морали, от личных качеств которого зависит вера граждан в справедливость закона» [1]. Руководитель осуществляет государственную власть и реализует через свою деятельность общие цели, задачи и интересы правоохранительной деятельности. В современных условиях вызовов и кризисных ситуаций, когда общество предъявляет повышенные требования к доступности и честности полиции, изучение нравственного аспекта деятельности руководителя в Министерстве внутренних дел Российской Федерации (далее — МВД России) приобретает научную и практическую значимость.

Изучение этого вопроса нашло отражение в трудах А. В. Губанова, В. Я. Кикотя, А. М. Столяренко и др.

Проведённый анализ этических и моральных принципов института руководителя в системе МВД России позволил выявить проблемы и определить пути их решения.

Еще со времен Российской империи нравственный облик начальника полиции находился под пристальным вниманием. От чиновника полиции требовались не только дисциплина и исполнительность, но и «милосердие к заблудшим» и «твердость в вере» [2]. Советский период сделал акцент на партийной принципиальности и идеологической выдержанности. В обоих случаях руководитель выступал не просто должностным лицом, а воспитателем. Руководить — значит воспитывать [3]. На современном этапе нововведения и преобразования в МВД России зависят не только от уровня квалификации, но и от профессионализма руководящих кадров. В современном руководителе в системе органов внутренних дел должны сочетаться образованность, воспитанность, профессионализм, правовая грамотность и

высокие нравственные принципы, которые проявляются в решениях, отношении к делу и подчиненным, поступках.

Институт руководителя в МВД России регулируется Дисциплинарным уставом (далее — Устав) [4], Положением о порядке организации морально-психологического обеспечения деятельности органов внутренних дел Российской Федерации (далее — Положение) [5], а также нормами Кодекса профессиональной этики сотрудника ОВД (далее — Кодекс) [6].

Устав определяет сущность служебной дисциплины в органах внутренних дел, обязанности сотрудников, обязанности и права руководителя по поддержанию служебной дисциплины, обязательное исполнение приказов, а также порядок поощрений и дисциплинарных взысканий. В свою очередь, служебная дисциплина в органах внутренних дел обеспечивается как личной ответственностью каждого сотрудника, так и уважением руководителем (начальником) чести и достоинства подчинённых [4].

В Положении четко определены основные цели работы, проводимой с сотрудниками ОВД: 1) формирование у сотрудников государственно-патриотического мировоззрения, их воспитание в духе преданности Отечеству, личной ответственности за его историческую судьбу, обеспечение глубокого понимания и поддержки личным составом политики, проводимой государством; 2) закрепление в сознании сотрудников традиционных российских духовно-нравственных ценностей, общероссийской гражданской идентичности; 3) освоение, поддержание и развитие системы полицейской культуры, приобщение личного состава к ее элементам: высшим целям профессиональной деятельности, моральным ценностям, профессиональным традициям и символам, правовым и нравственно-этическим нормам, образцам и идеалам служебного поведения; 4) достижение высокого уровня правосознания у личного состава, соблюдение им законности, требований к служебному поведению, антикоррупционных стандартов и норм профессиональной этики [5].

Кодекс определяет этические нормы, правила и требования к служебному поведению сотрудников органов внутренних дел Российской Федерации при осуществлении служебной деятельности, а также во внеслужебное время. Этические требования основываются на принятых в российском обществе нравственных принципах и ценностях, а также на лучших профессиональных традициях органов внутренних дел Российской Федерации [6].

Рассмотрим нравственный аспект профессиональной деятельности руководителя в органах внутренних дел через такие категории, как:

1) честь и долг;

2) справедливость;

3) ответственность и совесть.

Руководитель на службе обязан стать образцом служебного поведения, и его поведение не должно порочить высокое звание сотрудника полиции. Если рассматривать долг как объективную общественную необходимость, которая выражается в системе нравственных требований, предъявляемых к личности руководителя, то его профессиональная деятельность представляет собой реализацию служебного долга и моральной ответственности, возложенных на него обществом. Служебный долг сотрудника полиции является ключевой составляющей долга человека и гражданина и предполагает выполнение одной из важнейших государственных задач: защиты прав и свобод граждан, обеспечения безопасности страны и правопорядка. В этом смысле роль руководителя ОВД заключается в организации служебной деятельности подчинённых и воспитании у них чувства профессионального долга. Для руководителя ОВД честь — это фундаментальный ориентир, и она должна проявляться в каждом принимаемом служебном решении. Именно честь подразумевает обязательное следование моральным нормам и этическим принципам.

В процессе реализации управленческой деятельности руководителем ОВД принимаются решения, которые затрагивают интересы личного состава: решения, связанные с поощрением наиболее отличившихся сотрудников, назначением дисциплинарных взысканий за проступки, планированием служебной нагрузки и функциональных обязанностей подчинённых сотрудников. Основным требованием к принятию управленческих решений руководителем выступает их объективность и честность, которые являются ключевыми для формирования доброжелательной морально-психологической обстановки во вверенном коллективе. Следует отметить, что принятие объективного и справедливого управленческого решения является одной из наиболее сложных задач в работе руководителя. Сложность заключается в том, что в реальной практике при решении таких задач не существует четкой формулы справедливости как единственно верного и правильного решения. Каждая ситуация требует рассмотрения через множество факторов — личностных особенностей сотрудника, обстоятельств и мотивов поступков и их последствий. Отсутствие конкретных шаблонов делает справедливость категорией, которая требует от руководителя нравственной зрелости и сформированного правосознания. Справедливость представляет собой соответствие, единство между человеческими отношениями, действиями и поступками, с одной

стороны, и действующими в обществе моральными, правовыми и этическими нормами — с другой. Это понятие связано с принципом: каждый получает то, что заслужил, будь то награда за честный труд или ответственность за совершенный проступок. В связи с этим справедливость выступает критерием соответствия действия (бездействия) и оценки этого действия (бездействия) со стороны общества и государства. Следовать принципу справедливости для руководителя ОВД является не просто предпочтительной, а обязательной установкой, определяющей само содержание правоохранительной деятельности, главным принципом которой является защита справедливости.

Обязанность органов внутренних дел — охранять права и законные интересы граждан, обеспечивать неотвратимость наказания и равенство всех перед законом, поэтому и управленческие решения руководителя ОВД должны быть пронизаны справедливостью. Только в этом случае они будут восприниматься подчиненными как правомерные.

Игнорирование руководителем ОВД принципа справедливости, проявление необъективности или предвзятого отношения влекут за собой негативные и разрушительные последствия для служебной деятельности органа внутренних дел. Прежде всего, это разрушение социально-психологического климата в коллективе, которое приводит к возникновению конфликтов, снижению уровня доверия сотрудников друг к другу и к самому руководству, а также к недобросовестному выполнению служебных обязанностей. Кроме того, несправедливые решения, принимаемые в отношении подчиненных, могут привести к такому опасному явлению, как правовой нигилизм среди сотрудников. Если сотрудники видят, что принцип справедливости нарушается внутри самой системы, цель которой направлена именно на достижение справедливости, то подрывается вера не только в силу закона и собственное чувство ответственности, но и может снизиться эффективность всей профессиональной деятельности органа внутренних дел.

Затрагивая такую важную категорию нравственного аспекта профессиональной деятельности руководителя органов внутренних дел, как ответственность, стоит выделить два ее вида: нравственную и моральную. В «Российской педагогической энциклопедии» под редакцией В. В. Давыдова нравственная ответственность рассматривается как «моральное качество личности и категория этики, отражающая, с одной стороны, способность человека отвечать за свои поступки, с другой — возможность для общества подвергать эти действия моральной оценке» [7]. По сравнению с юридической ответственностью, которая наступает исключительно за противоправные деяния, строго регламентированные правовыми нормами, сфера нравственной ответственности распространяется шире рамок закона. Руководитель ОВД несет персональную ответственность за поддержание служебной дисциплины во вверенном ему органе внутренних дел.

Персональную ответственность руководителя территориального органа внутренних дел можно представить как вид личной ответственности должностного лица, на которое возложена обязанность по принятию управленческих решений, включающая в себя чувство долга, самооценку, решительность и ответственность за последствия, возникающие в результате достижения служебной цели.

Фундаментом морально-психологического климата в коллективе можно считать доверие, взаимопомощь и доброжелательность. Профессионально подготовленный руководитель — это не только квалифицированный специалист, имеющий диплом о высшем образовании и впечатляющий послужной список. По меткому выражению М. Монтеня, «тому, кто не постиг науку добра, всякая иная наука приносит лишь вред». Именно руководитель несет персональную ответственность за то, каким будет поведение его подчиненных при выполнении служебных обязанностей: проявят ли они уважение, такт, беспристрастие и законность в общении с гражданами. Руководитель отвечает за так называемую «честь мундира», за поддержание авторитета и положительного имиджа всей системы органов внутренних дел в глазах общества.

Моральная ответственность как важнейшее качество личности, присущее руководителю и как личности, и как должностному лицу, является составной частью его профессионального долга и тем самым определяет суть его профессиональной деятельности. Моральная ответственность достаточно хорошо определена в «Вестминстерском словаре теологических терминов» как «обладание способностью совершать выбор между правильными и неправильными действиями и, таким образом, быть ответственным за сделанный выбор» [8]. Термин «мораль» происходит от латинского слова «mores», что в переводе означает характер, нрав, обычай, проявляющийся в процессе общения и совместного проживания людей.

Мораль — это специфическая форма общественного сознания и общественного поведения, которая базируется не на писаных законах и предписаниях, а на исторически сложившихся обычаях, традициях и общепринятых в обществе представлениях о добре и зле, должном и недостойном, справедливом и несправедливом.

В повседневной жизни именно неписаные, но устойчивые, исторически сложившиеся представления направляют поступки людей.

Деятельность руководителя ОВД представляет собой непрерывную последовательность разнообразных управленческих решений. Это может быть как оперативное решение о направлении ближайшего наряда полиции на место только что совершенного преступления, от которого напрямую зависят жизнь, здоровье и безопасность граждан, так и стратегическое кадровое решение о назначении того или иного сотрудника на вышестоящую должность, что затрагивает не только его дальнейшую карьеру, но и благополучие его семьи.

Принимая каждое решение, руководитель обязан учитывать сложную систему интересов с разных сторон. С одной стороны, это интересы граждан, оказавшихся в трудной жизненной ситуации и обратившихся за помощью к государству в лице сотрудника полиции; с другой стороны, это интересы личного состава — подчиненных, для которых каждое решение руководителя означает либо поощрение и поддержку, либо ужесточение требований и контроль. В таком сложном процессе, как принятие управленческого решения, затрагивающего интересы людей, на первый план выходит такая категория нравственности, как совесть.

Совесть в данном случае стоит понимать не как условную категорию, а как важнейшую способность личности к нравственному самоконтролю. Этот внутренний механизм позволяет руководителю осознавать возможные последствия своих действий или бездействия как для подчинённых, так и для рядовых граждан. Руководитель, который в своей повседневной деятельности будет опираться не только на букву закона, но и на нормы морали и совести, сможет найти верное решение даже в самых сложных ситуациях.

Культура общения, или управленческая культура руководителя ОВД, включает в себя этику общения с подчиненными и гражданами. Современный руководитель должен научить подчиненных работать вежливо, но при этом принципиально. Руководитель должен быть примером профессионализма, образцового выполнения служебных обязанностей, соблюдения этических требований, служебной дисциплины и законности [6]. В свою очередь, профессиональная этика — это система моральных норм и принципов, действующих в особых условиях взаимоотношений людей в определенной профессии [9].

Профессиональная этика в правоохранительных органах сама по себе специфична, поскольку затрагивает интересы не только граждан, общества и правопорядка, но и самих сотрудников полиции. К сотруднику полиции как стражу порядка предъявляется ряд специальных требований: понимание общественной значимости своей роли, отношение к человеку как к высшей ценности, принципиальность, мужество, самоотверженность в борьбе с преступностью, образцовое личное поведение на службе и в быту. Обязанность руководителя в данном случае — стать гарантом реализации этих требований. Особого внимания заслуживает нравственный аспект принятия управленческих решений в экстремальных ситуациях, когда руководитель обязан брать на себя ответственность за риск, не перекладывая ее на подчиненных. Руководитель ОВД, не обладающий стойкостью, решительностью, порядочностью и уверенностью в себе, теряет авторитет.

Несомненно, одним из наиболее серьезных явлений, представляющих реальную угрозу для института руководителя в системе МВД России, является профессионально-нравственная деформация личности [10]. Сам процесс выражается в искажении моральных ориентиров, снижении критического отношения к себе и утрате тех высоких этических стандартов, которые изначально должны быть присущи лицу, наделенному властными полномочиями. Природа таких полномочий связана с возможностью влиять на людей, принимать обязательные для исполнения решения и контролировать подчинённых, что может стать благоприятной почвой для развития ряда опасных изменений в поведении руководителя. Можно выделить несколько ключевых и наиболее губительных тенденций [10].

Достаточно того, что руководитель, который занимает высокую должность длительное время и привык к обязательному выполнению его распоряжений, рискует утратить способность к самокритике и самоконтролю не только в общении с подчиненными, но и в оценке своих собственных профессиональных решений. Это может выражаться в проявлении грубости или пренебрежительном отношении к подчиненным сотрудникам и гражданам. Такой руководитель начинает считать, что его должностное положение ставит его выше общепринятых норм и уважения к человеческому достоинству; он может позволить себе категоричный тон, публичные унижения и игнорирование чужого мнения. Такое поведение разрушает не только коллектив, но и дискредитирует понятие власти, лишая ее тем самым нравственного авторитета.

Одной из распространённых форм профессионально-нравственной деформации является подмена общения «человек-человек». Руководитель

ОВД за статистическими отчетами и цифрами перестает видеть реальные проблемы и людей. Главной и, по сути, единственной целью становится хороший отчет и статистика. Равнодушие руководителя к сотрудникам и гражданам становится нормой. Подмена понятий затрагивает суть правоохранительной деятельности — служение обществу, и тем самым может превратить ее в бюрократический механизм, где человек оказывается препятствием на пути к выполнению показателей.

На наш взгляд, одним из самых опасных проявлений деформации является трансформация понятия «честь мундира». Основной смысл этого понятия подразумевает поддержание высокого авторитета профессии, которое включает безупречное поведение, добросовестное исполнение профессионального долга и недопустимость нарушения закона. В искаженной трактовке «честь мундира» начинает означать обязанность замалчивать противоправное поведение сотрудника полиции, скрывать проступки не только от общественности, но и от вышестоящего руководства. Руководитель ОВД не должен поддерживать подобную практику, потому что вместо воспитания личного состава в духе законности и принципиальности он фактически будет поощрять безнаказанность. Это может привести к подрыву доверия к системе органов внутренних дел со стороны общества и сделать невозможным соблюдение законности.

Нравственно-ценностные ориентации и способность руководителя делать правильный выбор определяют, насколько власть будет использована во благо общества и государства. От того, насколько сам руководитель будет соблюдать принципы справедливости, гуманизма и законности, напрямую зависит, станут ли эти принципы ориентиром для его подчиненных. Очевидным становится то, что современные условия предъявляют принципиально новые требования к личности руководителя ОВД. Современный руководитель — это не просто эффективный управленец, который владеет административными технологиями, методами планирования и контроля, знает тонкости кадрового делопроизводства и умеет добиваться высоких показателей в служебной деятельности. Он обязан стать лидером во вверенном ему коллективе, служить тем нравственным принципам, которые заявляет МВД России. Именно такой руководитель способен воспитать у подчиненных чувство профессионального долга, сформировать сплочённый коллектив, который будет готов к выполнению самых сложных задач, и, в конечном счете, укрепить доверие граждан к полиции как к гаранту безопасности и защитнику их прав.

Вышесказанное позволяет сделать вывод, что институт руководителя в органах внутренних дел — это сложный правовой и нравственно-этический феномен, представляющий собой совокупность общепризнанных норм и должностей, регулирующих процесс управления в системе МВД России. Институт управления не ограничивается административно-властными полномочиями: его основой выступают как четкая иерархическая структура с определёнными функциями, так и система нравственных ценностей, предъявляемых к личности руководителя как носителя моральной ответственности. Роль руководителя ОВД заключается не только в обеспечении эффективного выполнения возложенных на полицию обязанностей, но и в поддержании авторитета государственной власти в глазах граждан.

На основании вышеизложенного предлагается:

1. Совершенствование системы отбора, оценки и ротации руководящих кадров. Внедрение многоступенчатой системы психологического и этического тестирования при выдвижении в кадровый резерв, которая позволит не только оценить управленческие компетенции кандидата, но и выявить склонность к авторитаризму, а также оценить правильное соотношение понятий служебного долга и личной выгоды. Введение института «нравственный наставник», выбираемого из числа ветеранов и руководителей, пользующихся безупречной репутацией как в оперативной, так и в служебной деятельности, который станет не только примером для подражания, но и помощником в освоении этических и нравственных стандартов управленческой деятельности.

2. Введение персональной оценки эффективности деятельности руководителя ОВД. Внедрение такого показателя, как нравственный, позволит при оценке эффективности деятельности руководителя учитывать не только цифры раскрываемости, но и информацию, отражающую нравственный климат в коллективе, а также рассматривать состояние служебной дисциплины и законности среди подчинённых не через количество наказанных, а через их отсутствие.

3. Участие общественных советов и институтов гражданского общества в оценке нравственного облика руководителя ОВД. Внедрение практики публичных отчётов руководителей перед общественностью с доведением результатов работы не в статистике, а с приведением примеров решения конкретных вопросов и обращений граждан, а также дальнейший учёт мнения общественных советов при аттестации руководителей на замещение вышестоящих должностей.

4. Развитие коммуникации и управленческой культуры руководителя в служебной деятельности. При прохождении обучения по программам профессиональной подготовки и повышения квалификации руководителями особое внимание

уделять развитию стрессоустойчивости и навыков саморегуляции. Разработка и внедрение «Памятки руководителя ОВД о правилах этического и нравственного поведения в служебной деятельности» с основным акцентом на публичности поведения, культуре речи и внешнего вида, соблюдении принципа справедливости при принятии управленческого решения.

На наш взгляд, реализация представленных предложений позволит сделать акцент не на выполнении показателей, а на профессиональном служении государству, что укрепит институт руководителя как нравственный фундамент всей системы МВД России.

ЛИТЕРАТУРА

1. Губанов А. В. Нравственные основы правоохранительной деятельности : монография. — М. : Академия управления МВД России, 2021. — 312 с.

2. Нижник Н. С., Стоцкий А. П. Полицейская этика в Российской империи: историко-правовой аспект // Вестник Санкт-Петербургского университета МВД России. — 2020. — № 3(87). — С. 34—41.

3. Кикоть В. Я. Профессиональная этика и служебный этикет : учебник для студентов вузов, обучающихся по специальностям «Юриспруденция», «Правоохранительная деятельность» / под ред. В. Я. Кикотя. — М. : ЮНИТИ-ДАНА : Закон и право, 2014. — С. 121.

4. О Дисциплинарном уставе органов внутренних дел Российской Федерации : указ Президента РФ от 14 октября 2012 г. № 1377. — URL: https://www.garant.ru (дата обращения: 05.03.2026).

5. Об утверждении Положения о порядке организации морально-психологического обеспечения деятельности органов внутренних дел Российской Федерации : приказ МВД России от 27 августа 2024 г. № 500. — URL: https://sudact.ru (дата обращения: 06.03.2026).

6. Об утверждении Кодекса этики и служебного поведения сотрудников органов внутренних дел Российской Федерации : приказ МВД России от 26 июня 2020 г. № 460. — URL: https://sudact.ru (дата обращения: 05.03.2026).

7. Российская педагогическая энциклопедия / под ред. В. В. Давыдова. — М. : Большая российская энциклопедия, 1993.

8. Мак-Ким Дональд К. Вестминстерский словарь теологических терминов. — М. : Республика, 2004. — 503 с.

9. Амельчаков И. Ф. Культура управленческой деятельности руководителя территориального органа МВД России // Труды Академии управления МВД России. — 2022. — № 2(62). — С. 9—15.

10. Кардашевский В. В. Профессиональная деформация сотрудников ОВД: причины, проявления, профилактика // Психопедагогика в правоохранительных органах. — 2023. — № 1(88). — С. 52—57.

REFERENCES

1. Gubanov A. V. Nravstvennye osnovy pravookhranitel′noj deyatel′nosti : monografiya. — M. : Akademiya upravleniya MVD Rossii, 2021. — 312 s.

2. Nizhnik N. S., Stotskij A. P. Politsejskaya etika v Rossijskoj imperii: istoriko-pravovoj aspekt // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. — 2020. — № 3(87). — S. 34—41.

3. Kikot′ V. Ya. Professional′naya etika i sluzhebnyj etiket : uchebnik dlya studentov vuzov, obuchayushchikhsya po spetsial′nostyam «Yurisprudentsiya», «Pravookhranitel′naya deyatel′nost′» / pod red. V. Ya. Kikotya. — M. : YuNITI-DANA : Zakon i pravo, 2014. — S. 121.

4. O Distsiplinarnom ustave organov vnutrennikh del Rossijskoj Federatsii : ukaz Prezidenta RF ot 14 oktyabrya 2012 g. № 1377. — URL: https://www.garant.ru (data obrashcheniya: 05.03.2026).

5. Ob utverzhdenii Polozheniya o poryadke organizatsii moral′no-psikhologicheskogo obespecheniya deyatel′nosti organov vnutrennikh del Rossijskoj Federatsii : prikaz MVD Rossii ot 27 avgusta 2024 g. № 500. — URL: https://sudact.ru (data obrashcheniya: 06.03.2026).

6. Ob utverzhdenii Kodeksa etiki i sluzhebnogo povedeniya sotrudnikov organov vnutrennikh del Rossijskoj Federatsii : prikaz MVD Rossii ot 26 iyunya 2020 g. № 460. — URL: https://sudact.ru (data obrashcheniya: 05.03.2026).

7. Rossijskaya pedagogicheskaya entsiklopediya / pod red. V. V. Davydova. — M. : Bol′shaya rossijskaya entsiklopediya, 1993.

8. Mak-Kim Donal′d K. Vestminsterskij slovar′ teologicheskikh terminov. — M. : Respublika, 2004. — 503 s.

9. Amel′chakov I. F. Kul′tura upravlencheskoj deyatel′nosti rukovoditelya territorial′nogo organa

MVD Rossii // Trudy Akademii upravleniya MVD Rossii. — 2022. — № 2(62). — S. 9—15.
10. Kardashevskij V. V. Professional′naya deformatsiya sotrudnikov OVD: prichiny, proyavleniya, profilaktika // Psikhopedagogika v pravookhranitel′nykh organakh. — 2023. — № 1(88). — S. 52—57.

СВЕДЕНИЯ ОБ АВТОРЕ

Волкодавова Галина Николаевна. Адъюнкт.
Воронежский институт МВД России.
E-mail: gvolkodavova@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Volkodavova Galina Nikolaevna. Post-graduate cadet.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: gvolkodavova@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: институт руководителя; органы внутренних дел; профессиональная этика; нравственный аспект; управленческая культура; профессиональная деформация.

Key words: the institution of a manager; internal affairs bodies; professional ethics; moral aspect; management culture; professional deformation.

УДК 342.92:174

М. С. Кочкина

СТЕЛСИНГ КАК ФОРМА СЕКСУАЛИЗИРОВАННОГО И РЕПРОДУКТИВНОГО НАСИЛИЯ

STEALTHING AS A FORM OF SEXUALIZED AND REPRODUCTIVE VIOLENCE

В статье стелсинг рассматривается как форма сексуализированного и репродуктивного насилия в контексте криминологического анализа. Исследуются мотивация правонарушителей, психологические последствия для потерпевших и существующие правовые пробелы. Подчеркивается, что данное явление подрывает доверие в интимных отношениях, способствует распространению инфекций, передающихся половым путем, и негативно влияет на репродуктивное здоровье женщин. Предлагаются некоторые меры профилактики.

The article examines stealthing as a form of sexualized and reproductive violence in the context of criminological analysis. It explores the motivations of perpetrators, the psychological consequences for victims, and the existing legal gaps. The article emphasizes that this phenomenon undermines trust in intimate relationships, contributes to the spread of sexually transmitted infections, and negatively affects women's reproductive health. The article also suggests some preventive measures.

Сексуализированное насилие — это сложная и многогранная проблема, представляющая серьезную угрозу для безопасности личности, общества и государства. Оно охватывает широкий спектр деяний, от сексуальных домогательств до сексуальной эксплуатации, и оказывает разрушительное воздействие на физическое и психическое здоровье жертв. Криминологическая опасность сексуализированного насилия заключается не только в его высокой латентности и сложности выявления, но и в его способности деформировать социальные нормы, формировать атмосферу страха и безнаказанности, а также воспроизводить циклы насилия в будущем. Одним из новых, но быстро набирающих популярность явлений в рассматриваемой области является стелсинг. Стелсинг (от англ. stealthing — незаметный, тайный) — это практика намеренного снятия презерватива во время ненасильственного полового акта без согласия партнера [1]. Из этого следует, что основным объектом рассматриваемого посягательства выступает девушка/женщина. Проблематика данного явления уже достаточно проработана зарубежными учеными [2, 3], в то время как для нашей страны данная тематика является малоисследованной.

Необходимо понимать, что согласие на секс не является абстрактным понятием и не означает, что сексуальный партнер априори соглашается на любые действия со своим телом. В зависимости от контекста оно охватывает, в частности, такие вопросы, как: с кем, в каком формате и при каких условиях человек готов вступить в половой контакт. Соответственно, любые умышленные действия, которые будут выходить за обговоренные при соглашении рамки могут считаться проявлением насилия.

Методологическую основу исследования составили общенаучные и частнонаучные методы познания. В работе использованы анализ, синтез, обобщение и систематизация научной литературы по проблематике сексуализированного насилия и стелсинга. Для выявления сущности рассматриваемого явления, его мотивов, последствий и криминологической опасности применялся формально-логический метод. С помощью сравнительно-правового метода проведено сопоставление российского подхода к квалификации стелсинга с зарубежным законодательством. Также использован формально-юридический метод при анализе норм уголовного законодательства Российской Федерации и зарубежных стран. Применение криминологического подхода позволило рассмотреть стелсинг как социально опасное и латентное явление, выявить его основные мотивы, формы проявления и последствия для потерпевших.

Распространенность стелсинга установить сложно из-за его латентного характера. Исследования, проведенные в зарубежных странах, показывают, что значительное количество людей сталкивались с этой практикой [4. — С. 176]. Существующие онлайн-форумы и сообщества, где обсуждаются и даже поощряются подобные действия, свидетельствуют о том, что стелсинг не

является единичным случаем, а представляет собой достаточно распространенное явление [5. — С. 219].

Повышенное внимание к стелсингу, как к относительно недавно выявленному и трудно доказуемому составу преступления, возникло в 2010-х годах после публикации доклада юриста Александры Бродски [6]. Ее работа представила результаты анализа онлайн-сообществ, где мужчины продвигали идею «контрацептивного саботажа», мотивируя это стремлением к большему удовольствию во время полового акта без использования средства контрацепции. Тем самым стелсинг впервые был концептуализирован не как частный эпизод недобросовестного сексуального поведения, а как самостоятельная форма нарушения сексуальной автономии и репродуктивных прав партнера. Это, в свою очередь, обусловило дальнейший рост научного и правового интереса к проблеме, включая исследование ее криминологической природы, мотивов совершения и последствий для потерпевших.

По нашему мнению, мотивационный комплекс, лежащий в основе совершения стелсинга, носит неоднородный характер и включает следующие побудительные факторы:

- стремление к доминированию и контролю (стелсинг в зарубежной научной литературе часто рассматривается как способ утвердить свою власть над партнером и лишить его контроля над собственной репродуктивной функцией и здоровьем. В такой ситуации мужчина пытается дискриминировать женщину по половому признаку, что является нарушением Конвенции о ликвидации всех форм дискриминации в отношении женщин [7]);

- нежелание использовать средство контрацепции по различным причинам, сопряженное с игнорированием права партнера на защиту и безопасность;

- наличие специфических сексуальных предпочтений и фетишизированных установок;

- стремление к наступлению беременности партнерши (в отдельных случаях стелсинг совершается с целью принудительного наступления беременности, что позволяет рассматривать его как одну из форм репродуктивного насилия);

- деформированное восприятие интимных отношений как пространства одностороннего волеизъявления и реализации властного превосходства, а не взаимного согласия, равноправия и партнерского взаимодействия.

Последствия стелсинга носят деструктивный характер и могут вести за собой как физический, так и психологический ущерб. При этом они крайне индивидуальны и обусловлены множеством факторов: культурными, социальными, экономическими и биологическими особенностями.

К наиболее распространенным последствиям стелсинга следует отнести:

- незапланированную беременность. Отечественные ученые отмечают, что незапланированная беременность неблагоприятно сказывается на психологическом благополучии женщины [8. — С. 36]. Результаты научных исследований свидетельствуют о том, что женщины с незапланированной беременностью обнаруживают более высокую чувствительность к воздействию психосоциальных стрессоров. В сравнении с группой лиц, планировавших беременность, у данной категории отмечаются статистически более высокие показатели депрессивной симптоматики, личностной и ситуативной тревожности, а также выраженные признаки психоэмоциональной дезадаптации и невротизации [9—11]. Следует также учитывать, что стелсинг, как правило, имеет место вне контекста устойчивых семейных отношений, вследствие чего наступившая беременность в большинстве случаев приобретает характер нежелательной и выступает дополнительным психотравмирующим фактором;

- риск заражения ВИЧ-инфекцией и возможность заражения инфекциями, передающимися половым путем (далее — ИППП). Травмирующий характер данного деяния заключается во внезапном устранении барьерного механизма защиты, что допускает прямой контакт слизистых оболочек с потенциально инфицированным биологическим субстратом в условиях, когда потерпевшая сторона пребывает в ложной уверенности относительно безопасности контакта;

- переживание чувства предательства и унижения со стороны партнера. Указанное последствие обусловлено тем, что стелсинг представляет собой сознательное нарушение ранее достигнутых условий сексуального взаимодействия, подрывающее доверие как базовый элемент межличностной и интимной коммуникации;

- тревогу, депрессию и симптомы посттравматического стрессового расстройства. Их возникновение объясняется переживанием ситуации как формы сексуализированного насилия, связанной с утратой контроля над происходящим, чувством беспомощности и нарушением телесной автономии;

- страх перед будущими сексуальными контактами. Подобная реакция имеет закономерный характер, поскольку пережитый опыт может закреплять у потерпевшей ассоциацию интимной близости с угрозой, небезопасностью и возможностью повторного нарушения согласия;

- чувство вины и стыда. Данные переживания нередко формируются вследствие внутренней

виктимизации, когда потерпевшая ретроспективно приписывает себе обязанность предотвратить произошедшее, несмотря на то что ответственность за совершенное деяние полностью лежит на виновном лице.

В настоящее время в России стелсинг не криминализирован. Рассматриваемые действия не могут быть квалифицированы по ст. 131 УК РФ (изнасилование) и ст. 132 УК РФ (насильственные действия сексуального характера), так как в отношении рассматриваемого явления в нашей стране действует концепция насилия, а не согласия. Данный подход предполагает, что к сексуализированному насилию относят только действия, совершенные с применением насилия, угрозой его применения или использованием беспомощного состояния жертвы, а не просто без ее согласия.

Так, в соответствии с УК РФ могут быть наказуемы только некоторые общественно-опасные последствия стелсинга: если в случае незащищенного полового акта виновный заразит партнера венерической болезнью, при условии заведомой осведомленности о наличии таковой (ст. 121 УК РФ), или если он заведомо поставит его в опасность заражения ВИЧ-инфекцией (ст. 122 УК РФ). В случае же возникновения незапланированной беременности или проблем психологического спектра виновный не может быть привлечен к ответственности, так как рассматриваемые насильственные действия не регулируются ни одной отраслью права на сегодняшний день.

В зарубежном законодательстве некоторых стран (Австралия, Германия, Швейцария) стелсинг уже криминализирован или регулируется гражданско-правовыми нормами. В некоторых штатах США данное деяние признано формой сексуализированного насилия. В 2021 году Калифорния первой ввела закон, запрещающий стелсинг в гражданско-правовой сфере, что позволило пострадавшим требовать компенсацию [12]. Гражданский кодекс Калифорнии закрепляет, что помимо материальной компенсации суд вправе наложить на виновного судебный запрет, судебные издержки и любое другое возмещение, которое он сочтет целесообразным.

В Великобритании ответственность за стелсинг не предусмотрена какой-либо уголовно-правовой нормой, однако судебная практика страны также признает такие действия сексуализированной формой насилия. В 2021 году суд Великобритании признал мужчину виновным в сексуализированном насилии за стелсинг, отразив в приговоре, что согласие женщины распространялось только на защищенный половой акт [13].

В российском научном сообществе некоторые ученые уже высказывали предложения о криминализации стелсинга как отдельного преступления [14. — С. 130; 15]. По нашему мнению, ключевым препятствием для введения данной нормы является неустранимая сложность доказывания субъективной стороны деяния: в условиях абсолютной приватности интимного контакта практически невозможно объективно разграничить умышленное тайное снятие средства контрацепции и его случайное соскальзывание. В отсутствие независимых свидетелей и материальных следов насилия обвинение будет строиться исключительно на противоречивых показаниях сторон, что в силу принципа презумпции невиновности сделает вынесение объективного решения маловероятным. Подобная новелла неизбежно приведет к появлению декларативной, «мертвой» нормы, не применимой на практике, и создаст почву для злоупотребления правом в виде ложного доноса или шантажа.

Таким образом, решение проблемы стелсинга должно оставаться в плоскости гражданско-правовой ответственности или социальной превенции, так как уголовная репрессия в данном случае является избыточной и заведомо неэффективной с точки зрения доказывания. Вместе с тем отсутствие уголовно-правовых механизмов реагирования не исключает необходимости научного осмысления стелсинга как социально опасного и латентного явления. Напротив, именно криминологический подход позволяет выявить его распространенность, мотивационные детерминанты, виктимологические особенности и деструктивные последствия для личности и общества. В этой связи стелсинг следует рассматривать не только как правовой пробел, но и как самостоятельный объект криминологического анализа, требующий разработки мер профилактического и общесоциального воздействия.

Представляется, что для эффективной борьбы с этим видом сексуализированного насилия необходим комплекс мер общесоциальной профилактики, включающий:

1. Образование и воспитание. Необходимо формировать у молодежи культуру согласия, уважения к партнеру и ответственность за свои действия.

«В отношении сексуального просвещения подростков и молодежи Россия, можно даже сказать, совершает некие шаги в обратном направлении», — отмечают некоторые авторы [16. — С. 27]. Действительно, на сегодняшний день вопрос полового воспитания молодого поколения является табуированным и воспринимается обществом скорее негативно. Многочисленные представители власти, педагоги, родители несовершеннолетних детей в своем большинстве пола-

гают, что подобная инициатива приведет к ранним половым дебютам, незапланированным беременностям и иным негативным последствиям для молодого поколения, что в действительности не подкреплено никакими доказательствами.

Необходимо понимать, что сексуальная сфера жизни является одной из центральных в жизни каждого человека, и то, что рано или поздно подросток будет в нее вовлечен. Отсутствие должного уровня знаний в области отношений и секса, вот что представляет реальную угрозу для молодежи. Поиск ответов на интересующие вопросы через интернет, порнографию и знания таких же неосведомленных в этой области одноклассников не даст положительного результата, а приведет к дезинформированности и антинаучности, что позже может повлечь за собой проблемы в романтических и сексуальных отношениях.

Ранее нами уже вносилось предложение о введении нравственно-полового воспитания для несовершеннолетних [17. — С. 112]. Его цель, по нашему мнению, заключается в способствовании гармоничному развитию подрастающего поколения, повышению уровня сексологических знаний у подростков, полноценному формированию детородной функции, чувства ответственности за здоровье и благополучие будущей жены (мужа), детей, т. е. укреплению брака и семьи [18. — С. 25]. Молодежь должна иметь возможность говорить друг с другом об отношениях, нормах, ожиданиях, друг о друге. Нравственно-половое воспитание несовершеннолетних — это предпосылка для ответственной сексуальности. «Ведь секс — это больше, чем просто соитие. Секс неотделим от любви и взаимоотношений, зависим от самооценки, доверия, сопереживания» [19. — С. 408].

2. Повышение осведомленности населения о сексуализированном насилии в общем. Представляется, что на сегодняшний день наиболее массовым освещение проблемы можно сделать через работу со СМИ, инфлюенсерами и блогерами. Также необходимо создать вебсайты и онлайн-ресурсы, предоставляющие информацию о сексуализированном насилии, доступных услугах поддержки и способах защиты от таких посягательств; использовать социальные сети как обширную площадку для распространения информации; организовывать онлайн-дискуссии со специалистами в области сексуализированного насилия. Важно преодолевать мифы и стереотипы, связанные с сексуализированным насилием, а также вовлекать различные социальные группы в процесс повышения осведомленности.

3. Поддержка жертв: обеспечение доступа к медицинской, психологической и юридической помощи для лиц, переживших факт стелсинга.

Первоочередной задачей после совершения акта стелсинга является оказание медицинской помощи. Основными задачами здесь будут являться предоставление доступа к экстренной контрацепции для предотвращения нежелательной беременности. Важно обеспечивать конфиденциальность и доступность этой услуги, особенно для несовершеннолетних, а также профилактику и лечение ИППП.

Психологическая поддержка жертвам сексуализированного насилия в настоящее время оказывается различными кризисными центрами: «Насилию.нет» [20], «Сестры» [21], «Тебе поверят» [22]. Существует также группа поддержки «ТыНеОдна» [23]. Эти организации оказывают бесплатную психологическую помощь жертвам сексуального и сексуализированного насилия.

4. Проведение научных исследований. На сегодняшний день стелсинг является малоизученным явлением, необходимы дальнейшие исследования для изучения распространенности, мотивов и последствий стелсинга, а также для разработки эффективных профилактических программ [24. — С. 6]. Видится, что исследования должны проводить ученые из разных областей: социологии, психологии, сексологии, криминологии.

Резюмируя, можно сказать, что стелсинг является неприемлемой формой сексуализированного и репродуктивного насилия, представляющей серьезную криминологическую угрозу. Для эффективной борьбы с этим явлением необходимо объединение усилий институтов государства, общества и специалистов различных областей. Важно повышать осведомленность о наличии такой проблемы, формировать культуру согласия, совершенствовать законодательство и обеспечивать поддержку жертвам насилия.

ЛИТЕРАТУРА

1. Inside The Online Community Of Men Who Preach Removing Condoms Without Consent. — URL: https://www.huffpost.com/entry/inside-the-online-community-of-men-who-preach-removing-condoms-without-consent_n_58f75eb2e4b05b9d613eb997 (дата обращения: 12.02.2026).

2. Non-consensual condom removal, reporting of sexual violence and associated factors: a cross-sectional study among women attending a sexual health service in Australia / R. L. Latimer [et al.]. — URL: https://srh.bmj.com/content/45/3/175 (дата обращения: 12.02.2026).

3. Prevalence and correlates of non-consensual condom removal ('stealthing') among men who have sex with men and women attending a sexual health service in Melbourne, Australia / Rosie Latimer [et al.]. — URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0209716 (дата обращения: 12.02.2026).

4. Broad A. M. Rape-Adjacent: Imagining Legal Responses to Stealthing // Columbia Journal of Gender and Law. — 2017. — № 32(2). — P. 171—218.

5. Scoping Review of Nonconsensual Condom Removal («Stealthing») Research / K. C. Davis, J. F. Hammett, W. Chen [et al.] // Trauma Violence Abuse. — 2024. — № 25(1). — P. 215—230.

6. Rape-Adjacent: Imagining Legal Responses to Nonconsensual Condom Removal. — URL: https://papers.ssrn.com/sol3/ (дата обращения: 04.03.2026).

7. Конвенция о ликвидации всех форм дискриминации в отношении женщин. Принята резолюцией 34/180 Генеральной Ассамблеи ООН от 18 декабря 1979 года. — URL : https://www.un.org/ru/documents/decl_conv/conventions/cedaw.shtml (дата обращения: 13.02.2026).

8. Савина Л. Незапланированная беременность: социальные и клинические аспекты // Врач. — 2012. — № 8. — С. 36—39.

9. Добряков И. В. Диагностика и лечение невротических расстройств у беременных женщин // Перинатальная психология в родовспоможении : сб. материалов конф. — СПб., 1997. — С. 57—61.

10. Eggleston E., Tsui A., Kotelnichuk M. Unintended pregnancy and low birth weight in Ecuador // Am. J. Public Health. — 2001. — P. 91.

11. Orr S., Miller C. Unintended pregnancy and the psychosocial wellGbeing of pregnant women // Women's health iss. — 1997. — № 7(1). — P. 38—44.

12. California makes it illegal to remove condom without consent. — URL: https://apnews.com/article/ (дата обращения: 13.02.2026).

13. В Лондоне осудили мужчину, который снял презерватив во время секса. — URL: https://weekend.rambler.ru/crazy-world/54289436/ (дата обращения: 13.02.2026).

14. Обеднин Е. В. К вопросу о стелсинге как правовом пробеле в российском уголовном законодательстве // Интеллектуальный потенциал Сибири : сборник научных трудов 31-й Региональной научной студенческой конференции. — Новосибирск : Новосибирский государственный технический университет, 2023. — С. 128—131.

15. Бобырева А. Д., Байдаков А. Я., Клоков С. Н. К вопросу о возможности криминализации стелсинга в России // Аграрное и земельное право. — 2022. — № 6(210). — С. 106—107. — DOI 10.47643/1815-1329_2022_6_106.

16. Травкова М. Р. Родители как агенты неформального сексобразования: что делать? // Психология и психотерапия семьи. — 2018. — № 3. — С. 18—29.

17. Кочкина М. С. Нравственно-половое воспитание несовершеннолетних как форма профилактики преступлений в сфере сексуализированного насилия // Вестник Казанского юридического института МВД России. — 2025. — Т. 16. — № 2(60). — С. 106—112. — DOI 10.37973/2227-1171-2025-16-2-106-112.

18. Романовский Г. Б. О праве на половое воспитание // Гражданин и право. — 2016. — № 2. — С. 25—39.

19. Леннеер-Аксельсон Б. О любви, гендерном равноправии, сексуальности и насилии // Журнал исследований социальной политики. — 2003. — Т. 1. — № 3-4. — С. 397—409.

20. Центр «Насилию.нет». — URL: https://nasiliu.net (дата обращения: 14.03.2026).

21. Центр помощи «Сестры». — URL: https://sisters-help.ru (дата обращения: 14.03.2026).

22. Тебе поверят. — URL: https://verimtebe.ru (дата обращения: 14.03.2026).

23. Ты не одна. — URL: https://tineodna.ru (дата обращения: 14.03.2026).

24. Польшиков А. В., Кравцов И. А., Буданов С. А. Основные направления повышения эффективности ранней профилактики девиантного поведения учащихся общеобразовательных организаций // Вестник Воронежского института МВД России. — 2021. — № 1. — С. 252—258.

REFERENCES

1. Inside The Online Community Of Men Who Preach Removing Condoms Without Consent. — URL: https://www.huffpost.com/entry/inside-the-online-community-of-men-who-preach-removing-condoms-without-consent_n_58f75eb2e4b05b9d613eb997 (data obrashcheniya: 12.02.2026).

2. Non-consensual condom removal, reporting of sexual violence and associated factors: a cross-sectional study among women attending a sexual health service in Australia / R. L. Latimer [et al.]. — URL: https://srh.bmj.com/content/45/3/175 (data obrashcheniya: 12.02.2026).

3. Prevalence and correlates of non-consensual condom removal (\'stealthing\') among men who have sex with men and women attending a sexual health service in Melbourne, Australia / Rosie Latimer [et al.]. — URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0209716 (data obrashcheniya: 12.02.2026).

4. Broad A. M. Rape-Adjacent: Imagining Legal Responses to Stealthing // Columbia Journal of Gender and Law. — 2017. — № 32(2). — P. 171—218.

5. Scoping Review of Nonconsensual Condom Removal («Stealthing») Research / K. C. Davis, J. F. Hammett, W. Chen [et al.] // Trauma Violence Abuse. — 2024. — № 25(1). — P. 215—230.

6. Rape-Adjacent: Imagining Legal Responses to Nonconsensual Condom Removal. — URL: https://papers.ssrn.com/sol3/ (data obrashcheniya: 04.03.2026).

7. Konventsiya o likvidatsii vsekh form diskriminatsii v otnoshenii zhenshchin. Prinyata rezolyutsiej 34/180 General′noj Assamblei OON ot 18 dekabrya 1979 goda. — URL : https://www.un.org/ru/documents/decl_conv/conventions/cedaw.shtml (data obrashcheniya: 13.02.2026).

8. Savina L. Nezaplanirovannaya beremennost′: sotsial′nye i klinicheskie aspekty // Vrach. — 2012. — № 8. — S. 36—39.

9. Dobryakov I. V. Diagnostika i lechenie nevroticheskikh rasstroĭstv u beremennykh zhenshchin // Perinatal′naya psikhologiya v rodovspomozhenii : sb. materialov konf. — SPb., 1997. — S. 57—61.

10. Eggleston E., Tsui A., Kotelnichuk M. Unintended pregnancy and low birth weight in Ecuador // Am. J. Public Health. — 2001. — R. 91.

11. Orr S., Miller C. Unintended pregnancy and the psychosocial wellGbeing of pregnant women // Women's health iss. — 1997. — № 7(1). — P. 38—44.

12. California makes it illegal to remove condom without consent. — URL: https://apnews.com/article/ (data obrashcheniya: 13.02.2026).

13. V Londone osudili muzhchinu, kotoryj snyal prezervativ vo vremya seksa. — URL: https://weekend.rambler.ru/crazy-world/54289436/ (data obrashcheniya: 13.02.2026).

14. Obednin E. V. K voprosu o stelsinge kak pravovom probele v rossijskom ugolovnom zakonodatel′stve // Intellektual′nyj potentsial Sibiri : sbornik nauchnykh trudov 31-j Regional′noj nauchnoj studencheskoj konferentsii. — Novosibirsk : Novosibirskij gosudarstvennyj tekhnicheskij universitet, 2023. — S. 128—131.

15. Bobyreva A. D., Bajdakov A. Ya., Klokov S. N. K voprosu o vozmozhnosti kriminalizatsii stelsinga v Rossii // Agrarnoe i zemel′noe pravo. — 2022. — № 6(210). — S. 106—107. — DOI 10.47643/1815-1329_2022_6_106.

16. Travkova M. R. Roditeli kak agenty neformal′nogo seksobrazovaniya: chto delat′? // Psikhologiya i psikhoterapiya sem′i. — 2018. — № 3. — S. 18—29.

17. Kochkina M. S. Nravstvenno-polovoe vospitanie nesovershennoletnikh kak forma profilaktiki prestuplenij v sfere seksualizirovannogo nasiliya // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii. — 2025. — T. 16. — № 2(60). — S. 106—112. — DOI 10.37973/2227-1171-2025-16-2-106-112.

18. Romanovskiĭ G. B. O prave na polovoe vospitanie // Grazhdanin i pravo. — 2016. — № 2. — S. 25—39.

19. Lenneer-Aksel′son B. O lyubvi, gendernom ravnopravii, seksual′nosti i nasilii // Zhurnal issledovanij sotsial′noj politiki. — 2003. — T. 1. — № 3-4. — S. 397—409.

20. Tsentr «Nasiliyu.net». — URL: https://nasiliu.net (data obrashcheniya: 14.03.2026).

21. Tsentr pomoshchi «Sestry». — URL: https://sisters-help.ru (data obrashcheniya: 14.03.2026).

22. Tebe poveryat. — URL: https://verimtebe.ru (data obrashcheniya: 14.03.2026).

23. Ty ne odna. — URL: https://tineodna.ru (data obrashcheniya: 14.03.2026).

24. Pol′shikov A. V., Kravtsov I. A., Budanov S. A. Osnovnye napravleniya povysheniya effektivnosti rannej profilaktiki deviantnogo povedeniya uchashchikhsya obshcheobrazovatel′nykh organizatsij // Vestnik Voronezhskogo instituta MVD Rossii. — 2021. — № 1. — S. 252—258.

СВЕДЕНИЯ ОБ АВТОРЕ

Кочкина Мария Сергеевна. Преподаватель кафедры уголовного права и криминологии.
Воронежский институт МВД России.
E-mail: mari.koshkina.98@bk.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Kochkina Maria Sergeevna. Lecture of the chair of Criminal Law and Criminology.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: mari.koshkina.98@bk.ru
Work address: Russia, 394065, Voronezh, Prospect Patriots, 53.

Ключевые слова: стелсинг; сексуализированное насилие; репродуктивное насилие; безопасность; профилактика; незащищенный половой акт.

Key words: stealth; sexualized violence; reproductive violence; safety; prevention; unprotected sex.

УДК 343.9

М. М. Курашова

ВОПРОСЫ ЭТИКО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ПУБЛИЧНОГО УПРАВЛЕНИЯ

TOWARDS A PHILOSOPHY OF ETHICAL AND LEGAL REGULATION OF DIGITAL TRANSFORMATION OF PUBLIC ADMINISTRATION

В статье этико-правовые аспекты цифровой трансформации рассматриваются в качестве необходимого элемента правового регулирования деятельности органов публичной власти, а также отмечается актуальная проблема отсутствия целостной нормативно-этической основы цифровизации государственного управления. На основе анализа зарубежного опыта и отечественных инициатив автором формулируется вывод о необходимости создания единого рамочного документа — кодекса (стандарта) цифровой этики для сферы права, который стал бы фундаментом нормативно-правового регулирования цифрового взаимодействия между государством и гражданином.

The article considers the ethical principles of digital transformation as a necessary element of the legal regulation of the activities of public authorities, and also highlights the urgent problem of the lack of a holistic regulatory and ethical framework for the digitalization of public administration. Based on the analysis of foreign experience and domestic initiatives, the author concludes that it is necessary to create a single framework document — a code (standard) of digital ethics for the field of law, which would become the foundation of a new socio-legal agreement between the state and the citizen in the digital age.

Современное правовое пространство России находится в процессе интенсивной цифровой трансформации. Очевидно, что информационные технологии оказывают значительное воздействие не только на общественные отношения, урегулированные правом, но и непосредственно на само право (правовую систему) [1. — С. 5]. Вместе с тем стремительное технологическое развитие опережает формирование адекватных нормативно-правовых и этических рамок, способных минимизировать системные риски цифровизации [2].

Сегодня этико-правовой проблематике цифровизации правоприменения уделяется активное внимание представителей юридической науки. Исследователи всё чаще обращаются к вопросам определения правового статуса новых субъектов информационного права [3], дискриминационного потенциала алгоритмов [4], ответственности за машинные решения [5], баланса между эффективностью цифрового управления и неотъемлемыми гарантиями правового статуса личности [6] и другим. На наш взгляд, значимость этических аспектов цифровой трансформации публичного управления трудно переоценить.

На сегодняшний день нормативно-правовой фундамент использования цифровых технологий в процессе правоприменения представляет собой мозаику из разрозненных нормативных предписаний. Действующие федеральные законы и подзаконные акты, сопровождающие рассматриваемые нами трансформационные процессы, регулируют их отдельные аспекты либо в определенный период времени, либо в конкретной сфере, либо направлены на конкретных акторов или, напротив, неопределённый круг лиц. Иными словами, отсутствует систематизированная нормативная база, специально адаптированная для нужд правоприменительной практики в цифровую эпоху, в том числе регулирующая и вопросы цифровой этики. Абсолютно справедлива позиция С. М. Зубарева, полагающего, что «такое количество одновременно действующих различных по статусу документов, которые, по идее, должны способствовать цифровизации государственного управления, на самом деле содержит очень серьезные риски дестабилизации этого процесса…» [7].

Полагаем, проблема формирования целостной нормативно-правовой и этической основы, которая обеспечила бы не только скорость, но и предсказуемость, безопасность, а главное, легитимность цифровизации, может быть решена посредством принятия систематизированного нормативного акта (кодекса, стандарта) цифровой этики для сферы права.

Следует отметить, что идея разработки и принятия цифрового кодекса не нова, она активно обсуждается представителями научного сообщества и власти в течение последнего десятилетия. Сегодня в Стратегии развития отрасли связи Российской Федерации на период до 2035 г. отмечается: «Оптимальным видом законодательного акта, позволяющим сформировать стройную связанную систему отраслевых правовых норм, является федеральный закон (Цифровой кодекс Российской Федерации), обеспечивающий комплексное регулирование развития и использования информационных технологий, сетей связи и инфраструктуры связи» [8]. Вместе с тем, в декабре 2023 года Совет при Президенте РФ по кодификации и совершенствованию гражданского законодательства выступил против идеи Минцифры России по разработке Цифрового кодекса [9]. Советом было указано, что создание кодекса преждевременно, а предмет его регулирования определен «расплывчато и противоречиво» [10].

В продолжение работы по конструированию и наполнению будущего кодекса первый заместитель председателя комитета Совета Федерации Федерального Собрания РФ по конституционному законодательству и государственному строительству И. В. Рукавишникова обозначила «два главных направления, которым необходимо следовать при разработке этого закона: 1) систематизация информационного законодательства (принятие кодекса должно будет упорядочить его); 2) создание контуров (определенных рамок) цифровой безопасности и защиты от возможных рисков» [11].

Вместе с тем вопросам цифровой этики в рассматриваемом нами контексте экспертами уделяется значительно меньше внимания: они либо воспринимаются как декларативные, либо сводятся к общим моральным установкам, не получая должного самостоятельного отражения в структуре будущего регулирования.

В рамках настоящего исследования особый интерес представляют уже принятые сегодня Цифровые кодексы в Республике Кыргызстан [12] и Республике Казахстан [13], а также разработанный и представленный правительству на согласование Цифровой кодекс Азербайджана [14]. Не менее значимым является принятый в 2022 г. в г. Самарканде модельный Информационный кодекс для государств — участников СНГ [15]. В указанных актах этические нормы не выделены в отдельную главу или разделы, вместо этого они включены в общие положения, закрепляющие принципы цифрового законодательства, правосубъектность в цифровой среде, порядок взаимодействия субъектов, обеспечения доверия к цифровым системам и ответственного использования технологий.

Безусловно, тезисы о необходимости систематизации законодательства, регулирующего цифровое взаимодействие государства и общества, не подлежат сомнению. Более того, отрицать их не позволяет и успешный опыт зарубежных государств. При этом именно этические принципы способны обеспечить баланс между технологической эффективностью и защитой фундаментальных прав личности, что делает их невторостепенным, а одним из ключевых элементов любого современного цифрового законодательства. На наш взгляд, они не должны оставаться разрозненными, фрагментарно распределёнными по различным нормативным правовым актам, поскольку это снижает их юридическую определённость, затрудняет применение на практике и ослабляет их регулятивный потенциал. Гораздо более эффективной представляется целенаправленная аккумуляция этических норм в рамках единого правового инструмента — будь то специальный раздел кодифицированного акта, отдельный закон или признанный нормативный стандарт.

Так, в течение последних лет как профессиональными сообществами, так и государственными организациями разрабатываются и принимаются кодексы цифровой этики, охватывающие различные аспекты общественного взаимодействия в цифровой среде. Например:

Кодекс этики использованиях данных, разработанный Ассоциацией участников рынка больших данных при поддержке АНО «Аналитический Центр при Правительстве РФ» (версия от 12 декабря 2019 г.) [16];

Кодекс этики в сфере искусственного интеллекта, разработанный Альянсом в сфере искусственного интеллекта (версия от 26 октября 2021 г.) [17];

Кодекс этики в сфере разработки и применения искусственного интеллекта на финансовом рынке, разработанный Банком России (версия от 9 июля 2025 г.) [18] и др.

Важно подчеркнуть, что приведенные примеры кодексов цифровой этики являются демонстрацией эволюции этических норм от базовых правил вежливости в онлайн-пространстве к регулированию ИИ и устойчивого развития в конкретных сферах.

Каким мог бы быть кодекс (стандарт) цифровой этики для сферы права? Мы полагаем, что подобный документ, аккумулирующий основные этико-правовые постулаты цифровой трансформации правоприменительной деятельности органов публичной власти, не должен быть жестким нормативным актом. Вероятнее всего, им мог бы стать рамочный документ, устанавливающий основные этические принципы, цели и задачи взаимодействия «цифры»

и «права», на основе которых затем впоследствии будут разрабатываться конкретные административные процедуры.

Важно отметить, почему кодексу следует быть рамочным, а не принимать форму модельного акта по аналогии, например, с указанным нами выше модельным Информационным кодексом для государств — участников СНГ. В рассматриваемом вопросе считаем наиболее корректной доктринальную позицию, согласно которой категории «рамочный акт» и «модельный акт» не являются тождественными.

Так, заимствованная из нормотворческой практики иностранных государств категория «модельное законодательство» («model law») представляет собой «своеобразный мост» между нормами международного и внутреннего права [19. — С. 48]; является средством унификации и гармонизации, поскольку применение модельного акта в качестве самостоятельного источника права в рамках правоприменения не предполагается [20. — С. 16]; разрабатывается, как правило, в рамках деятельности различных международных объединений [21. — С. 62]. Основная цель модельного акта — выработка примерных правовых норм, регулирующих определённую сферу общественных отношений (в большинстве случаев экономическую или политическую), которые можно имплементировать в действующее внутригосударственное законодательство.

В свою очередь, также заимствованная из зарубежного нормотворчества категория «рамочный закон» («basic law») представляет собой особый вид нормативного правового акта, который устанавливает общие принципы, цели, основные направления правового регулирования в определенной сфере общественных отношений. Правовая природа рамочного закона характеризуется высоким уровнем абстракции норм, преобладанием принципов над конкретными правилами, установлением общих стандартов деятельности. Он не содержит подробных правил, а лишь очерчивает «рамку» правового регулирования, которая в последующем конкретизируется субъектом правоприменения под определенные нужды и специфику деятельности [22].

Возвращаясь к ранее высказанному тезису о наиболее уместной форме будущего кодекса (стандарта) цифровой этики для сферы права, сформулируем следующие аргументы в его поддержку:

- рамочная природа кодекса позволит квалифицировать его как инструмент внешнего выражения «мягкого права» («soft law»), что создает условия для формирования этических стандартов поведения субъектов публичной власти без избыточного императивного давления со стороны законодателя, но с опорой на авторитет и самоценность заложенных в нем этико-юридических постулатов;

- рамочный формат позволяет установить общие границы «надлежащего регулирования», оставляя при этом пространство для оперативного изменения непосредственно прикладных правовых норм. При этом сохраняется возможность делегирования полномочий по детализации таких норм конкретным органам власти. Подобная децентрализация повышает эффективность управленческого воздействия и гарантирует учет узкоотраслевой специфики, которую невозможно в полной мере охватить единым универсальным шаблоном. Кроме того, в условиях стремительной технологической трансформации правоприменения и внедрения систем ИИ в правовую среду такая форма кодекса, на наш взгляд, позволит минимизировать риски деактуализации норм, позволяя конкретному субъекту правоприменения адаптировать содержание правил под актуальные технологические вызовы;

- использование рамочного акта создает эффективный механизм имплементации универсальных международно-правовых нормы модельного Цифрового кодекса для государств — участников СНГ в отечественную правовую систему, сохраняя при этом юридическую автономию национального законодательства.

Полагаем, что ключевые разделы будущего кодекса (стандарта) цифровой этики для сферы права могли бы именоваться следующим образом:

1. Преамбула.
2. Цели и задачи кодекса.
3. Основные этические принципы.
4. Пределы и условия цифровизации государственно-властных полномочий.
5. Этические требования к субъектам публичной власти.
6. Механизм имплементации и актуализации.

Стоит оговориться, что детальное содержательное наполнение структурных разделов перспективного кодекса требует отдельного глубокого анализа и не является предметом настоящего исследования. Тем не менее принципиально важным представляется соблюдение баланса между общепризнанными принципами международного права и национальной спецификой правовой системы.

В заключение рассуждения следует констатировать следующее: сегодня отсутствует не просто отдельный документ — кодекс (стандарт) цифровой этики для сферы права, а целая философия этико-правового регулирования

цифровизации публичного управления. Безусловно, представленная в настоящем исследовании попытка решения указанной проблемы не является «истиной в первой инстанции» и решает далеко не все из существующих сегодня этических проблем цифровой трансформации управления. Однако не исключено, что такой кодекс (стандарт) мог бы выступить базисом, системообразующим документом, который предоставил бы правоприменителям ясные этические ориентиры в ситуациях, не урегулированных правом.

ЛИТЕРАТУРА

1. Амелин Р. В., Чаннов С. Е. Эволюция права под воздействием цифровых технологий. — М. : НОРМА, 2023. — 280 с.

2. Константинов А. В., Михайленко Н. В. Использование технологии больших данных (Big Data) в деятельности органов внутренних дел: проблемы и перспективы // Вестник Московского университета МВД России. — 2023. — № 3. — С. 129—132.

3. Ефремов А. А. Проблема субъектности в информационном праве // Журнал российского права. — 2025. — № 8. — С. 93—104.

4. Талапина Э. В. Дискриминационный потенциал алгоритмов // Административное право и процесс. — 2025. — № 2. — С. 55—58.

5. Талапина Э. В. Административные решения алгоритмов // Административное право и процесс. — 2024. — № 10. — С. 39—42.

6. Чернусь Н. Ю. Гарантии обеспечения прав граждан при предоставлении государственных и муниципальных услуг с использованием цифровых технологий // Государственная власть и местное самоуправление. — 2023. — № 6. — С. 51—53.

7. Зубарев С. М. Правовые риски цифровизации государственного управления // Актуальные проблемы российского права. — 2020. — № 6(115). — С. 23—32.

8. Об утверждении Стратегии развития отрасли связи Российской Федерации на период до 2035 года : распоряжение Правительства РФ от 24.11.2023 № 3339-р // Собрание законодательства РФ. — 2023. — № 50. — Ст. 9094.

9. В России началось обсуждение «Цифрового кодекса», который приведет в порядок законодательство в ИТ и связи. — URL: https://www.cnews.ru/news/top/2023-11-08 (дата обращения: 25.01.2026).

10. Цифра не дотянула до кодекса. Совет при президенте выступил против проекта Минцифры. — URL: https://www.kommersant.ru/doc/6397720 (дата обращения: 25.01.2026).

11. Что должен содержать Цифровой кодекс — мнение экспертов. — URL: https://www.garant.ru/news/1727243/ (дата обращения: 25.01.2026).

12. Цифровой Кодекс Кыргызской Республики от 31 июля 2025 года № 178. — URL: https://cbd.minjust.gov.kg/3-48/edition/35412/ru (дата обращения: 25.01.2026).

13. Цифровой кодекс Республики Казахстан от 9 января 2026 года № 255-VIII (не введен в действие). — URL: https://prg.kz/Document/?doc_id=38546537 (дата обращения: 25.01.2026).

14. В IRIA назвали основную цель цифрового кодекса. — URL: https://media.az/society/nazvana-osnovnaya-cel-cifrovogo-kodeksa-v-azerbaydzhane (дата обращения: 25.01.2026).

15. О новой редакции модельного Информационного кодекса для государств — участников СНГ : постановление № 54-12 Межпарламентской Ассамблеи государств — участников СНГ (принято в г. Самарканде 28.10.2022) // СПС «КонсультантПлюс».

16. Кодекс этики использования данных / Ассоциация участников рынка больших данных ; при поддержке АНО «Аналитический Центр при Правительстве РФ». — URL: https://rubda.ru/wp-content/themes/bigdata/codex.pdf (дата обращения: 20.01.2026).

17. Кодекс этики в сфере искусственного интеллекта / Альянс в сфере искусственного интеллекта. — URL: https://ethics.a-ai.ru/assets/ethics_files/2025/05/23/Кодекс_этики_20_10_1_yKu2UtZ.pdf (дата обращения: 20.01.2026).

18. Кодекс этики в сфере разработки и применения искусственного интеллекта на финансовом рынке / Банк России // СПС «Гарант». — URL: https://base.garant.ru/ (дата обращения: 20.08.2025).

19. Шестакова Е. В. Модельное законодательство СНГ // ЭЖ-Юрист. — 2005. — № 42. — URL : https://base.garant.ru/5196036/ (дата обращения: 20.01.2026).

20. Шестакова Е. В. Международная практика применения модельного законодательства // Законодательство и экономика. — 2006. — № 2. — С. 13—23.

21. Домрачев Д. Г., Кирилловых А. А. К вопросу о проблемах применения норм модельного законодательства: зарубежный опыт // Юридическая наука и практика : Вестник Нижегородской академии МВД России. — 2019. — № 4(48). — С. 61—64.

22. Довгань К. Е. Категория «рамочное законодательство» в национальной правовой системе РФ // Юрислингвистика. — 2022. — № 26(37).

REFERENCES

1. Amelin R. V., Channov S. E. Evolyutsiya prava pod vozdejstviem tsifrovykh tekhnologij. — M. : NORMA, 2023. — 280 s.

2. Konstantinov A. V., Mikhajlenko N. V. Ispol′zovanie tekhnologii bol′shikh dannykh (Big Data) v deyatel′nosti organov vnutrennikh del: problemy i perspektivy // Vestnik Moskovskogo universiteta MVD Rossii. — 2023. — № 3. — S. 129—132.

3. Efremov A. A. Problema sub″ektnosti v informatsionnom prave // Zhurnal rossijskogo prava. — 2025. — № 8. — S. 93—104.

4. Talapina E. V. Diskriminatsionnyj potentsial algoritmov // Administrativnoe pravo i protsess. — 2025. — № 2. — S. 55—58.

5. Talapina E. V. Administrativnye resheniya algoritmov // Administrativnoe pravo i protsess. — 2024. — № 10. — S. 39—42.

6. Chernus′ N. Yu. Garantii obespecheniya prav grazhdan pri predostavlenii gosudarstvennykh i munitsipal′nykh uslug s ispol′zovaniem tsifrovykh tekhnologij // Gosudarstvennaya vlast′ i mestnoe samoupravlenie. — 2023. — № 6. — S. 51—53.

7. Zubarev S. M. Pravovye riski tsifrovizatsii gosudarstvennogo upravleniya // Aktual′nye problemy rossijskogo prava. — 2020. — № 6(115). — S. 23—32.

8. Ob utverzhdenii Strategii razvitiya otrasli svyazi Rossijskoj Federatsii na period do 2035 goda : rasporyazhenie Pravitel′stva RF ot 24.11.2023 № 3339-r // Sobranie zakonodatel′stva RF. — 2023. — № 50. — St. 9094.

9. V Rossii nachalos′ obsuzhdenie «Tsifrovogo kodeksa», kotoryj privedet v poryadok zakonodatel′stvo v IT i svyazi. — URL: https://www.cnews.ru/news/top/2023-11-08 (data obrashcheniya: 25.01.2026).

10. Tsifra ne dotyanula do kodeksa. Sovet pri prezidente vystupil protiv proekta Mintsifry. — URL: https://www.kommersant.ru/doc/6397720 (data obrashcheniya: 25.01.2026).

11. Chto dolzhen soderzhat′ Tsifrovoj kodeks — mnenie ekspertov. — URL: https://www.garant.ru/news/1727243/ (data obrashcheniya: 25.01.2026).

12. Tsifrovoj Kodeks Kyrgyzskoj Respubliki ot 31 iyulya 2025 goda № 178. — URL: https://cbd.minjust.gov.kg/3-48/edition/35412/ru (data obrashcheniya: 25.01.2026).

13. Tsifrovoj kodeks Respubliki Kazakhstan ot 9 yanvarya 2026 goda № 255-VIII (ne vveden v dejstvie). — URL: https://prg.kz/Document/?doc_id=38546537 (data obrashcheniya: 25.01.2026).

14. V IRIA nazvali osnovnuyu tsel′ tsifrovogo kodeksa. — URL: https://media.az/society/nazvana-osnovnaya-cel-cifrovogo-kodeksa-v-azerbaydzhane (data obrashcheniya: 25.01.2026).

15. O novoj redaktsii model′nogo Informatsionnogo kodeksa dlya gosudarstv — uchastnikov SNG : postanovlenie № 54-12 Mezhparlamentskoj Assamblei gosudarstv — uchastnikov SNG (prinyato v g. Samarkande 28.10.2022) // SPS «Konsul′tantPlyus».

16. Kodeks etiki ispol′zovaniya dannykh / Assotsiatsiya uchastnikov rynka bol′shikh dannykh ; pri podderzhke ANO «Analiticheskij Tsentr pri Pravitel′stve RF». — URL: https://rubda.ru/wp-content/themes/bigdata/codex.pdf (data obrashcheniya: 20.01.2026).

17. Kodeks etiki v sfere iskusstvennogo intellekta / Al′yans v sfere iskusstvennogo intellekta. — URL: https://ethics.a-ai.ru/assets/ethics_files/2025/05/23/Kodeks_etiki_20_10_1_yKu2UtZ.pdf (data obrashcheniya: 20.01.2026).

18. Kodeks etiki v sfere razrabotki i primeneniya iskusstvennogo intellekta na finansovom rynke / Bank Rossii // SPS «Garant». — URL: https://base.garant.ru/ (data obrashcheniya: 20.08.2025).

19. Shestakova E. V. Model′noe zakonodatel′stvo SNG // EZh-Yurist. — 2005. — № 42. — URL: https://base.garant.ru/5196036/ (data obrashcheniya: 20.01.2026).

20. Shestakova E. V. Mezhdunarodnaya praktika primeneniya model′nogo zakonodatel′stva // Zakonodatel′stvo i ekonomika. — 2006. — № 2. — S. 13—23.

21. Domrachev D. G., Kirillovykh A. A. K voprosu o problemakh primeneniya norm model′nogo zakonodatel′stva: zarubezhnyj opyt // Yuridicheskaya nauka i praktika : Vestnik Nizhegorodskoj akademii MVD Rossii. — 2019. — № 4(48). — S. 61—64.

22. Dovgan′ K. E. Kategoriya «ramochnoe zakonodatel′stvo» v natsional′noj pravovoj sisteme RF // Yurislingvistika. — 2022. — № 26(37).

СВЕДЕНИЯ ОБ АВТОРЕ

Курашова Мария Михайловна. Преподаватель кафедры административного права.
Воронежский институт МВД России.
E-mail: km4498@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Kurashova Mariya Mikhailovna. Lecturer of the chair of Administrative Law.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: km4498@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: государственное управление; цифровая трансформация; право; этические принципы; правоприменительная деятельность; кодекс цифровой этики.

Key words: public administration; digital transformation; law; ethical principles; law enforcement; code of digital ethics.

УДК 342.92

В. В. Сенцов, *адъюнкт*

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ФИКТИВНОЙ РЕГИСТРАЦИИ И ПОСТАНОВКИ НА УЧЕТ ИНОСТРАННЫХ ГРАЖДАН И ЛИЦ БЕЗ ГРАЖДАНСТВА: ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ

CRIMINAL AND LEGAL CHARACTERISTICS OF FICTITIOUS REGISTRATION AND ACCOUNTING OF FOREIGN CITIZENS AND STATELESS PERSONS: PROBLEMS OF THEORY AND PRACTICE

В статье осуществлен анализ уголовно-правовых норм, содержащихся в статьях 322.2 и 322.3 УК РФ, и выявлены проблемы квалификации деяний, связанных с фиктивной регистрацией и постановкой на учет иностранных граждан и лиц без гражданства.

The article provides an analysis of the criminal law norms contained in Articles 322.2 and 322.3 of the Criminal Code of the Russian Federation and identifies problems in the qualification of acts related to the fictitious registration and recording of foreign citizens and stateless persons.

Уголовно-правовая охрана общественных отношений, складывающихся в ходе миграционных процессов, во многом обеспечивается за счёт введения ответственности за нарушения миграционных норм. Примером служат положения главы 32 Уголовного кодекса Российской Федерации (Далее — УК РФ), а именно статьи 322.2 и 322.3 УК РФ [1]. Как демонстрирует анализ, данные составы преступлений играют определяющую роль в системе охраны отношений, возникающих при осуществлении миграционного учёта.

Данные нормы имеют бланкетную конструкцию, отсылая правоприменителя к статье 2 Закона РФ от 25.06.1993 № 5242-1, регулирующего право граждан на свободу передвижения [2]. Однако на практике толкование этих статей сопряжено с трудностями из-за особенностей их юридической конструкции. Для выявления системных проблем и выработки предложений по модернизации уголовного законодательства необходимо провести сравнительный анализ общих и отличительных черт каждого из составов.

Если исходить из буквального толкования статей 322.2 и 322.3 УК РФ, то к числу их общих характеристик в первую очередь относят субъективные признаки. Здесь в качестве субъекта выступает лицо, осуществляющее регистрацию, которое наделено правомочиями по пользованию, владению или распоряжению жильем, с обязательным соблюдением установленной законом процедуры.

В научной среде единство мнений по данному вопросу отсутствует. Например, О. А. Михаль и Н. А. Черемнова указывают, что сложившаяся судебная практика идет по пути привлечения к ответственности исключительно регистрирующей стороны [3]. Подтверждением служит приговор Теучежского районного суда Республики Адыгея по ст. 322.3 УК РФ, по которому владелица квартиры ФИО1, не имея намерения предоставлять квартиру для фактического проживания, фиктивно зарегистрировала по месту пребывания гражданина Узбекистана ФИО2. Она не была знакома с иностранцем, но подала в МФЦ уведомление о его прибытии, указав свой адрес, и помещение для проживания не предоставила [4].

Следующая общая характеристика — сходство субъективной стороны, которая отражает психическую деятельность, сопровождающую преступление, где интеллектуальные и волевые аспекты выступают в единстве. Ключевой элемент здесь вина.

В Постановлении Пленума Верховного Суда РФ № 18 от 09.07.2020 (абз. 1 п. 14) разъяснено, что деяния по статьям 322.2 и 322.3 УК РФ совершаются исключительно с прямым умыслом. Лицо осознает общественную опасность своих действий, когда фиктивно выступает в роли «принимающей стороны». Вопрос установления прямого умысла является наиболее спорным при отграничении преступления от административного правонарушения (ст. 19.27 КоАП РФ —

предоставление ложных сведений), поэтому необходимо рассмотреть некоторые отличительные характеристики вышеуказанных преступлений от административного правонарушения.

Квалификация деяния как преступления возможна лишь при условии, что умысел лица был ориентирован на фиктивность совершаемой регистрации либо постановки на учёт. Согласно примечаниям к статьям, фиктивность состоит из двух признаков: во-первых, принимающая сторона не имеет подлинного намерения обеспечить жильём; во-вторых, регистрируемое лицо не намеревается там проживать либо оно ставится на учёт по адресу, отличному от реального места нахождения. Таким образом, для уголовно-правовой оценки содеянного требуется подтвердить, что злоумышленник действовал в рамках имитации законных регистрационных правоотношений, осознавая отсутствие фактических оснований. Объективная сторона преступлений по ст. 322.2 и 322.3 УК РФ заключается в формальном выполнении регистрационной процедуры, тогда как субъективная сторона охватывает знание лица о фиктивности своих действий и отсутствие воли на наступление реальных правовых последствий (фактическое предоставление жилого помещения или выполнение трудовой функции). При этом ключевое значение для квалификации приобретает именно направленность умысла виновного на создание видимости законного основания для пребывания иностранного гражданина на территории Российской Федерации.

В правоприменительной практике доказывание подобной направленности умысла, суть которого заключается в умышленном введении государственных органов в заблуждение посредством создания внешне безупречной юридической конструкции, осуществляется с опорой на совокупность косвенных доказательств. К ним, в частности, относятся показания соседей, участковых уполномоченных полиции, работников управляющих организаций, подтверждающие факт непроживания лица по месту регистрации. Несмотря на то, что сама по себе процедура постановки на миграционный учет нередко проведена в строгом соответствии с требованиями закона, последующие контрольные мероприятия выявляют отсутствие у принимающей стороны намерения предоставить жилое помещение, а у иностранного гражданина — намерения в нем проживать. В этой связи в научной литературе неоднократно обсуждался вопрос о допустимости квалификации самого факта непредоставления жилья в качестве объективного индикатора, свидетельствующего о наличии преступного умысла изначально. Данный вопрос вполне целесообразен, так как заранее продуманный механизм преступного поведения свидетельствует о том, что лицо не собиралось предоставлять жилое помещение изначально. Но с позиции правоприменительной практики ответ на вышепредставленный вопрос является отрицательным, поскольку требуется установить, что изначально, в момент подачи документов, у иностранного контингента и принимающей стороны, не было намерения породить реально существующие общественные отношения по поводу договора найма жилого помещения для таких целей, как жилье или пребывание.

Также важно отличать преднамеренную фикцию от неумышленных ошибок (опечатки в паспорте, неверная дата въезда, ошибка в адресе). Если лицо реально проживает по адресу, но допустило неточность в документах, состав преступления отсутствует, и деяние должно квалифицироваться по ст. 19.27 КоАП РФ.

Ещё одной областью совпадения выступают объективные признаки преступлений. В частности, по рассматриваемым статьям объектом посягательства признаются общественные отношения, возникающие в процессе миграционного учёта иностранных лиц и лиц без гражданства в РФ.

Обобщённые черты объективной стороны таковы:

- фиксация фиктивной регистрации (учёта) с использованием заведомо не соответствующих действительности сведений или фальшивых документов;

- регистрация без реального намерения регистрируемого лица проживать (находиться) в помещении;

- регистрация без реального намерения владельца или арендатора жилья предоставить это помещение для фактического проживания.

В научном сообществе ежегодно дискутируется вопрос: оправдано ли существование статей 322.2 и 322.3 УК РФ в их текущем виде [5]?

По мнению ряда исследователей, уровень общественной опасности данных деяний недостаточен для того, чтобы привлечение к уголовной ответственности было обоснованным. В связи с этим существующее уголовно-правовое регулирование рассматривается ими как избыточное [6].

Если в одной норме объединить деяния, обладающие различным уровнем общественной опасности, и при этом установить для них одни и те же санкции, то произойдёт выравнивание (нивелирование) характера и степени опасности каждого состава. Полагается, что такой подход законодателя не вполне учитывает специфику охраняемых общественных отношений. Фиктивная регистрация иностранца или лица без гражданства по адресу жительства несёт в себе существенные риски для миграционной безопасности и государственного

суверенитета, следовательно, нуждается в отдельной уголовно-правовой регламентации. Тогда как ответственность за фиктивную регистрацию гражданина РФ по месту временного пребывания или постоянного жительства было бы правильным перевести в разряд административных правонарушений, тем самым осуществив декриминализацию ст. 322.2 УК РФ в той её части, которая касается российских граждан. Исходя из этого, предлагается изложить ст. 322.2 УК РФ в следующей редакции: *«Фиктивная регистрация иностранного гражданина или лица без гражданства по месту жительства в жилом помещении в Российской Федерации».*

Кроме того, диспозиции статей 322.2 и 322.3 УК РФ необходимо дополнить указанием на специальную цель «из корыстной заинтересованности», поскольку судебная практика показывает, что большинство осужденных действуют именно из корысти. Обоснованность введения заключается в том, что существующая судебная практика, в своем многообразии приговоров, среди осужденных лиц трактует совершение вышеуказанных преступлений из-за корыстной заинтересованности. Так, например, в деле № 1-89/2025 Гурьевского районного суда Калининградской области (приговор от 22 сентября 2025 г.) фигурирует осуждённая ФИО2 по статьям 322.2 и 322.3 УК РФ. Суд констатировал: «…ФИО2 осуществила фиктивные постановки на учёт и регистрацию иностранных граждан соответственно по местам пребывания и жительства в Российской Федерации…», а также «…подсудимая, выступая принимающей стороной, решила в принадлежащем ей доме, расположенном по адресу: <адрес>, осуществить за денежное вознаграждение фиктивную постановку на учёт различных иностранных граждан без намерения их проживания…». Помимо этого, во время «…проведения судебного разбирательства в общем порядке и дополнительно показала, что в результате фиктивных постановок на учёт и регистрации иностранных граждан она выручила около 150 000 рублей…» [7].

В литературе высказывалось предложение о введении признака неоднократности (административной преюдиции), чтобы за первое нарушение следовала административная, а за повторное — уголовная ответственность [8]. П. А. Филиппов считает, что вред от фиктивной регистрации больше соответствует административному правонарушению [9].

Высказанное мнение автора не соответствует действительности, так как представленный подход не учитывает современные реалии. Рост миграционных потоков приобрел неконтролируемый характер, так как в настоящее время Российская Федерация является одной из стран-реципиентов. Даже единичный факт фиктивной регистрации создает условия для появления «резиновых» квартир и теневого рынка миграционных услуг. Уголовная ответственность в данном случае — это необходимый механизм противодействия систематическому извлечению дохода из фиктивной миграции. Последствия подобных нарушений далеко не всегда носят обратимый характер.

Фиктивная регистрация и постановка на учет нередко выступают первым звеном в цепи более тяжких преступлений, совершенных иностранными гражданами и лицами без гражданства. Устранить такие последствия мерами административной ответственности, например штрафом, практически невозможно, потому как размер санкции становится не более чем формальной платой за возможность легализовать пребывание неограниченного числа иностранного контингента.

Кроме того, административная ответственность не позволяет в полной мере реализовать принцип неотвратимости наказания применительно к лицам, которые систематически извлекают доход из фиктивной миграции. Уголовная же ответственность по статьям 322.2 и 322.3 УК РФ создает необходимый правовой механизм для противодействия подобным злоупотреблениям, позволяя дифференцировать ответственность в зависимости от масштаба деяния, наличия корыстного мотива и наступивших последствий.

В условиях, когда миграционные процессы оказывают непосредственное влияние на состояние общественной безопасности, социальную стабильность и демографическую структуру, нельзя признать уголовную ответственность за фиктивную регистрацию избыточной мерой. Напротив, именно уголовно-правовые средства способны обеспечить адекватную реакцию государства на деяния, которые в своей совокупности создают угрозу необратимых изменений в сфере миграционного контроля.

Спорным является вопрос квалификации при предоставлении в регистрирующий орган подложного документа, связанного с «ширмой» возникновения гражданско-правовых правоотношений, например, таким может быть договор аренды жилого помещения. Исходя из положений общей теории уголовного права, совокупность преступлений происходит даже тогда, когда одно действие (или бездействие) одновременно содержит признаки деяний из двух и более статей. Это означает, что допускается идеальная совокупность. В связи с этим возникает вопрос: образуют ли идеальную совокупность нормы, предусмотренные ст. 322.2 (322.3) и ч. 3 ст. 327 УК РФ? И далее: может ли использование ложных документов в

миграционном органе считаться способом совершения преступления, не порождая при этом идеальной совокупности? Привлечение по ч. 3 ст. 327 УК РФ обусловлено уже самим применением подделного документа, в то время как для ст. 322.2 и 322.3 УК РФ главное — направленность умысла на фиктивную регистрацию или постановку на учёт. Соответственно, в рассматриваемой ситуации присутствует идеальная совокупность, но лишь при условии, что предметом преступления выступает официальный документ (например, паспорт).

В случае если документ имеет гражданско-правовую природу (например, фиктивный договор найма жилого помещения), идеальная совокупность отсутствует, а представление такого документа квалифицируется как способ совершения преступления, предусмотренного ст. 322.2 или 322.3 УК РФ. Касаемо данного вопроса, необходимо уделить внимание судебной практике. Судебная практика иллюстрируется приговором Искитимского районного суда Новосибирской области от 10.09.2025 по ст. 322.2 УК РФ. Судом установлено, что собственница жилого дома, действуя с прямым умыслом, оформила договор найма с гражданином Республики Казахстан и осуществила его регистрацию по месту жительства, заведомо зная, что фактическое вселение последнего не производилось и жилое помещение ему не предоставлялось [10].

Следующим примером судебной практики является приговор, в результате которого осуждены граждане ФИО1 и ФИО2. Как установлено судом, участниками преступной группы были распределены роли: один из соучастников согласился за плату обеспечить фиктивную регистрацию по месту пребывания для иностранных граждан — с целью последующего получения ими патентов на трудовую деятельность в Республике Крым. В свою очередь, второй член группы, действуя по предварительному сговору, не позднее 1 марта 2024 года подыскал нескольких граждан Республики Таджикистан, у которых отсутствовали законные основания для учёта, патента и официальной работы. Он добровольно взял на себя обязанность помочь им легально находиться на территории РФ, а именно организовать для них фиктивную постановку на миграционный учёт [11].

Этот приговор наглядно демонстрирует, что действия, совершенные в соучастии и из корысти, квалифицируются так же, как и действия одного бескорыстного правонарушителя. Такое положение не соответствует степени общественной опасности [12, 13].

В настоящее время Российская Федерация является одной из самых многочисленных принимающих стран в мире. Масштабы миграционных потоков, обусловленные экономическими и геополитическими факторами, достигли уровня, при котором миграционная сфера превратилась в сложный комплекс общественных отношений, требующих особой охраны со стороны государства. Однако правовое регулирование не успевает за динамикой развития этих отношений. В условиях высокой миграционной нагрузки многократно возрастают риски, связанные с утратой контроля над миграционными процессами. Появляются новые формы организации преступной деятельности.

Проведенный анализ позволяет сделать вывод, что статьи 322.2 и 322.3 УК РФ, обладая бланкетным характером и являясь звеном уголовно-правовой охраны миграционных отношений, имеют ряд существенных законодательных пробелов.

Во-первых, отсутствие дифференциации ответственности в действующей редакции приводит к тому, что деяния, совершенные в соучастии и из корысти, квалифицируются так же, как действия одного бескорыстного нарушителя, что не соответствует степени общественной опасности.

Во-вторых, в условиях, когда Российская Федерация является одной из крупнейших принимающих стран, назрела необходимость дополнения статей 322.2 и 322.3 УК РФ квалифицирующими признаками, что позволит обеспечить соразмерность наказания и отнести деяния к категории тяжких и особо тяжких преступлений.

В-третьих, с учетом различной степени общественной опасности и характера охраняемых общественных отношений представляется обоснованным предложение о декриминализации указанного деяния в части, касающейся граждан РФ, и отнесение его к категории административных правонарушений с одновременным сохранением и усилением ответственности за фиктивную регистрацию иностранных граждан и лиц без гражданства, что позволит сосредоточить уголовно-правовые средства на наиболее значимых угрозах миграционной безопасности государства.

ЛИТЕРАТУРА

1. Уголовный кодекс Российской Федерации : Федеральный закон от 13.06.1996 № 63-ФЗ // Собрание законодательства Российской Федерации. — 1996. — № 25. — Ст. 2954.

2. О праве граждан Российской Федерации на свободу передвижения, выбор места пребывания и жительства в пределах Российской Федерации : закон РФ от 25.06.1993 № 5242-1(в ред. от 13.12.2024) // СПС «КонсультантПлюс» (дата обращения: 20.03.2026).

3. Михаль О. А., Черемнова Н. А. Квалифицирующие признаки организации незаконной миграции // Юридическая наука и правоохранительная практика. — 2016. — № 4 (38). — С. 66—73.

4. Приговор Теучежского районного суда Республики Адыгея по ст. 322.3 УК РФ. — URL: https://sudact.ru/regular/court/reshenya-teuchezhskii-raionnyi-sud-respublika-adyg (дата обращения: 21.03.2026).

5. Нурадинов Ш. М., Курдюк П. М. Актуальные проблемы квалификации фиктивной постановки на миграционный учет // Вестник Московского университета МВД России. — 2025. — № 3. — С. 91—98.

6. Петрова И. А. Уголовная ответственность за фиктивную регистрацию и фиктивную постановку на учёт иностранного гражданина или лица без гражданства. — URL: http://www.gramota.-net/materials/3/2015/9-2/34.html (дата обращения: 06.03.2026).

7. Приговор Гурьевского районного суда Калининградской области по статьям 322.3 и 322.2 УК РФ. — URL: https://sudact.ru/regular/doc/ah2hed5fH8Nl/?ysclid=mnfyqz829z28931333 (дата обращения: 21.03.2026).

8. Островская А. С. Фиктивная регистрация по месту жительства (месту пребывания) в Российской Федерации) // Право и политика. — 2017. — № 8. — С. 63—72.

9. Филиппов П. А. Организация незаконной миграции: практика применения ст. 322.1 УК РФ и новеллы законодательства // СПС «КонсультантПлюс» (дата обращения: 07.03.2026).

10. Приговор Искитимского районного суда Новосибирской области по ст. 322.2 УК РФ. — URL: https://iskitimsky--nsk.sudrf.ru/modules.php?name=press_dep&op=1&did=47 (дата обращения: 21.03.2026).

11. Приговор № 1-14/2025 1-179/2024 от 29 января 2025 г. Судакского городского суда Республики Крым. — URL: https://sudact.ru/regular/doc/qE4qK4JyZHWa/?ysclid=mn8jcxnkot762582 (дата обращения: 22.03.2026).

12. Бриллиантов А. В. Сущность и значение неоднократности в уголовном праве России // Правосудие. — 2024. — № 2. — С. 137—158.

13. Уторова Т. Н. Фиктивная постановка на миграционный учет: практика применения статьи 322.3 УК РФ // Пенитенциарная наука. — 2015. — № 1 (29). — С. 10—14.

REFERENCES

1. Ugolovnyj kodeks Rossijskoj Federatsii : Federal′nyj zakon ot 13.06.1996 № 63-FZ // Sobranie zakonodatel′stva Rossijskoj Federatsii. — 1996. — № 25. — St. 2954.

2. O prave grazhdan Rossijskoj Federatsii na svobodu peredvizheniya, vybor mesta prebyvaniya i zhitel′stva v predelakh Rossijskoj Federatsii : zakon RF ot 25.06.1993 № 5242-1(v red. ot 13.12.2024) // SPS «Konsul′tantPlyus» (data obrashcheniya: 20.03.2026).

3. Mikhal′ O. A., Cheremnova N. A. Kvalifitsiruyushchie priznaki organizatsii nezakonnoj migratsii // Yuridicheskaya nauka i pravookhranitel′naya praktika. — 2016. — № 4 (38). — S. 66—73.

4. Prigovor Teuchezhskogo rajonnogo suda Respubliki Adygeya po st. 322.3 UK RF. — URL: https://sudact.ru/regular/court/reshenya-teuchezhskii-raionnyi-sud-respublika-adyg (data obrashcheniya: 21.03.2026).

5. Nuradinov Sh. M., Kurdyuk P. M. Aktual′nye problemy kvalifikatsii fiktivnoj postanovki na migratsionnyj uchet // Vestnik Moskovskogo universiteta MVD Rossii. — 2025. — № 3. — S. 91—98.

6. Petrova I. A. Ugolovnaya otvetstvennost′ za fiktivnuyu registratsiyu i fiktivnuyu postanovku na uchyot inostrannogo grazhdanina ili litsa bez grazhdanstva. — URL: http://www.gramota.-net/materials/3/2015/9-2/34.html (data obrashcheniya: 06.03.2026).

7. Prigovor Gur′evskogo rajonnogo suda Kaliningradskoj oblasti po stat′yam 322.3 i 322.2 UK RF. — URL: https://sudact.ru/regular/doc/ah2hed5fH8Nl/?ysclid=mnfyqz829z28931333 (data obrashcheniya: 21.03.2026).

8. Ostrovskaya A. S. Fiktivnaya registratsiya po mestu zhitel′stva (mestu prebyvaniya) v Rossijskoj Federatsii) // Pravo i politika. — 2017. — № 8. — S. 63—72.

9. Filippov P. A. Organizatsiya nezakonnoj migratsii: praktika primeneniya st. 322.1 UK RF i novelly zakonodatel′stva // SPS «Konsul′tantPlyus» (data obrashcheniya: 07.03.2026).

10. Prigovor Iskitimskogo rajonnogo suda Novosibirskoj oblasti po st. 322.2 UK RF. — URL: https://iskitimsky--nsk.sudrf.ru/modules.php?name=press_dep&op=1&did=47 (data obrashcheniya: 21.03.2026).

11. Prigovor № 1-14/2025 1-179/2024 ot 29 yanvarya 2025 g. Sudakskogo gorodskogo suda Respubliki Krym. — URL: https://sudact.ru/regular/doc/qE4qK4JyZHWa/?ysclid=mn8jcxnkot762582 (data obrashcheniya: 22.03.2026).

12. Brilliantov A. V. Sushchnostʹ i znachenie neodnokratnosti v ugolovnom prave Rossii // Pravosudie. — 2024. — № 2. — S. 137—158.

13. Utorova T. N. Fiktivnaya postanovka na migratsionnyj uchet: praktika primeneniya statʹi 322.3 UK RF // Penitentsiarnaya nauka. — 2015. — № 1 (29). — S. 10—14.

СВЕДЕНИЯ ОБ АВТОРЕ

Сенцов Вячеслав Владимирович. Адъюнкт.
Воронежский институт МВД России.
E-mail: slavasencov@mai.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Sentsov Vyacheslav Vladimirovich. Post-graduate cadet.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: slavasencov@mai.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: иностранный гражданин; лицо без гражданства; фиктивная регистрация; фиктивная постановка на учет.

Key words: foreign citizen; stateless person; fictitious registration; fictitious registration.

УДК 343.3

Е. И. Сидорова

СЛЕДСТВЕННАЯ ГРУППА КАК ОПТИМАЛЬНАЯ ОРГАНИЗАЦИОННАЯ ФОРМА ВЗАИМОДЕЙСТВИЯ СЛЕДОВАТЕЛЯ С ОПЕРАТИВНЫМИ ПОДРАЗДЕЛЕНИЯМИ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

INVESTIGATIVE TEAM AS AN OPTIMAL ORGANIZATIONAL FORM OF INTERACTION BETWEEN AN INVESTIGATOR AND OPERATIONAL UNITS IN THE INVESTIGATION OF CRIMES

В рамках статьи рассмотрена такая форма взаимодействия следователя с органами, как следственно-оперативная группа, проанализированы требования к формированию и функционированию следственно-оперативных групп, выделены основные способы планирования расследования в составе следственно-оперативной группы.

The article examines the form of interaction between an investigator and law enforcement agencies, such as an investigative-operational group, analyzes the requirements for the formation and functioning of investigative-operational groups, and highlights the main methods of planning investigations within an investigative-operational group.

Особенности механизма совершения преступлений, наличие широких возможностей их субъектов в противодействии правоохранительным органам и оговоренный ими перечень тактических задач расследования требует поиска наиболее оптимальных групповых организационных форм взаимодействия следователя с оперативными подразделениями при расследовании преступлений. Такая форма взаимодействия следственных и оперативных подразделений должна обеспечивать органичное сочетание процессуальных (гласных) и оперативно-розыскных (негласных) методов получения доказательств в условиях состязательности уголовного судопроизводства, без чего выявлять такие преступления, а также изобличить лиц, их совершивших, оказалось практически невозможным [1].

В течение своей долгой истории развития следственная практика показала, что значительные объемы сложной следственной работы в уголовном производстве требуют распределения ее между несколькими субъектами, использующими разные методы в решении общих задач. Таким образом, постепенно сложилось учение о групповом (бригадном) методе расследования преступлений, которое предусматривало проведение предварительного расследования не единолично следователем, а группой уполномоченных лиц.

Групповой метод расследования открывал новые возможности осуществления расследования одновременно в нескольких направлениях (возможность производства следственных действий и оперативно-розыскных мероприятий сразу в разных местах одновременно, с достаточно глубокой и параллельной проверкой всех версий, возможность сосредоточить усилия нескольких квалифицированных сотрудников на одном наиболее важном эпизоде или на этапе и т. д.).

В советское время групповой метод расследования преступлений нашел свое оформление в виде работы следственных и следственно-оперативных групп, при формировании следственных групп к ним «в помощь», как правило, придавались сотрудники оперативных подразделений, что давало основания для более правильного наименования данных групп — следственно-оперативные группы (далее — СОГ) [2].

Следственно-оперативная группа по своей сути представляет собой организационную форму взаимодействия следователей, сотрудников оперативных и других подразделений полиции с целью выявления, фиксации, изъятия и упаковки следов преступления, вещественных доказательств, установления свидетелей и потерпевших, выяснения обстоятельств преступления, имеющих значение для всестороннего, полного и беспристрастного их исследования и установления лиц, совершивших преступление. Следует отметить, что СОГ, как правило, создаются преимущественно для расследования преступлений отдельных видов или групп. Представляется, что именно

с этих позиций целесообразно рассматривать СОГ как организационную форму взаимодействия следователей и сотрудников оперативных подразделений по расследованию преступлений. В то же время в организации деятельности следственно-оперативных групп в досудебном расследовании существует проблема, которая связана с соблюдением принципа непосредственности в исследовании доказательств. Это, в частности, может быть использовано стороной защиты в суде как основание для сомнения в допустимости доказательств, полученных теми или иными членами СОГ при проведении следственных действий и оперативно-розыскных мероприятий. Для сведения к минимуму возможности возникновения такой ситуации необходимо надлежащее взаимное информирование о ходе расследования, которое осуществляется отдельными членами группы. Это должно касаться принятых процессуальных решений, протоколов следственных действий, наличия тех или иных ключевых доказательств и их оценки — по ним должны быть проинформированы все члены группы.

Следует обратить внимание, что весь ход расследования преступления должен обеспечивать достоверность и допустимость получаемых сведений, обоснованность выводов и решений, возможность проведения анализа доводов, оснований и аргументов [3].

Для того чтобы любой член группы, самостоятельно не получавший из первоисточника соответствующую информацию, получил ее от другого следователя и имел возможность должным образом оперировать этими сведениями (доказательствами), они должны быть истинными и достоверными. К примеру, если доказательства на всем пути своего формирования проходят через нескольких субъектов (например, свидетеля, следователя, проводившего допрос, другого следователя — члена группы), то при несоблюдении требования надлежащей фиксации сведений они могут быть так извращены, что это приведет к потере их достоверности. Таким образом, в многоступенчатом процессе познания, который имеет место при групповом расследовании преступлений, важнейшим аспектом выступает обеспечение всех членов СОГ достоверными сведениями, потому что они оказывают существенное влияние на выполнение отдельных задач каждым членом следственно-оперативной группы.

Анализ научных публикаций и нормативных правовых актов, на которые они опираются, позволяет систематизировать информацию для определения принципиально важных требований к формированию и функционированию следственно-оперативных групп.

К числу данных требований можно отнести следующие [4]:

1. Своевременность создания СОГ. СОГ должны создаваться безотлагательно, как только определились задачи, решение которых невозможно одним субъектом судопроизводства, в частности, в установленные сроки. Представляется, что СОГ может быть создана как непосредственно к моменту начала предварительного расследования (например, при окончании документирования оперативно-розыскными мероприятиями признаков экономических преступлений и т. п.), так и после его начала (например, при поступлении материалов проверки от государственных контролирующих органов). Опоздание в создании СОГ и начале ее работы может привести к потере определенной части доказательств в условиях противодействия расследованию со стороны организованных преступных групп.

2. Компетентность создания. В соответствии с ч. 2 ст. 163 УПК РФ указанные группы должны образовываться на основании решения компетентного должностного лица — руководителя следственного органа надлежащего уровня, определяемого масштабностью преступления, его особой общественной значимостью и т. п. (например, совершение экономического преступления организованной группой с межгосударственными связями требует создания СОГ соответствующего уровня).

3. Привлечение к работе группы сотрудников различных подразделений. В частности, к работе в составе СОГ следственными органами привлекаются сотрудники не только оперативных подразделений, но и других подразделений правоохранительных органов, которые выполняют разные функции и используют разные методы и помощь которых нужна для решения определенных задач [5].

4. Временный характер деятельности. Деятельность таких групп всегда ограничивается во времени в отличие от других (штатных) формирований, например следственного подразделения или подразделения уголовного розыска. Это связано с тем, что деятельность указанных групп не предусмотрена штатным расписанием в структуре правоохранительных органов, поскольку они создаются для расследования определенного преступления.

5. Освобождение членов СОГ от исполнения текущих служебных обязанностей. Вовлеченные в группу сотрудники разных подразделений должны быть освобождены от исполнения своих обязанностей по штатному расписанию и подчинены только руководителю СОГ, которым является следователь. Это нужно для того, чтобы они

могли сосредоточиться на решении задач расследования конкретного преступления (преступлений). Несоблюдение этого требования порождает конкуренцию между текущими задачами определенного должностного лица и порученными заданиями в расследовании конкретного преступления и может привести к негативным последствиям.

6. Приоритет процессуального руководства. Руководителем СОГ всегда должно назначаться лицо, которое реально может отвечать за результаты проведенных на стадии возбуждения уголовного дела мероприятий и принятых решений и владеет процессуальными полномочиями согласно УПК РФ. Такими руководителями назначаются следователи (старшие следователи) по особо важным делам, которые имеют значительный опыт расследования преступлений определенной направленности.

7. Общность целей и задач. Следователи и оперативные сотрудники, включенные в состав СОГ, должны находиться в едином организационно-управленческом объединении, направленном на достижение единой цели — качественное расследование преступления. В этом объединении каждый из них должен осознавать, что он выполняет свой объем работы с помощью своих профессиональных знаний и практических умений, различных форм, методов и средств, свойственных характеру его профессиональной деятельности. Это требование реализуется путем создания творческой рабочей атмосферы, каждый член группы должен чувствовать свою принадлежность к этому профессиональному объединению, а это требует психологической совместимости ее членов и доброжелательных профессиональных отношений [5].

8. Постоянство (стабильность) состава группы. Данное требование означает, что формирование ее состава должно быть таким, чтобы он обеспечил неизменность СОГ к окончанию предварительного расследования. Периодические изменения ее руководства и состава на практике приводят к затягиванию расследования (новым членам нужно время для ознакомления с материалами дела и осознания своих функций), нежелательной утечке следственной информации, что значительно тормозит следствие и приводит к появлению затруднений, а иногда и к потере уголовным производством судебной перспективы.

Представляется, что именно при соблюдении приведенных требований формирования и функционирования СОГ создаются надлежащие условия для органичного сочетания процессуальных и оперативно-розыскных методов в процедуре поиска и фиксации улик.

Важным аспектом деятельности СОГ выступает вопрос планирования. Безусловно, своевременность и полнота всего расследования будет зависеть от того, как качественно, тактически правильно, в установленные сроки и в рамках действующего уголовно-процессуального законодательства исполняются следственные действия и оперативно-розыскные мероприятия членами СОГ. Грамотное составление четкого плана следственных и оперативных действий является обязательным залогом эффективного и быстрого расследования уголовного дела. Помимо этого, исполнение пунктов плана действий СОГ дает возможность обеспечить надлежащую организацию досудебного производства [6].

Вопросы грамотного составления плана расследования преступлений неоднократно являлись предметом рассмотрения в научной доктрине. Вместе с тем применительно к СОГ процесс планирования предстоящей деятельности обладает определенной спецификой, обусловленной тем, что он представляет собой некий мыслительный процесс, который заключается в установлении предстоящих задач следователя и выборе максимально эффективных способов, а также средств их разрешения в установленные уголовно-процессуальным кодексом сроки.

В современной следственной практике выделяются следующие способы планирования расследования в составе СОГ [7]:

1. Разработка и формирование общего плана следственных действий и оперативно-розыскных мероприятий, на базе которого потом составляют индивидуальные планы.

2. Разработка и формирование индивидуальных планов следственных действий и оперативно-следственных мероприятий членов СОГ, а затем сведение их в общий план.

3. Разработка и формирование только индивидуальных планов членов СОГ, общий план работы группы не формируется.

4. Разработка и формирование только общего плана расследования без индивидуального плана действий, необходимых к проведению каждым членом следственно-оперативной группы.

Безусловно, если исходить из принципа рациональности в оценке выделенных выше способов планирования, то наиболее целесообразен к применению первый способ, а наиболее прост в плане составления общего плана расследования — второй, поэтому у него больше шансов для применения на практике. Третий и четвертый способы наименее целесообразны, их применение не сможет гарантировать успешное решение всего комплекса задач, стоящих перед следственно-оперативной группой в ходе раскрытия и расследования преступных деяний. Необходимо отметить,

что ранее отдельными советскими учеными, в частности В. А. Толоконниковым, указывалось на целесообразность составления отдельно плана следственных и плана оперативно-розыскных мероприятий, но отмечается, что данные планы должны быть обязательно согласованы между собой. Целесообразность наличия двух планов в работе СОГ Толоконников В. А. обосновывал достижением четкого разграничения следственных действий и оперативно-розыскных мер [8].

Подобная инициатива представляется излишней и не востребована следственной практикой с учетом того факта, что создание следственно-оперативных групп в рамках расследования преступления носит исключительный характер, общим правилом же является проведение расследования преступления следователем единолично. Кроме того, очень сложно будет добиться согласования пунктов обоих планов, не определив общих направлений действий с постановкой цели, круга решаемых основных и промежуточных задач и т. п. Всё это на практике неизбежно приведет к сложностям, особенно при изменении ситуации по делу и корректировке обоих планов, а также необходимости их повторной проверки на соответствие.

В общем плане расследования СОГ не следует отражать ход и содержание мероприятий, проведенных с использованием негласных средств и методов работы. Данные мероприятия фиксируются, однако не в общем плане расследования, а в индивидуальных планах оперативных сотрудников, обеспечивающих оперативно-розыскное сопровождение расследования. В общий же план расследования вносятся главные задачи, поставленные перед оперативными сотрудниками в процессе их работы в составе данной следственно-оперативной группы. В частности, поиск и выявление свидетелей преступлений при помощи проведения оперативно-розыскных мероприятий, поиск мест сбыта похищенного имущества и т. п. Отдельные ученые полагают, что общий план расследования обязательно должен составляться руководителем СОГ единолично. Поэтому на этапе планирования руководитель должен составлять общий план с привлечением старшего из приданных в его распоряжение органом дознания оперативных сотрудников, что позволит реально оценить и максимально эффективно использовать оперативный ресурс. На заключительном этапе планирования происходит контроль исполнения пунктов плана и оценка выполнения предусмотренных планом следственных, оперативно-розыскных и иных мероприятий. Контроль осуществляет руководитель СОГ. При выявлении новой информации, имеющей значение для расследования, являющейся основой для подтверждения или опровержения следственных версий уголовного дела, общий план расследования подлежит корректировке и цикл планирования повторяется до определения способов разрешения поставленных перед следствием задач.

Важным практическим моментом планирования действий СОГ является недопущение их производства в ночное время, установленное в ч. 3 ст. 164 УПК РФ. В данной связи следует отметить, что на практике производство неотложных следственных действий ночью допускается. Так, президиум Нижегородского областного суда в постановлении от 25.07.2018 № 44У-84/2018 признал законным проведение осмотра места происшествия с участием собственника помещения, в период с 21 часа 20 минут до 22 часов 20 минут на основании информации об изготовлении наркотических средств, поступившей в ОМВД России по Балахнинскому району Нижегородской области [9].

Решение о допустимости принимает суд, о чем неоднократно отмечалось в постановлениях не только Верховного Суда РФ, но и Конституционного Суда РФ. В частности, определением Конституционного Суда РФ от 20.12.2018 № 3356-О был дан отказ по жалобе А. В. Сартакова [10].

Кроме того, в ч. 5 ст. 164 УПК РФ отмечается положение, что следователь, привлекая к предварительному расследованию иных участников уголовного судопроизводства, должен разъяснять им права, ответственность и непосредственно сам порядок тех процессуальных действий, которые эти участники должны будут совершить. В этой связи недопустимо использовать фиктивные показания участников уголовного судопроизводства. Данное обстоятельство стало причиной отмены приговора Черёмушкинского районного суда города Москвы от 23.08.2018 Судебной коллегией по уголовным делам Московского городского суда [11].

В рамках рассмотрения упомянутого выше приговора в отношении Н. и Е., осужденных по п. «г» ч. 4 ст. 228.1 УК РФ, в апелляционной инстанции судом в числе нарушений, совершенных членами СОГ, было установлено, что следователем, руководителем СОГ, принявшим уголовное дело к производству, допросов свидетелей не проводилось, он «ограничился приобщением копий материалов дел, ранее выделенных в отношении неустановленных лиц, сбывших наркотические средства лицам, задержанным сотрудниками полиции» [12].

В ряде случаев в правоприменительной практике важным моментом выступает также вопрос смены руководителя СОГ, который нередко при-

ходится решать незапланированно и в максимально короткие сроки. Данное обстоятельство часто становится основанием направления апелляционных жалоб адвокатами. Так, в апелляционной жалобе адвоката обвиняемого Ф., поданной на постановление Ленинского районного суда Республики Удмуртия, тот указал на смену руководства СОГ в процессе как на существенное нарушение уголовно-процессуального закона [13].

Кроме того, адвокатом было также указано на неознакомление обвиняемого о производстве предварительного следствия СОГ. Поэтому подход к принятию данного решения также должен быть взвешенным.

Помимо этого, очень часто в следственной практике применяют типовые общие планы расследования, типовые системы версий (по определенным категориям уголовных дел), типовые алгоритмы и программы расследования похожих преступлений. Безусловно, их применение значительно упрощает работу СОГ и сокращает время, необходимое для раскрытия и расследования преступления. Вместе с тем их применение должно быть очень аккуратным и четко учитывать конкретные обстоятельства уголовного дела, находящегося в производстве руководителя СОГ. В частности, в отношении обоснованности применения типового программного способа расследования нельзя не отметить, что программный алгоритм не всегда может предусмотреть правильное разрешение проблемных ситуаций, так как каждое преступление обладает индивидуальной спецификой. Поэтому, с нашей точки зрения, на современном этапе развития технологий типовые программы расследования целесообразно применять только в качестве некой справочной информации.

Особо тщательно следует подходить к планированию расследования уголовных дел, в которых планируется назначение различного рода экспертиз. Так, апелляционным постановлением Московского городского суда по делу № 10-3495/2017 был отменен приговор Басманного районного суда в отношении гр. К, работающего инженером, осужденного по ст. 138.1 УК РФ за незаконный сбыт видеокамеры в виде автобрелка с возможностью скрытого визуального наблюдения и документирования на 4 месяца лишения свободы. Основанием послужило то обстоятельство, что выводы технической экспертизы вызвали у стороны защиты обоснованные сомнения в компетентности и надлежащей квалификации привлеченного следствием эксперта [14].

Таким образом, подводя итог, представляется, что с учетом вышеизложенного вполне обоснованным является признание СОГ оптимальной организационной формой взаимодействия следователя с оперативными подразделениями при расследовании преступлений, особенно тех, что совершаются организованными группами лиц.

ЛИТЕРАТУРА

1. Пантюхина Г. А. Взаимодействие следователей и оперативных сотрудников при расследовании преступлений по делам организованных преступных групп // Вопросы следственной и оперативно-розыскной деятельности. — 2011. — № 5. — С. 57.

2. Баловина И. В. Становление и развитие отечественного института производства предварительного следствия следственной группой // Образование. Наука. Научные кадры. — 2021. — С. 154.

3. Мельников В. Ю. Проблемы доказывания по уголовным делам. — Ростов-на-Дону : Фонд науки и образования, 2020. — С. 81.

4. Ларичев В. Д., Кучкина В. Г. Понятие и сущность следственной и следственно-оперативной групп // Вестник Воронежского института МВД России. — 2016. — № 1. — С. 119.

5. Батурин В. Ю. Основные принципы деятельности следственно-оперативной группы в раскрытии и расследовании преступлений // Вестник экономики, управления и права. — 2024. — № 4. — С. 55—57.

6. Гаврилин Ю. В. Некоторые проблемы организации взаимодействия органов расследования с подразделениями ФСИН и пути их разрешения // Уголовно-исполнительная система: право, экономика, управление. — 2015. — № 4. — С. 11.

7. Кремнева Е. А. Характерные ошибки при производстве первоначальных следственных действий // Российский следователь. — 2018. — № 8. — С. 17.

8. Толоконников В. К Актуальные вопросы планирования при расследовании преступлений // Вестник СГА. — 2014. — № 1. — С. 136.

9. Постановление Президиума Нижегородского областного суда от 25.07.2018 № 44У-84/2018. — URL: http://www.pravo.gov.ru (дата обращения: 10.02.2026).

10. Об отказе к принятию к рассмотрению жалобы гражданина Сартакова А. В. на нарушение его конституционных прав ч. 3 ст. 164 УПК РФ : определение Конституционного Суда РФ от 20.12.2018 № 3356-О. — URL: http://www.pravo.gov.ru (дата обращения: 10.02.2026).

11. Апелляционное определение Московского городского суда от 12.12.2018 № 10-20478/2018. — URL: http://www.pravo.gov.ru (дата обращения: 10.02.2026).

12. Апелляционное определение Московского городского суда от 12.12.2018

№ 10-20478/2018. — URL: http://www.pravo.gov.ru(дата обращения: 10.02.2026).

13. Апелляционное постановление Верховного суда Удмуртской республики от 22.05.2015 № 10-20478/2018. — URL: http://www.pravo.gov.ru (дата обращения: 10.02.2026).

14. Апелляционное постановление Московского городского суда по делу № 10-3495/2017. — URL: http://www.pravo.gov.ru (дата обращения: 10.02.2026).

REFERENCES

1. Pantyukhina G. A. Vzaimodejstvie sledovatelej i operativnykh sotrudnikov pri rassledovanii prestuplenij po delam organizovannykh prestupnykh grupp // Voprosy sledstvennoj i operativno-rozysknoj deyatel′nosti. — 2011. — № 5. — S. 57.

2. Balovina I. V. Stanovlenie i razvitie otechestvennogo instituta proizvodstva predvaritel′nogo sledstviya sledstvennoj gruppoj // Obrazovanie. Nauka. Nauchnye kadry. — 2021. — S. 154.

3. Mel′nikov V. Yu. Problemy dokazyvaniya po ugolovnym delam. — Rostov-na-Donu : Fond nauki i obrazovaniya, 2020. — S. 81.

4. Larichev V. D., Kuchkina V. G. Ponyatie i sushchnost′ sledstvennoj i sledstvenno-operativnoj grupp // Vestnik Voronezhskogo instituta MVD Rossii. — 2016. — № 1. — S. 119.

5. Baturin V. Yu. Osnovnye printsipy deyatel′nosti sledstvenno-operativnoj gruppy v raskrytii i rassledovanii prestuplenij // Vestnik ekonomiki, upravleniya i prava. — 2024. — № 4. — S. 55—57.

6. Gavrilin Yu. V. Nekotorye problemy organizatsii vzaimodejstviya organov rassledovaniya s podrazdeleniyami FSIN i puti ikh razresheniya // Ugolovno-ispolnitel′naya sistema: pravo, ekonomika, upravlenie. — 2015. — № 4. — S. 11.

7. Kremneva E. A. Kharakternye oshibki pri proizvodstve pervonachal′nykh sledstvennykh dejstvij // Rossijskij sledovatel′. — 2018. — № 8. — S. 17.

8. Tolokonnikov V. K Aktual′nye voprosy planirovaniya pri rassledovanii prestuplenij // Vestnik SGA. — 2014. — № 1. — S. 136.

9. Postanovlenie Prezidiuma Nizhegorodskogo oblastnogo suda ot 25.07.2018 № 44U-84/2018. — URL: http://www.pravo.gov.ru (data obrashcheniya: 10.02.2026).

10. Ob otkaze k prinyatiyu k rassmotreniyu zhaloby grazhdanina Sartakova A. V. na narushenie ego konstitutsionnykh prav ch. 3 st. 164 UPK RF : opredelenie Konstitutsionnogo Suda RF ot 20.12.2018 № 3356-O. — URL: http://www.pravo.gov.ru (data obrashcheniya: 10.02.2026).

11. Apellyatsionnoe opredelenie Moskovskogo gorodskogo suda ot 12.12.2018 № 10-20478/2018. — URL: http://www.pravo.gov.ru (data obrashcheniya: 10.02.2026).

12. Apellyatsionnoe opredelenie Moskovskogo gorodskogo suda ot 12.12.2018 № 10-20478/2018. — URL: http://www.pravo.gov.ru (data obrashcheniya: 10.02.2026).

13. Apellyatsionnoe postanovlenie Verkhovnogo suda Udmurtskoj respubliki ot 22.05.2015 № 10-20478/2018. — URL: http://www.pravo.gov.ru (data obrashcheniya: 10.02.2026).

14. Apellyatsionnoe postanovlenie Moskovskogo gorodskogo suda po delu № 10-3495/2017. — URL: http://www.pravo.gov.ru (data obrashcheniya: 10.02.2026).

СВЕДЕНИЯ ОБ АВТОРЕ

Сидорова Елена Ивановна. Заместитель начальника кафедры уголовного процесса.
Воронежский институт МВД России.
E-mail: sidorova_vrn_2023@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Sidorova Elena Ivanovna. Deputy head of the chair of Criminal Procedure.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: sidorova_vrn_2023@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53

Ключевые слова: расследование уголовных дел; следственные подразделения; оперативные подразделения; следственно-оперативная группа; взаимодействие.

Key words: investigation of criminal cases; investigative units; operational units; investigative and operational group; interaction.

УДК 343.123.1

П. Г. Смагин

ЦИФРОВОЙ РУБЛЬ КАК ИНСТРУМЕНТ ПРОТИВОДЕЙСТВИЯ ФИНАНСОВЫМ ПРЕСТУПЛЕНИЯМ: ПЕРСПЕКТИВЫ И ОГРАНИЧЕНИЯ

THE DIGITAL RUBLE AS A TOOL FOR COUNTERING FINANCIAL CRIMES: PROSPECTS AND LIMITATIONS

В статье проводится комплексный анализ потенциала цифрового рубля как инструмента противодействия финансовым преступлениям в сравнении с существующими формами денег и частными цифровыми активами. На основе анализа текущего законодательства, научных публикаций и судебной практики автор выявляет ключевые преимущества цифрового рубля центрального банка России для повышения прозрачности финансовых потоков, борьбы с отмыванием доходов и коррупционными правонарушениями. Параллельно исследуются риски и ограничения, связанные с внедрением цифрового рубля: технические уязвимости, проблемы конфиденциальности, необходимость модернизации правоохранительной системы и адаптации уголовно-правовых и уголовно-процессуальных норм.

The article provides a comprehensive analysis of the potential of the digital ruble as a tool for countering financial crimes, compared to existing forms of money and private digital assets. Based on an analysis of current legislation, scientific publications, and judicial practice, the author identifies the key advantages of the digital ruble issued by the Central Bank of Russia for improving the transparency of financial flows, combating money laundering, and addressing corruption-related offenses. Additionally, the article explores the risks and limitations associated with the implementation of the digital ruble, including technical vulnerabilities, privacy concerns, and the need for modernizing the law enforcement system and adapting criminal law and procedure regulations.

Цифровая трансформация финансовой системы носит глобальный и необратимый характер. Одним из ее наиболее значимых проявлений является разработка центральными банками разных стран мира собственных цифровых валют. В России этот процесс воплощается в проекте цифрового рубля — третьей формы национальной валюты наряду с наличными и безналичными деньгами. Если наличные расчеты обеспечивают анонимность, а безналичные — контроль со стороны банков и государственных органов, то цифровой рубль, согласно концепции Банка России, призван совместить удобство электронных платежей с прямой эмиссией и инфраструктурой регулятора.

В 2021 году Центральным банком России была подготовлена Концепция цифрового рубля [1], положения которой нашли свое отражение и закрепили правовой статус цифрового рубля в федеральных законах «О Центральном банке Российской Федерации (Банке России)» [2], «О национальной платежной системе» [3], «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [4], Гражданском кодексе РФ и ряде других нормативных документах. Цифровой рубль является законным платежным средством, что отличает его от цифровой валюты (криптовалюты), которая, как подробно анализируют М. В. Арзамасцев и В. А. Никулина, признается имуществом (ст. 141.1 ГК РФ) [5]. Это различие критически важно: операции с законным платежным средством изначально попадают в сферу действия финансового регулирования и надзора, в то время как квалификация действий с криптовалютой как имуществом (например, для ст. 174, 174.1 Уголовного кодекса РФ о легализации) до сих пор вызывает сложности в судебной практике.

Немаловажную роль при решении вопроса о создании и внедрении цифрового рубля в России имеет «теневая экономика», к основным формам проявления которой авторы относят:

- «серые» заработные платы — частичную или полную выплату доходов вне официального учета, что лишает работников социальных гарантий и будущих пенсионных прав;

- уклонение бизнеса от налогов и страховых взносов, в том числе через сложные схемы между юридическими лицами;

- нелегальную деятельность (наркоторговлю, контрабанду, незаконный оборот оружия и др.),

часто вовлекающую социально уязвимые группы населения.

Международные оценки теневой экономики для России прогнозировались около 39% ВВП в 2025 году, что значительно превышает среднемировой уровень [6]. Внедрение цифрового рубля, на наш взгляд, позволит оказать прямое воздействие на уровень теневой экономики в России.

Цифровые валюты в настоящее время являются популярным инструментом для организованных преступных групп благодаря псевдоанонимности и децентрализованному характеру, что создает пробелы в регулировании и снижает риск обнаружения незаконных транзакций. При этом, как справедливо указывают Э. Л. Сидоренко и З. И. Хисамова [7], любая реформа финансовой системы, особенно внедрение нового цифрового инструмента, неизбежно становится катализатором новых форм преступных посягательств.

К ключевым элементам и механизмам функционирования цифрового рубля можно отнести: токенизацию рубля (уникальный программный код для защиты от изменений); аутентифицированные цифровые кошельки; централизованное администрирование Банком России; цифровой след и автоматический контроль; сокращение роли наличных денег.

Таким образом, цифровой рубль, с одной стороны, можно рассматривать как потенциально эффективный инструмент повышения прозрачности и контроля за финансовыми операциями, а с другой — как новый инструмент и среду для совершения киберпреступлений.

Цифровой рубль функционирует на основе двухуровневой модели: Банк России осуществляет эмиссию и ведет централизованный реестр (платформу), а финансовые организации (банки) предоставляют клиентам доступ к кошелькам и обслуживанию. Эта архитектура фундаментально отличается от анонимных и децентрализованных криптовалют (например, Bitcoin) и от стейблкоинов, выпускаемых частными компаниями.

Все транзакции с цифровым рублем фиксируются в инфраструктуре Банка России. Это создает единую защищенную точку учета, в отличие от фрагментированных данных в традиционной банковской системе. Технология цифрового рубля позволяет внедрять автоматизированные правила (смарт-контракты) исполнения платежей (например, целевое использование бюджетных средств, автоматические отчисления), что усложняет нецелевое расходование и хищения. В отличие от анонимных наличных и псевдоанонимных криптовалют доступ к цифровому рублю будет жестко привязан к идентифицированным клиентам банков.

Можно выделить несколько ключевых преимуществ цифрового рубля как инструмента противодействия финансовым преступлениям.

1. Повышение прозрачности и мониторинга финансовых потоков. Централизованный реестр Банка России позволяет в режиме, установленном законом (прежде всего, Федеральным законом № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»), осуществлять мониторинг транзакций. В отличие от текущей системы, где данные разрознены по тысячам кредитных организаций, цифровой рубль создает целостную картину движения средств.

2. Борьба с отмыванием доходов (легализацией). Программируемость цифрового рубля открывает возможности для использования встроенных механизмов контроля за переводами. Смарт-контракты могут автоматически проверять соответствие транзакций требованиям законов, маркировать средства, поступающие от государственных контрактов, или ограничивать операции с ними. По оценкам Банка России и экспертов, массовое использование цифрового рубля позволит выявлять до 70% подозрительных переводов и снизит объёмы отмывания денег внутри страны примерно на 20% [8].

3. Противодействие коррупционным правонарушениям, которые в последние время все чаще совершаются с использованием криптовалют (взятки, коммерческий подкуп, нецелевое использование бюджетных средств). Цифровой рубль, при условии обязательного декларирования его наличия госслужащими (что уже предусмотрено законодательством), усложняет сокрытие незаконных доходов. Транзакции, даже если они пытаются быть замаскированными, остаются в реестре ЦБ и могут быть восстановлены и проанализированы в ходе расследования. Кроме того, целевые бюджетные средства, переведенные в цифровых рублях, легче отследить на предмет нецелевого использования.

4. Повышение эффективности применения мер процессуального принуждения. Наложение ареста и конфискация цифровых активов сегодня представляет большую проблему. И. А. Безенков, исследуя правоприменительную практику рассматривает возможность ареста криптовалюты путем перевода на кошелек, контролируемый органами предварительного расследования, и последующей конфискации данных средств [9], однако этот процесс требует специальных технических знаний. Для цифрового рубля механизм ареста может быть реализован в упрощенной форме — через платформу Банка России по решению суда,

что сделает процедуру более простой и не требующей от следователей навыков обращения с криптокошельками.

Рассмотренные направления использования цифрового рубля в выявлении и расследовании преступлений могут быть реализованы следователем в следующих формах:

1. Запрос на получение информации (ч. 4 ст. 21 УПК РФ) может быть направлен в Банк России (оператору платформы цифрового рубля) или участникам платформы (банкам) при проверке сообщения о преступлении либо при производстве расследования по уголовному делу. Запрашиваются данные о кошельке; история операций; сведения о владельце и доступах.

2. В рамках расследования уголовного дела по постановлению суда возможно наложение ареста на денежные средства в цифровых рублях, который реализуется не физическим изъятием, а ограничением операций на уровне платформы ЦБ путем блокировки переводов.

3. Обыск и выемка электронных носителей информации с участием специалиста и копирование с них данных при производстве следственных действий.

4. Осмотр электронных носителей информации, изъятых ранее в ходе осмотра места происшествия, обыска или выемки с участием специалиста.

5. Осмотр мобильных устройств, сайтов, приложений на предмет использования цифровых рублей, транзакций с их участием, учетных записей, связанных с доступом к кошельку.

6. Обыск и выемка ключей доступа, токенов, логинов и иных данных для аутентификации и авторизации в банковской системе и приложениях для работы с цифровыми рублями.

7. Назначение и производство экспертиз (финансово-экономических, бухгалтерских, компьютерно-технических), направленных на установление цепочки операций; связи между кошельками; времени и способа распоряжения средствами.

Несмотря на рассмотренные нами позитивные перспективы, внедрение цифрового рубля сопряжено с серьезными рисками, которые могут не только нивелировать его преимущества, но и породить новые угрозы.

1. Технические уязвимости и киберугрозы. Как справедливо опасаются Э. Л. Сидоренко и З. И. Хисамова, инфраструктура цифрового рубля станет целью для хакеров. Успешная атака на платформу ЦБ или на банки-операторы может привести к катастрофическим последствиям: хищению средств, блокированию платежной системы, подрыву доверия к государству и т. д. [7]. Риск усугубляется офлайн-функционалом кошельков, где возможны «двойное списание» или потеря средств при переходе между онлайн- и офлайн-режимами, что может спровоцировать волну мошеннических действий.

2. Проблемы конфиденциальности и полный контроль над гражданами и организациями. Обратная сторона прозрачности — риск установления тотального финансового надзора со стороны государства. Цифровой рубль теоретически позволяет отслеживать каждую покупку гражданина. Это создает угрозу монополизации данных и их использования не по назначению. Необходим четкий законодательный баланс между интересами следствия и правом граждан на финансовую приватность. Как отмечается в публикациях разных авторов, вопрос защиты данных и конфиденциальности остается одним из ключевых и в международных обсуждениях [9].

3. Неготовность правоохранительной системы и уголовного законодательства. Авторы единодушны в оценке: правоохранительные органы и суды не готовы к расследованию преступлений в новой цифровой среде. Э. Л. Сидоренко и З. И. Хисамова прямо указывают на «дефицит кадров» для расследования высокотехнологичных преступлений. Уголовное законодательство, как показывает исследование М. В. Арзамасцева и В. А. Никулиной, с трудом адаптируется даже к криптовалюте как к имуществу [5]. Для цифрового рубля потребуется четкая квалификация новых способов хищения, разработка методик расследования и проведения цифровых экспертиз, подготовка кадров, владеющих как юридическими, так и техническими знаниями.

Для повышения эффективности выявления, раскрытия и расследования преступлений с использованием цифрового рубля должны активно применяться технологии искусственного интеллекта [10], которые способны существенно повысить эффективность выявления и расследования преступлений через:

- анализ транзакционных данных: алгоритмы машинного обучения позволяют выявлять аномалии и подозрительные схемы, которые могут указывать на мошеннические действия;

- прогнозирование рисков: на основе исторических данных можно прогнозировать потенциальные угрозы и определять приоритетные направления расследований;

- автоматизацию отчетности и мониторинга: аналитические системы могут автоматически формировать отчеты о подозрительных операциях и уведомлять соответствующие органы в режиме реального времени;

- расширение возможностей расследования «традиционных» преступлений: нейросети способны анализировать текстовые и визуальные

данные, выявляя связи между участниками преступных схем.

Внедрение технологий, основанных на алгоритмах искусственного интеллекта, в работу правоохранительных органов позволит сократить время расследования преступлений, повысить точность выявления мошеннических операций, снизить нагрузку на специалистов, сосредоточив их внимание на сложных аналитических задачах, повысить доверие общества к цифровым финансовым инструментам через более безопасное их использование.

4. Социальная инженерия и мошенничество. Широкое внедрение нового финансового инструмента может привести к росту мошенничества с применением социальной инженерии, а также к массовым хищениям средств через фишинг, вишинг или вредоносное программное обеспечение.

Для значительной части населения цифровой рубль будет сложным и малопонятным инструментом. Мошенники традиционно используют такие периоды, представляясь сотрудниками банков, Центрального банка или «операторами цифрового рубля», убеждая жертву совершить нужные им действия, так как у многих граждан цифровой рубль напрямую ассоциируется с государством и Центральным банком, что повышает уровень доверия к любым коммуникациям, в которых фигурируют эти структуры.

Кроме того, цифровой рубль, как и любые современные платежные инструменты, будет активно использоваться через смартфоны. Это увеличивает риски заражения устройств вредоносными программами.

Если цифровой рубль станет обязательным или широко используемым средством расчётов (например, для социальных выплат, зарплат бюджетникам или госзакупок), мошеннические схемы приобретут массовый характер. Даже небольшой процент успешных атак при большом количестве пользователей может привести к значительным совокупным потерям и подрыву доверия к инструменту в целом.

5. Проблема определения ответственности. В случае технического сбоя, уязвимости в системе или хищения средств из-за действий третьих лиц возникнет ряд вопросов об ответственности перед гражданами: кто несет ответственность перед гражданином? Банк России как оператор платформы? Банк как провайдер кошелька? Сам пользователь, не обеспечивший безопасность устройства? Как отмечают исследователи, этот вопрос до сих пор не решен удовлетворительно даже для традиционных платежных систем.

6. Международное сотрудничество. Криптовалютные биржи и сервисы часто находятся в других странах, что затрудняет взаимодействие. Цифровой рубль, будучи национальной валютой, изначально имеет четкую юрисдикцию, однако для эффективного противодействия отмыванию преступных доходов, полученных в криптовалюте и конвертированных в цифровой рубль (или наоборот), необходимо международное сотрудничество, что в современных условиях представляется весьма проблематичным. На наш взгляд, необходимо выработать единые подходы и стандарты к регулированию криптовалют и цифровых активов.

К направлениям минимизации рассмотренных минусов внедрения цифрового рубля необходимо отнести:

1. Совершенствование нормативных правовых актов, регламентирующих порядок обращения цифрового рубля в России.

2. Технологическую безопасность: инфраструктура цифрового рубля должна разрабатываться с приоритетом на защиту и подвергаться регулярным независимым аудитам и тестам на проникновение.

3. Модернизацию правоохранительной системы путем создания специализированных подразделений в правоохранительных органах, оснащенных современными техническими средствами и укомплектованных подготовленными кадрами.

4. Массовую разъяснительную кампанию о правилах безопасности при использовании цифрового рубля. Создание простых и эффективных механизмов восстановления доступа и возмещения ущерба в случаях, не связанных с виной пользователя.

5. Создание механизмов эффективного международного сотрудничества (возможно, через третьи «дружественные» страны) в рамках FATF (группа разработки финансовых мер борьбы с отмыванием денег), Интерпола, ЕАЭС по выработке общих стандартов регулирования криптовалют и взаимодействия при расследовании трансграничных преступлений.

Таким образом, цифровой рубль представляет собой весьма эффективный инструмент в борьбе с финансовыми преступлениями. С одной стороны, его архитектура, основанная на централизованном реестре, идентификации пользователей и программируемости, открывает широкие возможности для повышения прозрачности финансового оборота, автоматизации контроля за противоправными действиями, а с другой — внедрение цифрового рубля порождает серьезные риски: от кибератак на критическую финансовую инфраструктуру до установления полного контроля над частной жизнью граждан. В то же время нерешенными остаются вопросы ответственности и готовности правоохранительной системы к расследованию таких

категорий преступлений. С 2026 года планируется запуск пилотного этапа выплат заработной платы отдельным категориям работников бюджетной сферы в цифровых рублях [11], что позволит протестировать технологическую и правовую готовность системы, а также оценить социально-экономические эффекты нововведения, включая рост прозрачности бюджетных расходов, сокращение издержек и усиление контроля за целевым использованием денежных средств.

ЛИТЕРАТУРА

1. Концепция цифрового рубля (подготовлена Банком России). — URL: https://cbr.ru/Content/Document/File/120075/concept_08042021.pdf (дата обращения: 12.01.2026).

2. О Центральном банке Российской Федерации (Банке России) : Федеральный закон от 10.07.2002 № 86-ФЗ // СПС «КонсультантПлюс» (дата обращения: 16.01.2026).

3. О национальной платежной системе : Федеральный закон от 27.06.2011 № 161-ФЗ // СПС «КонсультантПлюс» (дата обращения: 19.01.2026).

4. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма : Федеральный закон от 07.08.2001 № 115-ФЗ // СПС «КонсультантПлюс» (дата обращения: 16.01.2026).

5. Арзамасцев М. В., Никулина В. А. Цифровая валюта как легализуемое имущество // Журнал российского права. — 2025. — № 5. — С. 122—135.

6. Сергеев В. М., Шадурская М. М., Бойтуш О. А. Цифровой рубль как средство противодействия теневой экономике в Российской Федерации // Креативная экономика. — 2021. — Т. 15. — № 7. — С. 2827—2846.

7. Сидоренко Э. Л., Хисамова З. И. Основные криминологические риски внедрения цифрового рубля // Безопасность бизнеса. — 2022. — № 2. — С. 45—49.

8. Никаких больше «отмывов»: вступил в силу закон по выведению преступников с цифровыми рублями на чистую воду // URL: https://www.comnews.ru/content/239927/2025-07-01/2025-w27/1008/ (дата обращения: 12.01.2026).

9. Безенков И. А. Международный опыт противодействия коррупционным правонарушениям, совершаемым с использованием цифровой валюты // Законность. — 2024. — № 4. — С. 44—48.

10. Смагин П. Г. Использование моделей машинного обучения при расследовании преступлений в сфере информационных технологий // Вестник Воронежского института МВД России. — 2024. — № 1. — С. 306—313.

11. Никтовенко Е., Славин Б. Опыт на бюджетниках. Первые выплаты в цифровом рубле начнутся в 2026 году // АиФ. — 2025. — 27 мая // URL: https://aif.ru/money/mymoney/ (дата обращения: 18.01.2026).

REFERENCES

1. Kontseptsiya tsifrovogo rublya (podgotovlena Bankom Rossii). — URL: https://cbr.ru/Content/Document/File/120075/concept_08042021.pdf (data obrashcheniya: 12.01.2026).

2. O Tsentral′nom banke Rossijskoj Federatsii (Banke Rossii) : Federal′nyj zakon ot 10.07.2002 № 86-FZ // SPS «Konsul′tantPlyus» (data obrashcheniya: 16.01.2026).

3. O natsional′noj platezhnoj sisteme : Federal′nyj zakon ot 27.06.2011 № 161-FZ // SPS «Konsul′tantPlyus» (data obrashcheniya: 19.01.2026).

4. O protivodejstvii legalizatsii (otmyvaniyu) dokhodov, poluchennykh prestupnym putem, i finansirovaniyu terrorizma : Federal′nyj zakon ot 07.08.2001 № 115-FZ // SPS «Konsul′tantPlyus» (data obrashcheniya: 16.01.2026).

5. Arzamastsev M. V., Nikulina V. A. Tsifrovaya valyuta kak legalizuemoe imushchestvo // Zhurnal rossijskogo prava. — 2025. — № 5. — S. 122—135.

6. Sergeev V. M., Shadurskaya M. M., Bojtush O. A. Tsifrovoj rubl′ kak sredstvo protivodejstviya tenevoj ekonomike v Rossijskoj Federatsii // Kreativnaya ekonomika. — 2021. — T. 15. — № 7. — S. 2827—2846.

7. Sidorenko E. L., Khisamova Z. I. Osnovnye kriminologicheskie riski vnedreniya tsifrovogo rublya // Bezopasnost′ biznesa. — 2022. — № 2. — S. 45—49.

8. Nikakikh bol′she «otmyvov»: vstupil v silu zakon po vyvedeniyu prestupnikov s tsifrovymi rublyami na chistuyu vodu // URL: https://www.comnews.ru/content/239927/2025-07-01/2025-w27/1008/ (data obrashcheniya: 12.01.2026).

9. Bezenkov I. A. Mezhdunarodnyj opyt protivodejstviya korruptsionnym pravonarusheniyam, sovershaemym s ispol′zovaniem tsifrovoj valyuty // Zakonnost′. — 2024. — № 4. — S. 44—48.

10. Smagin P. G. Ispol′zovanie modelej mashinnogo obucheniya pri rassledovanii prestuplenij v

sfere informatsionnykh tekhnologij // Vestnik Voronezhskogo instituta MVD Rossii. — 2024. — № 1. — S. 306—313.

11. Niktovenko E., Slavin B. Opyt na byudzhetnikakh. Pervye vyplaty v tsifrovom ruble nachnutsya v 2026 godu // AiF. — 2025. — 27 maya // URL: https://aif.ru/money/mymoney/ (data obrashcheniya: 18.01.2026).

СВЕДЕНИЯ ОБ АВТОРЕ

Смагин Павел Геннадьевич. Старший преподаватель кафедры уголовного процесса.
Воронежский институт МВД России.
E-mail: pasha_smagin@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Smagin Pavel Gennadiyevitch. Senior lecturer of the chair of Criminal Proceeding.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: pasha_smagin@mail.ru
Wok address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: цифровой рубль; информационные технологии; легализация преступных доходов; расследование преступлений; арест на имущество.

Key words: digital ruble; information technology; legalization of criminal proceeds; investigation of crimes; seizure of property.

УДК 343.121

М. Н. Чачхиани

СИСТЕМАТИЗАЦИЯ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ПРЕВЕНЦИИ НЕЗАКОННОГО ОБОРОТА НАРКОТИЧЕСКИХ СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ

SYSTEMATIZATION OF ACTIVITIES IN THE FIELD OF PREVENTION OF ILLICIT TRAFFICKING IN NARCOTIC DRUGS AND PSYCHOTROPIC SUBSTANCES

В статье автор рассматривает систему превенции незаконного оборота наркотических, психотропных веществ и их прекурсоров. Автор выделяет и подробно анализирует каждый элемент превентивной деятельности, выявляя в них пробелы и недостатки. Делается акцент на необходимости оптимизации законодательства в этой сфере, а также внедрении новых превентивных механизмов.

In the article, the author examines the system of prevention of illicit trafficking in narcotic drugs, psychotropic substances and their precursors. The author highlights and analyzes in detail each element of preventive activities, identifying gaps and shortcomings in them. The emphasis is placed on the need to optimize legislation in this area, as well as the introduction of new preventive mechanisms.

Правовая база превенции незаконного оборота наркотических средств, психотропных веществ и их прекурсоров (далее — наркотики) достаточно объемна, нормы превенции весьма разнообразны и имеют некую дифференциацию как по вертикали, так и по горизонтали.

Как утверждает С. Н. Махина, «говорить о том, что модель регулирования превенции является самодостаточным, целостным комплексом, порождающим эффективную правоприменительную практику, представляется преждевременным: нередко нормативные положения просто не имеют механизма собственной реализации; вступают в коллизии с иными нормами правовых актов; содержат «фиктивные» установления, которые в принципе не могут быть реализованы ввиду отсутствия соответствующей юридической и материально-организационной основ; действия субъектов, уполномоченных к осуществлению превенции, несогласованы; огромный потенциал институтов гражданского общества остается в значительной степени невостребованным и т. п.» [1].

Мы абсолютно согласны с таким мнением. Дабы конкретизировать вышесказанное применительно к превенции незаконного оборота наркотиков, необходимо попытаться выделить существующую на сегодняшний день систему превенции.

Термин «система» является универсальным почти для всех наук. Он зародился как категория диалектики и представлял собой совокупность отдельно взятых элементов окружающей среды, объединенных между собой общими связями [2].

Право, как и другие социальные нормы, в процессе эволюции превратилось в объективное явление. Следовательно, право подчиняется исторически сложившейся объективной системе, которая обуславливается экономическими, социальными и культурными процессами [3].

Под системой превентивной деятельности в области противодействия незаконному обороту наркотиков мы понимаем комплекс управленческих процессов, состоящих из взаимосвязанных между собой элементов системы, направленных на выявление и нейтрализацию причин и условий незаконного оборота наркотиков.

Выделим элементы превентивной деятельности, которые, по нашему мнению, образуют ее систему.

1. Объект превентивной деятельности. Под объектом понимается то, на что направлена превентивная работа. В наиболее общем понимании превенция в сфере незаконного оборота наркотиков направлена на устранение его причин и условий. Однако мы считаем целесообразным конкретизировать объект, определив более узкие направления представленной деятельности.

Первое направление — это организация легального оборота наркотиков. Наличие проработанной правовой базы, которая регулирует процедуры оборота наркотиков, само по себе исклю-

чает ряд условий незаконного оборота наркотиков. Как говорилось ранее, полностью исключить любой оборот наркотиков невозможно, поскольку они используются во многих сферах жизнедеятельности социума. Из этого и вытекает первая проблема систематизации превенции незаконного оборота наркотиков. Как верно отметила В. М. Еремеева, оборот наркотиков — это объект регулирования правовых норм, обладающих различной юридической силой, которые достаточно часто противоречат друг другу [4]. Такого же мнения придерживается и А. В. Жуйков, который утверждает, что оборот наркотиков регулируется различными отраслями права, которые нередко бывают противоречивы [5].

Организация легального оборота в свою очередь должна включать в себя ряд элементов: квотирование и лицензирование; организацию допуска лиц к работе с наркотиками; регистрацию и учет новых наркотиков; регистрацию и учет процедур с наркотиками [6].

Второе направление — установление ответственности за незаконный оборот наркотиков. Наличие ответственности за деяние само по себе является общей превенцией. Юридическая ответственность в области незаконного оборота наркотиков разнообразна. Мы рассмотрим административную и уголовную ответственность.

Четкой системы ответственности в рассматриваемой сфере нет, поэтому мы условно разделим ее на несколько видов:

1) ответственность за незаконный оборот наркотиков, связанный с их личным потреблением (ст. ст. 228, 228.3 Уголовного кодекса Российской Федерации (далее — УК РФ); ст. ст. 6.8, 6.9 Кодекса Российской Федерации об административных правонарушениях (далее — КоАП РФ));

2) ответственность за сбыт наркотиков (ст. ст. 228.1, ст. 228.4 УК РФ);

3) ответственность за нарушение порядка и процедур оборота наркотиков (ст. ст. 228.2, 233 УК РФ; ст. 6.16 КоАП РФ);

4) ответственность за пропаганду и склонение к употреблению наркотиков (ст. 230 УК РФ; ст. 6.13 КоАП РФ);

5) ответственность за культивирование растений, содержащих наркотики (ст. 231 УК РФ; ст. 10.5.1 КоАП РФ) [7, 8].

Это далеко не полный перечень составов, которые предусматривают ответственность за незаконный оборот наркотиков. Проводить их дальнейшую дифференциацию мы считаем нецелесообразным, поскольку основная цель наличия любой юридической ответственности — это предупреждение правонарушений.

Третье направление — общая превенция незаконного оборота наркотиков. Общая превенция является классическим подвидом превенции, который предусматривается законодательно и который предполагает под собой совокупность профилактических и предупредительных мер, направленных на неопределенный круг лиц (на все общество в целом) [9]. Такой вид превенции предполагает использование метода убеждения и диспозитивных норм. Связано это с тем, что применение метода принуждения (который связан с ограничением прав и свобод) к неопределенному кругу лиц запрещается.

Четвертое направление — индивидуальная превенция незаконного оборота наркотиков. Это превенция, направленная на конкретное лицо или на конкретную категорию лиц [10]. Индивидуальная превенция позволяет использовать по отношению к объекту превенции более широкий круг механизмов воздействия на него.

Индивидуальную превенцию в сфере незаконного оборота наркотиков условно можно разделить на две категории:

1) превентивное воздействие на лиц, употребляющих наркотики;

2) превентивное воздействие на лиц, распространяющих наркотики.

Представленные превентивные воздействия находятся в тесной взаимосвязи друг с другом и по отдельности не будут приносить видимого результата, поскольку, пока существует спрос на наркотики, будут существовать и лица, распространяющие их, и наоборот.

2. Субъекты превентивной деятельности. Традиционно вторым элементом системы является субъект, то есть лицо, непосредственно осуществляющее данный вид деятельности. Как утверждает О.Н. Каширина, субъектами любой превентивной деятельности являются государственные органы и общественность [11]. Несмотря на такой широкий и не конкретизированный круг субъектов, с мнением О. Н. Кашириной трудно не согласиться, поскольку, как отмечалось неоднократно, превенция — это комплексная работа, которой должен быть присущ широкий круг субъектов, находящихся в тесном взаимодействии. Такой же широкий круг субъектов, как общей превенции правонарушений, так и правонарушений в сфере незаконного оборота наркотиков дает законодатель.

Так, в соответствии с ч. 1 ст. 5 Федерального закона «Об основах системы профилактики правонарушений в Российской Федерации» субъектами превенции выступают:

- федеральные органы исполнительной власти;

- органы прокуратуры Российской Федерации;

- следственные органы Следственного комитета Российской Федерации;

- органы государственной власти субъектов Российской Федерации;

- органы местного самоуправления [12].

Если говорить о специальной превенции незаконного оборота наркотиков, можно сделать вывод о том, что круг ее субъектов также весьма широк и не ограничен конкретными органами. В соответствии со ст. 53.1 Федерального закона «О наркотических средствах и психотропных веществах» помимо федеральных органов исполнительной власти и органов государственной власти субъектов РФ, которые выделяются как основные субъекты превенции незаконного оборота наркотиков, участвовать в превентивных мероприятиях, а также самостоятельно разрабатывать и реализовывать превентивные мероприятия имеют право органы местного самоуправления, организации независимо от организационно-правовых форм и форм собственности и даже отдельно взятые граждане [13]. Таким образом, превенция незаконного оборота наркотиков имеет более широкий круг субъектов, нежели общая превенция.

3. Последним элементом превенции, который мы рассмотрим в нашем исследовании, является содержание превентивной работы. Его в свою очередь можно разделить на:

1) виды превенции;

2) полномочия субъектов превенции;

3) формы превентивного воздействия;

4) методы превенции;

5) формы взаимодействия между субъектами превенции.

Мы уже подробно рассмотрели виды превенции, но повторимся, что ее можно разделить на общую, частную (индивидуальную) и специальную.

Следующий элемент содержания превентивной деятельности (полномочия) можно классифицировать следующим образом:

1) в зависимости от субъекта превентивной деятельности: полномочия федеральных органов исполнительной власти; полномочия органов исполнительной власти субъекта РФ. В силу специфики темы исследования мы рассмотрим только полномочия федеральных органов исполнительной власти;

2) в зависимости от объекта превентивной деятельности: общие полномочия (характерные для превенции всех видов правонарушений); специальные полномочия (характерные для превенции незаконного оборота наркотиков).

Анализируя формы превенции, можно сделать вывод о том, что их наиболее подробная классификация приведена в Федеральном законе «Об основах системы профилактики правонарушений в Российской Федерации». Исходя из содержания ст. 17 закона, можно выделить следующий исчерпывающий перечень форм профилактического воздействия: правовое просвещение и правовое информирование; профилактическая беседа; объявление официального предостережения (предостережения) о недопустимости действий, создающих условия для совершения правонарушений, либо недопустимости продолжения антиобщественного поведения; профилактический учет; внесение представления об устранении причин и условий, способствующих совершению правонарушения; профилактический надзор; социальная адаптация; ресоциализация; социальная реабилитация; помощь лицам, пострадавшим от правонарушений или подверженным риску стать таковыми [12].

Несмотря на то, что Федеральный закон «Об основах системы профилактики правонарушений в Российской Федерации» дает исчерпывающий перечень форм профилактического воздействия, иные формы присутствуют и в других нормативных правовых актах.

Так, ст. 53.4 Федерального закона «О наркотических средствах и психотропных веществах» выделяет еще одну форму профилактики — раннее выявление незаконного потребления наркотиков.

Представленная форма включает в себя:

- социально-психологические тестирования обучающихся образовательных организаций (формы и порядок тестирования определяются федеральным органом исполнительной власти в сфере образования);

- профилактические медицинские осмотры обучающихся образовательных организаций (формы и порядок профилактического осмотра определяются федеральным органом исполнительной власти в сфере здравоохранения) [13].

В отличие от полномочий федеральных органов исполнительный власти в области превенции, где законодательство об общей превенции коррелирует с законодательством о превенции незаконного оборота наркотиков, законодательство об общих формах превенции никак не коррелирует с законодательством о превенции незаконного оборота наркотиков. Отсутствуют конкретизация форм превентивной деятельности применительно к противодействию незаконному обороту наркотиков, а также единое понимание форм этой деятельности (закон «Об основах системы профилактики правонарушений в Российской Федерации» содержит категорию «формы профилактического воздействия», а закон «О наркотических средствах и психотропных веществах» — категорию

«формы профилактики»). В законодательстве отсутствует и процессуально-процедурный аспект применения той или иной формы.

Также мы считаем целесообразным разграничить такие дефиниции, как «форма превентивного воздействия» и «мера превентивного воздействия». Законодатель не дает легального определения ни одной из представленных дефиниций, но, исходя из логики построения закона «Об основах системы профилактики правонарушений в Российской Федерации» и анализа отдельных форм превентивного воздействия, мы можем сделать вывод о том, что мера превентивного воздействия первична, а форма — это совокупность таких мер.

Следующий элемент — методы превентивной деятельности. Как и все методы управления, превенция может осуществляться посредством:

- метода убеждения;
- метода принуждения.

Метод убеждения в превенции заключается в психологическом и моральном воздействии на лицо, которое является объектом превентивной деятельности, с целью добровольного исполнения им воли субъекта превентивной деятельности [14]. Большинство форм превентивной деятельности применяются посредством метода убеждения, поскольку представляют собой совокупность мер социального, психологического, медицинского и организационного характера, которые применяются к объекту превентивного воздействия добровольно.

Метод принуждения же состоит в психическом и физическом воздействии на лицо, которое является объектом превентивной деятельности, с целью исполнения им воли субъекта превентивной деятельности против его собственной воли. Метод принуждения в превентивной деятельности встречается намного реже, чем метод убеждения. Связано это с тем, что применение метода принуждения предполагает претерпевание ограничений прав и свобод для лица, которое является объектом принудительного воздействия.

Несмотря на то, что использование преимущественно мер убеждения в превентивной деятельности является большим плюсом (поскольку права и свободы человека и гражданина остаются незыблемыми), у этого есть и большой недостаток. Отсутствие какого-либо принуждения и ответственности лишает превентивную деятельность реального обеспечения. Отсутствуют и реальные механизмы воздействия на лицо, которое является объектом превентивной деятельности, что может свести всю эту деятельность на нет.

Однако подходить к использованию метода принуждения в превентивной деятельности необходимо разумно.

Во-первых, меры превентивного воздействия, которые сопряжены с применением мер принуждения, могут быть предусмотрены только федеральным законодательством, поэтому мы не ставим целью нашего исследования создание новых форм и мер превентивного воздействия.

Во-вторых, поскольку каждая мера принуждения затрагивает права и свободы человека и гражданина (которые являются высшей конституционной ценностью [14]), их использование должно носить исключительный характер, когда другими способами достигнуть целей превенции не представляется возможным.

Рассматривая последний элемент — взаимодействие субъектов превенции, можно также сделать вывод о том, что он не получил достаточного законодательного развития. Говоря об общей превентивной деятельности, закон «Об основах системы профилактики правонарушений в Российской Федерации» не предусматривает реальных механизмов взаимодействия между субъектами превенции. На общем уровне существует лишь координационный орган — Правительственная комиссия по профилактике правонарушений [15], а более детальное и глубокое взаимодействие может быть предусмотрено различными межведомственными соглашениями. Специальное законодательство в сфере превенции незаконного оборота наркотиков не предусматривает механизмов взаимодействия в принципе.

Отсутствие проработанных и выверенных механизмов взаимодействия между субъектами является одним из самых больших пробелов превентивной деятельности. Как уже отмечалось, превенция — это комплексная деятельность, которая состоит из множества элементов. Превентивные задачи не могут быть решены посредством полномочий только одного органа или структурного подразделения органа.

Еще одним недостатком системы превенции незаконного оборота наркотиков в деятельности ОВД РФ является отсутствие адекватных критериев оценки результатов рассматриваемой деятельности. Из-за отсутствия таких критериев достаточно сложно осуществлять контрольно-надзорную деятельность, которая является обязательным этапом любой управленческой деятельности.

Проведя глубокий анализ отдельно взятых элементов превентивной деятельности и подводя итоги исследования, мы можем сделать ряд выводов и предложений.

1. Наличие большого количества нормативных правовых актов, в содержании которых присутствуют вопросы, связанные с превенцией незаконного оборота наркотиков, и отсутствие единого структурированного документа, который

отражал бы в себе все эти вопросы, пагубно сказывается на системе превенции незаконного оборота наркотиков, порождая различного рода противоречия и пробелы, что в свою очередь может негативно отражаться на правоприменительной практике.

2. Основными элементами содержания системы превенции являются «меры превентивного воздействия» и «форма превентивного воздействия». Несмотря на широкое использование этих дефиниций как в правовой теории, так и в законодательстве, до сих пор отсутствуют их определения, которые позволили бы разграничить понятия. Мы предлагаем следующее понимание данных дефиниций:

«Мера превентивного воздействия — это действие (или действия) правового, организационного, социального, медицинского, воспитательного или иного характера уполномоченного на то субъекта, которое направлено на недопущение совершения преступлений, административных правонарушений и иных антиобщественных деяний».

«Форма превентивного воздействия — это совокупность мер превентивного воздействия, объединенных конкретной целью превенции, предполагающая комплексное воздействие на конкретный объект превентивной деятельности».

3. Несмотря на тот факт, что превентивная деятельность по большей части реализуется посредством применения метода убеждения, отсутствие реальной юридической ответственности за неисполнение и несоблюдение некоторых форм профилактического воздействия является реальной проблемой. Метод убеждения сам по себе, безусловно, является действенным, но лишь в совокупности с применением метода принуждения. По нашему мнению, целесообразно ввести административную ответственность за неисполнение таких форм превентивного воздействия, как «объявление официального предостережения о недопустимости действий, создающих условия для совершения правонарушений, либо недопустимости продолжения антиобщественного поведения» и «внесение представления об устранении причин и условий, способствующих совершению правонарушения». Настоящие формы превентивного воздействия будут эффективны только в том случае, если за их неисполнение субъект понесет реальную ответственность.

ЛИТЕРАТУРА

1. Махина С. Н., Дорофеева Ж. П. Нормативно-правовое и программно-целевое регулирование превенции административных правонарушений несовершеннолетних: проблемы и перспективы совершенствования // Юридические записки. Воронежский государственный университет. — 2014. — № 4(27). — С. 81—89.

2. Категории диалектики и методологии современной науки. — Воронеж : Изд-во Воронежского ун-та, 1970. — 390 с.

3. Шебанов А. Ф. Система законодательства как научная основа кодификации // Современное государство и право. — 1971. — № 12. — С. 3.

4. Еремеев В. М. Предмет преступлений, связанных с незаконным оборотом наркотиков // Мир науки и образования. — 2018. — № 1(13). — С. 8—14.

5. Жуйков А. В. Административно-правовые средства борьбы с наркоманией и их применение органами внутренних дел (По материалам Дальневосточного региона) : дис. ... канд. юрид. наук. — Хабаровск, 2002. — С. 45.

6. Белоусов С. В. Административно-правовые средства противодействия незаконному обороту наркотических средств и психотропных веществ // Юридическая наука: история и современность. — 2020. — № 1. — С. 93—97.

7. Уголовный кодекс Российской Федерации : Федеральный закон от 13.06.1996 № 63-ФЗ // Собрание законодательства Российской Федерации. — 1996. — № 25. — Ст. 2954.

8. Кодекс Российской Федерации об административных правонарушениях : Федеральный закон от 30.12.2001 № 195-ФЗ // Собрание законодательства Российской Федерации. — 2002. — № 1 (ч. 1). — Ст. 1.

9. Панферкина И. С., Воробьёва Е. А., Савина С. С. Причины административных правонарушений несовершеннолетних и меры по профилактике их совершения // Научный альманах. — 2019. — № 2-1(52). — С. 188—190.

10. Дугенец А. С. О проблемах определения оснований для проведения профилактической работы с лицами, больными алкоголизмом // Российская юстиция. — 2019. — № 10. — С. 60—62.

11. Каширина О. Н. О некоторых аспектах проведения субъектами профилактики правонарушений мониторинга в сфере профилактики правонарушений в Российской Федерации // Инновационная экономика и право. — 2018. — № 1(10). — С. 106—108.

12. Об основах системы профилактики правонарушений в Российской Федерации : Феде-

ральный закон от 23.06.2016 № 182-ФЗ // Собрание законодательства Российской Федерации. — 2016. — № 26 (ч. 1). — Ст. 3851.

13. О наркотических средствах и психотропных веществах : Федеральный закон от 08.01.1998 № 3-ФЗ // Собрание законодательства Российской Федерации. — 1998. — № 2. — Ст. 219.

14. Шумакова Е. В. Методы убеждения и принуждения в правоприменительной деятельности полиции // Право и управление. — 2025. — № 1. — С. 135—140.

15. О правительственной комиссии по профилактике правонарушений : постановление Правительства Российской Федерации от 28.03.2008 № 216 // Собрание законодательства Российской Федерации. — 2008. — № 14. — Ст. 1410.

REFERENCES

1. Makhina S. N., Dorofeeva Zh. P. Normativno-pravovoe i programmno-tselevoe regulirovanie preventsii administrativnykh pravonarushenij nesovershennoletnikh: problemy i perspektivy sovershenstvovaniya // Yuridicheskie zapiski. Voronezhskij gosudarstvennyj universitet. — 2014. — № 4(27). — S. 81—89.

2. Kategorii dialektiki i metodologii sovremennoj nauki. — Voronezh : Izd-vo Voronezhskogo un-ta, 1970. — 390 s.

3. Shebanov A. F. Sistema zakonodatel′stva kak nauchnaya osnova kodifikatsii // Sovremennoe gosudarstvo i pravo. — 1971. — № 12. — S. 3.

4. Eremeev V. M. Predmet prestuplenij, svyazannykh s nezakonnym oborotom narkotikov // Mir nauki i obrazovaniya. — 2018. — № 1(13). — S. 8—14.

5. Zhujkov A. V. Administrativno-pravovye sredstva bor′by s narkomaniej i ikh primenenie organami vnutrennikh del (Po materialam Dal′nevostochnogo regiona) : dis. ... kand. yurid. nauk. — Khabarovsk, 2002. — S. 45.

6. Belousov S. V. Administrativno-pravovye sredstva protivodejstviya nezakonnomu oborotu narkoticheskikh sredstv i psikhotropnykh veshchestv // Yuridicheskaya nauka: istoriya i sovremennost′. — 2020. — № 1. — S. 93—97.

7. Ugolovnyj kodeks Rossijskoj Federatsii : Federal′nyj zakon ot 13.06.1996 № 63-FZ // Sobranie zakonodatel′stva Rossijskoj Federatsii. — 1996. — № 25. — St. 2954.

8. Kodeks Rossijskoj Federatsii ob administrativnykh pravonarusheniyakh : Federal′nyj zakon ot 30.12.2001 № 195-FZ // Sobranie zakonodatel′stva Rossijskoj Federatsii. — 2002. — № 1 (ch. 1). — St. 1.

9. Panferkina I. S., Vorob′yova E. A., Savvina S. S. Prichiny administrativnykh pravonarushenij nesovershennoletnikh i mery po profilaktike ikh sovershеniya // Nauchnyj al′manakh. — 2019. — № 2-1(52). — S. 188—190.

10. Dugenets A. S. O problemakh opredeleniya osnovanij dlya provedeniya profilakticheskoj raboty s litsami, bol′nymi alkogolizmom // Rossijskaya yustitsiya. — 2019. — № 10. — S. 60—62.

11. Kashirina O. N. O nekotorykh aspektakh provedeniya sub″ektami profilaktiki pravonarushenij monitoringa v sfere profilaktiki pravonarushenij v Rossijskoj Federatsii // Innovatsionnaya ekonomika i pravo. — 2018. — № 1(10). — S. 106—108.

12. Ob osnovakh sistemy profilaktiki pravonarushenij v Rossijskoj Federatsii : Federal′nyj zakon ot 23.06.2016 № 182-FZ // Sobranie zakonodatel′stva Rossijskoj Federatsii. — 2016. — № 26 (ch. 1). — St. 3851.

13. O narkoticheskikh sredstvakh i psikhotropnykh veshchestvakh : Federal′nyj zakon ot 08.01.1998 № 3-FZ // Sobranie zakonodatel′stva Rossijskoj Federatsii. — 1998. — № 2. — St. 219.

14. Shumakova E. V. Metody ubezhdeniya i prinuzhdeniya v pravoprimenitel′noj deyatel′nosti politsii // Pravo i upravlenie. — 2025. — № 1. — S. 135—140.

15. O pravitel′stvennoj komissii po profilaktike pravonarushenij : postanovlenie Pravitel′stva Rossijskoj Federatsii ot 28.03.2008 № 216 // Sobranie zakonodatel′stva Rossijskoj Federatsii. — 2008. — № 14. — St. 1410.

СВЕДЕНИЯ ОБ АВТОРЕ

Чачхиани Максим Николаевич. Преподаватель кафедры теории и истории государства и права.
Воронежский институт МВД России.
E-mail: mayrond3@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Chachkhiani Maksim Nikolaevich. Lecturer of the chair of Theory and History of State and Law.

Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: незаконный оборот наркотических средств и психотропных веществ; превенция незаконного оборота; систематизация превентивной деятельности.

Key words: illicit trafficking in narcotic drugs and psychotropic substances; prevention of illicit trafficking; systematization of preventive activities.

УДК: 342.518

Е. И. Чунихина

АДМИНИСТРАТИВНАЯ ОТВЕТСТВЕННОСТЬ В СИСТЕМЕ СРЕДСТВ ПРОТИВОДЕЙСТВИЯ РАСПРОСТРАНЕНИЮ ИНФОРМАЦИИ, ПОСЯГАЮЩЕЙ НА ТРАДИЦИОННЫЕ РОССИЙСКИЕ ДУХОВНО-НРАВСТВЕННЫЕ ЦЕННОСТИ

ADMINISTRATIVE RESPONSIBILITY IN THE SYSTEM OF MEANS OF COUNTERING THE DISSEMINATION OF INFORMATION THAT ENCROACHES ON TRADITIONAL RUSSIAN SPIRITUAL AND MORAL VALUES

Статья посвящена развитию административно-деликтного законодательства как средства защиты традиционных российских духовно-нравственных ценностей. Автором отмечено, что конвергенция социальных запросов и соответствующей нормотворческой деятельности привела к своевременной деликтолизации деяний, дискредитирующих традиционные институты семьи и брака, оправдывающих чуждую российскому обществу либеральную идеологию, привлекательность потребления наркотических средств и психотропных веществ. Исследование законодательных конструкций составов административных правонарушений, предусмотренных статьями 6.13, 6.13[1], 6.21, 6.21[1] и 6.21[2] Кодекса Российской Федерации об административных правонарушениях, позволило выявить существующие правовые неопределенности, снижающие эффективность мер административной ответственности, а также предложить некоторые пути их преодоления.

The article is devoted to the development of administrative and tort legislation as a means of protecting traditional Russian spiritual and moral values. The author notes that the convergence of social demands and relevant rule-making activities has led to the timely delictalization of acts discrediting the traditional institutions of family and marriage, justifying the liberal ideology alien to Russian society, the attractiveness of the consumption of narcotic drugs and psychotropic substances. Investigation of legislative structures of administrative offenses provided for in articles 6.13, 6.13[1], 6.21, 6.21[1] и 6.21[2] the Code of Administrative Offences of the Russian Federation made it possible to identify existing legal uncertainties that reduce the effectiveness of administrative liability measures, as well as to suggest some ways to overcome them.

Традиционные российские духовно-нравственные ценности являются одним из важных сегментов государственной политики России, который раскрывается в ряде нормативных правовых актов — документов стратегического планирования [1—3]. Их разработка и утверждение обусловливается необходимостью обеспечения национальной безопасности, сохранения идентичности многонационального народа России и единого культурного пространства нашей страны, духовного и исторического развития. Говоря о России как оплоте традиционных духовно-нравственных ценностей, Президент Российской Федерации В.В. Путин обращает внимание на то, что в мире всё больше людей, поддерживающих позицию нашей страны «по защите традиционных ценностей, которые тысячелетиями составляли духовную, нравственную основу цивилизации каждого народа: ценностей традиционной семьи, подлинной человеческой жизни, в том числе и жизни религиозной, жизни не только материальной, но и духовной, ценностей гуманизма и разнообразия мира» [4].

Защита духовно-нравственных ценностей приобретает особую значимость в условиях глобализации, которая выступает существенным фактором риска для распространения среди населения нашей страны идеологем, направленных на дискредитацию традиционных институтов семьи и брака, развращение несовершеннолетних, популяризацию потребления веществ, вызывающих наркотическое и иные виды опьянения. Противодействие распространению такой информации представляется многоаспектной деятельностью, важное место в которой наряду с мерами убеждения занимают административно-деликтные средства.

Одним из наиболее эффективных средств защиты традиционных российских духовно-нравственных ценностей выступает административная ответственность, используемая для предупреждения деяний, направленных на распространение чуждых гражданам нашей страны идеологий, посредством применения наказательных мер. При этом административно-деликтное законодательство развивается системно, демонстрируя конвергенцию социальных запросов и соответствующей нормотворческой деятельности.

Государственная политика, направленная на воспрепятствование распространению чуждой российскому обществу идеологии, закономерно привела к закреплению административно-правовых запретов, которые нашли свое место в диспозициях деяний, предусмотренных, прежде всего, статьями 6.13, 6.13^1, 6.21, 6.21^1 и 6.21^2 Кодекса Российской Федерации об административных правонарушениях (далее — КоАП РФ).

Признакам любого административного правонарушения является социальная опасность. Распространение информации, направленной на искажение традиционных российских духовно-нравственных ценностей, имеет ярко выраженный указанный признак.

Современное информационное пространство представляет собой одну из ключевых сред для распространения контента, что обусловливает необходимость более тщательного правового регулирования действий, совершаемых в сети Интернет, с целью защиты публичных интересов, эффективной охраны общественной нравственности и безопасности.

Отмеченное в своей совокупности позволяет констатировать, что использование сети Интернет как основного канала коммуникации обусловливает повышенную общественную опасность действий, связанных с распространением деструктивного контента, по сравнению с аналогичными деяниями, совершаемыми в офлайн-пространстве.

Ввиду множащегося деструктивного контента в цифровой среде законодатель включил использование сети Интернет в качестве квалифицирующего признака деяний, предусмотренных статьями 6.13, 6.13^1, 6.21, 6.21^1 и 6.21^2 КоАП РФ.

Рассматриваемые статьи можно разделить на две группы. К первой группе деликтов относятся правонарушения, связанные с незаконным оборотом наркотических средств, психотропных веществ или их прекурсоров, веществ, вызывающих наркотическое и иные виды опьянения. Их совершение представляет одну из наиболее серьезных угроз национальной безопасности, которая выражается в оказании негативного влияния на здоровье населения и генофонд страны, а также выступает фактором риска для совершения других правонарушений, включая преступления. Злоупотребление наркотиками оказывает пагубное воздействие не только на граждан, употребляющих наркотические средства, но и на экономику страны в целом [5].

Статьи 6.13 и 6.131 КоАП РФ содержат однородные составы административных правонарушений, сопряженных с пропагандой (распространением) наркотических средств, психотропных веществ, их аналогов или прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры (далее — наркотические средства), а также закиси азота, известной как оксид азота и «веселящий газ».

Вступившие в силу с 1 сентября 2025 г. поправки дополнили статью 6.13 КоАП РФ [6] новым способом распространения запрещенной информации о наркотических средствах посредством использования произведений литературы и искусства, не имеющих маркировки, предусмотренной законодательством. Потенциальная опасность распространения такой информации определяется тем, что не осведомленный о содержании литературного произведения читатель (в особенности несовершеннолетний) может становиться объектом пропаганды, что, в свою очередь, выступает безусловным фактором риска для вовлечения такого лица в наркопотребление. Новеллой следует считать введение законодательной возможности дисквалификации должностных лиц и ужесточающей нормы для повторных нарушителей согласно ч. 3 ст. 6.13 КоАП РФ.

С 1 марта 2026 г. по ст. 6.13 КоАП РФ ужесточается ответственность за пропаганду наркотиков путем увеличения размеров административных штрафов.

Очевидно, что общественная опасность рассматриваемой группы правонарушений определяется деструктивным влиянием наркотических средств, закиси азота, которое находит свое выражение в достижении состояния опьянения, вызывающего эйфорию. В качестве дополнительных побочных эффектов можно отметить временную утрату ориентации во времени и в пространстве, а также сдерживающих начал. Как отмечают исследователи данной проблематики, при вдыхании высоких концентраций газа быстро развивается состояние опьянения и сонливость, а «вред от совместного потребления многих психоактивных веществ с закисью азота многократно возрастает» [7], что может причинить существенный вред здоровью потребителя.

Вполне очевидно, что административно-правовое противодействие названным деяниям требует реализации действенной государственной политики как на правоустановительном, так и на

правоприменительном уровне [8—13]. Одним из наиболее важных направлений такой деятельности выступает борьба с пропагандой наркотических средств, психотропных веществ или их прекурсоров, то есть распространением сведений о запрещенных веществах в различных источниках, направленным на формирование повышенного социального интереса и положительного отношения к таким веществам [14], утверждение идеи привлекательности потребления или пропаганду образа жизни, связанного с их потреблением [15].

Необходимо подчеркнуть, что статьи 6.13 и 6.13^1 КоАП РФ выступают важным элементом системы мер административного-правового регулирования распространения информации, посягающей на традиционные духовно-нравственные ценности, логически взаимодействуя с иными противоправными деяниями, связанными с незаконным оборотом наркотических средств (статьи 6.8, 6.9, 20.20, 20.22 КоАП РФ).

Эффективность противодействия рассматриваемой группе деликтов осложняется наличием отдельных организационно-правовых и процессуальных проблем, существующих в правоприменительной практике.

Следует отметить некоторую пробельность современного административно-деликтного законодательства в части противодействия пропаганде наркотических средств. Не секрет, что одежду с логотипами и принтами, значки и другую атрибутику, вызывающую прямые ассоциации с наркотическими средствами, достаточно легко приобрести как в розничных торговых точках, так и на интернет-площадках крупнейших маркетплейсов нашей страны, что делает возможным ее приобретение не только взрослыми, но и несовершеннолетними подростками, которые могут появляться в такой одежде в общественных местах, тем самым прямо или опосредованно продвигая указанные деструктивные идеологемы.

Пропаганда закиси азота является относительной новеллой для российского административно-деликтного законодательства, в связи с чем практика применения указанной статьи находится в стадии формирования.

Однако уже существуют определенные процессуальные проблемы привлечения к ответственности по статье 6.13^1 КоАП РФ, которые выражаются в следующем:

1. Закись азота употребляют ингаляционно, в основном с использованием воздушных шариков, заполненных бесцветным негорючим газом, обладающим инертными свойствами, с характерным сладковатым запахом. Отмеченное затрудняет изъятие и последующее исследование химического вещества.

2. Закись азота имеет химическую формулу (N_2O), но не имеет каких-либо устоявшихся в правоприменительной практике изображений, логотипов или аббревиатур, позволяющих визуализировать (по аналогии с наркотическими веществами) пропаганду указанного вещества.

3. Для привлечения к административной ответственности лица, совершившего пропаганду немедицинского потребления закиси азота, может потребоваться проведение химического исследования (экспертизы), что, учитывая ограниченный срок административного расследования (не более двух месяцев) и давности (три месяца) по делам данной категории, может послужить основанием для прекращения производства.

Быстрота деликтолизации того или иного девиантного поведения обусловливается степенью его влияния на общественные отношения и силой его деструктивного воздействия. Например, деликтолизация фактов пропаганды смены пола или отказа от деторождения, пропаганда педофилии, несмотря на многолетнюю историю таких движений в мире, нашла свое закрепление в качестве противоправной в отечественном административном законодательстве лишь в 2022—2024 гг.

Ко второй группе рассматриваемых административных деликтов в сфере общественной нравственности справедливо относятся деяния, сопряженные с пропагандой нетрадиционных сексуальных отношений и (или) предпочтений, смены пола, отказа от деторождения, педофилии, а также распространением среди несовершеннолетних информации, демонстрирующей нетрадиционные сексуальные отношения и (или) предпочтения либо способной вызвать у несовершеннолетних желание сменить пол (ст. 6.21, 6.21^1 и 6.21^2 КоАП РФ). Общественная опасность указанных поступков не вызывает сомнений, поскольку все они вступают в прямое противоречие с традиционными российскими духовно-нравственными ценностями.

Исследования в области социальной и педагогической психологии подтверждают, что ценностные ориентации и модель будущей семейной жизни закладываются в детском и подростковом возрасте, а их деформация под внешним информационным воздействием может иметь долгосрочные негативные последствия для личности и общества в целом [16].

При этом, как справедливо отмечает С. Р. Дробязко, в информационном поле западноевропейских государств продолжает активно развиваться гендерная теория, согласно которой «различия между мужчинами и женщинами определяются не биологическим полом и соответствующими особенностями физиологии и психики, а

социальными установками и стереотипами, которые буквально навязываются личности» [17]. Наибольшее опасение вызывает тот факт, что указанная и ей подобные «теории» развиваются не просто в границах отдельно взятых стран, поддерживающих программы гендерной идентичности на уровне государственной политики [18, 19], но и пытаются информационно насаждаться в Российской Федерации. Отмеченное позволяет согласиться с мнением И. В. Понкина, который относит распространение деструктивной информации в условиях современного уровня глобализации к разновидности «гибридной войны», используемой геополитическими противниками России [20].

Пропаганда любых половых девиаций, сознательного отказа от продолжения рода, в том числе путем изменения гендерной принадлежности, подрывает традиционные российские семейные ценности и выступает фактором риска для национальной безопасности, создает очаги социальной напряженности и снижает человеческий потенциал. Более того, отмеченные деяния нередко выступают средством причинения вреда нравственному здоровью, в первую очередь родственников и близких людей, подвергшихся влиянию такой деструктивной идеологии.

Трудно не согласиться с мнением Е. В. Епифановой, которая обоснованно аргументирует, что отклонения в нравственном здоровье выступают своего рода триггером для потенциального нарушения физического и психического благополучия человека [21]. Соответственно, делает вывод автор, «любая пропаганда такого рода действий не только толкает человека в пучину безнравственности, но и способствует возникновению у него психических расстройств» [22].

Справедливо отмечено также Е. С. Ивашкиной, что «при расследовании дела об административном правонарушении обязательно подлежит доказыванию то обстоятельство, что информация о нетрадиционных сексуальных отношениях способна формировать в сознании неопределенного круга лиц предпочтения либо побуждать к совершению действий, т. е. оказывать воздействие» [23]. В связи с тем что такие правонарушения совершаются только с умышленной формой вины, деяния, побуждающие формирование определенных предпочтений, должны охватываться умыслом правонарушителя.

Следует подчеркнуть, что диспозиция статьи 6.212 КоАП РФ, по сути, содержит тождественное «пропаганде» понятие «распространение информации», конечной целью которого является популяризация нетрадиционных сексуальных отношений среди несовершеннолетних, а также смены пола.

Административно-деликтные нормы, содержащиеся в ст. 6.21 и 6.21^2 КоАП РФ, выступают важным инструментом защиты фундаментальных ценностей российского общества, сдерживающим фактором для бесконтрольного распространения деструктивных идеологий. Их эффективность напрямую зависит от четкости правовых формулировок, единообразия судебной практики и развития механизмов выявления и пресечения нарушений, в том числе в цифровой среде.

При этом в качестве ключевой проблемы следует отметить наличие правовой неопределенности в разграничении объективной стороны деяний, выражающихся в формах «пропаганды» и «распространения информации». У правоприменителя справедливо возникают сомнения, связанные с правильной квалификацией рассматриваемой группы деяний, отграничением объективной стороны действий, выражающихся в «распространении» информации и ее «пропаганде». Конкуренция между административно-деликтными нормами выражается в том, что два или более правовых предписания одновременно претендуют на регулирование одного и того же либо смежного административного правоотношения [24].

Правовой базой введения запрета на пропаганду педофилии выступают нормы Конституции Российской Федерации [25], закрепляющие приоритет государственной политики в сфере защиты семьи и традиционных ценностей. Введение административной ответственности за совершение указанных деяний обусловливается масштабной популяризацией девиаций через каналы массовой культуры. В связи с этим дополнение КоАП РФ статьей 6.21^1 стало логическим развитием государственной политики, направленной на максимальную защиту физического, психического и нравственного здоровья детей. Как справедливо отмечают А. Н. Берестовой и П. В. Цветков, в условиях цифровизации риски распространения деструктивного контента, направленного на детей, многократно возросли, что требует адекватного правового ответа, сочетающего карательные и превентивные меры [26].

Ключевой проблемой для однозначной квалификации рассматриваемой нормы является отсутствие установленного понятия «педофилия». Согласно определению, представленному в Большой российской энциклопедии, педофилия интерпретируется как расстройство сексуального поведения, характеризующееся наличием полового влечения к детям и совершением сексуальных действий с ними для достижения сексуального удовлетворения [27].

В целом ряде нормативных правовых актов Российской Федерации [28—32] содержатся

нормы, признающие пропаганду педофилии противоправной, но не раскрывающие ее понятия.

Термин «педофилия» используется в Уголовном кодексе Российской Федерации (далее — УК РФ) в нормах, регламентирующих применение принудительных мер медицинского характера. Так, часть 4.1 статьи 79, часть 4 статьи 80 и пункт «д» части 1 статьи 97 УК РФ предусматривают их назначение лицам, страдающим расстройством сексуального предпочтения (педофилией), не исключающим вменяемости. Таким образом, системное толкование указанных положений позволяет сделать вывод, что уголовный закон квалифицирует педофилию как одну из форм расстройства сексуального предпочтения (парафилию).

Ключевой проблемой правового регулирования является определение юридической природы педофилии в контексте установления запрета на ее пропаганду. Если рассматривать данное явление исключительно как психическое расстройство, то возникает закономерный вопрос о правомерности использования термина «пропаганда» в отношении медицинского диагноза.

Это порождает правоприменительные трудности, которые видятся, во-первых, в ограниченном сроке давности привлечения к административной ответственности, установленном статьей 4.5 КоАП РФ (общий срок составляет 3 месяца, а в случаях совершения данного правонарушения в отношении несовершеннолетних — 1 год) и, во-вторых, в недостаточном сроке, отводимом статьей 28.7 КоАП РФ на проведение административного расследования, который в соответствии с частью 5 не может превышать 2 месяцев. Учитывая, что полное, всестороннее и объективное рассмотрение дел данной категории может потребовать проведения ряда экспертиз (судебно-психиатрической, лингвистической, искусствоведческой и др.), сроки, установленные законодателем для привлечения лиц к административной ответственности, нуждаются в разумном увеличении.

Наличие указанных препятствий создает проблемы привлечения лиц, совершающих рассматриваемую группу деяний, к административной ответственности, что подтверждается статистическими данными. Так, за 2023 год судами Российской Федерации в общей сложности было рассмотрено 186 дел (подвергнуто наказанию 106 лиц, или 57%, прекращено дел по реабилитирующим основаниям — 8, или 5%) об административных правонарушениях, предусмотренных статьями 6.21, 6.21^1, 6.21^2, а в 2024 году — 221 дело (подвергнуто наказанию 151 лицо, или 68%, прекращено по реабилитирующим основаниям 12 дел, или 5%) [33], что, по нашему мнению, свидетельствует о наличии нерешенных задач в вопросе противодействия рассматриваемой группе правонарушений.

Таким образом, административно-деликтные нормы, содержащиеся в статьях 6.13, 6.13^1, 6.21, 6.21^1 и 6.21^2 КоАП РФ, выступают важным инструментом защиты фундаментальных традиционных духовно-нравственных ценностей российского общества. Эффективность их применения напрямую зависит от четкости правовых формулировок, выработки единообразной правоприменительной практики и развития механизмов выявления и пресечения нарушений, в том числе в цифровой среде, поскольку именно бесконтрольное использование возможностей сети Интернет подрывает традиционные ценности и порождает существенные сложности в привлечении виновных лиц к административной ответственности, создавая условия для дальнейшего распространения деструктивного контента.

ЛИТЕРАТУРА

1. О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы : указ Президента Российской Федерации от 09.05.2017 № 203 // Собрание законодательства РФ. — 2017. — № 20. — Ст. 2901.

2. О Стратегии национальной безопасности Российской Федерации : указ Президента Российской Федерации от 02.07.2021 № 400 // Собрание законодательства РФ. — 2021. — № 27 (ч. II). — Ст. 5351.

3. Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей : указ Президента Российской Федерации от 09.11.2022 № 809 // СПС «КонсультантПлюс».

4. Текст послания Президента Федеральному Собранию 2013 года // URL: https://rg.ru/2013/12/12/poslanie.html (дата обращения: 12.01.2026).

5. Занина Т. М., Орехова Н. А. Обязательное лечение лиц, употребляющих наркотические средства и психотропные вещества, как особый вид административного принуждения // Вестник Воронежского института МВД России. — 2017. — № 3. — С. 123—127.

6. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях : Федеральный закон от 08.08.2024 № 285-ФЗ // Собрание законодательства РФ. — 2024. — № 33 (ч. I). — Ст. 4921.

7. Административная ответственность за правонарушения, предусмотренные статьями 6.13, 6.13[1] КоАП РФ : учебное пособие / А. Ю. Иванов, Н. Н. Цуканов, П. Ю. Овсянников [и др.] ; под общ. ред. Н. Н. Цуканова. — Красноярск : СибЮИ МВД России, 2024. — С. 18—19.

8. Анисифорова М. В. Административная ответственность за нарушения законодательства в сфере оборота наркотических средств, психотропных веществ и их прекурсоров : дис. … канд. юрид. наук. — М., 2018. — 254 с.

9. Степанова О. А. Правовое регулирование судебного порядка пересмотра постановлений и решений по делам об административных правонарушениях : дис. … канд. юрид. наук. — М., 2014. — 243 с.

10. Рожкова Э. В. Административная ответственность за правонарушения в сфере оборота наркотических средств, психотропных веществ и их прекурсоров : автореф. дис. … канд. юрид. наук. — Саратов, 2009. — 27 с.

11. Слободчук С. В. Административная ответственность за правонарушения, связанные с наркотиками : автореф. дис. … канд. юрид. наук. — Воронеж, 2005. — 24 с.

12. Корнев А. А. Административно-правовые средства борьбы с незаконным оборотом наркотиков в Российской Федерации : автореф. дис. … канд. юрид. наук. — СПб., 2010. — 23 с.

13. Насонов А. Н. Административно-правовое регулирование оборота наркотических средств и психотропных веществ : автореф. дис. … канд. юрид. наук. — М., 2008. — 31 с.

14. Газизов Д. А., Газизова Т. Г. Административная ответственность за пропаганду наркотических средств // Право и практика. — 2013. — № 1. — С. 88—94.

15. Цуканов Н. Н. Административная ответственность за правонарушения в сфере оборота наркотиков : учеб. пособие. — М. : ИНФРА-М, 2015. — С. 74.

16. Реан А. А., Ставцев А. А. Семья и дети как факторы психологического благополучия и жизнестойкости личности педагогов Российской Федерации // Известия Российского государственного педагогического университета им. А. И. Герцена. — 2024. — № 214. — С. 116—126.

17. Дробязко С. Р. Образ жизни личности как предмет конституционно-правовой защиты на примере вопроса о смене пола // Конституционное и муниципальное право. — 2023. — № 1. — С. 55.

18. В США суд разрешил трансгендерам служить в вооруженных силах // URL: https://www.rbc.ru/rbcfreenews/5a2f85a99a7947245ec482aa (дата обращения: 23.07.2025).

19. В США трансгендерам вновь разрешили служить в армии // URL: https://iz.ru/1145135/2021-04-01/pentagon-utverdil-pravila-priema-transgenderov-na-sluzhbu-v-vs-ssha.

20. Понкин И. В. Неклассические войны : монография. М. : ИНФРА-М, 2019. — С. 87.

21. Об основах охраны здоровья граждан в Российской Федерации : Федеральный закон от 21.11.2011 № 323-ФЗ (в ред. от 17.11.2025) ст. 2 // Собрание законодательства РФ. — 2011. — № 48. — Ст. 6724.

22. Епифанова Е. В. Нравственное здоровье как объект административно-правовой охраны // Административное право и процесс. — 2025. — № 2. — С. 41.

23. Ивашкина Е. С. Вопросы целесообразности введения ст. 6.212 КоАП РФ // Россия в XXI веке: глобальные вызовы, приоритеты и перспективы развития : материалы XVII Всероссийской научно-практической конференции студентов и молодых ученых, Барнаул, 16—17 апреля 2024 года. — Барнаул : Пять плюс, 2024. — С. 217—219.

24. Кисин В. Р., Попугаев Ю. И. О коллизии (конкуренции) норм, предусматривающих административную и уголовную ответственность, и способы ее разрешения // Научный портал МВД России. — 2013. — № 2(22). — С. 79—88.

25. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993, с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «КонсультантПлюс».

26. Берестовой А. Н. Цветков П. В. Законодательная регламентация вопросов, касающихся противодействия новым формам девиантного поведения в сети Интернет // От Псковской судной грамоты к принципам современного правосудия: традиции и новации в российском судопроизводстве : сборник научных статей всероссийской научно-практической конференции, Псков, 26—27 сентября 2024 года. — СПб. : Центр научно-информационных технологий «Астерион», 2024. — С. 287—297.

27. Большая российская энциклопедия // URL: https://old.bigenc.ru/medicine/text/2708885?ysclid=mfw7rw2w9p78900878.

28. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (в ред. от 24.06.2025) (с изм. и доп., вступ. в силу 01.01.2026) // Собрание законодательства РФ. — 2006. — № 31 (1 ч.). — Ст. 3448.

29. О государственной поддержке кинематографии Российской Федерации : Федеральный закон от 22.08.1996 № 126-ФЗ (в ред. от 31.07.2025) (с изм. и доп., вступ. в силу

01.12.2025) // Собрание законодательства РФ. — 1996. — № 35. — Ст. 4136.

30. Об основных гарантиях прав ребенка в Российской Федерации : Федеральный закон от 24.07.1998 № 124-ФЗ (в ред. от 28.12.2024) // Собрание законодательства РФ. — 1998. — № 31. — Ст. 3802.

31. О рекламе : Федеральный закон от 13.03.2006 № 38-ФЗ (в ред. от 31.07.2025) (с изм. и доп., вступ. в силу 01.09.2025) // Собрание законодательства РФ. — 2006. — № 12. — Ст. 1232.

32. О защите детей от информации, причиняющей вред их здоровью и развитию : Федеральный закон от 29.12.2010 № 436-ФЗ (в ред. от 30.11.2024) // Собрание законодательства РФ. — 2011. — № 1. – Ст. 48.

33. Судебная статистика РФ // URL: https://stat.апи-пресс.рф/stats/adm/t/31/s/66 (дата обращения: 23.12.2025).

REFERENCES

1. O Strategii razvitiya informatsionnogo obshchestva v Rossijskoj Federatsii na 2017—2030 gody : ukaz Prezidenta Rossijskoj Federatsii ot 09.05.2017 № 203 // Sobranie zakonodatel′stva RF. — 2017. — № 20. — St. 2901.

2. O Strategii natsional′noj bezopasnosti Rossijskoj Federatsii : ukaz Prezidenta Rossijskoj Federatsii ot 02.07.2021 № 400 // Sobranie zakonodatel′stva RF. — 2021. — № 27 (ch. II). — St. 5351.

3. Ob utverzhdenii Osnov gosudarstvennoj politiki po sokhraneniyu i ukrepleniyu traditsionnykh rossijskikh dukhovno-nravstvennykh tsennostej : ukaz Prezidenta Rossijskoj Federatsii ot 09.11.2022 № 809 // SPS «Konsul′tantPlyus».

4. Tekst poslaniya Prezidenta Federal′nomu Sobraniyu 2013 goda // URL: https://rg.ru/2013/12/12/poslanie.html (data obrashcheniya: 12.01.2026).

5. Zanina T. M., Orekhova N. A. Obyazatel′noe lechenie lits, upotreblyayushchikh narkoticheskie sredstva i psikhotropnye veshchestva, kak osobyj vid administrativnogo prinuzhdeniya // Vestnik Voronezhskogo instituta MVD Rossii. — 2017. — № 3. — S. 123—127.

6. O vnesenii izmenenij v Kodeks Rossijskoj Federatsii ob administrativnykh pravonarusheniyakh : Federal′nyj zakon ot 08.08.2024 № 285-FZ // Sobranie zakonodatel′stva RF. — 2024. — № 33 (ch. I). — St. 4921.

7. Administrativnaya otvetstvennost′ za pravonarusheniya, predusmotrennye stat′yami 6.13, 6.13[1] KoAP RF : uchebnoe posobie / A. Yu. Ivanov, N. N. Tsukanov, P. Yu. Ovsyannikov [i dr.] ; pod obshch. red. N. N. Tsukanova. — Krasnoyarsk : SibYuI MVD Rossii, 2024. — S. 18—19.

8. Anisiforova M. V. Administrativnaya otvetstvennost′ za narusheniya zakonodatel′stva v sfere oborota narkoticheskikh sredstv, psikhotropnykh veshchestv i ikh prekursorov : dis. … kand. yurid. nauk. — M., 2018. — 254 s.

9. Stepanova O. A. Pravovoe regulirovanie sudebnogo poryadka peresmotra postanovlenij i reshenij po delam ob administrativnykh pravonarusheniyakh : dis. … kand. yurid. nauk. — M., 2014. — 243 s.

10. Rozhkova E. V. Administrativnaya otvetstvennost′ za pravonarusheniya v sfere oborota narkoticheskikh sredstv, psikhotropnykh veshchestv i ikh prekursorov : avtoref. dis. … kand. yurid. nauk. — Saratov, 2009. — 27 s.

11. Slobodchuk S. V. Administrativnaya otvetstvennost′ za pravonarusheniya, svyazannye s narkotikami : avtoref. dis. … kand. yurid. nauk. — Voronezh, 2005. — 24 s.

12. Kornev A. A. Administrativno-pravovye sredstva bor′by s nezakonnym oborotom narkotikov v Rossijskoj Federatsii : avtoref. dis. … kand. yurid. nauk. — SPb., 2010. — 23 s.

13. Nasonov A. N. Administrativno-pravovoe regulirovanie oborota narkoticheskikh sredstv i psikhotropnykh veshchestv : avtoref. dis. … kand. yurid. nauk. — M., 2008. — 31 s.

14. Gazizov D. A., Gazizova T. G. Administrativnaya otvetstvennost′ za propagandu narkoticheskikh sredstv // Pravo i praktika. — 2013. — № 1. — S. 88—94.

15. Tsukanov N. N. Administrativnaya otvetstvennost′ za pravonarusheniya v sfere oborota narkotikov : ucheb. posobie. — M. : INFRA-M, 2015. — S. 74.

16. Rean A. A., Stavtsev A. A. Sem′ya i deti kak faktory psikhologicheskogo blagopoluchiya i zhiznestojkosti lichnosti pedagogov Rossijskoj Federatsii // Izvestiya Rossijskogo gosudarstvennogo pedagogicheskogo universiteta im. A. I. Gertsena. — 2024. — № 214. — S. 116—126.

17. Drobyazko S. R. Obraz zhizni lichnosti kak predmet konstitutsionno-pravovoj zashchity na primere voprosa o smene pola // Konstitutsionnoe i munitsipal′noe pravo. — 2023. — № 1. — S. 55.

18. V SShA sud razreshil transgenderam sluzhit′ v vooruzhennykh silakh // URL: https://www.rbc.ru/rbcfreenews/5a2f85a99a7947245ec482aa (data obrashcheniya: 23.07.2025).

19. V SShA transgenderam vnov′ razreshili sluzhit′ v armii // URL: https://iz.ru/1145135/2021-04-01/pentagon-utverdil-pravila-priema-transgenderov-na-sluzhbu-v-vs-ssha.

20. Ponkin I. V. Neklassicheskie vojny : monografiya. M. : INFRA-M, 2019. — S. 87.

21. Ob osnovakh okhrany zdorov′ya grazhdan v Rossijskoj Federatsii : Federal′nyj zakon ot 21.11.2011 № 323-FZ (v red. ot 17.11.2025) st. 2 // Sobranie zakonodatel′stva RF. — 2011. — № 48. — St. 6724.

22. Epifanova E. V. Nravstvennoe zdorov′e kak ob″ekt administrativno-pravovoj okhrany // Administrativnoe pravo i protsess. — 2025. — № 2. — S. 41.

23. Ivashkina E. S. Voprosy tselesoobraznosti vvedeniya st. 6.212 KoAP RF // Rossiya v XXI veke: global′nye vyzovy, prioritety i perspektivy razvitiya : materialy XVII Vserossijskoj nauchno-prakticheskoj konferentsii studentov i molodykh uchenykh, Barnaul, 16—17 aprelya 2024 goda. — Barnaul : Pyat′ plyus, 2024. — S. 217—219.

24. Kisin V. R., Popugaev Yu. I. O kollizii (konkurentsii) norm, predusmatrivayushchikh administrativnuyu i ugolovnuyu otvetstvennost′, i sposoby ee razresheniya // Nauchnyj portal MVD Rossii. — 2013. — № 2(22). — S. 79—88.

25. Konstitutsiya Rossijskoj Federatsii (prinyata vsenarodnym golosovaniem 12.12.1993, s izmeneniyami, odobrennymi v khode obshcherossijskogo golosovaniya 01.07.2020) // SPS «Konsul′tantPlyus».

26. Berestovoj A. N. Tsvetkov P. V. Zakonodatel′naya reglamentatsiya voprosov, kasayushchikhsya protivodejstviya novym formam deviantnogo povedeniya v seti Internet // Ot Pskovskoj sudnoj gramoty k printsipam sovremennogo pravosudiya: traditsii i novatsii v rossijskom sudoproizvodstve : sbornik nauchnykh statej vserossijskoj nauchno-prakticheskoj konferentsii, Pskov, 26—27 sentyabrya 2024 goda. — SPb. : Tsentr nauchno-informatsionnykh tekhnologij «Asterion», 2024. — S. 287—297.

27. Bol′shaya rossijskaya entsiklopediya // URL: https://old.bigenc.ru/medicine/text/2708885?ysclid=mfw7rw2w9p78900878.

28. Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii : Federal′nyj zakon ot 27.07.2006 № 149-FZ (v red. ot 24.06.2025) (s izm. i dop., vstup. v silu 01.01.2026) // Sobranie zakonodatel′stva RF. — 2006. — № 31 (1 ch.). — St. 3448.

29. O gosudarstvennoj podderzhke kinematografii Rossijskoj Federatsii : Federal′nyj zakon ot 22.08.1996 № 126-FZ (v red. ot 31.07.2025) (s izm. i dop., vstup. v silu 01.12.2025) // Sobranie zakonodatel′stva RF. — 1996. — № 35. — St. 4136.

30. Ob osnovnykh garantiyakh prav rebenka v Rossijskoj Federatsii : Federal′nyj zakon ot 24.07.1998 № 124-FZ (v red. ot 28.12.2024) // Sobranie zakonodatel′stva RF. — 1998. — № 31. — St. 3802.

31. O reklame : Federal′nyj zakon ot 13.03.2006 № 38-FZ (v red. ot 31.07.2025) (s izm. i dop., vstup. v silu 01.09.2025) // Sobranie zakonodatel′stva RF. — 2006. — № 12. — St. 1232.

32. O zashchite detej ot informatsii, prichinyayushchej vred ikh zdorov′yu i razvitiyu : Federal′nyj zakon ot 29.12.2010 № 436-FZ (v red. ot 30.11.2024) // Sobranie zakonodatel′stva RF. — 2011. — № 1. – St. 48.

33. Sudebnaya statistika RF // URL: https://stat.api-press.rf/stats/adm/t/31/s/66 (data obrashcheniya: 23.12.2025).

СВЕДЕНИЯ ОБ АВТОРЕ

Чунихина Екатерина Игоревна. Преподаватель-методист группы методического обеспечения.
Рязанский филиал Московского университета МВД России имени В. Я. Кикотя.
E-mail: katerina_k_92@inbox.ru
Россия, 390043, Рязань, ул. 1-я Красная, 18.

Chunikhina Ekaterina Igorevna. Teacher-methodologist of the methodological support group.
Ryazan branch of the Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot.
E-mail: katerina_k_92@inbox.ru
Work address: Russia, 390043, Ryazan, 1st Krasnaya Str., 18.

Ключевые слова: духовно-нравственные ценности; правовая неопределенность; административное правонарушение; административная ответственность.

Key words: spiritual and moral values; legal uncertainty; administrative offense; administrative responsibility.

УДК 342.9

ИНФОРМАЦИЯ ДЛЯ АВТОРОВ

И. И. Иванов, П. П. Петров

НАЗВАНИЕ СТАТЬИ НА РУССКОМ ЯЗЫКЕ

НАЗВАНИЕ СТАТЬИ НА АНГЛИЙСКОМ ЯЗЫКЕ

Настоящая инструкция одновременно является примером оформления статьи, подготовленной в «Вестник Воронежского института МВД России». В ней содержатся требования, предъявляемые к форматированию текста, оформлению библиографического описания, а также примеры составления ключевых слов и сведений об авторах[1].

Аннотация на английском языке[2].

1. Статья представляется в одном экземпляре, заверенном подписью автора (-ов) с обратной стороны первой страницы, отпечатанном на одной стороне листов формата А4 (210 х 297 мм) на лазерном принтере.

Статья должна быть снабжена аннотациями на русском и английском языках, списком литературы (на русском языке и транслитерированным). К статье должны быть приложены сведения об авторах на русском и английском языках с указанием Ф.И.О., места работы (название организации в именительном падеже), занимаемой должности, учёной степени, учёного звания и полного почтового (служебного и домашнего) адреса *(пример см. ниже)*, а также адреса электронной почты.

К статье также прилагается список ключевых слов на русском и английском языках, наиболее полно характеризующий её тематику *(пример см. ниже)*. В соответствии с тематикой статьи автором указывается её **УДК**.

Предоставляемая электронная версия статьи в виде файла MS Word в формате ***.docx** должна соответствовать распечатке и включать вышеперечисленные сведения об авторе (-ах) и ключевые слова. Файл должен иметь в названии фамилию автора (-ов), *например:* Ivanov.docx, Ivanov-Petrov.docx.

К статье прилагаются следующие сопроводительные документы:

1) выписка из протокола заседания кафедры (при ее наличии по месту работы автора) с рекомендацией к опубликованию;

2) экспертное заключение об отсутствии сведений, запрещенных к опубликованию в открытой печати, заверенное гербовой печатью учреждения;

3) заявление автора(-ов) о том, что статья публикуется впервые, не содержит в значительном объеме изданных ранее материалов и не передана в другие редакции;

4) согласие автора(-ов) на размещение сведений об авторе(-ах), указанных выше (за исключением домашнего адреса):

- в открытой печати в журнале «Вестник Воронежского института МВД России» и на сайте Воронежского института МВД России;

[1] Аннотация к статье на русском языке.

[2] Аннотация на английском языке составляется автором и приводится в обязательном порядке.

- в информационных системах Российского индекса научного цитирования (РИНЦ), Российского центра научной информации (РЦНИ);

- в иной системе научного цитирования, определяемой международными договорами (соглашениями) Российской Федерации и (или) рекомендациями Высшей аттестационной комиссии при Министерстве науки и высшего образования Российской Федерации.

2. Объём статьи не должен превышать:

- по направлению «Юридические науки» — 12 стр.;

- по направлениям «Радиотехника и связь», «Информатика, вычислительная техника и управление» — 9 стр.

По направлениям «Радиотехника и связь», «Информатика, вычислительная техника и управление» журнал не публикует статей, носящих преимущественно реферативный характер. Статьи обзорного характера могут предоставляться только после предварительного согласования с редакцией.

Статьи по направлениям «Радиотехника и связь», «Информатика, вычислительная техника и управление» обязательно должны быть структурированы, отдельные разделы статей должны иметь подзаголовки, в том числе:

- введение, в котором обосновывается актуальность работы;

- разделы, в которых описываются полученные результаты и их новизна;

- заключение, содержащее выводы и/или направления дальнейших исследований.

3. Все поля на страницах должны быть одинаковы и равны 25 мм. Номера страниц не проставляются.

4. Статья должна быть набрана шрифтом нормальной жирности, прямого начертания гарнитуры Times New Roman, с одинарным межстрочным интерлиньяжем (интервалом). Абзацный отступ должен быть одинаков и равен 1,25 см.

Кегль (размер) основного шрифта должен быть равен:

- для статей по направлению «Юридические науки» — 14 пунктов;

- для статей по направлениям «Радиотехника и связь», «Информатика, вычислительная техника и управление» — 12 пунктов (в т.ч. в формулах, подготовленных при помощи формульного редактора MS Equation).

5. Рисунки и таблицы (кегль используемого шрифта — 12 пунктов) должны быть размещены в тексте после абзацев, содержащих ссылки на них.

Таблица 1

Заголовок таблицы

Боковик таблицы	Головка таблицы			
	Текст	Текст	Текст	Текст

Размещение таблиц, рисунков, диаграмм, схем и другого иллюстративного материала на страницах с альбомной (горизонтальной) ориентацией не допускается. Графики, диаграммы не должны иметь сплошную (в т.ч. цветную) заливку.

Размеры рисунков должны быть по возможности минимальны, но обеспечивать их дальнейшее качественное полиграфическое воспроизведение.



Рис. 1. Название рисунка

Отступ от рисунка до текста сверху и снизу должен быть равен 10 мм. Подрисуночная подпись ставится по центру страницы без абзацного отступа. Рисунок должен выполняться средствами MS Word, иметь общую группировку всех объектов, входящих в него, быть центрированным относительно полосы набора.

6. Название статьи набирается на русском и английском языках полужирным шрифтом ЗАГЛАВНЫМИ БУКВАМИ без абзацного отступа и центрируется относительно полосы набора.

7. Единицы физических величин должны соответствовать системе единиц СИ. Названия химических элементов в тексте пишутся полностью.

8. Формулы подготавливаются при помощи редактора формул MS Equation 3.0. Нумерация формул осуществляется арабскими цифрами в круглых скобках, выровненными по правому краю текста, *например*:

$$A = B + C: (2K^2 + n_3). \quad (1)$$

9. Нумерация ссылок на литературу осуществляется арабскими цифрами в квадратных скобках, *например*: «Как указано П. П. Петровым [2], данный эффект проявляется при…».

10. Библиография должна быть оформлена в соответствии с ГОСТ Р 7.05 — 2008 «Библиографическая ссылка». Список использованной литературы, на которую ссылается автор, приводится в конце статьи (*см. пример ниже*). Сноски (как внизу каждой страницы, так и в конце статьи) не допускаются.

ПРИМЕР ОФОРМЛЕНИЯ СПИСКА ЛИТЕРАТУРЫ

ЛИТЕРАТУРА

1. Синцов Г. В. К вопросу об этическом воспитании юристов современной России // Российская юстиция. — 2012. — № 11. — С. 37—42.

2. Братусь Б. С. Нравственное сознание личности. — М. : Знание, 1985. — 64 с.

3. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка. — 4-е изд. — М., 1997. — 790 с.

4. О полиции : Федеральный закон от 7 февраля 2011 г. № 3-ФЗ (в ред. от 3 марта 2012 г.) // Собрание законодательства Российской Федерации. — 2011. — № 7. — Ст. 900.

5. Желонкин С. С. Недействительность антисоциальных сделок, нарушающих основы правопорядка и нравственности : автореф. дис. ... канд. юрид. наук : 12.00.03. — СПб., 2011. — 25 с.

REFERENCES

1. Sintsov G. V. K voprosu ob eticheskom vospitanii yuristov sovremennoy Rossii // Rossiyskaya yustitsiya. — 2012. — № 11. — S. 37—42.

2. Bratus B. S. Nravstvennoe soznanie lichnosti. — M. : Znanie, 1985. — 64 s.

3. Ozhegov S. I., Shvedova N. Yu. Tolkovyiy slovar russkogo yazyika. — 4-e izd. — M., 1997. — 790 s.

4. O politsii : Federalnyiy zakon ot 7 fevralya 2011 g. № 3-FZ (v red. ot 3 marta 2012 g.) // Sobranie zakonodatelstva Rossiyskoy Federatsii. — 2011. — № 7. — St. 900.

5. Zhelonkin S. S. Nedeystvitelnost antisotsialnyih sdelok, narushayuschih osnovyi pravoporyadka i nravstvennosti : avtoref. dis. ... kand. yurid. nauk : 12.00.03. — SPb., 2011. — 25 s.

ПРИМЕР ОФОРМЛЕНИЯ СВЕДЕНИЙ ОБ АВТОРАХ

СВЕДЕНИЯ ОБ АВТОРЕ (-АХ)[1]

Иванов Иван Иванович. Профессор кафедры теоретической физики. Доктор физико-математических наук, доцент.
Воронежский государственный педагогический университет.
E-mail: aspo@vspu.ac.ru
Россия, 394065, Воронеж, ул. Ленина, 86.

Петров Петр Петрович. Доцент кафедры гражданского, трудового и финансового права. Кандидат юридических наук, доцент.
Воронежский институт МВД России.
E-mail: vorhmscl@comch.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Ivanov Ivan Ivanovich. Professor of the chair of Theoretical Physics. Doctor of Sciences (Physics and Mathematics), Assistant Professor.
Voronezh State Pedagogical University.
E-mail: aspo@vspu.ac.ru
Work address: Russia, 394006, Voronezh, Lenina Str., 86.

Petrov Pyotr Petrovich. Assistant Professor of the chair of Civil, Labor and Financial Law. Candidate of Sciences (Jurisprudence / Law), Assistant Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: vorhmscl@comch.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: фазоманипулированный сигнал; мешающие сигналы; фазовый детектор; алгоритм обработки.

Key words: phase-manipulated signal; interfering signals; phase detector; processing algorithm.

УДК 517.9 (указывается автором).

Домашний почтовый адрес (полностью)[2].

Подпись (-и), дата _____ «___» _____ 202 ___ г.

[1] Оформляются на отдельном листе и включаются в состав основного файла. Не входят в объём статьи.
[2] Домашний адрес в журнале не публикуется.

AUTHOR'S GUIDELINES

I. I. Ivanov, P. P. Petrov

TITLE OF THE ARTICLE IN RUSSIAN

TITLE OF THE ARTICLE IN ENGLISH

These guidelines is also an example of layout of papers submitted to "Vestnik of Voronezh Institute of the Ministry of Interior of Russia". It contains requirements to the text formatting, bibliographic references and examples of key words and author affiliations.

1. Please submit one laser copy of the article printed on one side of white A4 paper (210 × 297 mm) and signed by the author overleaf the head page.

The paper must be accompanied by an abstract in Russian and in English. The article should enclose references and author affiliations in Russian and in English indicating author's full name, place of employment, job title, scientific degrees and academic titles, work and home address (*see the example below*) and e-mail address.

The article is accompanied by key words in Russian and in English which should reflect the content of the article. **UDC code is** specified by the author according to the question area of the paper.

The softcopy of the article should be submitted in MS Word file format — ***docx**. and must be identical to the hardcopy including author affiliations and key words mentioned above. The file name should contain the author's surname, *for example*, Ivanov.docx, Ivanov-Petrov.docx.

Each article should contain the following enclosures:

1) an extract from the minutes of the department meeting (if available at the author's place of work) with a recommendation for publication;

2) an expert opinion on the absence of information prohibited from publication in the open press, certified by the official seal of the institution;

3) the statement of the author(s) that the article is being published for the first time does not contain a significant amount of previously published materials and has not been transferred to other editorial offices;

4) the consent of the author(s) to post the information about the author(s) indicated above (with the exception of the home address):

- in the open press in the journal "Vestnik of Voronezh Institute of the Ministry of the Interior of Russia" and on the website of the Voronezh Institute of the Ministry of the Interior of Russia;

- in the information systems of the Russian Science Citation Index (RISC), the Russian Center for Scientific Information (RCNI);

- in another scientific citation system determined by international treaties (agreements) Of the Russian Federation and (or) recommendations of the Higher Attestation Commission under the Ministry of Science and Higher Education of the Russian Federation.

2. Submitted articles should not exceed
- in the field “Legal sciences” — 12 pages;
- in the fields “Radioengineering and Communication”, “Informatics, Computer Engineering and Automatic Control System” — 9 pages.

3. All page margins should be 25 mm. Pages aren’t numbered.

4. Articles should be typed in normal block-letter type Times New Roman font with single line spacing. The paragraph indent is 1,25 cm.

Base font size should be of 14 points for articles in the fields “Legal sciences”; 12 points for articles in the fields “Radioengineering and Communication”, “Informatics, Computer Engineering and Automatic Control System” (including equations edited using MS Equation editing program).

5. Figures and tables (12 points font size) should be placed right after the referenced paragraphs.

Table 1

Table heading

Stub column	Column heading			
	Text	Text	Text	Text

Tables, figures, diagrams, schemes and other illustrations shouldn’t be inserted in landscape oriented pages. Graphs and diagrams shouldn’t have solid (colour) fill.

Figures should be of minimal possible size which provides their proper printing quality.

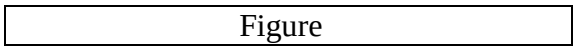


Fig.1 Figure caption

Upper and lower spacing between the figure and the text should be adjusted at 10 mm. The figure caption is centered on the page with no paragraph indention. Figures should be drawn using MS Word text editor; all the objects must be grouped together and centered.

6. The title of the paper in Russian and in English is centered and typed with **bold CAPITAL LETTERS** without an indent.

7. SI units should be used for physical magnitudes. Chemical symbols are written without any contraction.

8. Formulas are created with the MS Equation editing program. They are numbered using Arabic numerals in parentheses, aligned right. *For example*:

$$A = B + C: (2K^2 + n_3). \quad (1)$$

9. Quoted literature is numbered using Arabic numerals in square brackets, *for example*: “As it is stated by P.P. Petrov [2], this effect is revealed…”.

10. References must be listed in accordance with State Standard 7.05.-2008 “Bibliographic References”. References are placed at the end of the article *(see the sample below)*. **It is unacceptable to use endnotes and footnotes**.

EFERENCES SAMPLE

REFERENCES

1. Ivanov I. I. Fizika. — M. : Nauka, 1985. — 167 s. *(author, title of book, place of publication, publishing house, year of publication, total amount of pages are required).*

2. Matematika / pod red. P. P. Petrova. — M. : Vyisshaya shkola, 1993. — 125 s. (*editor is required*).

3. Sidorov S. S., Antonov A. A. Problemyi vospitaniya nesovershennoletnih // Militsiya. — 1997. — № 2. — S. 25—26. (*author(s), title of article, responsibility data, serial publication (journal or newspaper), year of publication and issue, page number(s) are required*).

4. Kurs obschey fiziki : ucheb. posobie dlya studentov vtuzov. — 2-e izd., pererab. — T. 1. Mehanika / pod obsch. red. P. P. Popova. — M. : Nauka, 1987. — 345 s. (*type of multivolume publication and volume are required*).

5. Kovalev K. K. Oborudovanie s pnevmovakuumnyim privodom : dis. ... kand. tehn. nauk. — M., 1982. — 212 s. (*reference to thesis*).

SAMPLE AUTHOR AFFILIATIONS

AUTHOR AFFILIATIONS

Ivanov Ivan Ivanovich. Professor of the chair of Theoretical Physics. Doctor of Physics and Mathematics, Assistant Professor.

Voronezh State Pedagogical University.

Work address: Russia, 394006, Voronezh, Lenina Str., 86.

Petrov Petr Petrovich. Assistant Professor of the chair of Civil, Labour and Financial Law, PhD in Law, Assistant Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Key words: phase-manipulated signal; interfering signals; phase detector; processing algorithm.

UDC (is stated by the author)

Personal address (in full):

Signature(s), date _____«____»_____20____