
ВЕСТНИК

Воронежского института МВД России

№ 2 / 2025

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 № ФС 77 - 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 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, заслуженный сотрудник органов внутренних дел Российской Федерации, 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, заведующая 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, начальник кафедры Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С. М. Штеменко Министерства обороны Российской Федерации, доктор технических наук, доцент;
Ю. В. Сорокина, профессор кафедры теории и истории государства и права Воронежского государственного университета, доктор юридических наук, профессор;
Ю. Н. Старилов, декан юридического факультета Воронежского государственного университета, доктор юридических наук, профессор;
В. И. Сумин, профессор кафедры информационной безопасности телекоммуникационных систем Воронежского института ФСИН России, 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, проректор по научной работе и стратегическому развитию Центрально-Казахстанской Академии, 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. Калининская, Н. Ф. Палихова — редакторы;
М. М. Старченко, С. М. Шапиро — верстка номера

Подписано в печать 24.06.2025
 Выход в свет 30.06.2025
 Формат 60x84^{1/8}
 Усл. печ. л. 34,41
 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, 2025

VESTNIK

of Voronezh Institute of the Ministry of the Interior of Russia

№ 2 / 2025

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. FS 77 - 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 specialties: 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 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 Penitentiary and Criminal Law Chair of Voronezh Institute of the Russian Federal Penitentiary Service, Honored Worker of the Interior of the Russian Federation, 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 the Belgorod State National Research University Law Institute, Doctor of Law, Professor;

A. B. Sizonenko, Head 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, Associate 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, Dean of Juridical Faculty of Voronezh State University, Doctor of Law, Professor;

V. I. Sumin, Professor of the Chair of Information Security of Telecommunication Systems of Voronezh Institute of the Russian Federal Penitentiary Service, 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, Vice-Rector for Research and Strategic Development of Central Kazakhstan Academy, 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;

M. M. Starchenko, S. M. Shapiro — Layout Designer

Passed for printing on June 24th, 2025
 Data of edition June 30th, 2025
 Format 60x84 ¹/₈
 Conventional printed sheets 34,41
 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://bi.mbd.pf/Nauka/nauchnij-zhurnal-vestnik>
 ISSN 2071-3584
 © Voronezh Institute of the Ministry of the Interior of Russia, 2025

СОДЕРЖАНИЕ

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Попова А. Д., Дровникова И. Г. Результаты экспериментального исследования защищенности программного обеспечения автоматизированных систем органов внутренних дел.....	9
Панкова М. А., Ожерельев В. В., Коротков Л. Н. Моделирование тонкопленочной базовой структуры нелинейных радиоэлектронных компонентов	21
Пьянков О. В., Терентьев А. А., Захаров М. С. Прогноз потребностей подразделений органов внутренних дел в средствах связи и автоматизации	30
Бабкин А. Н., Акчурина Л. В., Алексеенко С. П. Графический способ обнаружения внутреннего нарушителя информационно-телекоммуникационной сети организации.....	38
Звягин Д. С., Масловская А. А. Моделирование процесса противодействия получению видовой информации при помощи беспилотных воздушных судов.....	44
Тихомирова А. А., Фурсова А. В., Яковлев А. В. Представление теоретико-множественной модели угроз безопасности информации сетями Петри	52
Жирнов А. А. Модель формирования графика участия подразделений в проекте противодействия криминальным угрозам профилактического типа: скалярная оптимизация.....	65

РАДИОТЕХНИКА И СВЯЗЬ

Володько А. В., Кузьменко Р. В., Андреева Н. А. К вопросу о реализации амплитудного метода самонаведения в системах перехвата беспилотных воздушных судов	74
Белозерцев Ю. В., Климов А. И., Петров М. С. Широкополосная антенна для носимых радиостанций диапазона УВЧ	83
Ерошенко Д. А., Климов А. И., Фомин Н. Е. Полосковая антенная решетка диапазона КВЧ.....	94
Шерстюков С. А., Толстых О. В. Алгоритмы и устройства радиоэлектронного противодействия беспилотным летательным аппаратам с бортовыми автоматическими радиопеленгаторами	103
Калинин В. И., Лунев А. Д., Чернышов А. Г., Попов Д. А. Алгоритм совместной адаптации по мощности излучения передатчиков и скорости передачи сообщений в радиолиниях специального назначения.....	119
Лазарев И. В. Синтез модели надежности многорубежных периметрических охранных систем распределённых объектов.....	131

ЮРИДИЧЕСКИЕ НАУКИ

Латыпов В. С., Галлямов Б. А. Использование искусственного интеллекта в уголовном судопроизводстве: вопросы правового регулирования	142
Насонова И. А., Красноруцкая Т. А. О дознавателе как участнике отечественного уголовного судопроизводства и необходимости коррекции нормативного определения, ему посвященного.....	149
Ахмедов У. Н., Кретинин А. В. Типовые процессуальные нарушения (ошибки), встречающиеся при вынесении органом дознания решения об отказе в возбуждении уголовного дела (на примере анализа прокурорской правоприменительной практики)	155
Буслов М. М., Иванченко О. С., Пугачев А. В. Незаконный оборот оружия в России: криминологическая характеристика и меры предупреждения.....	163

Гайдин А. И., Дутов Ю. И., Дутов Н. Ю., Касьянова Е. В. Проблемы расследования уголовных дел о преступлениях, связанных с оборотом средств платежей, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств	170
Задоров А. Г. К вопросу о возможности установления последовательности пересекающихся штрихов, выполненных различными материалами письма, в рамках производства технико-криминалистической экспертизы документов	182
Звягин И. С. Применение беспилотных летательных аппаратов для обеспечения криминалистических задач	189
Иванченко Р. Б., Польшиков А. В., Демидова О. В. Новые психоактивные вещества: общемировые тенденции и вызовы правоохранительным системам.....	194
Караваяев А. А., Галустян А. Г. К вопросу о совершенствовании форм и методов пропаганды безопасности дорожного движения	202
Кокорева Л. В., Кокорев Р. А. Перспективы совершенствования применения информационных технологий при проведении следственных действий.....	208
Новикова Е. П., Чернышова К. С. Сваттинг как разновидность терроризма: уголовно-правовой аспект.....	215
Пидусов Е. А. К вопросу о сущности криптовалюты.....	220
Пучнина М. Ю. Комплексный подход к обеспечению безопасности несовершеннолетних в сети Интернет: психологические и криминологические аспекты	225
Савицкая И. Г. Система следственных действий Российской Федерации и Республики Камерун: сравнительно-правовой анализ	230
Трусов Н. А., Кравцов И. А., Лукьянов Р. И. Современный отечественный опыт правовой регламентации института наказа избирателей: значение, причины, последствия	235
Чмырёв С. Н., Бохан А. П., Тимашкова Е. В. Молодёжный политический экстремизм как социальное явление	240
Антонова Л. Б. Реализация алкогольной продукции несовершеннолетним: вопросы привлечения к административной ответственности	245
Волкодавова Г. Н. Персональная ответственность руководителя территориального органа внутренних дел при принятии управленческого решения.....	252
Полухин Д. И., Жуков М. М., Телков А. Ю. Поиск текстовой информации на объектах компьютерной памяти при расследовании преступлений в сфере информационных технологий	258
Родин С. Г. Уголовная ответственность за фиктивную постановку на миграционный учет (ст. 322.3 УК РФ): вопросы дифференциации и квалификации	268
Смагин П. Г. Использование технологий машиночитаемого права в уголовном судопроизводстве	275
Титов А. А. Методы противодействия криптопреступности с использованием криминалистического анализа данных блокчейна	282
Информация для авторов.....	289

CONTENTS

INFORMATICS, COMPUTER ENGINEERING AND AUTOMATIC

Popova A. D., Drovnikova I. G. The results of an experimental study of the security of internal affairs bodies automated systems software	9
Pankova M. A., Ozhereliev V. V., Korotkov L. N. Modeling of thin-film base structure of nonlinear radioelectronic components	21
Pyankov O. V., Terentyev A. A., Zakharov M. S. Forecast of the needs of internal affairs units in communications and automation	30
Babkin A. N., Akchurina L. V., Alekseenko S. P. Graphic method of detecting internal intruder of information and telecommunication network of organization	38
Zvyagin D. S., Maslovskaya A. A. Modeling of the process of countering the acquisition of specific information using unmanned aircraft	44
Tikhomirova A. A., Fursova A. V., Yakovlev A. V. Presentation of a set-theoretical model of information security threats by Petri nets	52
Zhirnov A. A. A model for forming a schedule for the participation of units in a project to counteract criminal threats of a preventive type: scalar optimization	65

RADIOENGINEERING AND COMMUNICATION

Volodko A. V., Kuzmenko R. V., Andreeva N. A. On the question of implementing the amplitude self-guidance method in unmanned aircraft interception systems	74
Belozertsev Yu. V., Klimov A. I., Petrov M. S. Wideband antenna for uhf band portable radios	83
Eroshenko D. A., Klimov A. I., Fomin N. E. Ehf-band strip antenna array	94
Sherstyukov S. A., Tolstykh O. V. Algorithms and devices for radioelectronic counteraction to unmanned aerial vehicles with on-board automatic radio direction finders	103
Kalinin V. I., Lunev A. D., Chernyshov A. G., Popov D. A. Algorithm for joint adaptation in transmitter radiation power and message transmission rate in radio links special purpose	119
Lazarev I. V. Synthesis of a reliability model for multi-border perimeter security systems of distributed facilities	131

LEGAL SCIENCES

Latypov V. S., Gallyamov B. A. Using artificial intelligence in criminal proceedings: regulatory issues	142
Nasonova I. A., Krasnorutskaya T. A. On the interrogator as a participant in domestic criminal proceedings and the need to correct the normative definition devoted to him or her	149
Akhmedov U. N., Cretinin A. V. Typical procedural violations (errors) encountered when the body of inquiry makes a decision to refuse to initiate criminal proceedings (using the example of an analysis of prosecutorial law enforcement practice)	155
Buslov M. M., Ivanchenko O. S., Pugachev A. V. Illegal arms trafficking in Russia: criminological characteristics and preventive measures	163
Gaidin A. I., Dutov Y. I., Dutov N. Y., Kasyanova E. V. The problems of investigating criminal cases of crimes related to the turnover of funds of payments intended for the unlawful acceptance, issuance, transfer of funds	170
Zadorov A. G. On the question of the possibility of establishing a sequence of intersecting strokes made by various writing materials, within the framework of production technical and forensic examination of documents	182

Zvyagin I. S. The use of unmanned aerial vehicles to provide forensic tasks.....	189
Ivanchenko R. B., Polshikov A. V., Demidova O. V. New psychoactive substances: global trends and challenges to law enforcement systems	194
Karavaev A. A., Galustyan A. G. On the question of improving forms and methods of road safety propaganda	202
Kokoreva L. V., Kokorev R. A. Prospects for improving the use of information technology in conducting investigative actions.....	208
Novikova E. P., Chernyshova K. S. Swatting as a type of terrorism: the criminal law aspect...	215
Pidusov E. A. On the issue of the essence of cryptocurrency	220
Puchnina M. Y. An integrated approach to ensuring the safety of minors on the internet: psychological and criminological aspects	225
Savitskaya I. G. The system of investigative actions of the Russian Federation and the Republic of Cameroon: comparative legal analysis	230
Trusov N. A., Kravtsov I. A., Lukyanov R. I. Modern domestic experience of legal regulation of the institution of orders of voters: meaning, reasons, consequences	235
Chmyrev S. N., Bohan A. P., Timashkova E. V. Youth political extremism as a social phenomenon	240
Antonova L. B. Sale of alcoholic beverages to minors: issues of bringing to administrative responsibility	245
Volkodavova G. N. Personal responsibility of the head of the territorial body of internal affairs when making a managerial decision.....	252
Polukhin D. I., Zhukov M. M., Telkov A. Y. Search of text information on computer memory objects in the investigation of crimes in the sphere of information technologies.....	258
Rodin S. G. Criminal liability for fictitious registration for migration (art. 322.3 of the criminal code of the Russian Federation): issues of differentiation and qualification	268
Smagin P. G. The use of machine-readable law technologies in criminal proceedings.....	275
Titov A. A. Methods of countering cryptocrime using forensic analysis blockchain data	282
Information for authors	289

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

А. Д. Попова, адъюнкт

И. Г. Дровникова, доктор технических наук, профессор

РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТАЛЬНОГО ИССЛЕДОВАНИЯ ЗАЩИЩЕННОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

THE RESULTS OF AN EXPERIMENTAL STUDY OF THE SECURITY OF INTERNAL AFFAIRS BODIES AUTOMATED SYSTEMS SOFTWARE

В статье представлены результаты количественной оценки защищенности программного обеспечения (ПО) объектов информатизации органов внутренних дел (ОВД), полученные в ходе проведения вычислительного эксперимента на основе разработанного программного комплекса, на примере офисного пакета LibreOffice. Приведена динамика комплексного показателя защищенности ПО, рассчитаны времена нарушения защищенности и средние интервалы времени между выявлениями уязвимостей для версий пакета, позволяющие производить выбор оптимальной по уровню защищенности версии и осуществлять коррекцию времени устранения актуальных для нее уязвимостей. Перспективы использования результатов исследования связаны с обеспечением безопасной эксплуатации ПО в процессе его жизненного цикла в автоматизированных системах (АС) ОВД.

The article presents the results of a quantitative assessment of the security of the software of the objects of informatization of internal affairs bodies (ATS), obtained during a computational experiment based on the developed software package, using the example of the LibreOffice office suite. The dynamics of the integrated software security indicator is presented, the security breach times and the average time intervals between vulnerability disclosures for package versions are calculated, which allow selecting the optimal security version and correcting the time to eliminate vulnerabilities relevant to it. The prospects for using the research results are related to ensuring the safe operation of software during its lifecycle in ATS automated systems (AS).

Введение. При рассмотрении вопроса обеспечения безопасности служебной информации ограниченного распространения, циркулирующей в современных автоматизированных системах (АС) органов внутренних дел (ОВД), важнейшее значение приобретает осуществление количественной оценки защищенности программного обеспечения (ПО), используемого на объекте информатизации, в процессе его жизненного цикла [1, 2]. Это, в свою очередь, предполагает проведение процедуры оценивания защищенности различных версий ПО и их сравнительного анализа с последующим выбором оптимальной (наиболее защищенной) из версий для ее дальнейшей эксплуатации в системе.

Цель настоящей статьи заключается в верификации ранее разработанного программного комплекса (ПК) анализа и оценки защищенности ПО АС ОВД [3] в ходе проведения экспериментального исследования.

Для реализации поставленной цели с помощью ПК автоматизирован процесс решения следующих задач:

- проведение количественной оценки комплексных показателей защищенности для версий ПО;
- расчет времен нарушения защищенности для версий ПО;
- расчет интервала времени периодического нарушения защищенности версий ПО в процессе эксплуатации в АС ОВД;
- проведение сравнительного анализа полученных результатов эксперимента для версий ПО и выбор оптимальной по уровню защищенности версии для эксплуатации на объекте информатизации ОВД.

Исходные данные и условия проведения эксперимента. Предложенные количественные показатели защищенности ПО в процессе его эксплуатации в АС ОВД рассмотрены в [4]. В [5, 6] описаны разработанные аналитические модели расчета указанных показателей, которые реализованы в [7] в виде алгоритмов их оценки в соответствии с концепциями, характеризующими рациональное поведение системы, — концепциями пригодности, оптимальности и адаптивизации [8]. В [3] представлена структура разработанного ПК анализа и оценки защищенности ПО в процессе его эксплуатации в АС ОВД, написанного на языке программирования Python, реализующего указанные алгоритмы аналитического расчета показателей защищенности ПО с использованием пакета программ MATLAB, рассмотрены основные компоненты структуры. На основе результатов анализа процесса эксплуатации актуальных уязвимостей в ПО ПК позволяет проводить количественную оценку его защищенности в режиме реального времени и выбор наиболее защищенной версии ПО для дальнейшей эксплуатации на конкретных объектах информатизации ОВД.

Верификация разработанного ПК осуществлялась в ходе проведения экспериментального исследования защищенности ПО АС ОВД на примере широко используемого начиная с 2020 г. на объектах информатизации ОВД офисного пакета LibreOffice. Для проведения исследования выбраны девять версий LibreOffice, обновления которых выпущены в 2020—2024 гг.

В качестве исходных данных для проведения экспериментального исследования и определения комплексного показателя защищенности конкретной версии ПО ($V_{30 \text{ ПО}}$) в процессе ее эксплуатации в АС ОВД использованы следующие предварительно полученные результаты вычислительного эксперимента для различных версий ПО, описанные в [9]:

- общее количество уязвимостей в ПО (N);
- количество текущих уязвимостей высокого и критического уровней критичности, имеющих действующие эксплойты, — актуальных в процессе эксплуатации ПО уязвимостей (L);
- средние значения времен выявления и устранения текущей уязвимости в процессе эксплуатации ПО ($\tau_{\text{вы}}$, $\tau_{\text{уу}}$ соответственно);
- временные характеристики эксплуатации уязвимости в ПО в соответствии с разработанной и описанной в [9] графовой моделью процесса эксплуатации уязвимостей в ПО АС ОВД (τ_{ij} , где $i = 0..7$, $j = 1..8$).

При расчете среднего интервала времени между выявлениями уязвимостей в ПО (интервала времени периодического нарушения защищенности ПО) (T_0) с помощью разработанного ПК рассматривалась стационарная система защиты в АС ОВД как многоканальная система массового обслуживания (СМО) [10] с показательным распределением входного потока и потока обслуживаний ($M|M|C$), имеющая $M = 4$ канала обслуживания и $C = 1000$ обслуживающих приборов [5].

Для определения комплексного показателя защищенности ПО V_{30} ПО потребовался расчет показателя временной защищенности ПО $V_{в30}(t)$ в соответствии с рассмотренной в [5] динамической непрерывной аналитической моделью. При проведении расчетов использовались следующие предварительные значения мгновенных вероятностей переходов π_{ij} между состояниями r_{ij} на этапах процесса эксплуатации уязвимости в ПО:

$$\begin{aligned} \pi_{01} &= 1; & \pi_{57} &= 0,99; \pi_{56} = 0,01; \\ \pi_{12} &= 1; & \pi_{67} &= 0,99; \pi_{60} = 0,01; \\ \pi_{23} &= 0,99; \pi_{24} = 0,01; & \pi_{78} &= 1; \\ \pi_{35} &= 0,99; \pi_{30} = 0,01; & \pi_{80} &= 1. \\ \pi_{46} &= 0,99; \pi_{40} = 0,01; \end{aligned}$$

Дальнейшее изменение значений π_{ij} рассчитывалось по формуле (1) [5]:

$$\pi_{ij} = \frac{\tau_{ij}}{\sum_{j \in I} \tau_{ij}}. \quad (1)$$

Данное изменение основано на статистике, полученной в результате обработки экспериментальных данных, которые описывают времена выполнения вредоносных функций в процессе эксплуатации уязвимости нарушителем.

Для определения вероятностно-временных характеристик (ВВХ), раскрывающих динамику эксплуатации уязвимостей в ПО, в [5] использована система интегро-дифференциальных уравнений (2), описывающих полные вероятности переходов полумарковского процесса (ПМП) из всех возможных состояний в конечное (поглощающее) состояние в течение интервала времени, не превышающего t :

$$p_i(t) = \pi_{in} F_i(t) + \sum_{j=1}^{n-1} \pi_{ij} \int_0^t \varphi_i(\tau) p_j(t - \tau) d\tau, \quad i = 0..n - 1, \quad (2)$$

где: $p_i(t)$ — вероятность достижения находящимся в i -м состоянии ПМП конечного состояния n за время, не превышающее t ; π_{ij} — вероятности переходов ПМП из i -го состояния в j -е состояние при условии нахождения ПМП в состоянии i ; $F_i(t) = 1 - e^{-\lambda_i t}$ — функция распределения времени пребывания ПМП в состоянии i ; $\lambda_i = \frac{1}{\tau_i}$ — интенсивность перехода ПМП из i -го состояния в конечное состояние n ; τ_i — среднее значение времени нахождения ПМП в i -м состоянии; $\varphi_i(\tau) = F'_i(\tau) = \lambda_i e^{-\lambda_i \tau}$ — плотность распределения вероятностей (ПРВ) для случайной величины τ , описывающей время пребывания ПМП в i -м состоянии; $p_j(t - \tau)$ — вероятность последовательного достижения находящимся в i -м состоянии ПМП промежуточного состояния j и конечного состояния n , учитывающая временные задержки переходов ПМП. При расчете вероятности и ПРВ использовался экспоненциальный закон распределения времени срабатывания.

Согласно подробно описанной в [9, 11] графовой модели процесса эксплуатации уязвимостей в ПО АС ОВД, представленной на рисунке 1, из предпоследнего состояния 7 возможен единственный переход — в конечное состояние 8, таким образом, сумма по всем промежуточным состояниям в выражении (2) становится равной нулю. Учитывая

конкретные значения вероятности перехода π_{78} и среднего времени τ_{78} пребывания рассматриваемого процесса в состоянии 7 с его последующим переходом в состояние 8, получим следующее уравнение для расчета вероятности достижения находящимся в 7-м состоянии ПМП конечного состояния 8 за промежуток времени, не превышающий t :

$$p_7(t) = \pi_{78} F_7(t) = \pi_{78} \left(1 - e^{-\frac{t}{\tau_{78}}} \right) = 1 - e^{-\frac{t}{\tau_{78}}}. \quad (3)$$

В качестве одного из основных показателей незащищенности ПО в АС ОВД рассматривается величина $P_{30}(t)$ — вероятность перехода процесса эксплуатации актуальных уязвимостей из начального состояния в конечное. Она равна вероятности нарушения защищенности ПО за время, не превышающее времени восстановления его эксплуатационной информационной безопасности (ЭИБ) [5, 6].

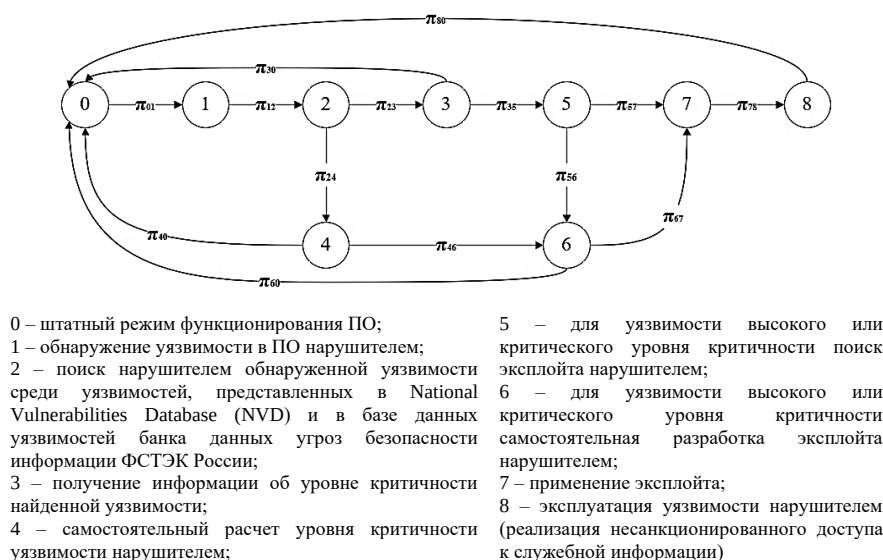


Рис. 1. Графовая модель процесса эксплуатации уязвимостей в ПО АС ОВД:

Анализ результатов эксперимента. На рисунке 2 представлен интерфейс разработанного ПК для проведения экспериментального исследования защищенности ПО АС ОВД.

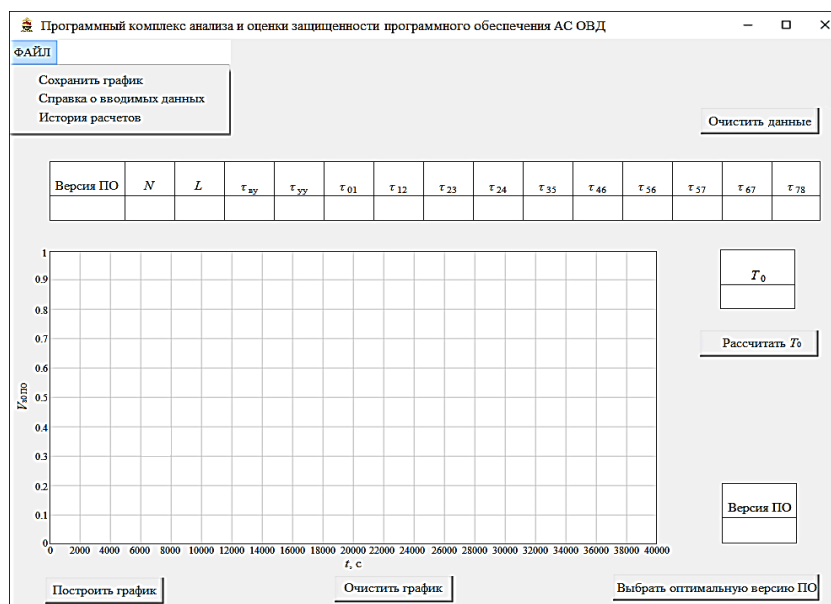
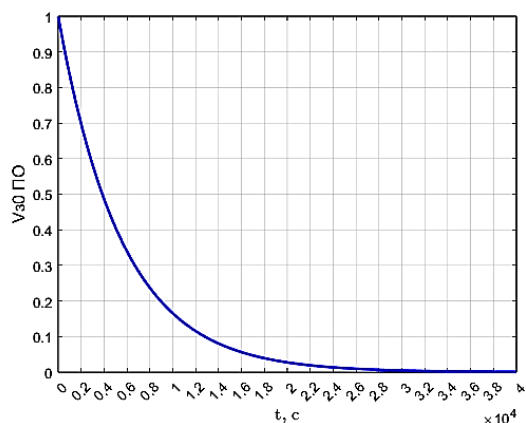
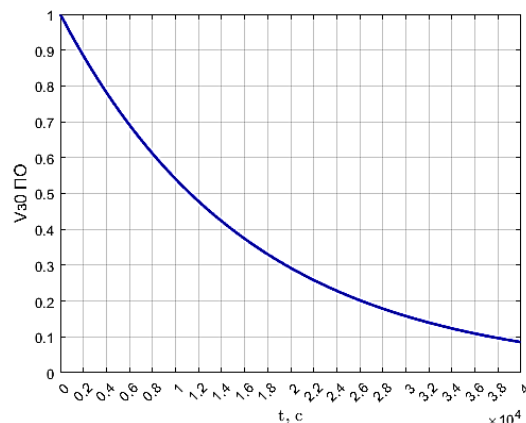


Рис. 2. Интерфейс ПК анализа и оценки защищенности ПО АС ОВД

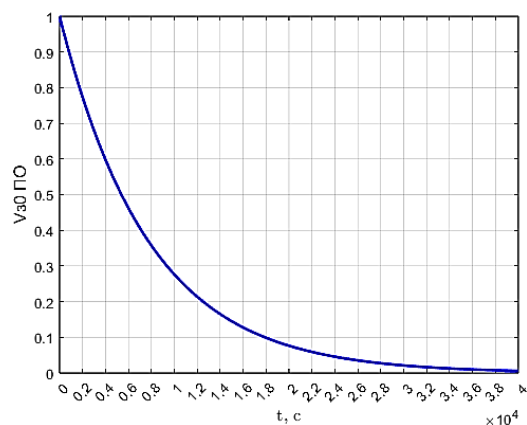
Временные зависимости $V_{\text{зО ПО}}$ в процессе эксплуатации ПО в АС ОВД, построенные с помощью разработанного ПК для девяти рассматриваемых версий LibreOffice, графически представлены на рисунках 3, 4. При этом рассчитанные значения $V_{\text{зО ПО}}$ в зависимости от времени приведены в отдельности для каждой из 5 версий ПО на рисунках 3, а; 3, б; 3, в; 3, г; 3, д; а для оставшихся 4 версий ПО — на рисунках 4, а; 4, б; 4, в; 4, г.



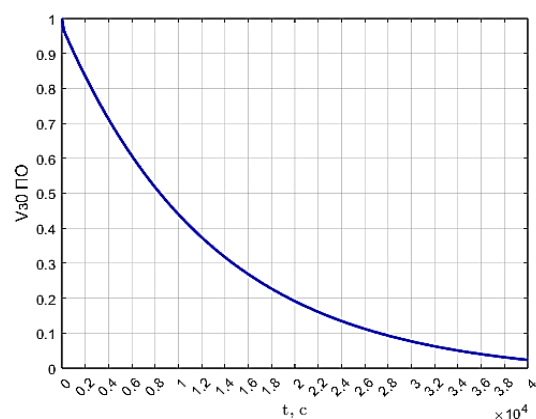
а) версия LO № 6.4



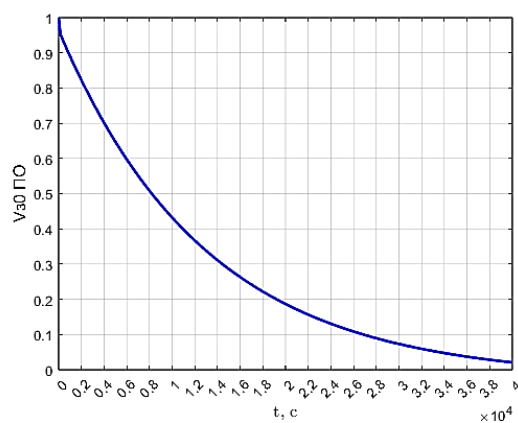
б) версия LO № 7.0



в) версия LO № 7.1

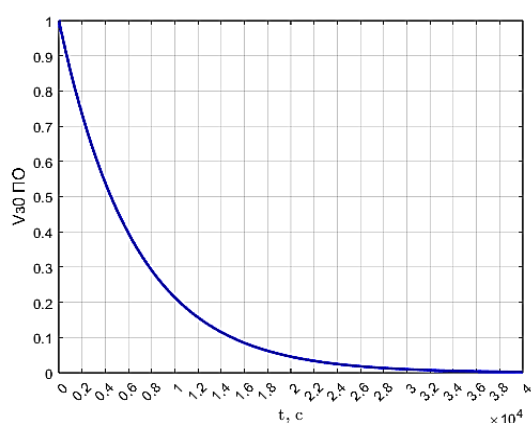


г) версия LO № 7.2

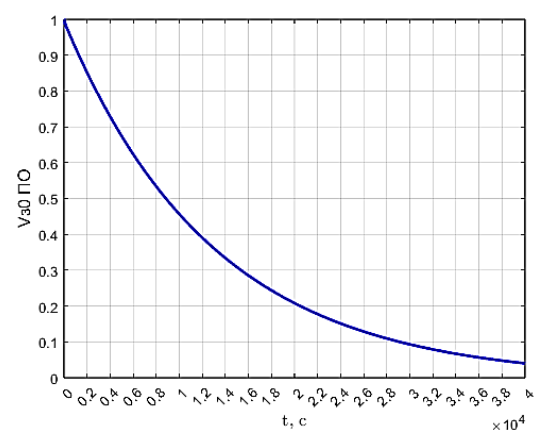


д) версия LO № 7.3

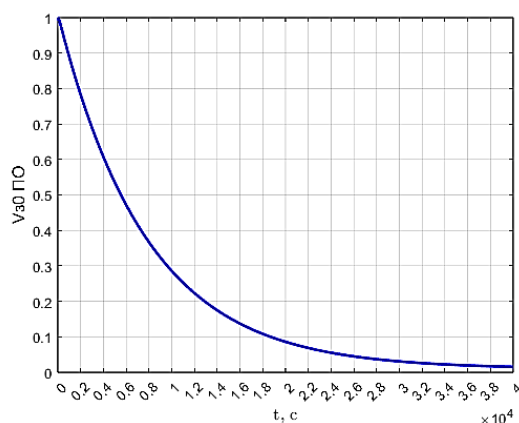
Рис. 3. Динамика комплексного показателя защищенности ПО для версий LO № 6.4, LO № 7.0, LO № 7.1, LO № 7.2, LO № 7.3 LibreOffice



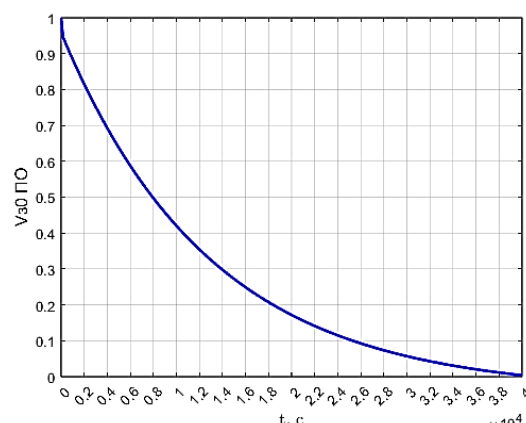
а) версия LO № 7.4



б) версия LO № 7.5



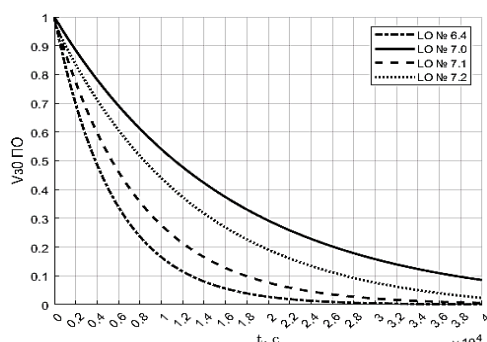
в) версия LO № 7.6



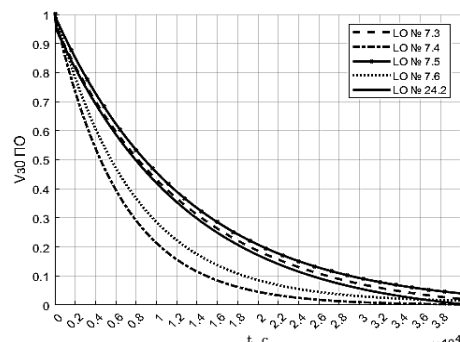
г) версия LO № 24.2

Рис. 4. Динамика комплексного показателя защищенности ПО для версий LO № 7.4, LO № 7.5, LO № 7.6, LO № 24.2 LibreOffice

На рисунке 5 рассчитанные значения $V_{30\text{ ПО}}$ в зависимости от времени приведены совместно для версий LO № 6.4, LO № 7.0, LO № 7.1, LO № 7.2 LibreOffice (рис. 5, а) и версий LO № 7.3, LO № 7.4, LO № 7.5, LO № 7.6, LO № 24.2 (рис. 5, б).



а) версии LO № 6.4, LO № 7.0, LO № 7.1, LO № 7.2



б) версии LO № 7.3, LO № 7.4, LO № 7.5, LO № 7.6, LO № 24.2

Рис. 5. Сравнение динамики комплексного показателя защищенности ПО для версий LibreOffice

Анализ графиков, представленных на рисунках 3—5, показывает, что комплексный показатель защищенности ПО $V_{30\text{ ПО}}$ убывает со временем t ($t \leq \tau_{\text{уу0}}$, где $\tau_{\text{уу0}} = \sum_{i=1}^L \tau_{\text{уу}i}$) и достигает значения 0,1 в момент времени нарушения защищенности (ЭИБ) версии ПО $t_{\text{нз}}$ (z — номер версии).

Это позволило определить $t_{\text{нз}}$ для каждой из девяти версий LibreOffice: $t_{\text{н1}} \sim 12800$ с — для версии LO № 6.4, $t_{\text{н2}} \sim 37440$ с — для версии LO № 7.0, $t_{\text{н3}} \sim 17920$ с — для версии LO № 7.1, $t_{\text{н4}} \sim 27200$ с — для версии LO № 7.2, $t_{\text{н5}} \sim 26880$ с — для версии LO № 7.3, $t_{\text{н6}} \sim 14880$ с — для версии LO № 7.4, $t_{\text{н7}} \sim 29120$ с — для версии LO № 7.5, $t_{\text{н8}} \sim 18720$ с — для версии LO № 7.6, $t_{\text{н9}} \sim 25280$ с — для версии LO № 24.2.

Известно, что для экспоненциальной функции распределения порог вероятности определяется вероятностью пребывания в состоянии в течение времени, равного сред-

нему времени пребывания в этом состоянии [12]. Таким образом, определен порог вероятности, равный 0,4, при котором время нарушения защищенности каждой версии используемого ПО t_{hz} не превышает суммы экспериментально полученных времен $\sum_i t_{zi}$, образующих кратчайший путь перехода процесса эксплуатации уязвимости в ПО из начального состояния 0 (штатный режим функционирования ПО) в состояние 8 (эксплуатация уязвимости нарушителем) (рис. 1) с учетом общего количества актуальных уязвимостей L в рассматриваемой версии ПО [9, 11]. Результаты сравнения указанных времен для различных версий LibreOffice приведены в таблице.

Результаты сравнения времен нарушения защищенности версий LibreOffice при их использовании в АС ОВД для порога вероятности 0,4

№ пп	Версии ПО	Количество актуальных уязвимостей в версиях ПО, L	Времена нарушения за- щищенности версий ПО, t_{hz} , с	Сумма времен кратчайшего пе- рехода между состояниями для одной уязви- мости в версиях ПО, $\sum_i t_{zi}$, с	Сумма времен кратчайшего пе- рехода между состояниями для актуальных уяз- вимостей в вер- сиях ПО, $L \cdot \sum_i t_{zi}$, с
1	LO № 6.4	7	5120	3961,53	27730,71
2	LO № 7.0	4	14880	3965,05	15860,2
3	LO № 7.1	5	7040	3971,89	19859,45
4	LO № 7.2	3	11040	3973,7	11921,1
5	LO № 7.3	3	10880	3973,71	11921,13
6	LO № 7.4	6	5920	3975,95	23855,7
7	LO № 7.5	3	11680	3976,8	11930,4
8	LO № 7.6	5	7360	3979,45	19897,25
9	LO № 24.2	3	10560	3986,07	11958,21

Анализ результатов, представленных на рисунке 5 и в таблице 1, показывает, что рассматриваемые версии ПО отличаются по значениям их комплексных показателей защищенности и времен нарушения защищенности в процессе функционирования в АС ОВД. Разброс V_{30} ПО для рассматриваемых версий ПО достигает ~38 %. Более высокий уровень защищенности по сравнению с другими имеют три версии ПО — LO № 7.0, LO № 7.2, LO № 7.5, однако максимальным временем нарушения защищенности характеризуется версия LO № 7.0 — $t_{hz} \sim 14880$ с. Следовательно, указанная версия ПО является наиболее защищенной и, соответственно, в любой момент времени она имеет более высокий комплексный показатель защищенности и более низкую по сравнению с остальными версиями вероятность эксплуатации уязвимостей при ее функционировании в АС ОВД (рис. 5, а).

Адекватность разработанной модели подтверждается тем, что полученные с помощью описанной в [9, 11] графовой модели численные результаты согласуются с простыми оценками, которые основаны на расчете суммы средних времен пребывания исследуемого процесса эксплуатации актуальных уязвимостей в ПО в определенных состояниях. Применение модели переходов между различными состояниями процесса эксплуатации актуальных уязвимостей для версий ПО позволяет более точно вычислять его ВВХ.

Проведение расчетов для конкретных версий используемого ПО, являющегося типичным для АС ОВД, обеспечивает повышение адекватности полученных результатов, а учет в системе интегро-дифференциальных уравнений (2) всех возможных переходов между состояниями исследуемого процесса — повышение их точности.

График $V_{30\text{ ПО}2}(t)$ для наиболее защищенной (оптимальной) версии рассматриваемого ПО (LO № 7.0), отдельно представленный на рисунке 6, позволяет не только оценивать количественно ее комплексный показатель защищенности за любое указанное время t и определять время нарушения защищенности $t_{н2}$, но также предоставляет возможности для коррекции среднего времени устранения уязвимостей $\tau_{уу02}$ и определения оптимального времени устранения уязвимостей, актуальных для данной версии ПО $\tau_{уу02\text{ опт}} = t_{н2}$, с целью обеспечения ее безопасной эксплуатации в течение времени t ($t \leq \tau_{уу02}$).

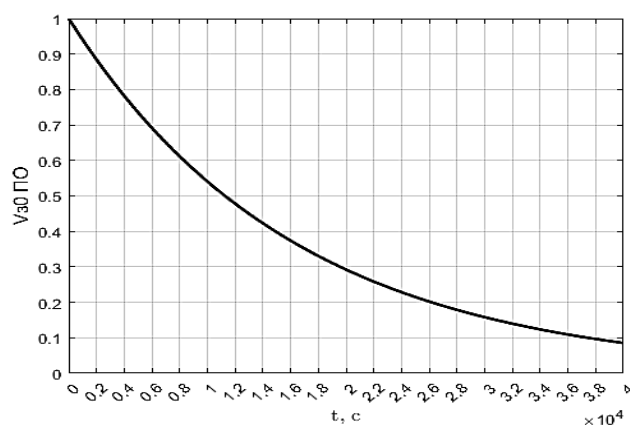


Рис. 6. Динамика комплексного показателя защищенности ПО $V_{30\text{ ПО}2}(t)$ для наиболее защищенной версии LibreOffice (LO № 7.0)

Учет среднего интервала времени между выявлениями уязвимостей в оптимальной версии ПО ($T_{02} = 934$ час), рассчитанного с помощью разработанного ПК, позволяет обеспечивать ЭИБ рассматриваемой версии в течение ее жизненного цикла в АС ОВД.

Проведение аналогичных расчетов для ПО, эксплуатируемого в конкретной АС ОВД, дает возможность выявлять его наиболее защищенную версию и определять оптимальное время устранения актуальных уязвимостей для обеспечения безопасного функционирования данной версии ПО в системе.

Выводы. Таким образом, в статье представлены результаты расчетов моделей, описывающих динамику эксплуатации актуальных уязвимостей в ПО в режиме реального времени, которые проведены с помощью разработанного ПК анализа и оценки защищенности ПО АС ОВД на примере широко используемого на объектах информатизации ОВД офисного пакета LibreOffice.

Полученные количественные результаты оценки комплексных показателей защищенности для версий LibreOffice, времен нарушения их защищенности и средних интервалов времени между выявлениями уязвимостей в версиях ПО позволяют выбирать оптимальную по уровню защищенности версию и корректировать время устранения актуальных для нее уязвимостей с целью повышения безопасности функционирования данной версии ПО в процессе ее жизненного цикла в АС ОВД.

Результаты проведенного исследования могут быть использованы для повышения ЭИБ ПО на конкретных объектах информатизации ОВД.

ЛИТЕРАТУРА

1. Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации : приказ МВД России от 6 июля 2012 г. № 678 (в ред. приказов МВД России от 15.07.2013 № 538, 20.04.2015 № 447, 07.12.2016 № 807). — URL : <https://base.garant.ru/70230320/?ysclid=lmdv18b7g0759105782> (дата обращения: 10.01.2025).
2. Ефремов А. Ф. Проблемы обеспечения информационной безопасности в системе МВД России при работе с базами данных // Вопросы российского и международного права. — 2020. — Т. 10. — № 11 А. — С. 229—235. — DOI: 10.34670/AR.2020.76.82.048.
3. Попова А. Д., Дровникова И. Г. Разработка программного комплекса анализа и оценки защищенности программного обеспечения автоматизированных систем органов внутренних дел // Вестник Воронежского института ФСИН России. — 2025. — № 1. — С. 102—109.
4. Дровникова И. Г., Попова А. Д. Показатели защищенности программного обеспечения, используемого на объектах информатизации органов внутренних дел // Вестник Воронежского института МВД России. — 2024. — № 1. — С. 50—59.
5. Дровникова И. Г., Попова А. Д. Аналитические модели расчета показателей защищенности программного обеспечения автоматизированных систем органов внутренних дел // Вестник Воронежского института МВД России. — 2024. — № 2. — С. 22—33.
6. Попова А. Д., Дровникова И. Г. Методика анализа и оценки уровня защищенности программного обеспечения, используемого на объектах информатизации органов внутренних дел // Безопасность информационных технологий = IT Security. — 2024. — Т. 31. — № 2. — С. 51—64.
7. Попова А. Д. Алгоритм функционирования программного комплекса анализа и оценки защищенности программного обеспечения автоматизированных систем органов внутренних дел // Вестник Дагестанского государственного технического университета. Технические науки. — 2024. — Т. 51. — № 2. — С. 128—136.
8. Дровникова И. Г., Попова А. Д. Теоретические аспекты расчета показателей защищенности программного обеспечения автоматизированных систем органов внутренних дел // Вестник Воронежского института ФСИН России. — 2024. — № 2. — С. 55—59.
9. Попова А. Д., Попов А. Д., Дровникова И. Г. Методика эксперимента для оценивания защищенности программного обеспечения автоматизированных систем органов внутренних дел // Безопасность информационных технологий = IT Security. — 2025. — Т. 32. — № 1. — С. 95—111.
10. Плескунов М. А. Теория массового обслуживания : учебное пособие для студентов вуза, обучающихся по УГН 01.00.00 «Математика и механика». — Екатеринбург : Издательство Уральского университета, 2022. — 264 с. — ISBN 978-5-7996-3539-8. — EDN RSQUKA.
11. Попова А. Д. Методика определения временных характеристик уязвимостей при подготовке к их эксплуатации в программном обеспечении автоматизированных систем // Вестник Воронежского института МВД России. — 2024. — № 4. — С. 101—116.
12. Гмурман В. Е. Теория вероятностей и математическая статистика : учебное пособие для вузов. — 9-е изд., стереотип. — М. : Высшая школа, 2003. — 479 с.

REFERENCES

1. Ob utverzhdenii Instrukcii po organizacii zashhity` personal`ny`x danny`x, soderzhashhixsya v informacionny`x sistemax organov vnutrennix del Rossijskoj Federacii : prikaz MVD Rossii ot 6 iyulya 2012 g. № 678 (v red. prikazov MVD Rossii ot 15.07.2013 № 538, 20.04.2015 № 447, 07.12.2016 № 807). — URL : <https://base.garant.ru/70230320/?ysclid=lmdv18b7g0759105782> (data obrashheniya: 10.01.2025).
2. Efremov A. F. Problemy` obespecheniya informacionnoj bezopasnosti v sisteme MVD Rossii pri rabote s bazami danny`x // Voprosy` rossijskogo i mezhdunarodnogo prava. — 2020. — T. 10. — № 11 A. — S. 229—235. — DOI: 10.34670/AR.2020.76.82.048.
3. Popova A. D., Drovnikova I. G. Razrabotka programmno kompleksa analiza i ocenki zashhishhennosti programmno obespecheniya avtomatizirovanny`x sistem organov vnutrennix del // Vestnik Voronezhskogo instituta FSIN Rossii. — 2025. — № 1. — S. 102—109.
4. Drovnikova I. G., Popova A. D. Pokazateli zashhishhennosti programmno obespecheniya, ispol`zuemogo na ob`ektax informatizacii organov vnutrennix del // Vestnik Voronezhskogo instituta MVD Rossii. — 2024. — № 1. — S. 50—59.
5. Drovnikova I. G., Popova A. D. Analiticheskie modeli rascheta pokazatelej zashhishhennosti programmno obespecheniya avtomatizirovanny`x sistem organov vnutrennix del // Vestnik Voronezhskogo instituta MVD Rossii. — 2024. — № 2. — S. 22—33.
6. Popova A. D., Drovnikova I. G. Metodika analiza i ocenki urovnya zashhishhennosti programmno obespecheniya, ispol`zuemogo na ob`ektax informatizacii organov vnutrennix del // Bezopasnost` informacionny`x texnologij = IT Security. — 2024. — T. 31. — № 2. — S. 51—64.
7. Popova A. D. Algoritm funkcionirovaniya programmno kompleksa analiza i ocenki zashhishhennosti programmno obespecheniya avtomatizirovanny`x sistem organov vnutrennix del // Vestnik Dagestanskogo gosudarstvennogo texnicheskogo universiteta. Texnicheskie nauki. — 2024. — T. 51. — № 2. — S. 128—136.
8. Drovnikova I. G., Popova A. D. Teoreticheskie aspekty` rascheta pokazatelej zashhishhennosti programmno obespecheniya avtomatizirovanny`x sistem organov vnutrennix del // Vestnik Voronezhskogo instituta FSIN Rossii. — 2024. — № 2. — S. 55—59.
9. Popova A. D., Popov A. D., Drovnikova I. G. Metodika e`ksperimenta dlya ocenivaniya zashhishhennosti programmno obespecheniya avtomatizirovanny`x sistem organov vnutrennix del // Bezopasnost` informacionny`x texnologij = IT Security. — 2025. — T. 32. — № 1. — S. 95—111.
10. Pleskunov M. A. Teoriya massovogo obsluzhivaniya : uchebnoe posobie dlya studentov vuza, obuchayushhixsya po UGN 01.00.00 «Matematika i mexanika». — Ekaterinburg : Izdatel`stvo Ural`skogo universiteta, 2022. — 264 s. — ISBN 978-5-7996-3539-8. — EDN RSQUKA.
11. Popova A. D. Metodika opredeleniya vremenny`x xarakteristik uyazvimostej pri podgotovke k ix e`kspluatacii v programmnom obespechenii avtomatizirovanny`x sistem // Vestnik Voronezhskogo instituta MVD Rossii. — 2024. — № 4. — S. 101—116.
12. Gmurman V. E. Teoriya veroyatnostej i matematicheskaya statistika : uchebnoe posobie dlya vuzov. — 9-e izd., stereotip. — M. : Vy`sshaya shkola, 2003. — 479 s.

СВЕДЕНИЯ ОБ АВТОРАХ

Попова Арина Дмитриевна. Адъюнкт.
Воронежский институт МВД России.
E-mail: arnpva@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

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

Popova Arina Dmitrievna. Post-graduate cadet.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: arnpva@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 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.

Ключевые слова: экспериментальное исследование; программный комплекс; комплексный показатель защищенности; время нарушения защищенности; время устранения уязвимостей; оптимальная версия программного обеспечения.

Key words: experimental research; software package; integrated security indicator; security breach time; vulnerability resolution time; optimal software version.

УДК 004.056

М. А. Панкова, кандидат технических наук

В. В. Ожерельев, кандидат физико-математических наук, доцент

Л. Н. Коротков, доктор физико-математических наук, профессор

МОДЕЛИРОВАНИЕ ТОНКОПЛЕНОЧНОЙ БАЗОВОЙ СТРУКТУРЫ НЕЛИНЕЙНЫХ РАДИОЭЛЕКТРОННЫХ КОМПОНЕНТОВ

MODELING OF THIN-FILM BASE STRUCTURE OF NONLINEAR RADIOELECTRONIC COMPONENTS

В статье рассмотрена модель тонкопленочной двухслойной структуры сегнетоэлектрик — линейный диэлектрик, построенная на основе феноменологической теории Ландау, предложено ее использование для получения электрофизических характеристик сегнетоэлектрических тонких пленок как базовых структур радиоэлектронных компонентов. С использованием данной модели выполнен расчет и анализ характеристик конкретной структуры, получены результаты, актуальные для технического применения. В частности, варьирование параметров структуры и величины приложенного напряжения позволило выделить на электрополевой зависимости диэлектрической проницаемости сегнетоэлектрического слоя участок с устойчивой отрицательной диэлектрической проницаемостью. Использование модели дает возможность прогнозирования свойств тонкопленочных сегнетоэлектрических структур на основе конкретных материалов в условиях определенных внешних воздействий.

The article considers a model of a thin-film two-layer structure of a ferroelectric — linear dielectric, formed on the basis of the phenomenological theory of Landau, its use is proposed to obtain electrophysical characteristics of ferroelectric thin films as basic structures of radio-electronic components. Using this model, the calculation and analysis of the characteristics of a specific structure are performed, the results are relevant for technical applications. In particular, varying the parameters of the structure and the magnitude of the applied voltage made it possible to select a section with a stable negative dielectric constant on the electric field dependence of the dielectric permittivity of the ferroelectric layer. Using the model makes it possible to predict the properties of thin-film ferroelectric structures based on specific materials under certain external influences.

Введение. Требования к системам обработки и передачи информации обычно определяются двумя основными факторами: уменьшением стоимости создания систем и возрастанием скорости передачи данных в них. Это требует, в частности, пересмотра существующей элементной базы и применения принципиально новой, а именно улучшения массогабаритных показателей радиоэлектронных компонентов и уменьшения мощности, требуемой для работы, при одновременном увеличении емкости каналов связи.

Электронные приборы с интегрированными сегнетоэлектриками обладают рядом особых возможностей, а именно: возможностью перестройки диэлектрической проницаемости внешним электрическим полем, высокой радиационной стойкостью, совместимостью с микрополосковыми линиями, высокой надежностью, возможностью использования в широком диапазоне частот (от 0, ГГц до 0,4 ТГц).

Удачным решением в технологии создания электрически-перестраиваемых устройств для систем обработки и передачи информации в миллиметровом и субмиллиметровом диапазонах длин волн является использование сегнетоэлектрических пленок наноразмерной толщины. Однако получение таких пленок, интегрированных в микроэлектронное устройство, предполагает использование весьма трудоемкого технологического цикла, содержащего процесс осаждения тонкого сегнетоэлектрического слоя [1]. Кроме того, выбор новых материалов и структур для применения в электронных приборах, содержащих интегрированные сегнетоэлектрики, исследование параметров и характеристик структур представляет собой достаточно трудоемкую задачу.

В связи с этим для оценки перспективности того или иного технического решения целесообразно прибегнуть к использованию компьютерного моделирования, которое позволяет в короткие сроки оценить базовые параметры и эксплуатационные характеристики структур без получения их на основе конкретных материалов и проведения экспериментальных исследований.

В настоящей статье представлена модель тонкопленочной базовой структуры с использованием сегнетоэлектрика и линейного диэлектрика, построенная на основе феноменологической теории Ландау. С помощью модели получены электрофизические характеристики конкретной структуры для конкретных материалов и внешних электропотенциальных воздействий.

Расчеты выполнялись с помощью приложения, написанного на языке C++ с использованием библиотек Qt и среды разработки QtCreator. Приложение имеет графический интерфейс, позволяющий легко варьировать необходимые параметры и визуализировать результаты с помощью графиков.

1. Модель тонкопленочной структуры сегнетоэлектрик — линейный диэлектрик и ее параметры

Рассмотрим тонкопленочную структуру, содержащую слой сегнетоэлектрика (СЭ) толщиной h_c и слой диэлектрика линейного диэлектрика Д толщиной h_d (рис. 1).

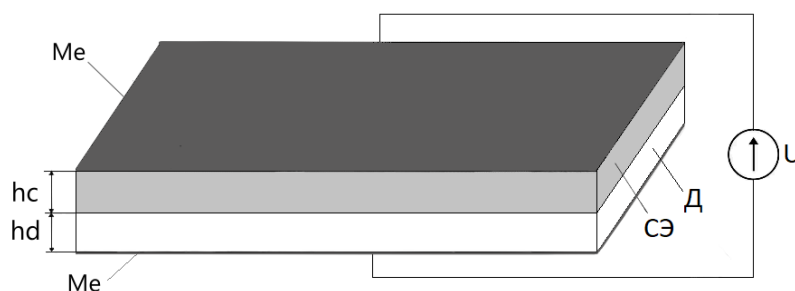


Рис. 1. Тонкопленочная двухслойная базовая структура, включающая слой сегнетоэлектрика СЭ и линейного диэлектрика Д и тонкие металлические электроды Me

Согласно термодинамической теории Ландау, свободная энергия полярного диэлектрика (плотность свободной энергии) дается выражением [2]:

$$F = F_0 + \frac{1}{2} \alpha D_c^2 + \frac{1}{4} \beta D_c^4 - E_c D_c, \quad (1)$$

где F_0 — не зависящая от вектора электрической индукции D_c , составляющая F ; α и β — коэффициенты разложения в ряд свободной энергии; E_c — напряженность внешнего электрического поля, приложенного к СЭ.

Продифференцировав F по D_c , получим:

$$\frac{dF}{dD_c} = \alpha D_c + \beta D_c^3 = E_c. \quad (2)$$

Электрическая индукция диэлектрического слоя D_d определяется известным выражением:

$$D_d = \varepsilon_d \varepsilon_0 E_d, \quad (3)$$

где E_d — напряжённость электрического поля в диэлектрической пленке, ε_0 — абсолютная электрическая постоянная.

Численное значение вектора электрической индукции D равно плотности поверхностного заряда. Поскольку СЭ и диэлектрик имеют соприкасающиеся поверхности, то $D_c = D_d = D$. Тогда из уравнений (3) и (2) получим:

$$\alpha \varepsilon_d \varepsilon_0 E_d + \beta (\varepsilon_d \varepsilon_0 E_d)^3 = E_c. \quad (4)$$

Примем во внимание, что $E_c = \frac{U_c}{h_c}$ и $E_d = \frac{U_d}{h_d}$, U_c и U_d — электрические напряжения, приложенные к СЭ и диэлектрическому слою соответственно. Очевидно, что $U_c + U_d = U$ (U — напряжение, приложенное к структуре). Таким образом $U_c = U - U_d$, тогда

$$E_c = \frac{U - U_d}{h_c}.$$

Перепишем (4) с учетом указанных соотношений:

$$\alpha \varepsilon_d \varepsilon_0 \frac{U_d}{h_d} + \beta (\varepsilon_d \varepsilon_0 \frac{U_d}{h_d})^3 = \frac{U - U_d}{h_c}. \quad (5)$$

В уравнении (6), решаемом относительно U_d , напряжение U , толщина слоя СЭ h_c , толщина слоя диэлектрика h_d являются параметрами, которые в дальнейшем будут варьироваться, значения параметров α и β зависят от используемого сегнетоэлектрического материала.

На основе решения уравнения (5) нетрудно получить электрофизические характеристики моделируемой структуры, важные для ее технического применения, в частности, зависимости $D(U)$, $D(E_c)$, диэлектрической проницаемости $\varepsilon_c(U)$, удельной емкости структуры $C(U)$.

В качестве конкретного объекта моделирования была рассмотрена двухслойная структура (рис. 1), состоящая из сегнетоэлектрического слоя толщиной $h_c = 2 \cdot 10^{-6}$ м и тонкой пленки линейного диэлектрика, толщина которой h_d варьировалась в пределах 0–50 нм, внешнее напряжение U — в пределах от –30 до +50 В. В качестве материала диэлектрической пленки был взят широко применяемый в микроэлектронике диоксид кремния SiO_2 , относительная диэлектриче-

ская проницаемость которого $\varepsilon_d \approx 4$. Сегнетоэлектрический слой представлял собой монокристаллический триглицинсульфат (TGS), физические свойства которого в настоящее время хорошо изучены [2, 3]. Коэффициенты разложения в ряд по параметру порядка D его термодинамического потенциала в теории Ландау (1) [3]: $\alpha = \alpha_0 (T - T_C)$, где $\alpha_0 \approx 3.77 \cdot 10^7 \text{ В} \cdot \text{м} \cdot \text{Кл}^{-1} \cdot \text{К}^{-1}$, температура Кюри $T_C \approx 50^\circ \text{C}$, $\beta \approx 6.03 \cdot 10^{11} \text{ В} \cdot \text{м}^5 \cdot \text{Кл}^{-3}$. Все вычисления проводились для температуры 20°C .

Для упрощения задачи механические напряжения, возникающие на границах слоев, и контактные явления в модели не учитывались.

Для численного решения уравнения (1) применялся метод Ньютона.

2. Результаты моделирования и их обсуждение

Обсудим результаты, полученные в результате моделирования.

На рис. 2 показаны кривые $D(U)$ изучаемой структуры для температуры $T = 20^\circ \text{C}$. Кривые получены путем расчетов при варьировании параметра толщины диэлектрической пленки h_d и напряжения U . Полученные зависимости, по сути, представляют собой характерные для сегнетоэлектриков петли диэлектрического гистерезиса. Можно увидеть, что участок «ав» (вставка к рис. 2) характеризуется отрицательной дифференциальной диэлектрической проницаемостью и является неустойчивым. Поэтому при уменьшении напряжения электрическая индукция скачкообразно «переходит» из точки «а» в точку «б». Аналогичная ситуация имеет место при увеличении напряжения U . В этом случае индукция D , достигнув точки «в», скачком увеличивается до величины, соответствующей точке «г».

Можно увидеть, что по мере увеличения параметра толщины диэлектрической пленки h_d происходит уменьшение индукции D и сужение интервала напряжений, в пределах которого наблюдается отрицательная диэлектрическая проницаемость. В случае когда $h_d \geq 10 \text{ нм}$, участок с отрицательным наклоном зависимости $D(U)$ отсутствует (кривая 4 на рис. 2).

При толщине диэлектрической пленки 50 нм и более зависимость $D(U)$ становится линейной. Это показывает, что при таких толщинах h_d диэлектрические свойства структуры преимущественно определяются свойствами пленки линейного диэлектрика, а не сегнетоэлектрика.

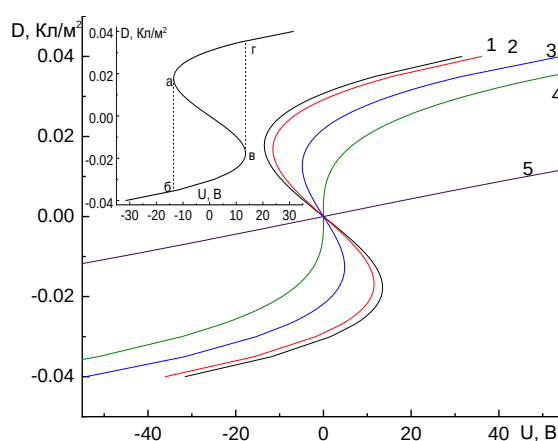


Рис. 2. Зависимости $D(U)$, полученные в результате моделирования при варьировании параметра U и параметра толщины диэлектрической пленки: 0 (1), 1 (2), 5 (3), 10 (4) и 50 (5) нм. На вставке — петля диэлектрического гистерезиса

Рассмотрим подробно результаты моделирования структуры с диэлектриком толщиной 10 нм.

Как упоминалось выше, для этого образца участок с отрицательной диэлектрической проницаемостью на зависимости $D(U)$ не наблюдается (рис. 2 и 3), а следовательно, отсутствуют предпосылки для возникновения диэлектрической неустойчивости и гистерезисных явлений.

Вместе с тем для сегнетоэлектрической составляющей моделируемой структуры на зависимости $D(U_c)$ наблюдается участок с отрицательным наклоном dD/dU_c (участок «аб» кривой 1 на рис. 3).

Согласно экспериментальным исследованиям [4, 5], состояние с отрицательной диэлектрической проницаемостью в сегнетоэлектрическом слое является устойчивым. По-видимому, его стабилизация достигается понижением напряжения U_c , действующего на сегнетоэлектрическом слое на участке с отрицательной диэлектрической проницаемостью (рис. 4), что препятствует необратимому переключению вектора электрической индукции D .

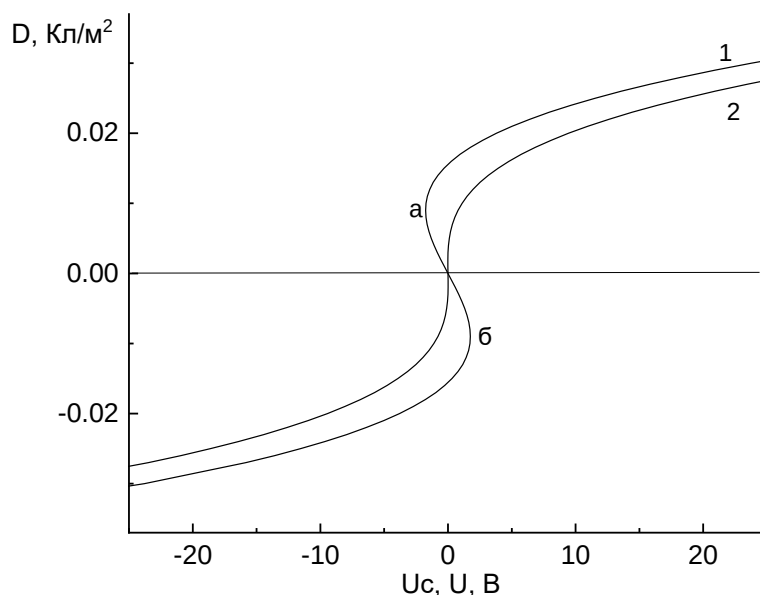


Рис. 3. Зависимости индукции D от электрического напряжения U_c на сегнетоэлектрическом слое (1) и от полного напряжения U (2) для моделируемой структуры с толщиной диэлектрической пленки 10 нм

Путем численного дифференцирования зависимости $D(U)$, изображенной на рис. 3 (кривая 2), получим зависимость удельной электрической емкости C моделируемой структуры от приложенного напряжения: $C = dD/dU$ (рис. 5).

Можно увидеть, что при $U \rightarrow 0$ емкость C принимает экстремально высокое значение. Однако величина C очень чувствительна как к напряжению, так, очевидно, и к температуре в силу зависимости от нее коэффициента α в соотношении (1). При увеличении напряжения по абсолютной величине емкость C быстро уменьшается почти на три порядка, а ее зависимость от напряжения становится более слабой.

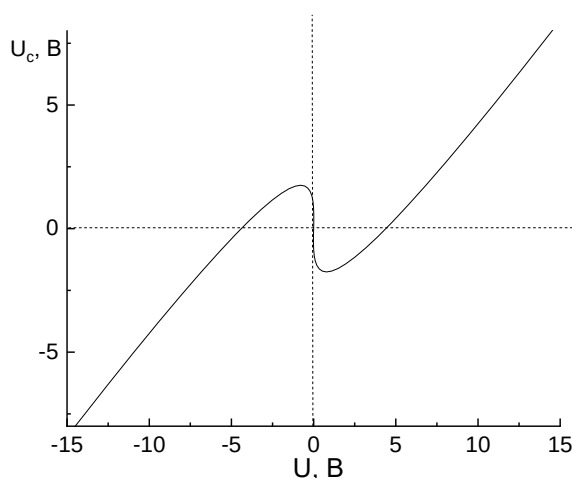


Рис. 4. Зависимость напряжения U_c на сегнетоэлектрическом слое от полного напряжения U для структуры с толщиной диэлектрической пленки 10 нм

Достаточно сильная зависимость емкости структуры C от приложенного напряжения U делает ее перспективной для создания элементов интегральных схем с перестраиваемой в широких пределах емкостью.

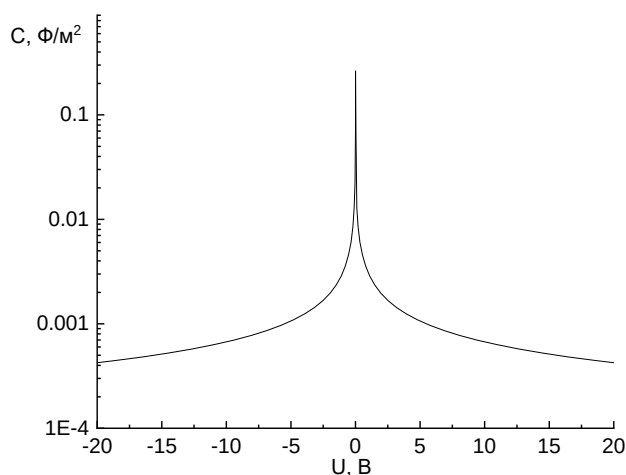


Рис. 5. Зависимость удельной емкости структуры сегнетоэлектрик — диэлектрик от приложенного напряжения

Рассмотрим теперь зависимость диэлектрической проницаемости сегнетоэлектрического слоя ϵ_c моделируемой структуры от напряженности приложенного к ней электрического поля E_c (рис. 6). Представленная на этом рисунке кривая $\epsilon(E_c)$ была получена с помощью соотношения: $\epsilon_c = dD/d(\epsilon_0 E_c)$.

Кривая $\epsilon(E_c)$ имеет нетривиальный вид. При этом величина ϵ_c существенно зависит от предыстории. При возрастании E_c от отрицательных значений происходит монотонное возрастание ϵ_c вплоть до точки «б» (рис. 6), вблизи которой $\epsilon_c \rightarrow \infty$, а зависимость

претерпевает разрыв 2 рода. При дальнейшем увеличении внешнего напряжения электрическое напряжение на сегнетоэлектрическом слое падает (рис. 4), что соответствует переходу на участок с отрицательной диэлектрической проницаемостью, который расположен в промежутке между точками «а» и «б» на кривой $\epsilon(E_c)$ (рис. 6). В случае когда поле $E_c \approx 0$, диэлектрическая проницаемость, оставаясь отрицательной и достаточно высокой, слабо зависит от поля E_c .

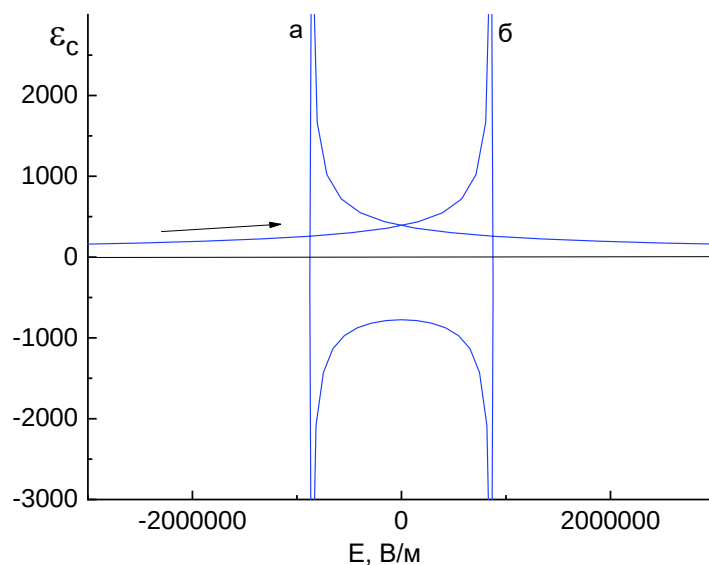


Рис. 6. Зависимость диэлектрической проницаемости сегнетоэлектрического слоя от напряженности электрического поля

Дальнейший рост U продолжает снижать напряженность поля E_c в сегнетоэлектрическом слое, что по мере приближения к точке «а» (рис. 6) приводит к неограниченному по абсолютной величине росту отрицательной диэлектрической проницаемости. В точке «а» зависимость $\epsilon(E_c)$ еще раз испытывает разрыв второго рода и меняет свой знак. Теперь повышение напряжения U ведет к возрастанию E_c и монотонному уменьшению ϵ .

Заключение. Моделирование двухслойной структуры сегнетоэлектрик — диэлектрик, построенной на базе феноменологической теории сегнетоэлектрических фазовых переходов, позволяет обнаружить ряд специфических свойств данной структуры, перспективных для практического использования. На примере тонкопленочной структуры TGS — SiO_2 установлено, в частности, что она обладает эффектом памяти, а ее электрическая емкость может регулироваться в широких пределах с помощью приложенного к ней электрического напряжения.

Пожалуй, наиболее важным в техническом отношении свойством является обнаруженная отрицательная диэлектрическая проницаемость сегнетоэлектрического слоя, управляемая внешним напряжением.

Структуры такого типа обладают высоким потенциалом как для практического применения в уже существующих радиоэлектронных устройствах, таких, например, как фазовращатели, диэлектрические усилители, элементы энергонезависимой памяти, смесители и т. д., так и для создания принципиально новых приборов. Широкое применение рассмотренная структура с отрицательной ϵ может обрести также в быстродействующих интегральных

схемах благодаря уменьшению времени задержки, которое определяется, в частности, диэлектрической проницаемостью диэлектрических слоев интегральной схемы.

При этом следует принимать во внимание, что СЭ слой, обладающий отрицательной ϵ , сформирован на поверхности пластины (рис. 1), поэтому для наиболее эффективной его «эксплуатации» целесообразно использовать планарные структуры слоя [6, 7], когда электроды расположены на поверхности сегнетоэлектрического слоя, в пределах которого будет концентрироваться электрическое поле.

Таким образом, предложенная модель дает возможность оперативно, без проведения физических экспериментов определить оптимальные параметры двухслойной тонкопленочной структуры сегнетоэлектрик — диэлектрик, позволяющие получить необходимые для практического применения электрофизические характеристики.

Работа выполнена при поддержке Министерства науки и высшего образования Российской Федерации в рамках государственного задания, проект № FZGM-2023-0006.

ЛИТЕРАТУРА

1. Воротилов К. А., Мухортов В. М., Сигов А. С. Интегрированные сегнетоэлектрические устройства. — М. : Энергоатомиздат, 2011. — 175 с.
2. Лайнс М., Гласс А. Сегнетоэлектрики и родственные им материалы. — М. : Мир. 1981. — 736 с.
3. Гриднев С. А. Физика полярных диэлектриков. — Саарбрюккен : Палмариум, 2014. — 219 с.
4. Experimental evidence of ferroelectric negative capacitance in nanoscale heterostructures / A. I. Khan, D. Bhowmik, P. Yu [et al.] // Appl. Phys. Lett. — 2011. — V. 99. — P. 113501-1-3.
5. Hoffmann M., Slesazek S. Mikolajick T. Progress and future prospects of negative capacitance electronics: A materials perspective // APL Mater. — 2021. — V. 9. — P. 020902.
6. Вендик О. Г., Зубко С. П., Никольский М. А. Моделирование и расчет емкости планарного конденсатора, содержащего тонкий слой сегнетоэлектрика // ЖТФ. — 1999. — Т. 69. — Вып. 4. — С. 1—8.
7. Вендик О.Г., Никольский М.А. Моделирование характеристик многослойного планарного конденсатора // ЖТФ. — 2001. — Т. 71. — Вып. 1. — С. 117—121.

REFERENCES

1. Vorotilov K. A., Muxortov V. M., Sigov A. S. Integrirovanny`e segnetoe`lektricheskie ustrojstva. — M. : E`nergoatomizdat, 2011. — 175 s.
2. Lajns M., Glass A. Segnetoe`lektriki i rodstvenny`e im materialy`. — M. : Mir. 1981. — 736 s.
3. Gridnev S. A. Fizika polyarny`x die`lektrikov. — Saarbryukken : Palmarium, 2014. — 219 s.
4. Experimental evidence of ferroelectric negative capacitance in nanoscale heterostructures / A. I. Khan, D. Bhowmik, P. Yu [et al.] // Appl. Phys. Lett. — 2011. — V. 99. — P. 113501-1-3.
5. Hoffmann M., Slesazek S. Mikolajick T. Progress and future prospects of negative capacitance electronics: A materials perspective // APL Mater. — 2021. — V. 9. — P. 020902.

6. Vendik O. G., Zubko S. P., Nikol'skij M. A. Modelirovanie i raschet emkosti planarnogo kondensatora, sodержashhego tonkij sloj segnetoelektrika // ZhTF. — 1999. — Т. 69. — Вып. 4. — С. 1—8.

7. Vendik O.G., Nikol'skij M.A. Modelirovanie xarakteristik mnogoslojnogo planarnogo kondensatora // ZhTF. — 2001. — Т. 71. — Вып. 1. — С. 117—121.

СВЕДЕНИЯ ОБ АВТОРАХ

Панкова Маргарита Александровна. Доцент кафедры математики и моделирования систем. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: m_a_pankova@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Ожерельев Виктор Вадимович. Доцент кафедры технологии сварочного производства и диагностики. Кандидат физико-математических наук.

Воронежский государственный технический университет.

E-mail: ozher@mail.ru

Россия, 394026, Воронеж, Московский проспект, 14.

Коротков Леонид Николаевич. Профессор кафедры физики твердого тела. Доктор физико-математических наук, профессор.

Воронежский государственный технический университет.

E-mail: l_korotkov@mail.ru

Россия, 394026, Воронеж, Московский проспект, 14.

Pankova Margarita Alexandrovna. Associate Professor of the chair of Mathematics and Systems Modeling. Candidate of Technical Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: m_a_pankova@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ozhereliev Victor Vadimovich. Associate Professor of the chair of Welding Production Technology and Diagnostics. Candidate of Physical and Mathematical Sciences.

Voronezh State Technical University.

E-mail: ozher@mail.ru

Work address: Russia, 394026, Voronezh, Moskovsky Prospect, 14.

Korotkov Leonid Nikolaevich. Professor of the chair of Solid State Physics. Doctor of Physical and Mathematical Sciences, Professor.

Voronezh State Technical University.

E-mail: l_korotkov@mail.ru

Work address: Russia, 394026, Voronezh, Moskovsky Prospect, 14.

Ключевые слова: моделирование тонкопленочной структуры сегнетоэлектрик — диэлектрик; феноменологическая теория Ландау; отрицательная диэлектрическая проницаемость; радиоэлектронные компоненты.

Key words: modeling of thin-film ferroelectric-dielectric structure; Landau's phenomenological theory; negative dielectric permittivity; radio-electronic components.

УДК 004.94

О. В. Пьянков, доктор технических наук, профессор

А. А. Терентьев, кандидат технических наук

М. С. Захаров

ПРОГНОЗ ПОТРЕБНОСТЕЙ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В СРЕДСТВАХ СВЯЗИ И АВТОМАТИЗАЦИИ

FORECAST OF THE NEEDS OF INTERNAL AFFAIRS UNITS IN COMMUNICATIONS AND AUTOMATION

Приводятся результаты анализа моделей прогнозирования с целью определения модели, обладающей наименьшей ошибкой прогноза относительно исходных данных. Исследование проведено на основе потребностей носимых радиостанций для нужд ГУ МВД России по Тульской области за период с 2013 по 2024 год. Исследование было разделено на два этапа: первый этап содержал построение прогнозных значений. В качестве исследуемых моделей были выбраны: модель скользящей средней, модель двойных скользящих средних, модель двойного экспоненциального сглаживания, модель тройного экспоненциального сглаживания, модель полиномиальной линии тренда. Второй этап заключался в расчете ошибки прогноза. Результаты проведенного исследования продемонстрировали, что выбранные три способа определения ошибки прогноза единогласно показали, что наименьшим расхождением обладает модель полиномиальной линии тренда.

The results of the analysis of forecasting models are presented in order to determine the model with the smallest forecast error relative to the initial data. The study was conducted based on the needs of wearable radio stations for the needs of the Ministry of Internal Affairs of Russia in the Tula region for the period from 2013 to 2024. The study was divided into two stages: the first stage included the construction of forecast values. The following models were selected as the studied models: the moving average model, the double moving averages model, the double exponential smoothing model, the triple exponential model, and the polynomial trend line model. The second stage was to calculate the forecast error. The results of the study demonstrated that the selected three methods for determining the forecast error unanimously showed that the model of the polynomial trend line has the smallest discrepancy.

Введение. Организация устойчивой связи между подразделениями органов внутренних дел всегда являлась одной из главных задач подразделений информационных технологий, связи и защиты информации. Применение средств связи в служебной деятельности органов внутренних дел позволяет оперативно производить обмен информацией между сотрудниками для координации действий при раскрытии преступления или для обмена информацией об оперативной обстановке при патрулировании выделенной территории. С активным развитием информационных технологий развивались и средства связи и автоматизации для нужд органов внутренних дел. Так, современные средства связи позволяют не только обмениваться информацией, а также обладают встроенными функциями вызова сил и средств при нештатной ситуации без голосового вызова сотрудника, что поз-

воляет обеспечить безопасность сотрудника при выполнении им своих служебных обязанностей. Для того чтобы сотрудники обеспечивали охрану общественного порядка и безопасность граждан, необходимо, чтобы каждый сотрудник был оснащен служебными средствами связи. Своевременное планирование закупок средств связи и автоматизации, позволяющее эффективно решать задачи обеспечения ими, невозможно без прогнозирования потребностей, основанного на использовании временных рядов.

Метод математического моделирования позволяет спрогнозировать требуемое количество средств связи на ближайшую перспективу, тем самым обеспечив необходимое количество средств связи для подразделения органов внутренних дел

Постановка задачи. Безусловно, прогнозирование является процессом, который позволяет сформулировать примерное количество средств связи и не дает точного значения. В связи с этим предлагается провести исследование для определения модели прогнозирования, обладающей наименьшей степенью погрешности (ошибки) расчета. В настоящее время существует достаточное количество научных работ, посвящённых данной тематике [1—5], но в этих работах не рассматривался вопрос выбора оптимальной модели прогнозирования с целью определения прогноза с наименьшей степенью отклонения от исходных данных. В работе [6] авторы предложили алгоритм выбора модели прогнозирования, демонстрирующей наименьшую степень отклонения от исходных данных. При этом в работе продемонстрированы расчеты только двух моделей прогнозирования, а в качестве способа расчета ошибки прогноза выбран расчет средней абсолютной ошибки (MAE). Обоснование выбора данной ошибки при сравнении моделей прогнозирования также не приводится.

Таким образом, требуется провести анализ нескольких моделей прогнозирования и осуществить выбор той модели, которая продемонстрирует наименьшее отклонение от исходных данных при расчете нескольких способов ошибок.

Решение задачи. Для решения поставленной задачи в данном исследовании будем использовать следующий перечень моделей прогнозирования:

- скользящей средней (MA);
- двойных скользящих средних (DMA);
- двойного экспоненциального сглаживания (DES);
- тройного экспоненциального сглаживания (TES);
- полиномиальной линии тренда.

В качестве примера произведем расчет прогноза количества требуемых носимых средств радиосвязи ГУ МВД России по Тульской области на основе каждой выбранной модели прогнозирования.

Расчет прогноза будем осуществлять согласно данным о носимых радиостанциях для нужд ГУ МВД России по Тульской области за период с 2013 по 2024 год (см. табл. 1).

Таблица 1

Число требуемых носимых радиостанций ГУ МВД России по Тульской области

Год	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Исх. ряд	3258	3388	3456	3491	3560	3632	3668	3778	3929	3968	4048	4188

Модель скользящей средней. Построение скользящей средней основано на процентном соотношении данных, берущихся за предшествующие годы. Примем, что количество наблюдений $M = 2$, тогда константа сглаживания:

$$\alpha = \frac{2}{M+1} \approx 0,667.$$

Первое искомое значение y_t за 2013 год принимается из исходного ряда. Последующие значения рассчитываются следующим образом:

$$F_t = \alpha y_t + (1 - \alpha)F_{t-1}. \quad (1)$$

Результаты расчета прогноза при помощи модели скользящей средней приведены в таблице 2.

Таблица 2

Результаты прогноза при помощи модели скользящей средней

Год	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Исх. ряд	3258	3388	3456	3491	3560	3632	3668	3778	3929	3968	4048	4188
2 года		3323	3422	3474	3526	3596	3650	3723	3854	3949	4008	4068
	3258	3345	3419	3467	3529	3598	3645	3734	3864	3933	4010	4129

Двойные скользящие средние (Double moving averages, DMA). Точно так же, как скользящие средние представляют собой «скользящее» среднее значение фактических наблюдений временного ряда, в данном случае используется «скользящее» среднее значение этих скользящих средних, или двойные скользящие средние:

$$M_t'' = \frac{\sum_{i=t}^{t-N+1} M_t'}{N}. \quad (2)$$

Используя одинарные и двойные скользящие средние, можно построить динамические коэффициенты перехвата и наклона, которые будут перемещаться и колебаться по мере движения исходного временного ряда. Эти два коэффициента рассчитываются следующим образом:

$$a_t = 2M_t' - M_t'', \quad (3)$$

$$b_t = \frac{2}{N-1} (M_t' - M_t'') = \frac{a_t}{N-1}, \quad (4)$$

где N — количество скользящих средних в интервале.

Эти два коэффициента позволяют рассчитывать прогнозы, которые динамически изменяются по мере изменения временных рядов.

Формула такова:

$$\hat{Y}_{t+1} = F_{t+1} = a_t + b_t. \quad (5)$$

Если нужно продлить прогнозы на m периодов в будущее, то формула для DMA принимает вид

$$\hat{Y}_{t+m} = F_{t+m} = a_t + b_t m. \quad (6)$$

Таблица 3

Результаты прогноза при помощи модели двойной скользящей средней

Год	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
2 года		3323	3422	3474	3526	3596	3650	3723	3854	3949	4008	4118
DMA (N=3)					3438	3503	3561	3625	3701	392	3888	3969
a					3566	3619	3679	3761	3882	3991	4075	4100
b					64	58	59	68	90	100	93	65
F_{DMA}						3631	3677	3738	3829	3972	4091	4168

Двойное экспоненциальное сглаживание (Double exponential smoothing, DES). Значения двойного экспоненциального сглаживания являются экспоненциально сглаженными значениями экспоненциально сглаженных значений.

Одиночное экспоненциальное сглаживание $F_t = \alpha y_t + (1 - \alpha)F_{t-1}$ было рассмотрено выше. Тогда двойное экспоненциальное сглаживание определяется как

$$F_t'' = \alpha F_t + (1 - \alpha)F_{t-1}''. \quad (7)$$

Аналогично DMA формула для прогнозирования будет следующей:

$$\hat{Y}_{t+m} = F_{t+m} = a_t + b_t m, \quad (8)$$

где

$$a_t = 2F_t - F_t'', \quad (9)$$

$$b_t = \frac{\alpha}{1-\alpha}(F_t - F_t''). \quad (10)$$

Таблица 4

Результаты прогноза при помощи модели двойного экспоненциального сглаживания

Год	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
DES	3258	3316	3385	3439	3499	3565	3618	3695	3808	3891	3970	4076
a		3374	3453	3494	3559	3630	3671	3772	3920	3975	4049	4181
b		58	69	55	60	66	53	77	113	84	79	106
F_{DES}			3431	3522	3549	3618	3696	3724	3849	4033	4059	4128

Тройное экспоненциальное сглаживание (Triple exponential smoothing, TES). Аналогично двойному экспоненциальному сглаживанию метод TES определяется следующим образом:

$$F_t''' = \alpha F_t'' + (1 - \alpha)F_{t-1}'''. \quad (11)$$

TES позволяет отойти от линейного подхода к прогнозированию и представить пример того, как использовать нелинейное уравнение для составления прогнозов.

На основе этих одинарных, двойных и тройных экспоненциально сглаженных значений рассчитываются следующие динамические коэффициенты:

$$a_t = 3F'_t - 3F''_t + F'''_t, \quad (12)$$

$$b_t = \frac{\alpha}{2(1-\alpha)} [(6 - 5\alpha)F'_t - 2(5 - 4\alpha)F''_t + (4 - 3\alpha)F'''_t], \quad (13)$$

$$c_t = \frac{\alpha^2}{2(1-\alpha)^2} [F'_t - 2F''_t + F'''_t]. \quad (14)$$

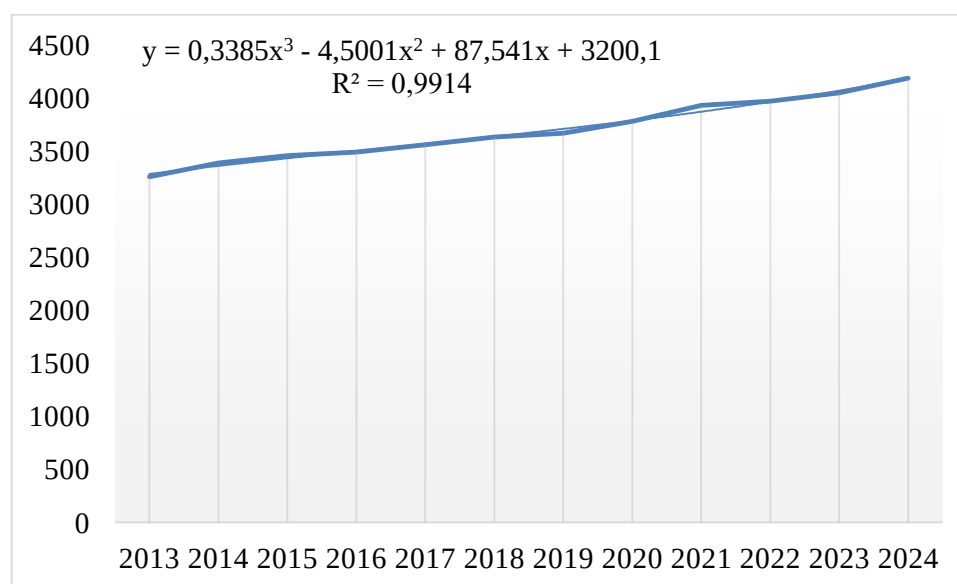
Тогда формула для прогнозирования будет иметь следующий вид:

$$\hat{Y}_{t+m} = F_{t+m} = a_t + b_t m + c_t m^2. \quad (15)$$

Таблица 5

Результаты прогноза при помощи модели тройного экспоненциального сглаживания

Год	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
TES	3258	3297	3355	3411	3470	3533	3590	3660	3758	3847	3929	4027
a		3383	3458	3494	3559	3632	3669	3775	3927	3973	4048	4185
b		116	99	51	63	73	43	98	155	69	69	129
c		19	10	-1	1	2	-3	7	14	-5	-3	8
F_{TES}			3518	3567	3544	3624	3707	3709	3880	4096	4037	4114



Полиномиальная линия тренда (степень = 3)

Таблица 6

Результаты прогноза при помощи модели полиномиальной линии тренда

Год	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
$F_{\text{поли}}$	3264	3338	3414	3492	3570	3649	3730	3811	3894	3978	4063	4149

Далее, после построения прогнозов при помощи нескольких моделей прогнозирования, рассчитаем погрешность расчетов прогнозирования относительно каждой модели:

- средней ошибки (среднее отклонение прогнозируемых данных от фактических):

$$ME = \bar{e} = \frac{\sum y_t - F_t}{n}, \quad (16)$$

где n — число рассматриваемых отсчетов (лет);

- средней абсолютной ошибки

$$MAE = \frac{\sum_{t=1}^n |e_t|}{n}, \quad (17)$$

- относительной погрешности:

$$\varepsilon = \frac{F_{\text{расч}} - F_{\text{опт}}}{F_{\text{опт}}} \cdot 100 \%. \quad (18)$$

Результаты расчета погрешности для всех моделей прогноза приведем в таблице 7.

Таблица 7

Результаты расчета относительной погрешности прогнозов

№ п/п	Модель прогнозирования, F_i	ME	MAE	ε , %
1	F_{MA}	36	36	0,96
2	F_{DMA}	- 28	38	0,38
3	F_{DES}	11	38	0,28
4	F_{TES}	- 8	53	0,25
5	$F_{\text{полин}}$	1	27	0,03

Приведенные результаты расчета ошибок прогноза для всех исследуемых моделей продемонстрировали, что использованные три способа определения ошибок прогноза показали приблизительно одинаковые результаты. Наилучшие результаты прогноза относительно исходных данных показала модель полиномиальной линии тренда. Необходимо отметить, что использованные методы расчета ошибок прогноза в данной работе составляют только малую часть из возможных вариантов расчета ошибок [7]. Каждый вариант определения ошибки прогноза необходимо выбирать, исходя из рассматриваемой ситуации.

Заключение. Проведенный анализ моделей прогнозирования числа требуемых носимых средств радиосвязи ГУ МВД России по Тульской области позволил определить модель прогнозирования, которая демонстрирует наиболее точные результаты прогноза. Таким образом, с целью прогнозирования числа требуемых носимых радиостанций для ГУ МВД России по Тульской области необходимо использовать модель полиномиальной линии тренда.

В дальнейшем исследование планируется продолжить с целью разработки алгоритма расчета дополнительных весовых коэффициентов для получения более точных результатов прогноза.

ЛИТЕРАТУРА

1. Терентьев А. А., Петров С. А., Печенин Е. А. Анализ прогнозирования компьютерных атак с применением информационных технологий // Вестник Воронежского института ФСИН России. — 2024. — № 3. — С. 124—132.

2. Применение методов ARIMA, ARIMAX, ARDLN, ARCH и GARCH авторегрессионных моделей в задаче прогнозирования состояния брандмауэра пассажирского самолёта / Д. Э. Потапов, Г. В. Москвитинов, П. М. Брусникин, Е. С. Неретин // XV Всероссийская научно-практическая конференция студентов и аспирантов «Актуальные проблемы развития авиационной техники и методов ее эксплуатации». — Иркутск, 2023. — С. 101—112.

3. Жиляков Е. Г., Скубилин В. В. О некоторых моделях краткосрочного прогнозирования // Научные ведомости БелГУ. Серия : История. Политология. Экономика. Информатика. — 2013. — № 22 (165). — С. 144—147.

4. Кузнецов И. П. Прогнозирование преступлений: теоретические и практические аспекты. — Екатеринбург : Урал. ун-т, 2019. — 224 с.

5. Романов А. В., Тихомиров П. С. Модели прогнозирования преступлений на основе анализа данных. — Владивосток : Дальневосточное издательство, 2020. — 245 с.

6. Терентьев А. А., Лукьянов А. С. Построение алгоритма прогнозирования числа киберпреступлений // Вестник Воронежского института МВД России. — 2024. — № 3. — С. 106—115.

7. Пьянков О. В., Лукьянов А. С., Терентьев А. А. Разработка моделей прогнозирования для проектирования систем связи специального назначения : учебно-методическое пособие. — Воронеж : Воронежский институт МВД России, 2025. — 108 с.

REFERENCES

1. Terent`ev A. A., Petrov S. A., Pechenin E. A. Analiz prognozirovaniya komp`yuterny`x atak s primeneniem informacionny`x texnologij // Vestnik Voronezhskogo instituta FSIN Rossii. — 2024. — № 3. — S. 124—132.

2. Primenenie metodov ARIMA, ARIMAX, ARDLN, ARCH i GARCH avtoregresionny`x modelej v zadache prognozirovaniya sostoyaniya brandmaue`ra passazhirskogo samolyota / D. E`. Potapov, G. V. Moskvitinov, P. M. Brusnikin, E. S. Neretin // XV Vserossiyskaya nauchno-prakticheskaya konferenciya studentov i aspirantov «Aktual`ny`e problemy` razvitiya aviacionnoj texniki i metodov ee e`kspluatatsii». — Irkutsk, 2023. — S. 101—112.

3. Zhilyakov E. G., Skubilin V. V. O nekotory`x modelyax kratkosrochnogo prognozirovaniya // Nauchny`e vedomosti BelGU. Seriya : Istoriya. Politologiya. E`konomika. Informatika. — 2013. — № 22 (165). — S. 144—147.

4. Kuznecov I. P. Prognozirovanie prestuplenij: teoreticheskie i prakticheskie aspekty`. — Ekaterinburg : Ural. un-t, 2019. — 224 s.

5. Romanov A. V., Tixomirov P. S. Modeli prognozirovaniya prestuplenij na osnove analiza danny`x. — Vladivostok : Dal`nevostochnoe izdatel`stvo, 2020. — 245 s.

6. Terent`ev A. A., Luk`yanov A. S. Postroenie algoritma prognozirovaniya chisla kiberpstuplenij // Vestnik Voronezhskogo instituta MVD Rossii. — 2024. — № 3. — S. 106—115.

7. P`yankov O. V., Luk`yanov A. S., Terent`ev A. A. Razrabotka modelej prognozirovaniya dlya proektirovaniya sistem svyazi special`nogo naznacheniya : uchebno-metodicheskoe posobie. — Voronezh : Voronezhskij institut MVD Rossii, 2025. — 108 s.

СВЕДЕНИЯ ОБ АВТОРАХ

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.

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.

Захаров Максим Сергеевич. Курсант.
Воронежский институт МВД России.
E-mail: lfeym@mail.ru
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.

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.

Zakharov Maxim Sergeevich. Cadet.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: lfeym@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: модели прогнозирования; носимые радиостанции; органы внутренних дел; средняя ошибка; средняя абсолютная ошибка; относительная погрешность.

Key words: forecasting models; portable radio stations; internal affairs agencies; average error; average absolute error; relative error.

УДК 519.254

А. Н. Бабкин, кандидат технических наук, доцент

Л. В. Акчурина, кандидат технических наук

С. П. Алексеенко, кандидат физико-математических наук, доцент

ГРАФИЧЕСКИЙ СПОСОБ ОБНАРУЖЕНИЯ ВНУТРЕННЕГО НАРУШИТЕЛЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ОРГАНИЗАЦИИ

GRAPHIC METHOD OF DETECTING INTERNAL INTRUDER OF INFORMATION AND TELECOMMUNICATION NETWORK OF ORGANIZATION

Статья посвящена реализации графического способа обнаружения внутреннего нарушителя информационно-телекоммуникационной сети организации. Данный способ позволяет наглядно представить поведение авторизованного пользователя сети и выявить внутреннего нарушителя.

The article is devoted to the implementation of a graphical method for detecting an internal intruder of an information and telecommunication network of an organization. This method allows you to visualize the behavior of an authorized network user and to identify an internal intruder.

Введение. Одной из основных угроз информационной безопасности является утечка информации за счет несанкционированного доступа [1, 2]. Субъектом несанкционированного доступа может быть внешний или внутренний нарушитель.

Наибольшую опасность представляет собой внутренний нарушитель, так как он является авторизованным пользователем информационно-телекоммуникационной сети (ИТКС) организации и выявление такого нарушителя представляет непростую задачу для службы безопасности организации, решение которой позволит выявлять и предотвращать риски ещё на стадии их формирования.

Поведенческие характеристики пользователей информационной системы составляют большой поток данных, исследование которого в «ручном режиме» ограничивают скорость и качество обработки подозрительных событий. Для получения этих характеристик необходимо обращаться к составлению модели допустимых действий пользователя в повседневной работе с информационными системами, находящимися под контролем. Такая модель позволит автоматизировать процесс анализа поведения пользователей и выявления подозрительных событий со значительно большей скоростью. Она будет основываться на статистических данных о типичном поведении пользователей в различных ситуациях и позволит определить границы допустимых действий.

Существуют различные способы предотвращения НСД от внутреннего нарушителя [2—5]. Предлагается к рассмотрению наглядный способ обнаружения аномального поведения внутреннего пользователя в ИТКС.

Основная часть. В [6] был рассмотрен алгоритм выявления внутреннего нарушителя ИТКС организации, который основан на анализе параметров функционирования авторизованных пользователей.

К параметрам функционирования авторизованных пользователей относятся параметры, определяющие доступ пользователей к информационным ресурсам организации, производительность программно-аппаратных средств рабочих станций пользователей, их рабочий график как в сети ИТКС, так и в организации.

Основой выявления возможных информационных атак со стороны авторизованных пользователей организации (внутренних нарушителей) являются поведенческие методы.

Отклонение параметров от номинальных значений рассматривается как попытка (возможность) организации информационной атаки.

Введем функцию

$$П = \{П_1, П_2, П_3, П_4\}, \quad (1)$$

где: $П_1$ — уровень загрузки работы центрального процессора рабочей станции пользователя (или уровень загрузки основной памяти, эти показатели находятся в прямой зависимости);

$П_2$ — максимальный объем используемого пространства внутренней памяти;

$П_3$ — максимальный объем используемого пространства внешнего запоминающего устройства, включая объем, который занимают временные файлы (программный кэш);

$П_4$ — максимальный объем информации, переданной пользователем по коммуникационной сети ИТКС.

Каждый параметр имеет некоторое среднее значение с допустимым отклонением $\Delta p_1, \Delta p_2, \Delta p_3, \Delta p_4$.

Будем считать, что для конкретного авторизованного сотрудника все параметры $П_i$, для $i = 1, \dots, 4$, и все отклонения Δp_i , $i = 1, \dots, 4$, известны.

Пусть $П_i$ — среднее значение одной из четырех рассматриваемых характеристик, которое в процессе работы принимает наблюдаемое значение $П_{набл_i}$ и должно попадать в интервал

$$П_i - \Delta p_i < П_{набл_i} < П_i + \Delta p_i$$

или удовлетворять неравенствам

$$П_{набл_i} + \Delta p_i - П_i > 0 \text{ и } -П_{набл_i} + \Delta p_i + П_i > 0.$$

Тогда следующая функция отслеживает ситуацию с выходом за допустимые границы исследуемой характеристики в рабочем процессе:

$$\begin{aligned} \overline{П}_i(П_i; \Delta p_i; П_{i,набл}) &= (П_{набл_i} + \Delta p_i - П_i); \\ \overline{П}_i(П_i; \Delta p_i; П_{i,набл}) &= (-П_{набл_i} + \Delta p_i + П_i). \end{aligned} \quad (2)$$

Функция будет иметь положительное значение только для добросовестного авторизованного сотрудника организации и может быть записана в виде

$$\overline{П}_i(П_i; \Delta p_i; П_{i,набл}) = (\Delta p_i)^2 - (П_i - П_{i,набл})^2.$$

Составим общую функцию, которая будет отслеживать сразу все четыре параметра функции $П_i$ (1).

Простое перемножение всех четырех параметров функции Π_i не информативно, т. к. два отрицательных значения показателей из четырех или отрицательные значения всех четырех показателей дадут положительное значение, которое не позволит определить внутреннего нарушителя:

$$\Pi_{i=1}^4 \left((\Delta p_i)^2 - (\Pi_i - \Pi_{i, \text{набл}})^2 \right) > 0.$$

Поведение будем считать подозрительным, если хотя бы один из четырех параметров показывает, что наблюдаемое значение $\Pi_{\text{набл}}$ значительно отличается от ожидаемого Π_i , для $i = 1, \dots, 4$.

Для выявления нарушений в работе пользователя составим функцию:

$$P(\bar{\Pi}_1; \bar{\Pi}_2; \bar{\Pi}_3; \bar{\Pi}_4) = \begin{cases} 1, & \text{если} \left| \begin{aligned} &(\bar{\Pi}_1(\Pi_1; \Delta p_1; \Pi_{1, \text{набл}}) > 0) \text{ и } (\bar{\Pi}_2(\Pi_2; \Delta p_2; \Pi_{2, \text{набл}}) > 0) \text{ и} \\ &(\bar{\Pi}_3(\Pi_3; \Delta p_3; \Pi_{3, \text{набл}}) > 0) \text{ и } (\bar{\Pi}_4(\Pi_4; \Delta p_4; \Pi_{4, \text{набл}}) > 0) \end{aligned} \right. \\ -1 \end{cases}$$

Введенная таким образом функция принимает значение $P(\bar{\Pi}_1; \bar{\Pi}_2; \bar{\Pi}_3; \bar{\Pi}_4) = +1$, если ни по одной из рассматриваемых характеристик отклонений нет, и $P(\bar{\Pi}_1; \bar{\Pi}_2; \bar{\Pi}_3; \bar{\Pi}_4) = -1$, если хотя бы в одной из переменных есть отклонения от регламентированного поведения.

Определенная выше функция $P(\bar{\Pi}_1; \bar{\Pi}_2; \bar{\Pi}_3; \bar{\Pi}_4)$ удобна тем, что позволяет вводить другие переменные, которые могут оказаться важными и дополняющими поведенческие свойства авторизованного пользователя, но не перечислены среди переменных $\Pi_1 \dots \Pi_4$.

В работе [6] была определена функция:

$$T = T(T_1, T_2, T_3, T_{\text{нач}}, T_{\text{оконч}}, T_{\text{min}}, T_{\text{max}}),$$

которая принимает отрицательное значение для авторизованного пользователя, нарушающего временной режим работы на своем рабочем месте.

Объединяя обе построенные функции $T(T_1, T_2, T_3, T_{\text{нач}}, T_{\text{оконч}}, T_{\text{min}}, T_{\text{max}})$ и $P(\bar{\Pi}_1; \bar{\Pi}_2; \bar{\Pi}_3; \bar{\Pi}_4)$ в вектор-функцию по формуле:

$$F(\bar{T}; \bar{P}) = T(T_1, T_2, T_3, T_{\text{нач}}, T_{\text{оконч}}, T_{\text{min}}, T_{\text{max}}) \cdot \bar{i} + P(\bar{\Pi}_1; \bar{\Pi}_2; \bar{\Pi}_3; \bar{\Pi}_4) \cdot \bar{j},$$

получим на плоскости $ТоР$ вектор, который своим положением в системе координат будет указывать, есть ли признаки нарушения со стороны авторизованного пользователя, которые создают угрозу информационной атаке.

При этом возможно определить, что конкретно нарушается пользователем.

На оси абсцисс $оТ$ вектор-функция $F(\bar{T}; \bar{P})$ указывает наличие нарушений или их отсутствие по времени присутствия на рабочем месте.

Если первая координата $T(T_1, T_2, T_3, T_{\text{нач}}, T_{\text{оконч}}, T_{\text{min}}, T_{\text{max}})$ положительна, то по данному критерию нарушений нет, соответственно, если знак отрицательный, то сотрудник не соблюдает своевременность прихода и ухода со своего рабочего места.

На оси ординат $оР$ вектор-функция $F(\bar{T}; \bar{P})$ указывает наличие нарушений или их отсутствие со стороны интенсивности загрузки памяти (процессора) компьютера, интенсивности работы в сети интернет или с дополнительными носителями.

Если вторая координата $P(\bar{P}_1; \bar{P}_2; \bar{P}_3; \bar{P}_4)$ положительна, то по данному критерию нарушений нет, соответственно, если знак отрицательный, то сотрудник имеет отклонения хотя бы по одному из указанных выше критериев.

На рисунке приводится пример графического способа обнаружения внутреннего нарушителя информационно-телекоммуникационной сети организации.

Радиус-вектор $F(\bar{T}; \bar{P})$ на плоскости ToP однозначно вычисляется для конкретного пользователя.

Вектор может находиться в одном из четырех квадрантов (четвертей), при этом наличие вектора:

- в I четверти указывает, что сотрудник работает добросовестно и ничего не нарушает;
- во II четверти указывает, что сотрудник нарушает только временной режим (не вовремя приходит и уходит с работы);
- в III четверти указывает, что сотрудник нарушает и временной режим на своем рабочем месте, и допустимые границы объема передаваемой информации по сети либо на дополнительные источники хранения и т. д.
- в IV четверти указывает, что сотрудник интенсивно работает с сетью Интернет, передает много информации по сети, пользуется дополнительными устройствами хранения информации, имеет высокий уровень загрузки памяти компьютера на своем рабочем месте и т. п.

Положение вектора в данной четверти однозначно сигнализирует о том, что пользователь имеет серьезные отклонения от принятых норм поведения на рабочем месте.

Наглядность предложенного способа имеет очевидные плюсы, т. к. графическое представление поведения сотрудника организации избавляет от проверки ряда условий и сразу указывает, на какой аспект его работы следует обратить внимание.

Сбор информации средних значений с допустимыми отклонениями по каждой из переменных должен быть репрезентативным по каждому из пользователей.



Реализация графического способа обнаружения внутреннего нарушителя информационно-телекоммуникационной сети организации

Заключение. Внутренние нарушители, являющиеся авторизованными пользователями ИТКС, представляют серьезную угрозу.

Выявление такого пользователя является сложной задачей для сотрудников безопасности организации.

Одним из возможных способов выявления такого нарушителя является анализ его поведения.

Поведенческие методы основаны на анализе параметров функционирования ИТКС и, в частности, авторизованных пользователей.

Отклонение параметров от номинальных значений рассматривается как попытка (возможность) организации информационной атаки.

Таким образом, реализуя алгоритм проверки критериев временного графика работы и нагрузки на ресурсы компьютера, можно составить вывод в виде графика, представленного на рисунке, по которому можно с высокой вероятностью выявить внутреннего нарушителя.

ЛИТЕРАТУРА

1. Меры защиты информации в государственных информационных системах : методический документ : утв. ФСТЭК России 11 февраля 2014 г.
2. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации : руководящий документ : утв. решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
3. Язов Ю. К., Соловьев С. В. Организация защиты информации в информационных системах от несанкционированного доступа : монография. — Воронеж : Кварт, 2018. — 588 с.
4. Сердюк В. А. Новое в защите от взлома корпоративных систем. — М. : Техносфера, 2007. — 360 с.
5. Марков А. С., Цирлов В. Л., Барабанов А. В. Методы оценки несоответствия средств защиты информации. — М. : Радио и связь, 2012. — 192 с.
6. Бабкин А. Н., Акчурина Л. В., Алексеенко С. П. Способ обнаружения внутреннего нарушителя информационно-телекоммуникационной сети организации // Вестник Воронежского института МВД России. — 2024. — № 4. — С.139—147.

REFERENCES

1. Mery` zashhity` informacii v gosudarstvenny`x informacionny`x sistemax : metodicheskij dokument : utv. FSTE`K Rossii 11 fevralya 2014 g.
2. Sredstva vy`chislitel`noj texniki. Zashhita ot nesankcionirovannogo dostupa k informacii. Pokazateli zashhishhennosti ot nesankcionirovannogo dostupa k informacii : rukovodyashhij dokument : utv. resheniem predsedatelya Gosudarstvennoj texnicheskoj komissii pri Prezidente Rossijskoj Federacii ot 30 marta 1992 g.
3. Yazov Yu. K., Solov`ev S. V. Organizaciya zashhity` informacii v informacionny`x sistemax ot nesankcionirovannogo dostupa : monografiya. — Voronezh : Kvarta, 2018. — 588 s.
4. Serdyuk V. A. Novoe v zashhite ot vzloma korporativny`x sistem. — M. : Texnosfera, 2007. — 360 s.

5. Markov A. S., Cirlov V. L., Barabanov A. V. Metody` ocenki nesootvetstviya sredstv zashhity` informacii. — M. : Radio i svyaz`, 2012. — 192 s.

6. Babkin A. N., Akchurina L. V., Alekseenko S. P. Sposob obnaruzheniya vnutrennego narushitelya informacionno-telekommunikacionnoj seti organizacii // Vestnik Voronezhskogo instituta MVD Rossii. — 2024. — № 4. — S.139 — 147.

СВЕДЕНИЯ ОБ АВТОРАХ

Бабкин Александр Николаевич. Доцент кафедры информатики и вычислительной техники. Кандидат технических наук, доцент.

Международный институт компьютерных технологий.

E-mail: alex_babk@mail.ru

Россия, 394026, Воронеж, ул. Солнечная, 29 б.

Акчурина Людмила Васильевна. Доцент кафедры прикладной математики и механики. Кандидат технических наук.

Воронежский государственный технический университет.

E-mail: ac.mila@yandex.ru

Россия, 394026, Воронеж, ул. 20-летия Октября, 84.

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.

Babkin Alexander Nikolaevich. Associate Professor of Computer Science and Applied Technology. Candidate of Technical Sciences, Associate Professor.

International Institute of Computer Technology.

Email: alex_babk@mail.ru

Work address: Russia, 394026, Voronezh, Solnechnaya Str., 29 b.

Akchurina Lyudmila Vasilyevna. Associate Professor of the chair of Applied Mathematics and Mechanics. Candidate of Technical Sciences.

Voronezh State Technical University.

E-mail: ac.mila@yandex.ru

Work address: Russia, 394026, Voronezh, 20-letiya Oktyabrya Str., 84.

Alekseenko Sergey Pavlovich. Assistant Professor of the chair of Information Security. Candidate of Sciences (Physics and Mathematics), Assistant Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: aleks_serg@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: авторизованный пользователь; внутренний нарушитель; несанкционированный доступ; угроза информационной безопасности; информационно-телекоммуникационная сеть; радиус-вектор.

Key words: authorized user; internal intruder; unauthorized access; information security threat; information and telecommunication network; radius vector.

УДК 004.056.53

Д. С. Звягин, кандидат технических наук

А. А. Масловская

МОДЕЛИРОВАНИЕ ПРОЦЕССА ПРОТИВОДЕЙСТВИЯ ПОЛУЧЕНИЮ ВИДОВОЙ ИНФОРМАЦИИ ПРИ ПОМОЩИ БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ

MODELING OF THE PROCESS OF COUNTERING THE ACQUISITION OF SPECIFIC INFORMATION USING UNMANNED AIRCRAFT

В статье авторами описываются возможные технические каналы утечки информации, которые могут возникнуть при использовании злоумышленником беспилотных воздушных судов. В ходе детального рассмотрения визуально-оптического канала утечки информации выделяются потенциальные или реально существующие опасности нарушения безопасности информации на контролируемом объекте. Для достижения задач по противодействию получению информации с помощью беспилотных воздушных судов, учитывая изменения состояний взаимозависимых процессов, авторами предлагается математическая модель. Представленная математическая модель была создана на основе аппарата сетей Петри и может имитировать как параллельные, так и асинхронные системы. В результате использования данной модели можно учитывать различные варианты действия злоумышленника по добыванию видовой информации.

In this article the authors describe possible technical channels of information leakage that may occur when an attacker uses unmanned aircraft. During a detailed examination of the visual-optical information leakage channel, potential or actual information security risks at the controlled facility are highlighted. To achieve the tasks of countering information acquisition using unmanned aircraft, taking into account changes in the states of interdependent processes, the authors propose a mathematical model. The presented mathematical model was created based on the apparatus of Petri nets, which can simulate both parallel and asynchronous systems. As a result of using this model, it is possible to take into account various options for an attacker to extract specific information.

Введение. В настоящее время беспилотные воздушные суда (далее — БВС) ко-птерного типа получили широкое применение в деятельности злоумышленников, в том числе в качестве носителя средства перехвата информации. Рассматривая противоправное применение БВС, подразумевается использование воздушной среды, что делает частично или полностью невозможным использование имеющихся средств обеспечения безопасности информации, так как они применяются для противодействия другим средствам разведки. К тому же стоит учесть, что процесс получения информации с помощью БВС является динамически изменяющимся и характеризуется возможностью управления и контроля полета оператором, находящимся вне борта воздушного судна.

Исходя из того, что технический канал утечки информации — это совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация [1], данная совокупность при использовании БВС будет состоять из следующих основных компонентов:

объект — желаемая для злоумышленника информация (человек, здание, событие, техническое средство, обстановка);

воздушная среда;

средство перехвата информации и оператор воздушного судна.

БВС имеет возможность нелегитимного доступа к информации за счет стационарных (антенна, камера с возможностью фото- и видеосъемки) или дополнительно установленных конструкций (микрофон, приемник побочных электромагнитных излучений, дополнительное программное обеспечение и т. д.), образующая каналы утечки информации, такие как визуально-оптический, акустический и электромагнитный.

Визуально-оптический канал утечки информации в случае использования БВС подразумевает наблюдение за объектами разведки и фиксацию необходимой информации (о сотрудниках и документах, с которыми они работают, событиях и действиях, происходящих в контролируемой зоне).

Акустические каналы утечки информации характеризуются возможностью получать информацию за счет распространяющихся от источника звуковых волн. В случае использования БВС данный канал реализуется за счет средств приема акустических сигналов с помощью специально установленных на его корпусе датчиков и последующей обработки информации.

Электромагнитные каналы утечки информации с помощью БВС возникают из-за перехвата и последующей расшифровки электромагнитных волн. На БВС могут быть установлены специальные приемные устройства, способные принимать побочные электромагнитные излучения и наводки, исходящие от технических средств, находящихся на контролируемом объекте.

В ходе данного исследования нами будет рассмотрен визуально-оптический канал на основе использования злоумышленником БВС коптерного типа. Современные БВС данного типа имеют возможность быстрого передвижения на удаленные от оператора расстояния и передачу данных на пульт управления со скоростью до нескольких тысяч мегабит в секунду. Благодаря современным характеристикам камер, осуществляющим фото- и видеосъемку в формате 4К, оператор БВС может проводить топографическую, опознавательную и (или) предметную съемку, вследствие чего получать информацию об общем или детальном виде интересующего объекта, идентифицировать личность человека или понять контекст события, происходящего в контролируемой зоне (рис. 1). В случае использования злоумышленником подобного БВС это может привести к угрозе безопасности информации (далее — УБИ), выражающейся в создании потенциальной или реально существующей опасности нарушения безопасности информации.



Рис. 1. УБИ в случае использования визуально-оптических средств БВС

Процесс получения информации с использованием БВС можно рассматривать как случайный. За счет этого возникает проблематичность оценки ущерба от реализации УБИ, связанная, во-первых, с многообразием сценариев, во-вторых, с неопределенностью относительно цели злоумышленника и последующей интерпретации полученной информации.

В соответствии с пунктом 40 части 1 статьи 13 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции» сотрудник полиции вправе пресекать функционирование БВС посредством подавления или преобразования сигналов дистанционного управления беспилотными аппаратами, воздействуя на их пульта управления, а также повреждения или уничтожения беспилотных аппаратов [2].

На данный момент противодействие БВС в системе МВД России осуществляется по следующему алгоритму [3]:

1. Получение информации о появлении БВС в воздушном пространстве.
2. Подготовительный этап:
 - 2.1. Определение приблизительного расстояния.
 - 2.2. Визуальный и акустический контроль.
 - 2.3. Развертывание средств для осуществления подавления или преобразования сигнала.
 - 2.4. По возможности идентификация БВС.
3. Этап противодействия. Оператор средства противодействия БВС включает те или иные каналы воздействия, которые соответствуют частотным диапазонам обнаруженного БВС. В случае отсутствия точной информации о частотных диапазонах оператор противодействия БВС включает все каналы. Если при выключении определенного канала БВС через несколько секунд начинает движение не по ветру, а по командам оператора, необходимо продолжать воздействие на БВС пока он не приземлится.
4. Заключительный этап:
 - 4.1. Документирование факта пресечения нахождения БВС в воздушном пространстве.

4.2. Передача воздушного судна в органы, уполномоченные на дальнейшее изучение обстоятельств возникновения и нахождения БВС.

Постановка задачи. Для достижения задач по противодействию получению информации с помощью БВС необходимо следовать действиям алгоритма, однако это не гарантирует, что информация не будет передана злоумышленнику, так как обмен данными между пультом управления и БВС происходит постоянно и с большой скоростью. Таким образом, имеет смысл учитывать различные сценария действия злоумышленника, такие как дальность нахождения средства разведки, вид и способ перехватываемой информации и другие.

Для оперативного развертывания и правильной последовательности действий оператора по противодействию БВС целесообразно использовать математическое моделирование.

Для создания математической модели процесса противодействия получению видовой информации при помощи БВС необходимо принять во внимание модели, учитывающие изменения состояний взаимозависимых процессов. Сети Петри представляют собой наиболее подходящий метод для построения таких моделей.

Решение. Сеть Петри определяется как четверка $\{P, T, I, O\}$, где P и T — конечные множества позиций и переходов, I и O — множества входных и выходных функций [4].

В качестве примера использования сетей Петри в моделировании процесса противодействия получению видовой информации при помощи БВС рассмотрим этап получения информации о приближении технического средства разведки (рис. 2).

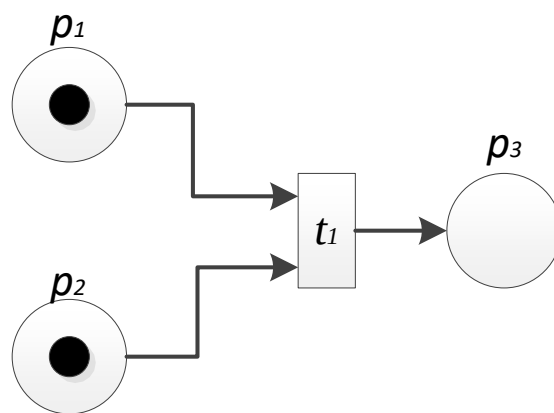


Рис. 2. Пример маркированной сети Петри

В рассматриваемой сети Петри:

$P = \{p_1, p_2, p_3\}$ — позиции;

$T = \{t_1\}$, где t_1 — переход (событие);

$I(t_1) = \{p_1, p_2\}$;

$O(t_1) = \{p_3\}$;

$\mu = (1, 1, 0)$.

В данном примере: p_1 — позиция, в которой на объекте имеется оператор (специалист), осуществляющий противодействие БВС и находящийся на посту; p_2 — условие, при котором оператор (специалист) акустически или визуально определил наличие БВС в воздушном пространстве; p_3 — позиция, в которой установлен факт приближения БВС.

Для того чтобы был установлен факт приближения БВС, необходимо наличие маркера в позиции p_3 . Для этого должен сработать переход t_1 , что возможно только тогда, когда во всех входных позициях данного перехода будут маркеры. Таким образом, рассматривая пример на рисунке 2, в рамках этапа получения информации о приближении технического средства разведки на объекте имеется оператор (специалист), осуществляющий противодействие БВС и находящийся на посту, а также выполнено условие, при котором он определил наличие БВС в воздушном пространстве.

Переход t_1 разрешен, так как в позициях p_1 и p_2 имеются метки: $\mu = (1, 1, 0)$. После срабатывания перехода t_1 маркировка сети меняется: $\mu' = (0, 0, 1)$ [5].

Рассматривая все этапы процесса противодействия получению видовой информации при помощи БВС, построим математическую модель при помощи сетей Петри (рис. 3).

В рассматриваемой сети Петри:

$P = \{p_1, p_2, \dots, p_{22}\};$

$T = \{t_1, t_2, \dots, t_9\}.$

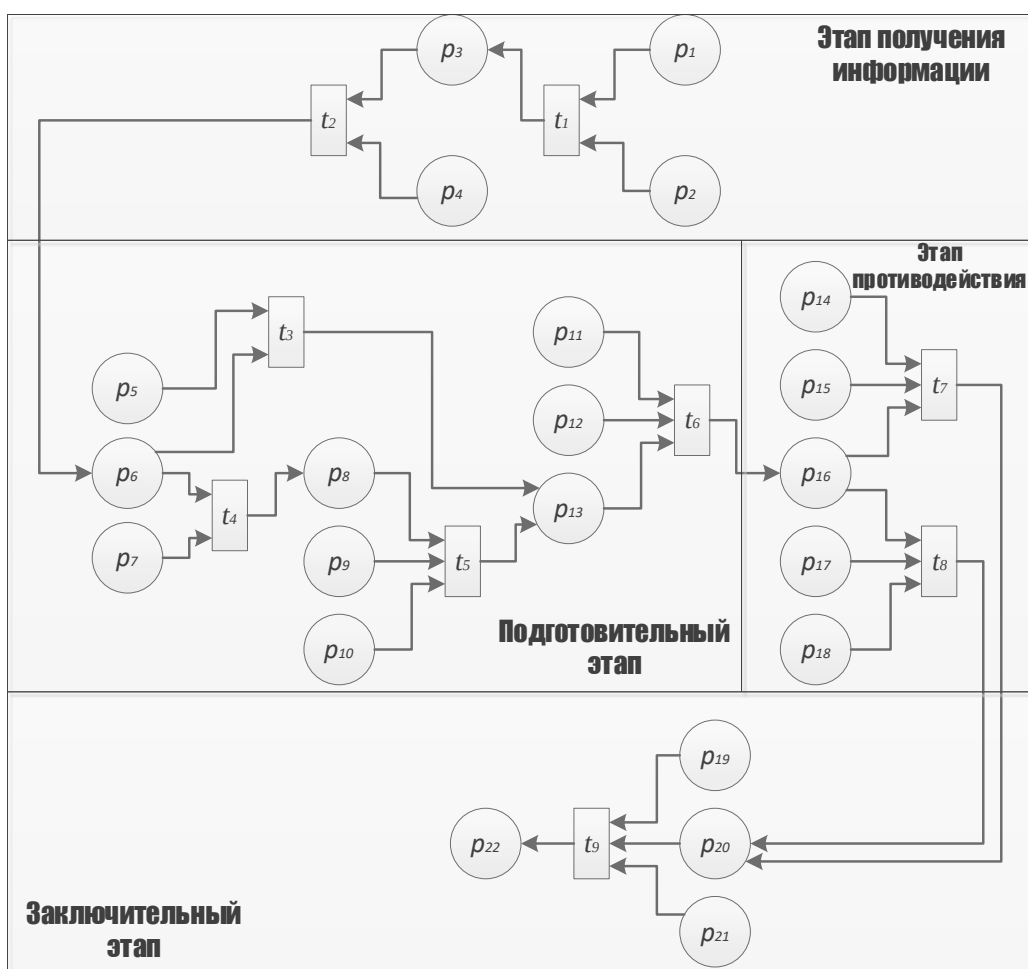


Рис. 3. Модель процесса противодействия получению видовой информации при помощи БВС

Таблица содержит описание всех позиций математической модели процесса противодействия получению видовой информации при помощи БВС.

Описание позиций математической модели процесса противодействия
получению видовой информации при помощи БВС

Условное обозначение позиции	Пояснение позиции
p_1	наличие объекта информатизации
p_2	наличие оператора (специалиста), осуществляющего противодействие БВС
p_3	позиция, в которой на объекте имеется оператор (специалист), осуществляющий противодействие БВС и находящийся на посту
p_4	условие, при котором оператор (специалист) акустически или визуально определил наличие БВС в воздушном пространстве
p_5	наличие БВС в зоне видимости
p_6	позиция, в которой установлен факт приближения БВС
p_7	БВС находится вне зоны видимости
p_8	определение приблизительного расстояния. На этом шаге оператор средства противодействия с помощью ориентиров или метода триангуляции определяет потенциальную возможность злоумышленника перехватить информацию с учетом расстояния, на котором находится БВС
p_9	доклад о факте приближения уполномоченному на принятие решения о пресечении нахождения БВС
p_{10}	развертывание стационарных средств для осуществления подавления или преобразования сигнала
p_{11}	постоянный акустический и визуальный контроль за БВС, благодаря которому операторы средства противодействия могут контролировать ситуацию и оперативно вносить корректировки своих действий
p_{12}	развертывание носимых средств противодействия (ружья) БВС
p_{13}	БВС находится в прямой видимости оператора
p_{14}	условие, при котором осуществлена идентификация БВС визуально, а также с помощью комплексов радиомониторинга с целью установления частоты, на которой оператор БВС осуществляет управление
p_{15}	включение определенных каналов воздействия на средства противодействия БВС
p_{16}	противодействие БВС средствами для осуществления подавления или преобразования сигнала
p_{17}	условие, при котором идентификация БВС не осуществлена
p_{18}	включение всех каналов воздействия на средства противодействия БВС
p_{19}	документирование факта пресечения нахождения БВС в воздушном пространстве
p_{20}	подавление БВС
p_{21}	передача воздушного судна в органы, уполномоченные на дальнейшее изучение обстоятельств возникновения и нахождения БВС
p_{22}	успешное противодействие БВС

Заключение. Разработанная модель позволит оптимизировать процесс противодействия получению видовой информации при помощи БВС, а также повысить оперативность развертывания и использования средств противодействия.

При дальнейшем исследовании необходимо рассмотреть возможные действия при неудачном подавлении БВС, а также учитывать вариативность действий при помощи стохастических сетей Петри.

ЛИТЕРАТУРА

1. Хорев А. А. Техническая защита информации. Т. 1 : Технические каналы утечки информации. — М. : НПЦ «Аналитика», 2008. — 436 с.
2. О полиции : Федеральный закон от 07 февраля 2011 г. №3-ФЗ // Собрание законодательства РФ. — 2011. — № 7. — Ст. 900.
3. Об утверждении Порядка принятия решения о пресечении функционирования беспилотных воздушных, подводных и надводных судов и аппаратов, беспилотных транспортных средств и иных автоматизированных беспилотных комплексов в целях защиты жизни, здоровья и имущества граждан, сотрудников органов внутренних дел, в том числе в месте проведения публичного (массового) мероприятия и прилегающей к нему территории, проведения неотложных следственных действий и оперативно-розыскных мероприятий и Перечня должностных лиц полиции, уполномоченных на принятие такого решения : приказ МВД России от 16 ноября 2023 г. № 865 // СПС «Консультант Плюс».
4. Питерсон Дж. Теория сетей Петри и моделирование систем. — М. : Мир, 1984. — 264 с.
5. Звягин Д.С. Моделирование процесса поиска электронных устройств негласного получения информации при помощи нелинейных локаторов // Вестник Воронежского института МВД России. — 2024. — № 1. — С. 95—100.

REFERENCES

1. Xorev A. A. Texnicheskaya zashhita informacii. T. 1 : Texnicheskie kanaly` utechki informacii. — M. : NPCz «Analitika», 2008. — 436 s.
2. O policii : Federal`ny`j zakon ot 07 fevralya 2011 g. №3-FZ // Sobranie zakonodatel`stva RF. — 2011. — № 7. — St. 900.
3. Ob utverzhdenii Poryadka prinyatiya resheniya o presechenii funkcionirovaniya bespilotny`x vozdushny`x, podvodny`x i nadvodny`x sudov i apparatov, bespilotny`x transportny`x sredstv i iny`x avtomatizirovanny`x bespilotny`x kompleksov v celyax zashhity` zhizni, zdorov`ya i imushhestva grazhdan, sotrudnikov organov vnutrennix del, v tom chisle v meste provedeniya publichnogo (massovogo) meropriyatiya i prilegayushhej k nemu territorii, provedeniya neotlozhny`x sledstvenny`x dejstvij i operativnorozyskny`x meropriyatij i Perechnya dolzhnostny`x licz policii, upolnomochenny`x na prinyatie takogo resheniya : prikaz MVD Rossii ot 16 noyabrya 2023 g. № 865 // SPS «Konsul`tant Plyus».
4. Piterson Dzh. Teoriya setej Petri i modelirovanie sistem. — M. : Mir, 1984. — 264 s.
5. Zvyagin D.S. Modelirovanie processa poiska e`lektronny`x ustrojstv neglasnogo polucheniya informacii pri pomoshhi nelinejny`x lokatorov // Vestnik Voronezhskogo instituta MVD Rossii. — 2024. — № 1. — S. 95—100.

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.

Масловская Анастасия Александровна. Инженер отделения радиосвязи отдела организации системы связи и обеспечения ее функционирования ЦИТСиЗИ.

Главное управление МВД России по Воронежской области.

E-mail: maslovskaiiaa@mail.ru

Россия, 394036, Воронеж, ул. Володарского, 39.

Zvyagin Danil Sergeevich. Associate Professor of the Information Security Department. 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.

Maslovskaiia Anastasia Aleksandrovna. Engineer of the radio communications department of the department for organizing the communications system and ensuring its functioning of the information technology center for communications and information protection.

Main department of the Ministry of Internal Affairs of Russia for the Voronezh region.

E-mail: maslovskaiiaa@mail.ru

Work address: Russia, 394036, Voronezh, Volodarskogo Str., 39.

Ключевые слова: беспилотное воздушное судно; сети Петри; безопасность информации.

Key words: drone; Petri nets; information security.

УДК 004.056

А. А. Тихомирова, аспирант

А. В. Фурсова, аспирант

А. В. Яковлев, кандидат технических наук, доцент

ПРЕДСТАВЛЕНИЕ ТЕОРЕТИКО-МНОЖЕСТВЕННОЙ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ СЕТЯМИ ПЕТРИ

PRESENTATION OF A SET-THEORETICAL MODEL OF INFORMATION SECURITY THREATS BY PETRI NETS

Предложена форма представления теоретико-множественной модели, описывающей процедуру определения актуальных угроз согласно новой Методике оценки угроз безопасности информации ФСТЭК России. Для аналитического моделирования оценки угроз выбран аппарат сетей Петри. Построенная с использованием сетей Петри модель представляет собой целостное формальное описание процесса определения актуальных угроз безопасности информации и содержит графическое представление данного процесса, носящее последовательный характер выполнения этапов моделирования.

A form of representation of a set-theoretical model that describes the procedure of determining current threats according to the new "Information Security Threat Assessment Methodology" of the FSTEC of Russia is proposed. For analytical modeling of threat assessment, the device of Petri nets is selected. The model constructed using Petri nets is an integral formal description of the process of determining current threats to information security and contains a graphical representation of this process, which has a sequential nature of performing modeling stages.

Введение. В современном информационном пространстве, в эпоху цифровизации влияние информационных технологий на различные сферы жизни общества значительно увеличивается, следовательно, растут и объемы хранимой в электронном виде информации. Как результат повышается ценность цифровой информации, а значит, усиливается и необходимость обеспечения достаточного уровня безопасности информационных систем, обрабатывающих ее. Первоочередной задачей при проектировании системы защиты информационных систем является моделирование угроз безопасности информации (далее — УБИ).

Важность разработки актуальной модели угроз для конкретной информационной системы обусловлена следующими факторами:

- модель угроз позволяет создать абстрактное видение системы, определить границы моделирования УБИ и зоны ответственности сотрудников организации в части обеспечения безопасности ее информационных активов;
- сравнительный анализ существующей системы безопасности и модели угроз дает возможность выявить уязвимые места системы безопасности, выбрать правильный вектор ее модификации и тем самым избежать в дальнейшем нежелательных потерь для организации;
- моделирование УБИ помогает избежать избыточности при выборе мер защиты (например, использование средств защиты от угроз, реализация которых для данной системы невозможна) либо, наоборот, построения недостаточно эффективной системы защиты, не учитывающей все актуальные угрозы;

- процесс обеспечения эффективной защиты и поддержания ее на должном уровне связан со значительными финансовыми затратами, поэтому модель угроз дает возможность рационально подойти к выбору действительно необходимых для конкретной системы средств защиты, то есть избежать экономической нецелесообразности защиты.

Важно отметить, что процесс моделирования УБИ должен быть непрерывным, так как основная его цель — определение уязвимых мест системы, через которые могут быть реализованы УБИ. Вместе с тем со временем данные параметры неизбежно меняются, например, при модернизации и масштабировании системы (добавлении либо удалении элементов, изменении технологических процессов, усложнении компонентов вычислительных сетей и т. д.), что фиксируется практически ежемесячно (ежеквартально) по результатам инвентаризации информационных активов, анализа уязвимостей или тестирования на проникновение. Таким образом, только системный подход к моделированию УБИ позволит учесть изменение перечня актуальных угроз безопасности, а следовательно, обеспечить поддержание адекватной и эффективной системы защиты.

Анализ существующего подхода к моделированию угроз безопасности информации. В нашей стране вопрос моделирования УБИ находится в компетенции Федеральной службы по техническому и экспортному контролю России (ФСТЭК России). Вслед за динамично развивающимися технологиями приходится постоянно меняться и законодательству в сфере ИБ, в том числе и нормативной базе, регулирующей моделирование угроз [1]. Так, за последние почти пятнадцать лет ФСТЭК России предложено, как минимум, четыре методики, предлагающие различные подходы к разработке модели угроз безопасности информации [2]. Последней и актуальной на настоящий момент является Методика оценки угроз безопасности информации от 5 февраля 2021 года (далее — Методика), изменившая сам подход к моделированию, предложив специалистам в сфере информационной безопасности совершенно иную концепцию оценки угроз [3]. Данная концепция подразумевает, что все действия злоумышленников состоят из совокупности тактик и техник, описывающих сценарий реализации угрозы.

Предложенная Методика обладает рядом преимуществ по сравнению со своими предшественниками [4]:

- применение сценарного подхода при моделировании УБИ позволяет охватить максимально широкий круг угроз, актуальных для системы, заранее определить перечень контрмер для каждого сценария, а также прогнозировать возможные действия нарушителя при реализации им угрозы. Все это позволяет оперативно реагировать на атаку и успешно противодействовать ей;

- анализ актуальных угроз и уязвимостей информационной системы экспертной группой, а не отдельным специалистом позволит получить более точный и достоверный результат моделирования [5];

- основой моделирования являются негативные последствия от реализации угроз, определение перечня которых отводится заинтересованным лицам, что впоследствии облегчит задачу убедить бизнес в необходимости обеспечения информационной безопасности.

Но есть у новой Методики и ряд недостатков, а именно:

- Методика обязывает использовать Банк данных угроз (БДУ) ФСТЭК России в качестве источника данных об угрозах, но при этом абсолютно оторвана от него. Например, понятие «потенциал нарушителя» (который раньше рассчитывался по определенному алгоритму и имел три уровня) не соотносится с понятием «уровень возможностей нарушителя» (их в Методике 4, и для каждого вида нарушителя данный уровень уже определен). Таким

образом, моделирование УБИ с использованием БДУ потребует ручного анализа актуальных угроз [1];

- сценарный подход к моделированию делает процесс разработки модели угроз крайне сложным и требует от исполнителя очень высокого уровня компетентности в сфере информационной безопасности, ведь для получения перечня актуальных сценариев реализации угрозы необходимо просчитать все возможные комбинации 10 тактик и 145 техник для каждого объекта воздействия и вида актуального нарушителя, что практически невозможно вручную реализовать на практике;

- сведения об угрозах, содержащиеся в БДУ ФСТЭК, описаны вербально, что значительно усложняет их применение при автоматизации алгоритма оценки угроз [6, 7];

- перечень тактик и соответствующих им типовых техник, используемых для построения сценариев реализации УБИ, который представлен в приложении 11 Методики [3], чётко фиксирован, однако в действительности, в условиях постоянно расширяющегося спектра угроз, со временем растёт. Поэтому для периодической актуализации данного перечня потребуется создание и выпуск новой версии Методики.

Формальное описание задачи определения актуальных угроз. Для того чтобы нивелировать указанные выше недостатки определения актуальности УБИ по Методике ФСТЭК, предлагается перейти от качественной экспертной оценки УБИ к математическому моделированию процесса анализа угроз безопасности информации. В первую очередь для этого необходимо перейти от вербального описания УБИ к формальному. Ранее в [6] были рассмотрены правила формального описания этапов процесса оценки угроз. В таблице 1 приведен сводный перечень множеств элементов, фигурирующих при моделировании УБИ, и связывающих их логических выражений.

Таблица 1

Множества элементов, учитываемых при оценке УБИ, и отношения между ними

№ п\п	Наименование множества	Наименование на английском	Обозначение множества	Логическая связь
1.	Множество видов рисков (ущерба)	Risk	$RI = \{RI_m, m = \overline{1,3}\}$	RI_m может принимать одно из трёх значений: RI_1 — ущерб физическим лицам; RI_2 — ущерб организациям, юридическим лицам, индивидуальным предпринимателям, связанный с хозяйственной деятельностью; RI_3 — ущерб государству в различных областях и сферах деятельности (оборонной, социальной, экономической, политической, экологической и т. д.). Для каждого вида ущерба RI_m существует свое подмножество негативных последствий, объединение которых дает множество NC .

№ п/п	Наименование множества	Наименование на английском	Обозначение множества	Логическая связь
2.	Множество негативных последствий	Negative Consequences	$NC = \{NC_{ml}, m = \overline{1,3}, l = \overline{1,L}\}$	$NC = OI \times TI$
3.	Множество объектов воздействия	Objects of Influence	$OI = \{OI_t, t = \overline{1,T}\}$	
4.	Множество видов воздействия на объекты воздействия	Types of Impact	$TI = \{TI_u, u = \overline{1,U}\}$	
5.	Множество актуальных нарушителей	Actual Attackers	$AA = \{AA_d, d = \overline{1,D}\}$	$AA = TA \times TGA \times NC \times RI$
6.	Множество видов нарушителей	Types of Attackers	$TA = \{TA_k, k = \overline{1,K}\}$	
7.	Множество целей реализации угроз нарушителями	Targets of Attackers	$TGA = \{TGA_f, f = \overline{1,G}\}$	
8.	Множество категорий нарушителей	Categories of Attackers	$CA = \{CA_n, n = \overline{1,2}\}$	Для каждого вида актуального нарушителя определяются две основные характеристики – уровень возможностей по реализации УБИ и категория в зависимости от имеющихся прав и условий по доступу к системе, то есть каждому AA_d можно поставить в соответствие элемент из множества LAC и множества CA , который будет однозначно его характеризовать.
9.	Множество уровней возможностей нарушителей	Levels of Attackers' Capabilities	$LAC = \{LAC_p, p = \overline{1,4}\}$	
10.	Множество способов реализации (возникновения) угроз безопасности информации (УБИ)	Ways to Implement Threats	$WIT = \{WIT_s, s = \overline{1,S}\}$	$WIT = OI \times AA \times OA \times AIO$
11.	Множество возможностей нарушителей	Opportunities for Attackers	$OA = \{OA_f, f = \overline{1,F}\}$	
12.	Множество доступных интер-	Available Interfaces of impact Objects	$AIO = \{AIO_v, v = \overline{1,V}\}$	

№ п/п	Наименование множества	Наименование на английском	Обозначение множества	Логическая связь
	фейсов объектов воздействия			
13.	Множество возможных УБИ	Possible information security Threats	$PT = \{PT_c, c = \overline{1, C}\}$	$PT = AA \times OI \times WIT \times NC$
14.	Множество сценариев	Script	$SC = \{SC_w, w = \overline{1, W}\}$	$SC = TAC \times TEC \times AA \times WIT \times OI$
15.	Множество тактик	Tactics	$TAC = \{TAC_r, r = \overline{1, R}\}$	
16.	Множество техник	Technics	$TEC = \{TEC_q, q = \overline{1, Q}\}$	
17.	Множество актуальных угроз	Actual Threats (Current Threats)	$CT = \{CT_z, z = \overline{1, Z}\}$	Возможная угроза PT_c признается актуальной при наличии хотя бы одного сценария реализации данной угрозы SC_w .

Выбор математического аппарата для решения задачи. В качестве математического аппарата моделирования угроз безопасности информации выбран аппарат сетей Петри.

Графическим представлением сети Петри является двудольный ориентированный граф с двумя типами вершин — позициями (отображают условия) и переходами (отображают события), которые связаны между собой отношением непосредственной причинно-следственной связи, изображаемой с помощью направленных дуг. Для выражения причинно-следственных связей между условиями и событиями принимаются определенные правила срабатывания переходов. Последовательности событий отображаются срабатываниями переходов и собственно образуют моделируемый процесс. Сеть Петри позволяет в наглядной и хорошо формализованной форме проследить поведение параллельных систем с асинхронными взаимодействиями [8].

Явными преимуществами сетей Петри перед другими средствами графического представления процесса моделирования (например, деревьями атак [4], цепями Маркова [9], ориентированными графами [10, 11]) можно считать возможность отображать одновременно несколько параллельно-последовательных процессов на одной модели, а также использовать при моделировании дополнительные атрибуты, такие как цвет, приоритет переходов, время.

Ранее сети Петри уже использовались для описания некоторых задач технической защиты информации. Например, для моделирования процедуры анализа программного кода на предмет наличия в нем уязвимостей [12, 13, 14], для реализации алгоритма обнаружения сетевых атак на ИС [15].

Результаты моделирования и их анализ. На рисунке 1 представлена сеть Петри, моделирующая процесс определения актуальности УБИ в соответствии с алгоритмом, предложенным новой Методикой ФСТЭК России.

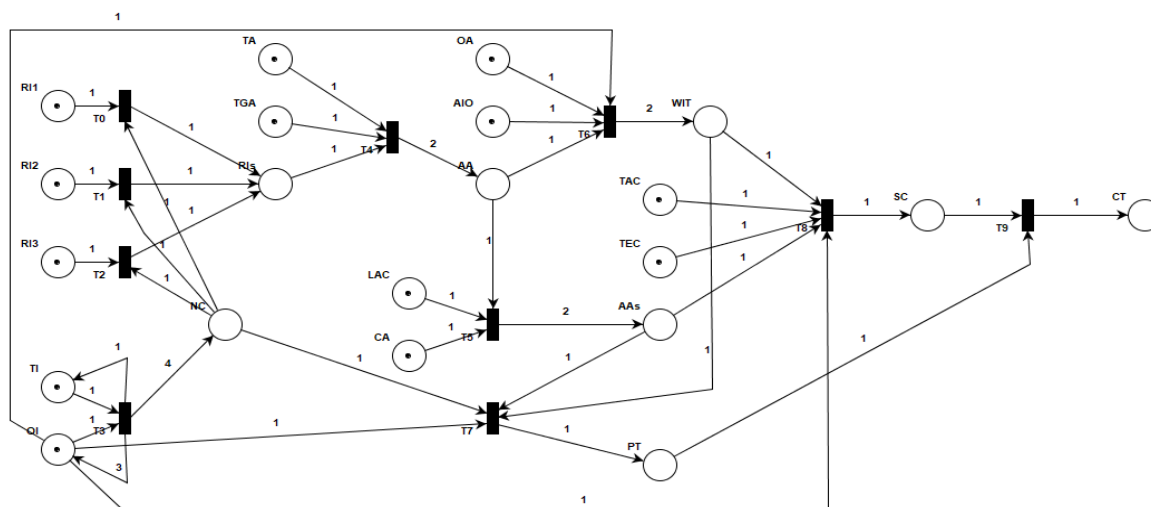


Рис. 1. Сеть Петри, моделирующая процесс определения актуальности УБИ

Ниже в таблицах описаны элементы множества позиций P (таблица 2) и множества переходов T (таблица 3) в терминах, введенных в таблице 1:

Таблица 2

Описание элементов множества позиций

№ п/п	Обозначение позиций	Описание позиций
1.	$RI_s (RI_1, RI_2, RI_3)$	Выбран(ы) релевантный(ые) вид(ы) рисков (ущерба)
2.	OI	Определено множество возможных объектов воздействия
3.	TI	Выявлено множество видов воздействия на объекты воздействия
4.	NC	Определено множество негативных последствий
5.	TA	Определено множество видов нарушителей
6.	TGA	Определено множество целей реализации угроз нарушителями
7.	AA	Определено множество актуальных нарушителей
8.	CA	Заданы категории нарушителей
9.	LAC	Заданы уровни возможностей нарушителей
10.	AA_s	Для актуальных нарушителей определены соответствующие категории и уровни возможностей
11.	OA	Определено множество возможностей нарушителей
12.	AOI	Выявлено множество доступных интерфейсов объектов воздействия
13.	WIT	Определено множество способов реализации (возникновения) УБИ
14.	PT	Сформировано множество возможных УБИ
15.	TAC	Выбрано множество тактик
16.	TEC	Выбрано множество техник
17.	SC	Установлено наличие сценария(ев) реализации УБИ
18.	CT	УБИ признана актуальной

Таблица 3

Описание элементов множества переходов

№ п/п	Обозначение переходов	Описание переходов
1.	t_0	Признание актуальными рисков, приводящих к ущербу физическим лицам
2.	t_1	Признание актуальными рисков юридическому лицу, индивидуальному предпринимателю, связанных с хозяйственной деятельностью
3.	t_2	Признание актуальными рисков, приводящих к ущербу государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности
4.	t_3	Селекция возможных негативных последствий от реализации УБИ
5.	t_4	Определение множества актуальных нарушителей
6.	t_5	Определение соответствующих категорий и уровней возможностей актуальных нарушителей
7.	t_6	Определение актуальных способов реализации угроз
8.	t_7	Определение множества возможных УБИ
9.	t_8	Определение наличия возможных сценариев реализации УБИ
10.	t_9	Принятие решения об актуальности УБИ

Определим разработанную сеть как $\langle P, T, I, O, \mu_0 \rangle$ и рассмотрим ее статические свойства:

1. Конечное множество позиций:

$P = \{RI_1, RI_2, RI_3, RI_5, TI, OI, NC, TA, TGA, OA, AIO, AA, LAC, CA, AA_s, WIT, PT, TAC, TEC, SC, CT\}$.

2. Конечное множество переходов:

$T = \{t_0, t_1, t_2, t_3, t_4, t_5, t_6, t_7, t_8, t_9\}$.

3. Множество входных позиций перехода:

$I = \{I(t_0), I(t_1), I(t_2), I(t_3), I(t_4), I(t_5), I(t_6), I(t_7), I(t_8), I(t_9)\}$.

$I(t_0) = \{RI_1, NC\}$, $I(t_1) = \{RI_2, NC\}$, $I(t_2) = \{RI_3, NC\}$, $I(t_3) = \{TI, OI\}$, $I(t_4) = \{TA, TGA, RI_5\}$, $I(t_5) = \{OA, AIO, AA, OI\}$, $I(t_6) = \{AA, LAC, CA\}$, $I(t_7) = \{OI, WIT, TAC, TEC, AA_s\}$, $I(t_8) = \{NC, OI, WIT, AA_s\}$, $I(t_9) = \{SC, PT\}$.

4. Множество выходных позиций перехода:

$O = \{O(t_1), O(t_2), O(t_3), O(t_4), O(t_5), O(t_6), O(t_7), O(t_8), O(t_9)\}$.

$O(t_0) = \{RI_5\}$, $O(t_1) = \{RI_5\}$, $O(t_2) = \{RI_5\}$, $O(t_3) = \{TI, OI, NC\}$, $O(t_4) = \{AA\}$, $O(t_5) = \{WIT\}$, $O(t_6) = \{AA_s\}$, $O(t_7) = \{SC\}$, $O(t_8) = \{PT\}$, $O(t_9) = \{CT\}$.

5. Начальная маркировка:

$\mu_0 = \{1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0\}$.

Одним из методов анализа сети Петри является построение его дерева достижимости, представляющего множество всех достижимых маркировок сети (вершины дерева), а также всех допустимых последовательностей её переходов (дуги дерева) [13]. На рисунке 2 представлено дерево достижимости описанной выше сети Петри.

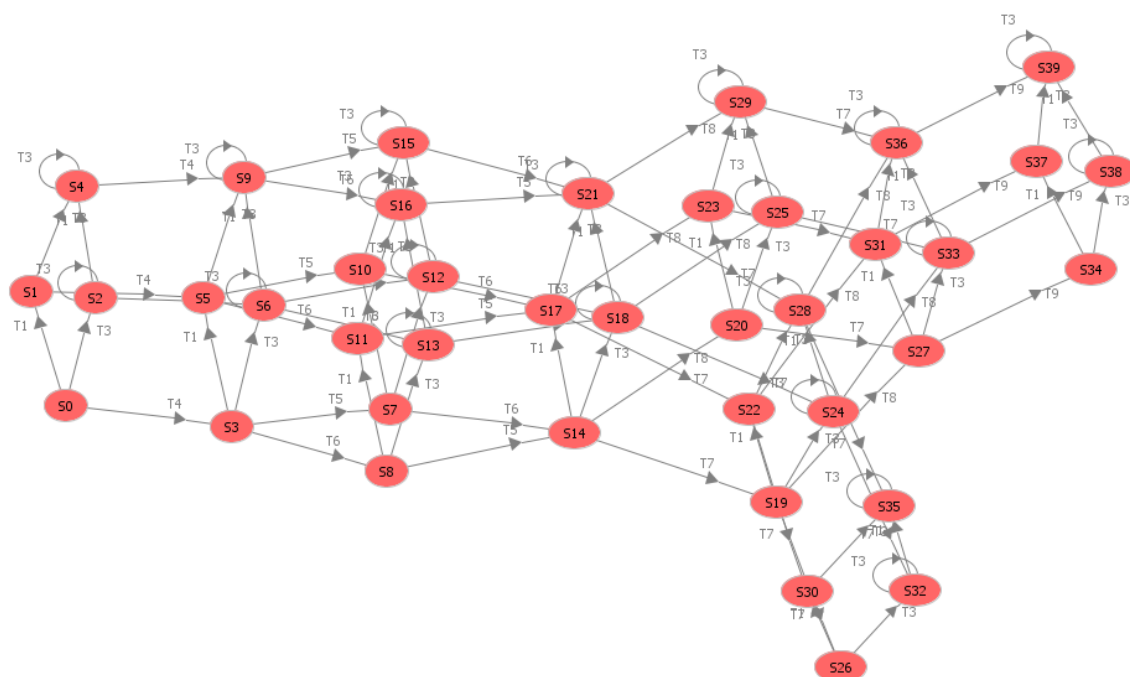


Рис. 2. Дерево достижимости сети Петри, моделирующей процесс определения актуальности УБИ

В таблице 4 перечислены маркировки, соответствующие вершинам S0-S39 дерева достижимости.

Таблица 4

Описание маркировок, соответствующих вершинам дерева достижимости

	RI_1	RI_2	RI_3	RI_s	TI	OI	NC	TA	TGA	OA	AIO	AA	LAC	CA	AA_s	WIT	PT	TAC	TEC	SC	CT
S0	0	1	0	2	1	ω	ω	1	1	1	1	0	1	1	0	0	0	1	1	0	0
S1	0	0	0	3	1	ω	ω	1	1	1	1	0	1	1	0	0	0	1	1	0	0
S2	0	1	0	2	1	ω	ω	1	1	1	1	0	1	1	0	0	0	1	1	0	0
S3	0	1	0	1	1	ω	ω	0	0	1	1	2	1	1	0	0	0	1	1	0	0
S4	0	0	0	3	1	ω	ω	1	1	1	1	0	1	1	0	0	0	1	1	0	0
S5	0	0	0	2	1	ω	ω	0	0	1	1	2	1	1	0	0	0	1	1	0	0
S6	0	1	0	1	1	ω	ω	0	0	1	1	2	1	1	0	0	0	1	1	0	0
S7	0	1	0	1	1	ω	ω	0	0	1	1	1	0	0	2	0	0	1	1	0	0
S8	0	1	0	1	1	ω	ω	0	0	0	0	1	1	1	0	2	0	1	1	0	0
S9	0	0	0	2	1	ω	ω	0	0	1	1	2	1	1	0	0	0	1	1	0	0
S10	0	0	0	2	1	ω	ω	0	0	1	1	1	0	0	2	0	0	1	1	0	0
S11	0	0	0	2	1	ω	ω	0	0	0	0	1	1	1	0	2	0	1	1	0	0
S12	0	1	0	1	1	ω	ω	0	0	1	1	1	0	0	2	0	0	1	1	0	0
S13	0	1	0	1	1	ω	ω	0	0	0	0	1	1	1	0	2	0	1	1	0	0
S14	0	1	0	1	1	ω	ω	0	0	0	0	0	0	0	2	2	0	1	1	0	0
S15	0	0	0	2	1	ω	ω	0	0	1	1	1	0	0	2	0	0	1	1	0	0
S16	0	0	0	2	1	ω	ω	0	0	0	0	1	1	1	0	2	0	1	1	0	0
S17	0	0	0	2	1	ω	ω	0	0	0	0	0	0	0	2	2	0	1	1	0	0
S18	0	1	0	1	1	ω	ω	0	0	0	0	0	0	0	2	2	0	1	1	0	0

	RI_1	RI_2	RI_3	RI_5	TI	OI	NC	TA	TGA	OA	AIO	AA	LAC	CA	AA_s	WT	PT	TAC	TEC	SC	CT
S19	0	1	0	1	1	ω	ω	0	0	0	0	0	0	0	1	1	1	1	1	0	0
S20	0	1	0	1	1	ω	ω	0	0	0	0	0	0	0	1	1	0	0	0	1	0
S21	0	0	0	2	1	ω	ω	0	0	0	0	0	0	0	2	2	0	1	1	0	0
S22	0	0	0	2	1	ω	ω	0	0	0	0	0	0	0	1	1	1	1	1	0	0
S23	0	0	0	2	1	ω	ω	0	0	0	0	0	0	0	1	1	0	0	0	1	0
S24	0	1	0	1	1	ω	ω	0	0	0	0	0	0	0	1	1	1	1	1	0	0
S25	0	1	0	1	1	ω	ω	0	0	0	0	0	0	0	1	1	0	0	0	1	0
S26	0	1	0	1	1	ω	ω	0	0	0	0	0	0	0	0	0	2	1	1	0	0
S27	0	1	0	1	1	ω	ω	0	0	0	0	0	0	0	0	0	1	0	0	1	0
S28	0	0	0	2	1	ω	ω	0	0	0	0	0	0	0	1	1	1	1	1	0	0
S29	0	0	0	2	1	ω	ω	0	0	0	0	0	0	0	1	1	0	0	0	1	0
S30	0	0	0	2	1	ω	ω	0	0	0	0	0	0	0	0	0	2	1	1	0	0
S31	0	0	0	2	1	ω	ω	0	0	0	0	0	0	0	0	0	1	0	0	1	0
S32	0	1	0	1	1	ω	ω	0	0	0	0	0	0	0	0	0	2	1	1	0	0
S33	0	1	0	1	1	ω	ω	0	0	0	0	0	0	0	0	0	1	0	0	1	0
S34	0	1	0	1	1	ω	ω	0	0	0	0	0	0	0	0	0	0	0	0	0	1
S35	0	0	0	2	1	ω	ω	0	0	0	0	0	0	0	0	0	2	1	1	0	0
S36	0	0	0	2	1	ω	ω	0	0	0	0	0	0	0	0	0	1	0	0	1	0
S37	0	0	0	2	1	ω	ω	0	0	0	0	0	0	0	0	0	0	0	0	0	1
S38	0	1	0	1	1	ω	ω	0	0	0	0	0	0	0	0	0	0	0	0	0	1
S39	0	0	0	2	1	ω	ω	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Используем построенное дерево достижимости для изучения динамических свойств сети Петри, таких как достижимость, ограниченность, активность, достижимость тупиковой разметки [16].

Проанализировав поведенческие свойства модели, можно сделать выводы о том, что сеть является:

- достижимой (заданная маркировка принадлежит множеству маркировок, достижимых в сети, при этом существует последовательность запусков, приводящих к заданной маркировке);
- неограниченной (количество меток в позициях OI и NC потенциально не ограничено);
- активной в течение одного цикла ее работы (независимо от достигнутой маркировки для любого перехода существует последовательность дальнейших запусков, приводящая к его запуску);
- тупиковой (маркировки S34, S37, S38, S39 являются тупиком).

Для того чтобы процесс определения актуальных угроз был циклическим, должна быть выполнена процедура репозиции, для чего необходимо добавить переход t_{10} , соединяющий входную позицию CT с позициями RI_1 , RI_2 , RI_3 , TA , TGA , OA , AIO , LAC , CA , TAC , TEC .

Таким образом, цель построения данной сети Петри состоит в том, чтобы представить совокупность условий, необходимых для успешного определения актуальности УБИ. Если эти условия существуют, то можно говорить о том, что УБИ актуальна. Достижение тупиковой разметки сети должно интерпретироваться как завершение работы алгоритма.

Заключение. Вербальное описание угроз, представленное в Банке данных угроз ФСТЭК России, в силу его слабой структурированности значительно усложняет процесс их оценки и анализа в рамках разработки Модели угроз, а также автоматизацию данного

процесса. Для формализации данной задачи предложена теоретико-множественная модель, описывающая процедуру определения актуальных угроз согласно новой Методике ФСТЭК России. Для аналитического моделирования оценки угроз безопасности информации выбран аппарат сетей Петри. В результате анализа поведенческих свойств модели выявлено, что построенная сеть Петри является достижимой, неограниченной, активной в течение одного цикла ее работы и достигающей тупиковой разметки в конце данного цикла, что свидетельствует о завершении алгоритма определения актуальности угрозы. Результатом одной итерации (цикла) полученной сети Петри является признание угрозы актуальной либо неактуальной для рассматриваемой системы.

Проведенное моделирование показало, что разработанная модель с использованием сети Петри адекватно отражает процессы, рассмотренные в Методике, и впоследствии позволяет перейти к автоматизации процесса моделирования и оценки угроз безопасности информации.

ЛИТЕРАТУРА

1. Михайлова Е. В. Эволюция нормативной базы моделирования угроз безопасности информации // Мавлютовские чтения : материалы XVI Всероссийской молодежной научной конференции : в 6 т. Уфа, 25—27 октября 2022 года. Т. 5. — Уфа : Уфимский государственный авиационный технический университет, 2022. — С. 615—621.
2. Суханов И. Д., Рыбкина О. В. Новые подходы к моделированию угроз безопасности информации // Научно-техническое и экономическое сотрудничество стран АТР в XXI веке. — 2021. — Т. 1. — С. 277—282.
3. Методика оценки угроз безопасности информации : методический документ : утвержден ФСТЭК России 5 февраля 2021 года // Официальный сайт Федеральной службы по техническому и экспортному контролю. — URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/> (дата обращения: 10.03.2024).
4. Карелова О. Л., Алюшина Е. Р. Сравнительный анализ методов моделирования угроз информационной безопасности // Современная наука: актуальные проблемы теории и практики. Серия : Естественные и технические науки. — 2023. — № 8. — С. 55—58.
5. Кузьмин И. Е. Проблема значимости согласованности мнений экспертов рабочей группы при моделировании угроз безопасности информации // Известия Тульского государственного университета. Технические науки. — 2021. — № 3. — С. 254—260.
6. Тихомирова А. А., Яковлев А. В., Алексеев В. В. Формальное описание моделирования угроз безопасности информации по методике ФСТЭК // Вестник Воронежского института МВД России. — 2023. — № 2. — С. 94—100.
7. Антонов Р. А., Карачанская Е. В. Проблемы построения модели оценки угроз безопасности информации и пути их решения // Евразийское Научное Объединение. — 2020. — № 6-2(64). — С. 80—83.
8. Сорокина А. Е. Сравнительный анализ методов моделирования угроз информационной системы // Информационные технологии в науке, бизнесе и образовании. Проблемы обеспечения цифрового суверенитета государства : материалы XIII Международной научно-практической конференции студентов, аспирантов и молодых ученых, Москва, 26 ноября 2021 года / под общ. ред. А. М. Прохорова, А. В. Царегородцева. — М. : Московский государственный лингвистический университет, 2022. — С. 92—97.

9. Гарате Гонзалес В. Применение сетей Петри, цепей Маркова и теории массового обслуживания при математическом моделировании дискретных систем // Информатика, вычислительная техника и управление. Известия СПбГЭТУ «ЛЭТИ». — 2019. — № 4.

10. Карманов А. Г. Моделирование угроз информационной безопасности с использованием ориентированных графов // Информация и космос. — 2010. — № 1. — С. 172—175.

11. Язов Ю. К., Соловьев С. В. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа. — СПб : Научные технологии, 2023. — 258 с.

12. Системный подход к построению программно-аппаратного комплекса для подготовки специалистов по информационной безопасности / В. В. Алексеев, В. А. Гриднев, А. В. Яковлев [и др.] // Вестник Тамбовского государственного технического университета. — 2021. — Т. 27. — № 1. — С. 20—30.

13. Котов В. Е. Сети Петри — М. : Наука. Главная редакция физико-математической литературы, 1984. — 160 с.

14. Питерсон Дж. Теория сетей Петри и моделирование систем : пер. с англ. — М. : Мир, 1984. — 264 с.

15. Knuth D.E. Semantics of context-free languages. — MST2, 1968.

16. Мараховский В. Б., Розенблюм Л. Я., Яковлев А. В. Моделирование параллельных процессов. Сети Петри. — СПб. : Профессиональная литература, 2014. — 400 с.

REFERENCES

1. Mixajlova E. V. E`volyuciya normativnoj bazy` modelirovaniya ugroz bezopasnosti informacii // Mavlyutovskie chteniya : materialy` XVI Vserossijskoj molodezhnoj nauchnoj konferencii : v 6 t. Ufa, 25—27 oktyabrya 2022 goda. T. 5. — Ufa : Ufimskij gosudarstvenny`j aviacionny`j texniceskij universitet, 2022. — S. 615—621.

2. Suxanov I. D., Ry`bkina O. V. Novy`e podxody` k modelirovaniyu ugroz bezopasnosti informacii // Nauchno-texniceskoe i e`konomiceskoe sotrudnichestvo stran ATR v XXI veke. — 2021. — T. 1. — S. 277—282.

3. Metodika ocenki ugroz bezopasnosti informacii : metodiceskij document : utverzhden FSTE`K Rossii 5 fevralya 2021 goda // Oficial`ny`j sayt Federal`noj sluzhby` po texniceskomu i e`ksportnomu kontrolyu. — URL: <https://fstec.ru/tekhniceskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/> (data obrashheniya: 10.03.2024).

4. Karelova O. L., Alyushina E. R. Sravnitel`ny`j analiz metodov modelirovaniya ugroz informacionnoj bezopasnosti // Sovremennaya nauka: aktual`ny`e problemy` teorii i praktiki. Seriya : Estestvenny`e i texniceskie nauki. — 2023. — № 8. — S. 55—58.

5. Kuz`min I. E. Problema znachimosti soglasovannosti mnenij e`kspertov rabochej gruppy` pri modelirovanii ugroz bezopasnosti informacii // Izvestiya Tul`skogo gosudarstvennogo universiteta. Texniceskie nauki. — 2021. — № 3. — S. 254—260.

6. Tixomirova A. A., Yakovlev A. V., Alekseev V. V. Formal`noe opisanie modelirovaniya ugroz bezopasnosti informacii po metodike FSTE`K // Vestnik Voronezhskogo instituta MVD Rossii. — 2023. — № 2. — S. 94—100.

7. Antonov R. A., Karachanskaya E. V. Problemy` postroeniya modeli ocenki ugroz bezopasnosti informacii i puti ix resheniya // Evrazijskoe Nauchnoe Ob`edinenie. — 2020. — № 6-2(64). — S. 80—83.

8. Sorokina A. E. Sravnitel'nyj analiz metodov modelirovaniya ugroz informacionnoj sistemy // Informacionny'e tehnologii v nauke, biznese i obrazovanii. Problemy obespecheniya cifrovogo suvereniteta gosudarstva : materialy XIII Mezhdunarodnoj nauchno-prakticheskoy konferencii studentov, aspirantov i molodyx uchenykh, Moskva, 26 noyabrya 2021 goda / pod obshh. red. A. M. Proxorova, A. V. Czaregorodceva. — M. : Moskovskij gosudarstvennyj lingvisticheskij universitet, 2022. — S. 92—97.
9. Garate Gonzales V. Primenenie setej Petri, cepej Markova i teorii massovogo obsluzhivaniya pri matematicheskom modelirovanii diskretnyx sistem // Informatika, vychislitel'naya texnika i upravlenie. Izvestiya SPbGE`TU «LE`TI». — 2019. — № 4.
10. Karmanov A. G. Modelirovanie ugroz informacionnoj bezopasnosti s ispol'zovaniem orientirovannyx grafov // Informaciya i kosmos. — 2010. — № 1. — S. 172—175.
11. Yazov Yu. K., Solov'ev S. V. Metodologiya ocenki effektivnosti zashhity informacii v informacionnyx sistemax ot nesankcionirovannogo dostupa. — SPb : Naukoemkie tehnologii, 2023. — 258 s.
12. Sistemnyj podxod k postroeniyu programmno-apparatnogo kompleksa dlya podgotovki specialistov po informacionnoj bezopasnosti/ V. V. Alekseev, V. A. Gridnev, A. V. Yakovlev [i dr.] // Vestnik Tambovskogo gosudarstvennogo texnicheskogo universiteta. — 2021. — T. 27. — № 1. — S. 20—30.
13. Kotov V. E. Seti Petri — M. : Nauka. Glavnaya redakciya fiziko-matematicheskoy literatury, 1984. — 160 s.
14. Piterson Dzh. Teoriya setej Petri i modelirovanie sistem : per. s angl. — M. : Mir, 1984. — 264 s.
15. Knuth D.E. Semantics of context-free languages. — MST2, 1968.
16. Maraxovskij V. B., Rozenblyum L. Ya., Yakovlev A. V. Modelirovanie paralelnyx processov. Seti Petri. — SPb. : Professional'naya literatura, 2014. — 400 s.

СВЕДЕНИЯ ОБ АВТОРАХ

Тихомирова Алина Александровна. Аспирант кафедры «Информационные системы и защита информации».

Тамбовский государственный технический университет.

E-mail: tihomirowaalina@yandex.ru

Россия, 392000, Тамбов, ул. Советская, 106/5.

Фурсова Арина Викторовна. Аспирант кафедры «Информационные системы и защита информации».

Тамбовский государственный технический университет.

E-mail: fursova_arina@inbox.ru

Россия, 392000, г. Тамбов, ул. Советская, 106/5.

Яковлев Алексей Вячеславович. Доцент кафедры информационных систем и защиты информации. Кандидат технических наук, доцент.

Тамбовский государственный технический университет.

E-mail: yava73@bk.ru

Россия, 392000, Тамбов, ул. Советская, 106/5.

Tikhomirova Alina Alexandrovna. Post-graduate student of the chair of Information Systems and Information Security.

Tambov State Technical University.

E-mail: tihomirowaalina@yandex.ru

Work address: Russia, 392000, Tambov, Sovetskaya Str., 106/5.

Fursova Arina Victorovna. Post-graduate student of the chair of Information Systems and Information Security.

Tambov State Technical University.

E-mail: fursova_arina@inbox.ru

Work address: Russia, 392000, Tambov, Sovetskaya Str., 106/5.

Yakovlev Alexey Vyacheslavovich. Assistant Professor of the chair of Information Systems and Information Security. Candidate of Technical Sciences, Assistant Professor.

Tambov State Technical University.

E-mail: yava73@bk.ru

Work address: Russia, 392000, Tambov, Sovetskaya Str., 106/5.

Ключевые слова: угрозы безопасности информации; моделирование угроз; актуальность угроз; методика оценки угроз; формальное описание; сети Петри.

Key words: information security threats; threat modeling; threat relevance; threat assessment methodology; formal description; Petri nets.

УДК 004.056.5

А. А. Жирнов, адъюнкт

**МОДЕЛЬ ФОРМИРОВАНИЯ ГРАФИКА
УЧАСТИЯ ПОДРАЗДЕЛЕНИЙ В ПРОЕКТЕ
ПРОТИВОДЕЙСТВИЯ КРИМИНАЛЬНЫМ УГРОЗАМ
ПРОФИЛАКТИЧЕСКОГО ТИПА:
СКАЛЯРНАЯ ОПТИМИЗАЦИЯ**

**A MODEL FOR FORMING A SCHEDULE
FOR THE PARTICIPATION OF UNITS IN A PROJECT
TO COUNTERACT CRIMINAL THREATS
OF A PREVENTIVE TYPE: SCALAR OPTIMIZATION**

В статье предлагается оптимизационная модель, позволяющая на основе заданных критериев и ограничений сформировать график участия различных подразделений органов внутренних дел в проекте противодействия криминальным угрозам профилактического типа. В данном графике отражено количество исполнителей от определенного подразделения, которое должно включаться в состав команды проекта на определенном сегменте разработанного ранее расписания проекта. В модели при формировании графика минимизируются критерии: разница в нагрузке между подразделениями; общее число исполнителей, включенных в состав команды проекта за весь период его реализации. В качестве метода многокритериальной оптимизации выбран метод скалярной оптимизации, с формированием скалярного критерия методом аддитивной свертки. Сравнение нагрузки между подразделениями производится по коэффициенту вариации нагрузки. Приведен пример постановки задачи в практической деятельности и вычислительный пример ее решения. Автором указано дальнейшее направление исследования, предполагающее разработку и сравнительный анализ альтернативных моделей, с использованием других методов многокритериальной оптимизации, для решения задачи, рассмотренной в статье.

The paper proposes an optimization model that allows, based on the specified parameters and constraints, to form a schedule for the participation of various departments of the internal affairs bodies in the project of countering criminal threats of a preventive type. This schedule shows the number of performers from a specific department that should be included in the project team for a specific segment of the project schedule. In the model, when forming a schedule, the criteria are minimized: the difference in workload between departments; the total number of performers included in the project team for the entire period of its implementation. The method of scalar optimization, with the formation of a scalar criterion by the method of additive convolution, is chosen as the method of multi-criteria optimization. The uniformity of load distribution between divisions is estimated by the coefficient of load variation. An example of setting a problem in practice and a computational example of its solution is given. The author indicates a further direction of research involving the development and comparative analysis of alternative models using other multicriteria optimization methods to solve the problem discussed in the article.

Введение. Одним из возможных направлений повышения эффективности деятельности крупных организационных систем является внедрение методов и моделей проектного управления. Перспективы и особенности реализации проектного управления в деятельности правоохранительных органов рассматривались в работах И. В. Горошко [1], В. Д. Кондратьева [2] и других.

В рамках разрабатываемой нами методологии управления проектами в сфере противодействия криминальным угрозам ранее была предложена модель разработки расписания проекта противодействия криминальным угрозам профилактического типа [3] (далее — проекта).

Проект данного типа, предполагает реализацию серий однотипных профилактических мероприятий (далее — работ проекта) подразделениями уголовного розыска и другими смежными подразделениями органов внутренних дел (далее — подразделениями).

Проект реализуется в рамках временных и ресурсных ограничений. То есть заданы его фиксированная продолжительность и требуемое для его осуществления количество ресурсов возобновляемого и невозобновляемого типа, где под первыми понимаются такие ресурсы, которые после использования в одних работах можно использовать в последующих, а под вторыми такие, количество (запас) которых в работах уменьшается по мере их использования. Трудовые ресурсы (исполнители, члены команды проекта) рассматриваются как отдельный подкласс возобновляемых ресурсов, так как при соблюдении режима труда и отдыха исполнителей проекта можно планировать к назначению на последующие работы [3].

При большой запланированной продолжительности проекта (например, от двух месяцев и более) и при условии, что характер работ проекта, будет исключать возможность совмещать исполнителям деятельность в проекте с оперативно-служебной деятельностью вне проекта (то есть выполнять задачи, не связанных с проектной деятельностью, в подразделении по месту службы исполнителей) актуализируется проблема, связанная длительным отрывом сотрудников подразделения от их основных обязанностей. Данная проблема может быть решена временным включением в состав команды проекта сотрудников из нескольких подразделений. В этом случае возникают задачи минимизации разницы в количестве сотрудников, включаемых в состав команды проекта от подразделений (распределения равной нагрузки на все подразделения), и минимизации времени отрыва исполнителей всех подразделений от их основной деятельности, то есть минимизации общего количества исполнителей, временно включаемых в состав команды проекта, при условии включения в состав команды проекта достаточного для выполнения работ числа исполнителей.

Решение данной задачи методом ручного заполнения табличной формы в целом и трудоемко (особенно при большой размерности задачи), и неэффективно, так как за приемлемое время затруднительно сформировать такой график участия подразделений в проекте (далее — график), в котором бы эти условия оптимальности и ограничение выполнялись.

В то же время сформировать допустимый график, удовлетворяющий заданным условиям и ограничению, можно, используя математический аппарат, методы математического моделирования и исследования операций.

Целью исследования являлась разработка модели формирования графика участия подразделений в проекте противодействия криминальным угрозам профилактического типа с формированием скалярного критерия оптимальности методом аддитивной свертки.

Методы и допущения. В связи с тем что для построения графика требуется минимизировать и разницу в нагрузке между подразделениями, и общее число исполнителей, требуется применение одного из методов многокритериальной оптимизации (далее — МКО).

В этом качестве в модели при получении оптимального решения по данным критериям используется метод аддитивной свертки с формированием скалярного критерия LSK по формуле (1), по классификации [4] относящийся к методам «поиска решения без участия лица, принимающего решения»:

$$LSK = \sum_{s=1}^{CHK} w_s \times f_s(x), \quad (1)$$

где CHK — число критериев оптимизации, $CHK > 1$;

$f_s(x)$ — целевая функция от x по s критерию, $s = \overline{1, CHK}$;

w_s — вес целевой функции по s критерию, $w_s > 0$, $\sum_{s=1}^{CHK} w_s = 1$.

Выбор метода аддитивной свертки для формирования скалярного критерия в большей степени обусловлен относительной простотой его реализации, в то же время оснований считать его наилучшим для решения поставленной в статье задачи по сравнению с другими возможными МКО пока не имеется.

При применении метода аддитивной свертки, чтобы изначально, до определения весов w_s , критерии имели равный вес в скалярном критерии, необходимо привести их к единой шкале (масштабу).

В модели, предложенной в статье, приведение критериев к единой шкале осуществляется по формуле (2):

$$value' = a + \frac{(value - \min(value)) \times (b - a)}{\max(value) - \min(value)}, \quad (2)$$

где $value'$ — величина $value$, приведенная к шкале от a до b ;

$\max(value)$ и $\min(value)$ — максимальное и минимальное значения, принимаемые величиной $value$.

Оценка равномерности распределения нагрузки между подразделениями (далее — равномерности нагрузки) производится вычислением отношения среднеквадратичного отклонения нагрузки (σ) к среднему значению нагрузки (μ), то есть по величине коэффициента вариации нагрузки (CV), по формуле (3):

$$CV = \frac{\sigma}{\mu}. \quad (3)$$

Коэффициент вариации нагрузки является безразмерным показателем, его увеличение указывает на увеличение разницы в нагрузке между подразделениями. При абсолютно равной нагрузке $CV = 0$.

Математическая модель. Для постановки задачи определим переменные:

$x_{i,j}$ — элемент матрицы $X = [x_{i,j}]_{SG \times PDR}$, принимающий значения согласно (4), указывающий на включение исполнителей j -го подразделения в состав команды проекта на i -м сегменте расписания проекта, где SG — число равных по продолжительности сегментов расписания, $i = \overline{1, SG}$, PDR — число подразделений, $j = \overline{1, PDR}$:

$$x_{i,j} = \begin{cases} 1, & \text{если исполнители } j\text{-го подразделения включены в состав команды} \\ & \text{проекта на } i\text{-м сегменте расписания проекта} \\ 0 & \text{в остальных случаях} \end{cases}; \quad (4)$$

ks_j — численность j -го подразделения, $ks_j \in \mathbb{Z}^+$;

trb_i — число исполнителей, требуемое для выполнения работ на i -м сегменте расписания проекта, $trb_i \in \mathbb{Z}^+$.

В модели принято, что число сотрудников подразделения, которое может быть включено в состав команды проекта в определенном сегменте расписания, фиксировано и задается параметром: $perc$ — общий для всех подразделений процент сотрудников от численности подразделения, включаемый в состав команды проекта в определенный сегмент расписания.

При этом каждое подразделение может подать сведения о том, в каком сегменте расписания подразделение не сможет обеспечить ресурсную поддержку проекта (например, в сегментах, приходящихся на периоды, когда треть сотрудников будет в отпусках, а оставшиеся сотрудники будут выполнять другие задачи подразделения).

$ses_{i,j}$ — элемент матрицы $SES = [ses_{i,j}]_{SG \times PDR}$, отражающий количество исполнителей j -го подразделения, которое может быть включено в состав команды проекта на i -м сегменте расписания проекта, принимающий значения согласно (5):

$$ses_{i,j} = \begin{cases} \left\lfloor \left(\frac{ks_j}{100} \times perc \right) \right\rfloor, & \text{в общем случае} \\ 0, & \text{если в } i\text{-м сегменте расписания } j\text{-е подразделение} \\ & \text{не может обеспечить ресурсную поддержку проекта.} \end{cases} \quad (5)$$

on_j — параметр, характеризующий нагрузку j -го подразделения как отношение количества исполнителей j -го подразделения, включенных в команду проекта за весь период реализации проекта, к численности j -го подразделения, по формуле (6):

$$on_j = \frac{\sum_{i=1}^{SG} (x_{i,j} \times ses_{i,j})}{ks_j}, \quad j = \overline{1, PDR}. \quad (6)$$

on^{CV} — коэффициент вариации нагрузки подразделений по показателю on_j , рассчитываемый по формуле (3).

naz_i — параметр, характеризующий суммарное количество исполнителей, включенных в команду проекта, от всех подразделений, для выполнения работ на i -м сегменте расписания проекта, вычисляемый по формуле (7):

$$naz_i = \sum_{j=1}^{PDR} (x_{i,j} \times ses_{i,j}), \quad i = \overline{1, SG}. \quad (7)$$

naz^{all} — параметр, характеризующий общее количество исполнителей, включенных в график проекта за весь период его реализации от всех подразделений ОВД, вычисляемый по формуле (8):

$$naz^{all} = \sum_{i=1}^{SG} naz_i. \quad (8)$$

onN^{CV} и $nazN^{all}$ — нормализованные, приведенные к шкале от 0 до 1, по формуле (2), где ($a = 0; b = 1$), параметры on^{CV} и naz^{all} , минимальные и максимальные значения которых можно получить с использованием описанной ниже модели, последовательно найдя минимальные и максимальные значения для целевых функций, отдельно по $on^{CV}(x_{i,j})$ и по $naz^{all}(x_{i,j})$.

Описанные переменные и параметры позволяют дать формальную постановку задачи и записать ее математическую модель в следующем виде:

Пусть для проекта ПКУ профилактического типа сформировано расписание работ, разбитое на SG равных по продолжительности сегментов, где для выполнения работ на каждом i -м сегменте требуется trb_i количество исполнителей. В проекте участвуют PDR подразделений с ks_j числом сотрудников в каждом j -м подразделении. От каждого j -го подразделения в команду проекта на каждом i -м сегменте расписания может быть включено $ses_{i,j}$ число исполнителей.

Требуется включить в команду проекта каждого i -го сегмента такое $ses_{i,j}$ количество исполнителей таких j -х подразделений, то есть определить такие значения переменных $x_{i,j}$ (1), при которых будет минимизировано значение скалярного критерия, вычисляемого по взвешенному произведению нормализованного коэффициента вариации нагрузки и нормализованного общего количества исполнителей, включенных в график проекта от всех подразделений (9), при условии что на каждом i -м сегменте в график проекта будет включено достаточное для выполнения работ количество исполнителей (10):

$$onN(x_{i,j})^{CV} \times w_{on^{CV}} + nazN(x_{i,j})^{all'} \times w_{naz^{all}} \rightarrow \min, i = \overline{1, SG}, j = \overline{1, PDR}; \quad (9)$$

$$naz_i \geq trb_i, \quad i = \overline{1, SG}, \quad (10)$$

где $w_{on^{CV}}$ и $w_{naz^{all}}$ — веса параметров on^{CV} и naz^{all} соответственно в скалярном критерии (10).

Задача будет иметь решение при выполнении условия (11):

$$\sum_{j=1}^{PDR} ses_{i,j} \geq trb_i, \quad i = \overline{1, SG}, \quad (11)$$

то есть когда суммарное количество исполнителей от всех подразделений, которое может быть включено в состав команды проекта на каждом из сегментов расписания проекта, превышает или равно требуемому количеству исполнителей в этих сегментах.

Вычислительный пример. Предположим, разработано расписание проекта ПКУ профилактического типа, продолжительность которого составляет один год. Это расписание разделено на 12 сегментов, по числу месяцев ($SG = 12$). Для каждого сегмента расписания определено число исполнителей, требуемое для выполнения работ в этом сегменте (месяце), trb_i (табл. 1).

Таблица 1

Количество исполнителей, требуемое для выполнения работ в i -м сегменте расписания

Месяц (i)	1	2	3	4	5	6	7	8	9	10	11	12
trb_i	8	8	8	7	5	9	8	7	10	8	8	8

Ресурсную поддержку проекта осуществляют 10 подразделений, исполнители которых могут быть включены в состав команды проекта на определенном сегменте его расписания ($PDR = 10$). Определено, что в состав команды проекта на определенном сегменте расписания от одного подразделения должна быть включена десятая часть от его фактической численности на начало года ($perc = 10\%$). Кроме того, от каждого подразделения поступили сведения о том, в какой месяц подразделение не сможет обеспечить ресурсную поддержку проекта. На основании поступивших данных по формуле (5) были рассчитаны данные, представленные в табл. 2.

Таблица 2

Количество исполнителей от подразделений, которое может быть включено в состав команды проекта на i -м сегменте расписания

Номер подр., № (j)	Факт. числ. подр., ks_j	Номер сегмента расписания (Месяц), (i)											
		1	2	3	4	5	6	7	8	9	10	11	12
1	33	3	3	3	3	0	3	3	3	3	3	3	3
2	33	2	2	2	2	2	0	2	2	2	2	2	2
3	26	2	2	2	2	2	2	0	2	2	2	2	2
4	26	3	3	3	3	3	3	3	0	3	3	3	3
5	22	2	2	2	2	2	2	2	2	0	2	2	2
6	22	3	3	3	3	3	3	3	3	0	3	3	3
7	22	2	2	2	2	2	2	2	0	2	2	2	2
8	11	2	2	2	2	2	2	0	2	2	2	2	2
9	11	2	2	2	2	2	0	2	2	2	2	2	2
10	11	2	2	2	2	0	2	2	2	2	2	2	2

Требуется сформировать график участия подразделений в проекте с минимизацией разницы в нагрузке (коэффициента вариации нагрузки) между подразделениями и общего количества исполнителей, включенных в график проекта от всех подразделений; с равными весами критериев ($w_{oncv} = w_{nazall} = 0,5$) в скалярном критерии.

С использованием табличного процессора MS Excel, надстройки «Поиск решения» (Excel Solver), метода «Эволюционный поиск решения», представляющего реализацию генетического алгоритма, за 4 минуты поиска нами было получено допустимое решение, позволившее сформировать график, представленный в табл. 3, где также представлены параметры, позволяющие оценить полученное решение.

Таблица 3

График участия подразделений в проекте

Номер подр., № (j)	Факт. числ. подр., ks_j	Номер сегмента расписания (Месяц), (i)												Кол-во исп. от подр.	Нагр. подр., on_j
		1	2	3	4	5	6	7	8	9	10	11	12		
1	33	0	3	0	0	0	3	3	0	3	0	0	3	15	0,45

2	33	0	3	0	0	0	0	0	3	3	3	3	0	15	0,45
3	26	2	0	2	2	2	0	0	0	2	2	0	0	12	0,46
4	26	0	0	0	2	2	2	2	0	0	0	2	2	12	0,46
5	22	2	0	2	0	0	2	2	0	0	2	0	0	10	0,45
6	22	0	0	0	0	0	2	2	2	0	0	2	2	10	0,45
7	22	2	0	2	2	0	0	0	0	2	0	0	2	10	0,45
8	11	0	1	1	0	1	0	0	1	0	0	0	1	5	0,45
9	11	1	0	1	1	0	0	1	1	0	0	0	0	5	0,45
10	11	1	1	0	0	0	0	0	0	0	1	1	1	5	0,45
naz_i		8	8	8	7	5	9	10	7	10	8	8	11		
trb_i		8	8	8	7	5	9	8	7	10	8	8	8		

При полученном решении, на основе которого сформирован представленный в табл. 3 график: величина коэффициента вариации нагрузки $on^{CV} = 0,006$, что характеризует крайне низкую изменчивость величин нагрузки подразделений относительно их среднего значения, то есть приблизительно равную нагрузку подразделений; общее количество исполнителей, включенных в график проекта за весь период его реализации от всех подразделений, $naz^{all} = 99$, превышающее требуемое количество ($\sum_{i=1}^{SG} trb_i = 94$) на 5 исполнителей (в 7 и 12 сегменте).

Обсуждение. Мы полагаем, что сформулированная задача, исходя из ее условий и ограничений, может рассматриваться как вариант обобщенной задачи о назначениях (англ. generalized assignment problem [5]), когда один исполнитель может быть назначен на несколько работ, а одну работу могут выполнять несколько исполнителей, которая, в свою очередь, является частным случаем транспортной задачи.

Для демонстрации общего подхода к формированию скалярного критерия в модели предлагается аддитивная свертка, как наиболее простая для реализации и интерпретации, но имеющая и ряд известных недостатков по сравнению с другими свертками. В связи с чем в дальнейшем модель может быть модифицирована за счет применения более совершенных механизмов формирования скалярного критерия, таких как: свертки на основе отклонения от идеальной точки; свертки Гермейера [6] и других.

В модели предусмотрено включение в состав команды проекта фиксированного количества исполнителей, по этой причине для выполнения работ в некоторых сегментах расписания в команду проекта будет включено несколько большее количество исполнителей (как в сегменте 7 и 12, в вычислительном примере), чем требуется для выполнения работ. В этом случае исполнителей, включенных сверх требуемого количества, следует рассматривать как резерв команды проекта. Поиск решения с количеством исполнителей, не превышающим требуемое в определенном сегменте, при переборе значений переменных от 0 до $ses_{i,j}$ доступных исполнителей потребовал бы многократно большее число вычислительных операций.

Отметим, что в модели для простоты ее описания предложено включение в состав команды проекта фиксированного и *равного в каждом* сегменте расписания количества исполнителей, кроме сегментов, в которых подразделение не может обеспечить ресурсную поддержку проекта, по формуле (5). На практике, если этого требуют обстоятельства, для каждого сегмента и каждого подразделения для включения в состав команды проекта может быть определена отличающаяся от *perc* часть подразделения.

Кроме того, в самой модели не конкретизировано, часть от какой, штатной или фактической, численности подразделения должна включаться в состав команды проекта. Мы полагаем, что этот вопрос должен решаться лицом, принимающим решения, на основе экспертной оценки различных сведений о функционировании подразделений (их укомплектованности, «текучести» кадров и других).

Отметим, путем замены формулы (5) на формулу (12) модель может быть масштабирована от распределения нагрузки между подразделениями к распределению нагрузки между отдельными должностными лицами:

$$ses'_{i,j} = \begin{cases} 1, & \text{в общем случае} \\ 0, & \text{если в } i\text{-м сегменте расписания } j\text{-й сотрудник} \\ & \text{не может принять участие в проекте} \end{cases} \quad (12)$$

В связи с чем мы полагаем, что рассмотренная модель может найти широкое применение в оперативно-служебной деятельности ОВД и вне контекста методологии проектного управления, для формирования всевозможных графиков мероприятий (например, участия в различных экспертных комиссиях, распределения командировок, формирования группы контроля исполнения поручений руководства и других), в которых необходимо минимизировать разницу в нагрузке между несколькими подразделениями (отделами, отделениями), или между отдельными должностными лицами.

Выводы. При заданных параметрах и ограничениях разработанная модель позволяет сформировать график участия подразделений в проекте противодействия криминальным угрозам профилактического типа с оптимизацией скалярного критерия, вычисляемого аддитивной сверткой взвешенного произведения нормализованного коэффициента вариации нагрузки и нормализованного общего количества исполнителей, включенных в график проекта от всех подразделений.

По нашему мнению, данная модель имеет широкое прикладное значение и при незначительной модификации может найти применение во множестве сфер деятельности и на различных уровнях управления ОВД.

Дальнейшее направление исследования предполагает разработку и сравнительный анализ альтернативных моделей на основе других МКО (например, лексикографического или уступок), позволяющих решить задачу по формированию графика с минимизацией разницы в нагрузке между подразделениями и общего числа исполнителей, включенных в состав команды проекта за весь период его реализации.

ЛИТЕРАТУРА

1. Горошко И. В. Цифровая трансформация и управление проектами. — М. : Университет прокуратуры Российской Федерации, 2021. — С. 23—32.
2. Кондратьев В. Д., Щепкин А. В. Проектное управление при реализации стратегии безопасности дорожного движения // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). — 2019. — № 4(59). — С. 112—119.
3. Жирнов А. А. Модель разработки расписания проекта противодействия криминальным угрозам профилактического типа // Моделирование, оптимизация и информационные технологии. — 2023. — Т. 11. — № 4 (43).
4. Лотов А. В., Поспелова И. И. Многокритериальные задачи принятия решений : учебное пособие. — М. : МАКС-ПРЕСС, 2008. — 197 с.

5. Martello S., Toth P. Generalized assignment problems // Algorithms and Computation Lecture Notes in Computer Science. — Berlin, Heidelberg : Springer, 1992. — С. 351—369.

6. Гермейер Ю. Б. Введение в теорию исследования операций. — М. : Наука, 1971. — 384 с.

REFERENCES

1. Goroshko I. V. Cifrovaya transformaciya i upravlenie proektami. — М. : Universitet prokuratury` Rossijskoj Federacii, 2021. — С. 23—32.

2. Kondrat`ev V. D., Shhepkin A. V. Proektnoe upravlenie pri realizacii strategii bezopasnosti dorozhnogo dvizheniya // Vestnik Moskovskogo avtomobil`nodorozhnogo gosudarstvennogo texnicheskogo universiteta (MADI). — 2019. — № 4(59). — С. 112—119.

3. Zhirnov A. A. Model` razrabotki raspisaniya proekta protivodejstviya kriminal`ny`m ugrozam profilakticheskogo tipa // Modelirovanie, optimizaciya i informacionny`e texnologii. — 2023. — Т. 11. — № 4 (43).

4. Lotov A. V., Pospelova I. I. Mnogokriterial`ny`e zadachi prinyatiya reshenij : uchebnoe posobie. — М. : MAKS-PRESS, 2008. — 197 s.

5. Martello S., Toth P. Generalized assignment problems // Algorithms and Computation Lecture Notes in Computer Science. — Berlin, Heidelberg : Springer, 1992. — С. 351—369.

6. Germejer Yu. B. Vvedenie v teoriyu issledovaniya operacij. — М. : Nauka, 1971. — 384 s.

СВЕДЕНИЯ ОБ АВТОРЕ

Жирнов Андрей Александрович. Адъюнкт.

Академия управления МВД России.

E-mail: AUMSKW@yandex.ru

Россия, 125171, Москва, ул. Зои и Александра Космодемьянских, 8.

Zhirnov Andrey Aleksandrovich. Post-graduate cadet.

Academy of Management of the Ministry of Internal Affairs of Russia.

E-mail: AUMSKW@yandex.ru

Work address: Russia, 125171, Moscow, Zoya and Alexander Kosmodemyanskikh Str., 8.

Ключевые слова: проект противодействия криминальным угрозам; проектный подход; скалярный критерий; график участия в проекте; распределение нагрузки.

Key words: project of countering criminal threats; project approach; scalar criterion; participation schedule; load distribution.

УДК 519.854

РАДИОТЕХНИКА И СВЯЗЬ

А. В. Володько, кандидат технических наук, доцент

Р. В. Кузьменко, доктор физико-математических наук, доцент

Н. А. Андреева, кандидат физико-математических наук, доцент

К ВОПРОСУ О РЕАЛИЗАЦИИ АМПЛИТУДНОГО МЕТОДА САМОНАВЕДЕНИЯ В СИСТЕМАХ ПЕРЕХВАТА БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ

ON THE QUESTION OF IMPLEMENTING THE AMPLITUDE SELF-GUIDANCE METHOD IN UNMANNED AIRCRAFT INTERCEPTION SYSTEMS

Обсуждаются вопросы построения системы обнаружения малозаметных беспилотных воздушных судов (БВС) с применением классических амплитудных методов радиолокации. Представлен комплекс наведения на БВС, состоящий из генератора подсветки цели и четырехканального приёмника отраженного от БВС сигнала подсветки. Использование штатных узлов и модулей спутникового телевидения Ku диапазона обеспечивает низкую стоимость комплекса и высокую эффективность работы. Предложенная система в дальнейшем может быть использована для наведения БВС-перехватчика на цель без задействования операторов (полностью автоматический режим работы, стационарное размещение на стенах охраняемого объекта) или с операторами (мобильный режим работы).

The issues of building a detection system for low-observable UAVs using classical amplitude radar methods are discussed. A UAV guidance system consisting of a target illumination generator and a four-channel receiver of the illumination signal reflected from the UAV is presented. The use of standard units and modules of Ku-band satellite television ensures low cost of the system and high efficiency of operation. The proposed system can be further used to guide an interceptor UAV to a target without involving operators (fully automatic operation mode, stationary placement on the walls of a protected facility) or with operators (mobile operation mode).

В связи с массовым применением портативных дистанционно управляемых или инерциальных беспилотных воздушных судов (БВС) с высоким уровнем защиты от обнаружения стандартными методами РЭБ благодаря использованному для их изготовления материалам, малым линейным размерам и низким высотам полета возникает задача разработки надежной технологии их обнаружения и подавления или поражения [1]. Данная задача играет важную роль для обеспечения безопасности на режимных объектах, поскольку с помощью БВС возможно и несанкционированное наблюдение за режимным объектом, осуществление терактов, переброс через оградительные сооружения запрещенных предметов, оружия, наркотиков.

При классическом подходе к решению поставленной выше задачи охраняемая территория должна быть «накрыта» постоянно активным полем радиолокационной станции

обнаружения целей, совмещенной со средствами подавления или поражения БВС. Однако имеющиеся разработки, как правило, обладают значительной стоимостью, превышающей сотни тысяч и даже миллионы рублей. Целью данной работы является разработка системы противодействия БВС с минимальными экономическими затратами. Система позволяет установить положение БВС в пространстве и на основе полученной информации осуществить наведение специализированного БВС-перехватчика, который, например, может подавить БВС путем выброса нитей или сети или поразить его при помощи иных методов. Концепция системы базируется на том, что с учетом большой подвижности цели ручное управление перехватчиком видится затруднительным, поэтому одной из первостепенных задач является разработка блока автоматического наведения БВС-перехватчика. При этом наведение на цель предлагается осуществлять на основе классического полуактивного метода как самого простого и технически легко реализуемого.

Амплитудный равносигнальный метод давно известен и широко применяется в системах автоматического наведения [2]. Сущность его заключается в следующем: цель подсвечивается внешним источником излучения (например, наземным локатором), выполняющим функцию целеуказания. Отраженный от цели сигнал принимает система автоматического наведения воздушного перехватчика. Автоматическое наведение основано на принципе сравнения амплитуд сигналов нескольких узконаправленных антенн (например, двух антенн — «1» и «2» на рис. 1), диаграммы направленности которых ориентированы с небольшим угловым смещением $\Theta_{см}$ относительно оси антенной системы. Принятые антеннами эхо-сигналы первого U_1 и второго U_2 каналов подаются на схему сравнения интенсивности эхо-сигналов, где вычисляется разность напряжения первого U_1 и второго каналов:

$$U_{\Delta} = U_1 - U_2.$$

Разностный сигнал поступает в схему управления силовым приводом устройства наведения воздушного перехватчика, который приводит систему в положение, когда разностный сигнал будет равен нулю. При этом пеленг БВС совпадет с антенной осью системы.

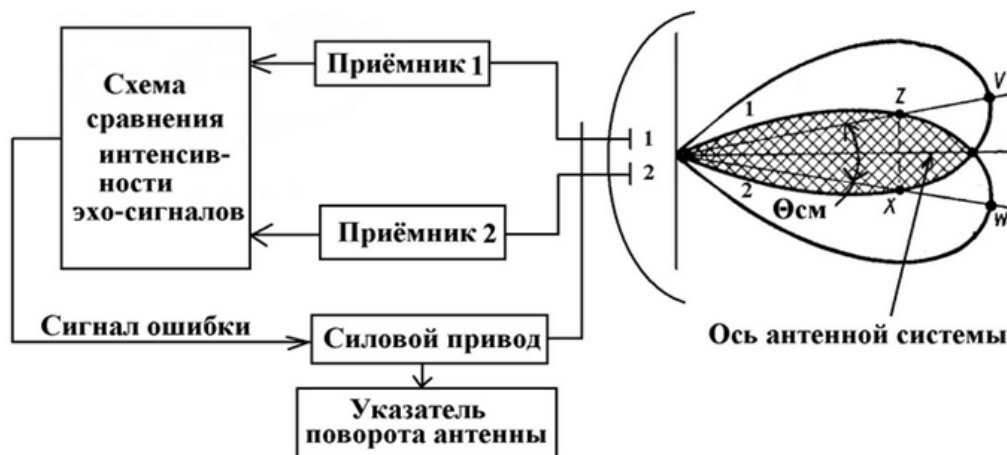


Рис. 1. Принцип амплитудного равносигнального автоматического наведения [2]

Предлагается следующий алгоритм работы системы: первоначально факт проникновения и приближения БВС к воздушному пространству охраняемой территории обнаруживается внешними средствами на дальних подступах при помощи стандартных методов обнаружения, позволяющих зафиксировать сам факт приближения. После получения сигнала о приближении БВС активируется система наведения. Система может иметь как стационарное, так и мобильное исполнение. В случае стационарного исполнения система должна быть размещена на внешней стене (например, на каждой внешней стене учреждения), а блоки системы должны будут осуществлять подсветку и отслеживание БВС в заданном секторе путем подачи управляющих сигналов на приводы, вращающиеся в горизонтальной и вертикальной плоскости. При этом наведение будет осуществляться полностью в автоматическом режиме. В случае мобильного исполнения управление системой осуществляется с помощью операторов, что позволяет сократить число необходимых экземпляров системы по сравнению со стационарным исполнением.

Пример использования системы с помощью двух операторов показан на рисунке 2. Один из них управляет ручным передатчиком СВЧ с целью обнаружения и подсветки цели, т. е. он сканирует воздушное пространство и обнаруживает сигнал, отраженный от БВС противника, и в ручном режиме удерживает луч излучателя СВЧ в направлении БВС, что реализует функции целеуказания и подсветки цели [3, 4].

Второй оператор осуществляет первоначальное наведение перехватчика на цель и активирует режим захвата цели, причем наведение на цель осуществляется автоматически за счет работы блока наведения. Подавление или поражение БВС может происходить различными методами [1], например выстрелом кевларовых нитей в винты БВС противника, сбросом сети или даже выстрелом заряда мелкой дроби. После проведенной атаки БВС-перехватчик возвращается к оператору.

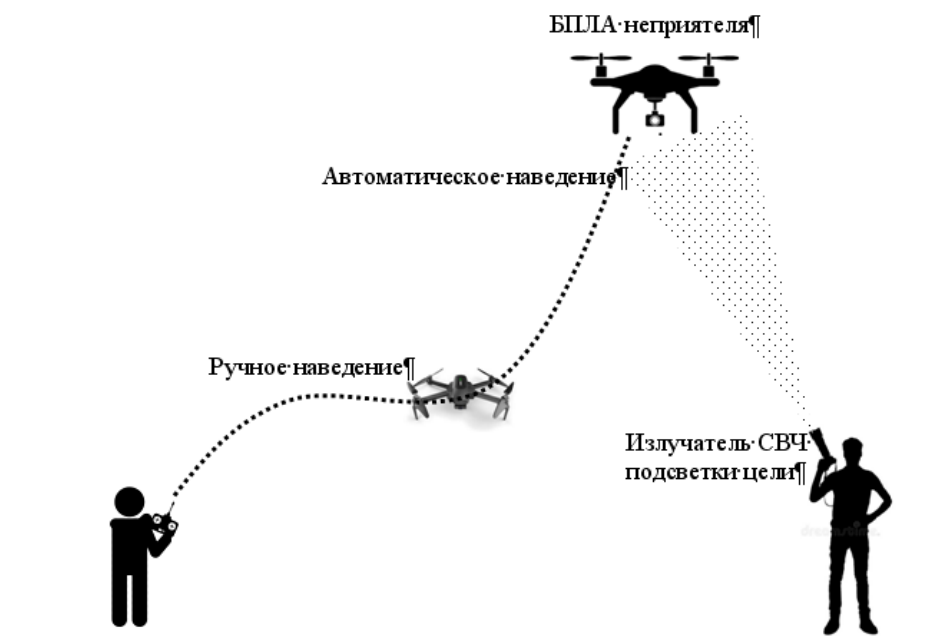


Рис. 2. Принцип наведения перехватчика на БВС неприятеля

С целью исследования возможности технической реализации подобной системы были осуществлены ее эскизная разработка и макетирование ее отдельных блоков.

В первую очередь выбор оптимального диапазона рабочих частот определялся требованиями точности определения положения цели в пространстве и доступностью комплекствующих. Кроме того, поскольку подсветка сигнала может осуществлять только в ограниченном секторе пространства, устройство подсветки также должно обладать приемным устройством для измерения величины отраженного сигнала подсветки с целью определения ее оптимальной ориентации. В качестве приемника отраженного от цели сигнала подсветки был использован спутниковый конвертер Gi-211 (рис. 3, а), сочетающий весьма низкую стоимость и хорошие технические параметры: частота принимаемого сигнала 10,7—12,7 ГГц, частота выходного сигнала 910—2150 МГц, усиление порядка 50 дБ и уровень собственных шумов 0,2 дБ. Металлический корпус конвертера выполнен в виде круглой рупорной антенны с диаграммой направленности главного лепестка порядка 60 градусов. Для измерения уровня принимаемого сигнала был использован модернизированный прибор для поиска спутников Satellite Finder GSF9504 (рис. 3, б). Аналоговый стрелочный индикатор позволяет оценить уровень сигнала, для ручной регулировки чувствительности установлен регулятор усиления. Звуковой зуммер облегчает наведение приемной антенны на источник излучения. Цифровая обработка выполнена на контроллере Arduino Uno. Изменения величины принимаемого сигнала в случае автоматического режима работы могут передаваться в аналитический блок, управляющий приводом вращающегося устройства с целью изменения направления подсветки по горизонтали и вертикали.



Рис. 3. Примененные в блоке подсветки приборы:
а) конвертор Gi-211;
б) прибор измерения уровня сигнала GSF9504

На рисунке 4 представлена структурная схема излучателя СВЧ подсветки в диапазоне 10—12 ГГц. Генератор СВЧ реализован на диоде Ганна AA703A по классической схеме с объёмным резонатором в виде отрезка прямоугольного волновода. Частота генерации регулируется положением подвижного поршня резонатора. Предусмотрена ручная установка тока генераторного диода с цифровой индикацией текущего значения тока и напряжения. Генератор нагружен на рупорную антенну оптимальной формы. Ширина основного лепестка диаграммы направленности около 30 градусов. Для повышения качества работы излучатель был оборудован дополнительным приемником со звуковым контролем уровня отраженного сигнала, позволяющим оператору «на слух» наводить излучатель на цель, не обращаясь к показаниям приборов.

Общий вид блока СВЧ подсветки цели представлен на рисунке 5.

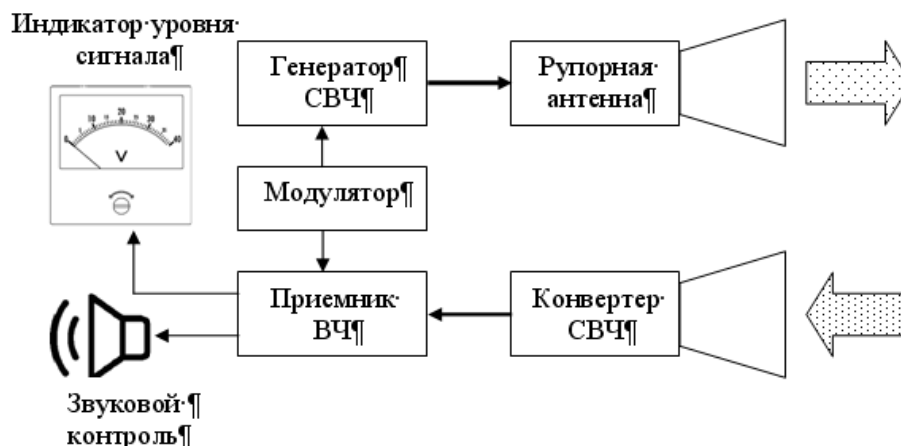


Рис. 4. Структурная схема генератора СВЧ подсветки цели с устройством наведения

Рассмотрим теперь особенности работы блока наведения (см. рис. 6). Необходимо отметить, что в процессе макетирования преследовались в первую очередь цели исследования работоспособности самого принципа наведения, вследствие чего экспериментальный макет при отслеживании цели частично управлялся вторым оператором вручную. Также конструктивно макет получился относительно больших размеров и устанавливался на отдельной треноге. В дальнейшем предполагается схему наведения минимизировать.



Рис. 5. Генератор СВЧ подсветки цели: а) рабочее положение генератора; б) вид панели контрольных приборов и регуляторов управления на обратной стороне. Здесь цифрами обозначены: 1 — рупорная излучающая антенна; 2 — генератор СВЧ на диоде

Ганна; 3 — конвертер контрольного приёмника наведения на цель; 4 — блок приборов контроля наведения и управления генератора СВЧ; 5 — стрелочный индикатор уровня сигнала контрольного приёмника; 6 — регулятор чувствительности контрольного приёмника; 7 — регулятор установки тока генератора Ганна; 8 — индикатор текущего значения тока и напряжения генератора Ганна; 9 — громкоговоритель контрольного приёмника; 10 — регулятор громкости звука контрольного приёмника.

Система автоматики, реализующая функцию наведения на цель, реализована по четырехканальной схеме (рис. 6) и использует амплитудный равносигнальный метод наведения в двух плоскостях: по азимуту и углу места.

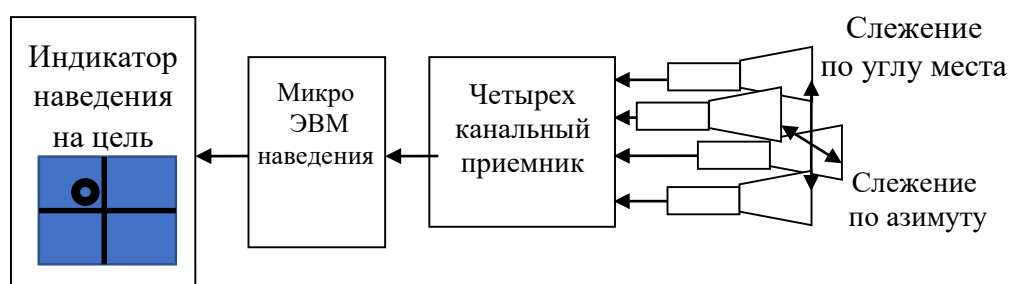


Рис. 6. Структурная схема макета системы наведения перехватчика

На рисунке 7 представлен внешний вид функционального макета системы наведения. Он выполнен в стационарном исполнении и устанавливается на специальной треноге. На лицевой панели установлены четыре приемных антенны, размещенные симметрично по углам квадрата (рис. 7, а). Для формирования резкого спада диаграммы направленности в равносигнальном направлении антенны разделены металлическими перегородками. На задней панели макета размещены индикаторы уровня сигналов приемных антенн (рис. 7, б), а также экран вычислителя ошибки наведения (рис. 7, в).

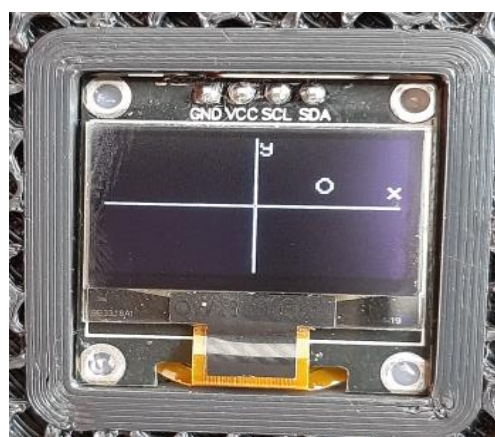
Расчет ошибки наведения осуществляется на основании оценки суммарного и разностного сигнала четырех каналов. Суммарный сигнал позволяет нормировать сигналы отдельных каналов и реализовать функцию цифровой системы регулировки усиления приемника. Разностный сигнал позволяет провести оценку ошибки наведения на цель по азимуту (ось X на рис. 7, в) и углу места (ось Y на рис. 7, в).



а)



б)



в)

Рис. 7. Лабораторная установка системы наведения на воздушную цель:

а) общий вид установки; б) вид панели органов управления;

в) вид индикатора направления на цель

Сигналы ошибки выводятся на индикатор наведения в виде кругового маркера, где, по аналогии с полярной системой координат, уровень сигнала ошибки можно оценить в виде расстояния маркера от точки начала координат, а направление на цель — в виде угла положения маркера. Таким образом, в пределах заданного сектора наведение на цель можно было осуществить в полностью автоматическом режиме.

Разработанные макеты были экспериментально протестированы в полевых условиях. Структурная схема эксперимента представлена на рисунке 8. Эксперимент проводился на открытой площадке. Так как вследствие проведения СВО полеты БВС в Воронежской области ограничены, объектом исследования был выбран плохо заметный в радиодиапазоне воздушный шар, наполненный гелием. Шар, удерживаемый нитью, находился на высоте 5 метров от поверхности земли. С земли шар облучался направленным сигналом подсветки. Отраженный

сигнал принимался системой из четырех ортогонально расположенных антенн, после чего четырехканальный приемник осуществлял усиление и фильтрацию полезного сигнала.



Рис. 8. Структурная схема эксперимента

Проведенные полевые испытания в целом показали высокую работоспособность предложенных схемных решений. Благодаря высокой частоте сигнала подсветки сигнал, отраженный от малозаметной цели, был устойчиво принят устройством наведения (см. значения показателей приборов на рис. 7). При перемещении цели его отметка на индикаторе цели пропорционально перемещалась по экрану, что говорит о правильной работе системы слежения.

В процессе экспериментов также было выявлено негативное влияние интерференции и переотражения сигнала при попадании в блок СВЧ излучения, отраженного от посторонних предметов (ветвей деревьев, соседних домов). При этом интенсивность отраженного сигнала может случайным образом меняться до 10 дБ по шкале индикаторных устройств.

Другим интересным эффектом является обнаружение отражения от стаи птиц (на фоне чистого неба) на расстоянии порядка 200 метров. Уровень отраженного сигнала при этом составлял +5 дБ относительно уровня фоновых шумов.

В целом, результаты проведенных экспериментов могут быть признаны успешными. В настоящее время ведутся работы над минимизацией размеров блока наведения, увеличением мощности излучения СВЧ передатчика целеуказания и совершенствованием его антенны. В дальнейшем предусматривается установка блоков на вращающиеся устройства с целью использования системы в стационарном режиме работы без участия операторов.

ЛИТЕРАТУРА

1. Макаренко С. И. Противодействие беспилотным летательным аппаратам : монография. — СПб. : Научное издание, 2020. — 204 с.
2. Леонов А. И., Фомичев К. И. Моноимпульсная радиолокация. — М. : Радио и связь, 1984. — 312 с.
3. Исследование эффективной площади рассеяния простых тел / С. А. Антипов, А. В. Володько, Е. А. Ищенко [и др.] // Вестник Воронежского государственного технического университета. — 2020. — Т. 16, № 5. — С. 81—85.
4. Майзельс Е. Н. Торгованов Е. Н. Измерение характеристик рассеяния радиолокационных целей. — М. : Советское радио, 1972 — 232 с.

REFERENCES

1. Makarenko S. I. Protivodejstvie bespilotny`m letatel`ny`m apparatam : monografiya. — SPb. : Naukoemkie tehnologii, 2020. — 204 s.
2. Leonov A. I., Fomichev K. I. Monoimpul`snyaya radiolokaciya. — M. : Radio i svyaz`, 1984. — 312 s.
3. Issledovanie e`ffektivnoj ploshhadi rasseyaniya prosty`x tel / S. A. Antipov, A. V. Volod`ko, E. A. Ishhenko [i dr.] // Vestnik Voronezhskogo gosudarstvennogo texnicheskogo universiteta. — 2020. — T. 16, № 5. — S. 81—85.
4. Majzel`s E. N. Torgovanov E. N. Izmerenie xarakteristik rasseyaniya radiolokacionny`x celej. — M. : Sovetskoe radio, 1972 — 232 s.

СВЕДЕНИЯ ОБ АВТОРАХ

Володько Александр Владиславович. Доцент кафедры радиоэлектронных устройств и систем. Кандидат технических наук, доцент.

Воронежский государственный технический университет.

E-mail: zavlabvgtu@rambler.ru

Россия, 394026, Воронеж, Московский проспект, 14.

Кузьменко Роман Валентинович. Профессор кафедры радиоэлектронных устройств и систем. Доктор физико-математических наук, доцент.

Воронежский государственный технический университет.

E-Mail: roman_kuzmenko@inbox.ru

Россия, 394026, Воронеж, Московский проспект, 14.

Андреева Наталья Александровна. Доцент кафедры физики и радиоэлектроники. Кандидат физико-математических наук, доцент.

Воронежский институт МВД России.

E-mail: andreevafsin@yandex.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Volodko Aleksandr Vladislavovich. Associate Professor of the chair of Radioelectronic Devices and Systems. Candidate of Technical Sciences, Associate Professor.

Voronezh State Technical University.

E-mail: zavlabvgtu@rambler.ru

Work address: Russia, 394026, Voronezh, Moskovsky Prospect, 14.

Kuzmenko Roman Valentinovich. Professor of the chair of Radioelectronic Devices and Systems. Doctor of Physical and Mathematical Sciences, Associate Professor.

Voronezh State Technical University.

E-mail: roman_kuzmenko@inbox.ru

Work address: Russia, 394026, Voronezh, Moskovsky Prospect, 14.

Andreeva Natalia Aleksandrovna. 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: andreevafsin@yandex.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: беспилотное воздушное судно БВС; автоматическое наведение; натурное моделирование; радиолокация.

Key words: unmanned aircraft UAV; automatic guidance; full-scale modeling; radar.

УДК 621.396.969

Ю. В. Белозерцев

А. И. Климов, доктор технических наук, профессор

М. С. Петров

ШИРОКОПОЛОСНАЯ АНТЕННА ДЛЯ НОСИМЫХ РАДИОСТАНЦИЙ ДИАПАЗОНА УВЧ

WIDEBAND ANTENNA FOR UHF BAND PORTABLE RADIOS

Представлены результаты разработки широкополосной антенны линейной поляризации с круговой диаграммой направленности диапазона УВЧ. Рабочая полоса частот антенны, ограниченная качеством согласования по значению коэффициента стоячей волны напряжения не более 2, в пределах 370—530 МГц. Антенна может быть использована в составе носимых радиостанций систем подвижной радиосвязи и аппаратуре других радиосистем диапазона УВЧ.

The results of the development of a broadband linear polarization antenna with a circular radiation pattern of the UHF band are presented. The operating frequency band of the antenna, limited by the matching quality in terms of the value of the voltage standing wave ratio of no more than 2, is in the range of 370—530 MHz. The antenna may be used as part of portable radio stations of mobile radio communication systems and equipment of other UHF radio systems.

В повседневной служебной деятельности ОВД широко используются системы конвенциональной и транкинговой подвижной радиосвязи диапазонов ОВЧ и УВЧ, в числе которых ключевую роль играют цифровые системы стандартов DMR и APCO-25 [1]. Известно, что тактико-технические характеристики систем радиосвязи, в частности форма и размеры зоны радиопокрытия, надежность и качество работы, в значительной степени зависят от электрических характеристик антенн, применяемых в составе носимых, возимых и стационарных радиостанций и ретрансляторов. К основным характеристикам антенн, определяемым в заданной полосе радиочастот, относятся поляризация, диаграмма направленности (ДН), коэффициент полезного действия (КПД), коэффициент направленного действия (КНД), коэффициент усиления (КУ), для антенн ОВЧ и УВЧ — входное сопротивление и коэффициент стоячей волны напряжения (КСВ) на входе антенны. Наиболее важными для антенн, работающих как в режиме передачи, так и приема, являются частотные характеристики КСВ и реализуемого КУ, от которого непосредственно зависит мощность радиосигнала в точке приема. При этом особого внимания заслуживают антенны мобильных (в частности, носимых) радиостанций, которые должны иметь по возможности небольшую длину, круговую азимутальную ДН, КУ (определяемый относительно КУ полуволнового симметричного вибратора) не менее -3 дБд (или абсолютный КУ относительно КУ идеального изотропного излучателя $-0,85$ дБи, или дБ) и КСВ не более 2,5 во всем диапазоне рабочих частот [2]. В качестве внешних компактных антенн для носимых радиостанций диапазонов ОВЧ и УВЧ в настоящее время в основном применяются укороченные несимметричные электрические вибраторы (так называемые штыревые антенны) длиной порядка четверти рабочей длины волны и различные варианты спиральных антенн, которые могут

иметь существенно меньшую длину [3]. Главными неприятными особенностями таких антенн являются: сильное влияние на их свойства (в том числе, на форму ДН, на в общем случае частотно-зависимое комплексное входное сопротивление и КУ) окружающих предметов, резонансное поведение частотных характеристик входного сопротивления и КСВ на входе [4—6]. Так, в диапазоне УВЧ большинство названных выше антенн для аппаратуры радиосвязи того или иного стандарта (TETRA, DMR, APCO-25 и др.) обеспечивают КСВ не более 2,5 и КУ не ниже 0 дБ в некоторой сравнительно узкой полосе частот, ширина которой не превышает единиц процентов (например, 450—470 МГц), причем без учета влияния окружающих предметов. Соответственно, такие антенны не могут быть использованы в других полосах частот. Кроме того, в зависимости от размещения радиостанции (в отсутствие близкорасположенных посторонних объектов, при удержании рукой на разных расстояниях от человеческого тела, головы и т. п.) существенно изменяются форма ДН, частотные характеристики входного сопротивления, КСВ, КПД и КУ, вплоть до неприемлемых. Например, если при идеально согласованной с выходом радиопередатчика антенне ($КСВ=1$) она обеспечивает максимально возможный $KU_{\text{макс}} = КПД \cdot КНД$, то при рассогласовании до $КСВ = 3$ реализуемый из-за отражения части мощности назад в передатчик $KU_{\text{реал}} = 0,75 KU_{\text{макс}}$ (снижение на 1,25 дБ), а при $КСВ=6$ $KU_{\text{реал}} = 0,49 KU_{\text{макс}}$ (снижение уже на 3,1 дБ). Нельзя не отметить и зависимость КПД КУ антенны от ее расположения, что обусловлено, например, поглощением энергии электромагнитного поля, формируемого антенной, человеческим телом [4].

Таким образом, определенный интерес вызывают вопросы исследования характеристик известных антенн в зависимости от условий их использования и от возможности построения достаточно компактных широкополосных антенн для носимых радиостанций и другой радиоаппаратуры диапазона УВЧ, в меньшей степени подверженных влиянию окружающих предметов в заданной рабочей полосе частот.

Целью данной работы является разработка и исследование широкополосной антенны с круговой диаграммой направленности для носимых радиостанций систем подвижной радиосвязи различных стандартов в диапазоне УВЧ, использование которой позволяет расширить зону радиопокрытия без увеличения выходной мощности радиопередатчиков, повысить надежность и качество связи.

Для достижения поставленной цели в работе решались следующие задачи:

1. Анализ конструкций и характеристик известных антенн вертикальной поляризации с круговой диаграммой направленности в горизонтальной плоскости для носимых радиостанций систем подвижной радиосвязи диапазона УВЧ.
2. Выбор базового варианта антенны для разработки новой антенны.
3. Разработка и исследование новой широкополосной антенны вертикальной поляризации с круговой диаграммой направленности в горизонтальной плоскости для носимых радиостанций систем подвижной радиосвязи диапазона УВЧ.

Во многих отечественных и зарубежных носимых радиостанциях диапазона УВЧ, в частности цифровых радиостанциях стандарта DMR (например, отечественной радиостанции ТАКТ-363.21 П45, рассчитанной для работы в полосе частот 400—470 МГц), используются укороченные антенны на основе различных конструкций из спиральных электрических проводников. Примером служит антенна Hytera AN0435H13 (рис. 1, а) [7]. Антенна имеет сравнительно небольшую длину (90 мм) и характеризуется широкой полосой рабочих частот в отличие от более коротких спиральных антенн. Информация о частотной характеристике КСВ, предоставляемая одним из поставщиков антенн (ЗАО «Вива-Телеком», Россия), иллюстрируется рис. 1, б [8].

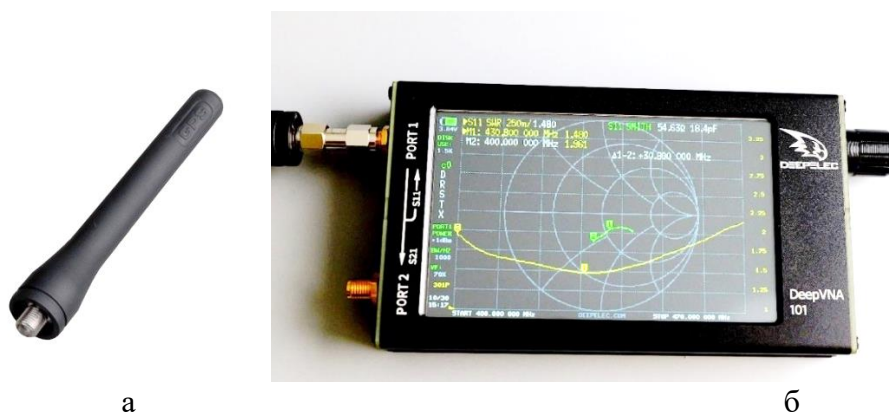


Рис. 1. Антенна Hytera AN0435H13 и ее частотная характеристика КСВ

Как видно из рис. 1, полоса частот по $K_{CB} \leq 2$ составляет от 400 до 463 МГц при минимальном $K_{CB} = 1,5$ на частоте 430 МГц.

Вместе с тем, значительный интерес в отношении антенн носимых радиостанций представляет собой вопрос о возможности расширения полосы частот приемлемого согласования и ее трансформации, например, в полосу от 380 МГц до 520 МГц.

Для работы в двухчастотном режиме или в расширенной полосе частот в ряде известных работ предложены оригинальные технические решения. Так, в [9] предложено использовать в антенне две спирали, как показано на рис. 2.

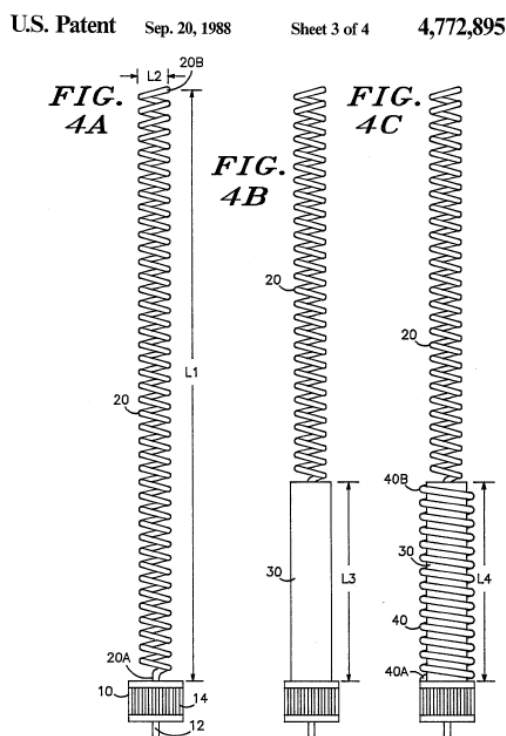


Рис. 2. Антенна с двумя спиралями

Двухчастотный режим обеспечивается реализацией двух резонансов в структуре антенны. С этой целью длинная спираль дополняется электромагнитно связанной с ней

короткой спиралью, причем нижний конец длинной спирали электрически соединяется с центральным проводником питающего коаксиального кабеля, а нижний конец короткой спирали — с его экранирующей оплеткой [9]. Расстояние между спиралями выбирается довольно малым, и они изолируются друг от друга диэлектрической трубкой.

В [10] приведены результаты разработки и исследований двухчастотной антенны с двумя спиралями для полосы частот 136—174 МГц, построенной по принципу, описанному выше. Показано, что на частотах диапазона ОВЧ действительно достигается двухчастотный режим, хотя качество согласования получается, вообще говоря, посредственным.

Известно множество других технических решений, направленных на обеспечение широкополосных, двух- и многочастотных режимов работы подобных антенн.

В настоящей работе для построения широкополосной антенны нами предложено использовать конструкцию типа спирально-стержневой замедляющей структуры поперечного (нормального) излучения, короткозамкнутой на конце. Это позволяет построить антенну, рабочая полоса частот которой будет находиться в окрестности частоты последовательного резонанса между достаточно близко расположенными частотами параллельных резонансов, что при оптимальном выборе геометрических параметров позволит существенно расширить полосу частот приемлемого согласования антенны по входу и в значительной степени стабилизировать положение рабочей полосы частот удовлетворительного согласования при различном размещении радиостанции с антенной относительно тела человека.

Новый вариант короткозамкнутой на конце спирально-стержневой антенны со спиралью из полоскового проводника представлен на рис. 2 (вид без защитного покрытия из диэлектрического материала).

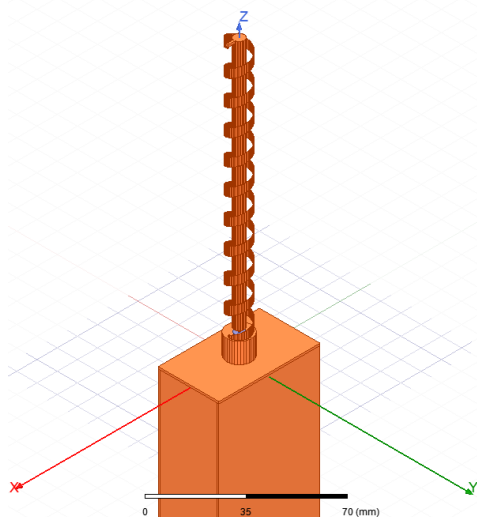


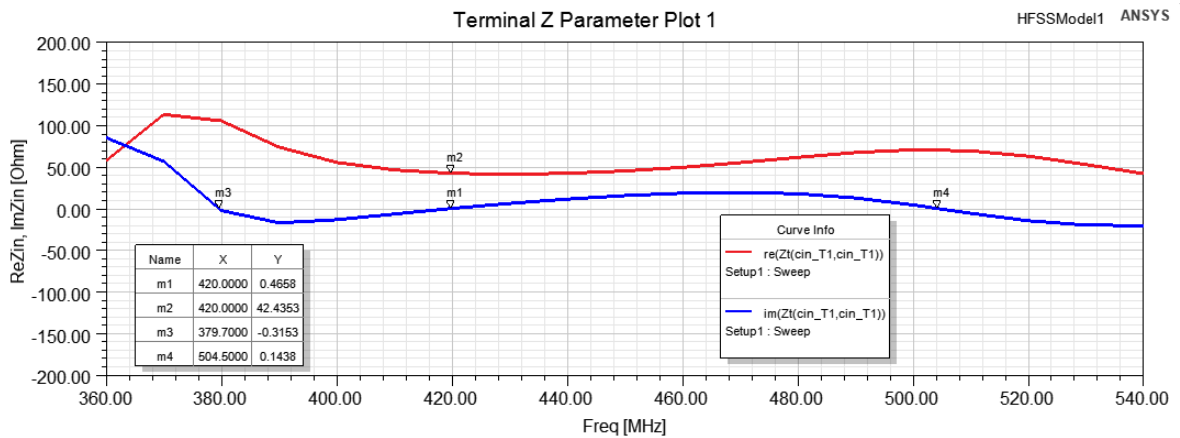
Рис. 2. Модель антенны на шасси радиостанции

Дисперсионные характеристики спирально-стержневых структур СВЧ подробно проанализированы в известной работе [11], однако пригодных расчетных формул для инженерного проектирования подобной антенны нет. Поэтому начальные параметры конструкции были выбраны с учетом обеспечения режима нормального излучения, необходимого для вертикальной антенны с круговой азимутальной ДН, а также из интуи-

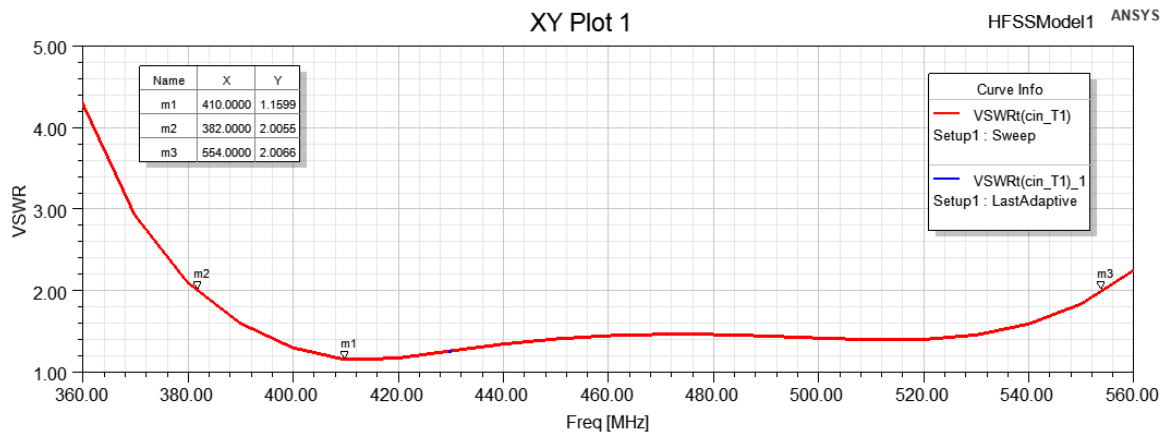
тивных соображений и затем были оптимизированы в процессе имитационного моделирования с помощью программы HFSS. При этом предполагалось, что длина антенны и другие параметры конструкции должны обеспечивать приемлемое согласование с КСВ не более 2 в полосе частот от 380 до 530 МГц, в которой в принципе работают системы подвижной радиосвязи стандартов TETRA, DMR и APCO-25.

В конструкции антенны используется полосковая спираль (из медной фольги). Нижний конец спирали электрически соединен с внешним цилиндрическим элементом коаксиального разъема. Центральный металлический стержень электрически соединен с центральным проводником коаксиального разъема. Верхние концы спирали и стержня также электрически соединены. Полная высота антенны 146 мм, внешний диаметр 11 мм.

На рис. 3 приведены частотные характеристики входного сопротивления и КСВ модели антенны, установленной на модели металлического шасси радиостанции с размерами $X \times Y \times Z = 50 \times 30 \times 130$ мм³, полученные при моделировании данной структуры в условиях свободного пространства.



а



б

Рис. 3. Частотные характеристики входного сопротивления (а) и КСВ (б)

Как видно из частотной характеристики КСВ на рис. 3, б, антенна обладает весьма широкой полосой частот по уровню КСВ=2, достигающей 170 МГц, что объясняется довольно интересным поведением частотных характеристик входного сопротивления, рис. 3, а, которые демонстрируют три резонанса на частотах порядка 380, 420 и 505 МГц.

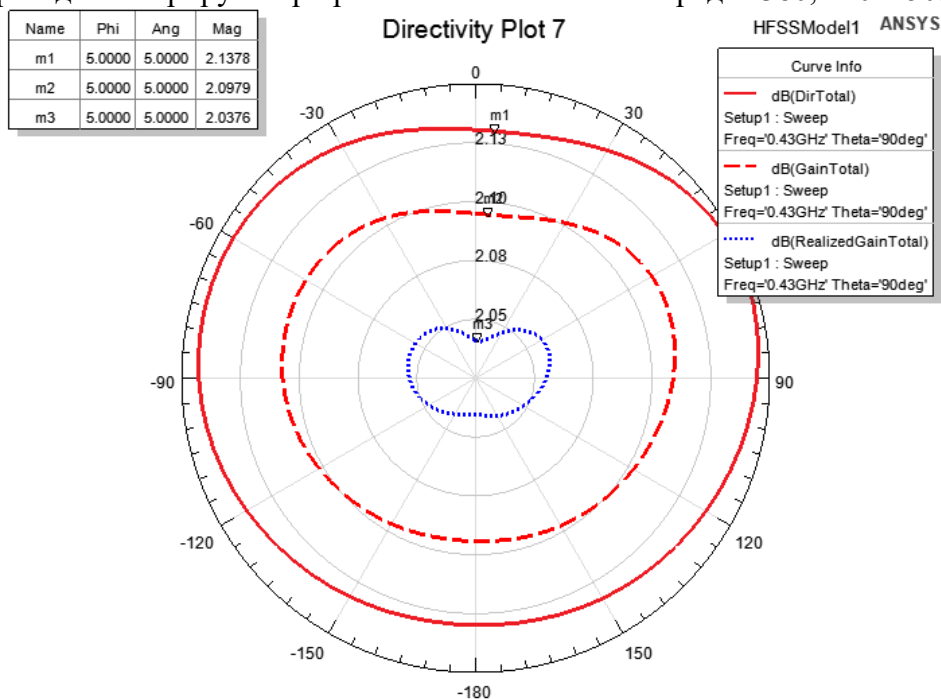


Рис. 4. Азимутальные ДН на частоте 430 МГц

Антенна обладает практически круговой азимутальной ДН (пример ДН для частоты 430 МГц приведен на рис. 4), небольшая неравномерность объясняется ограниченной точностью расчета при имитационном моделировании.

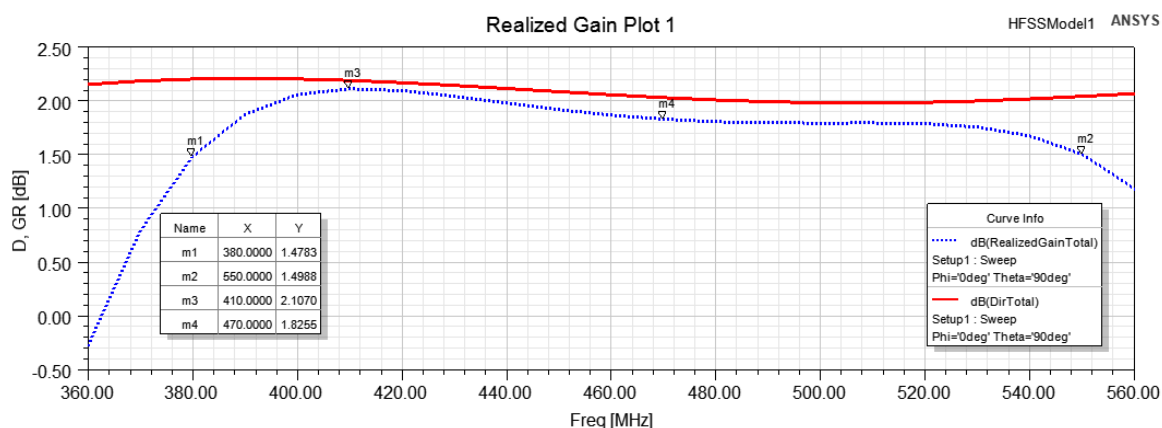


Рис. 5. Частотные характеристики КНД и реализуемого КУ в азимутальных направлениях

Из представленных на рис. 5 частотных характеристик КНД и реализуемого КУ видно, что реализуемый КУ антенны в полосе частот 410—520 МГц незначительно меньше КНД, превышает 1,5 дБ в полосе частот 380—550 МГц, причем в полосе частот 410—470 МГц его значение выше 1,8 дБ, а максимальное значение составляет 2,1 дБ на частоте 410 МГц.

На рис. 6 приведена частотная характеристика КСВ действующего макета новой антенны, измеренная в лаборатории при установке антенны на металлическом шасси радиостанции и подключении к измерителю КСВ отрезком длиной 50 см радиочастотного кабеля с волновым сопротивлением 50 Ом.

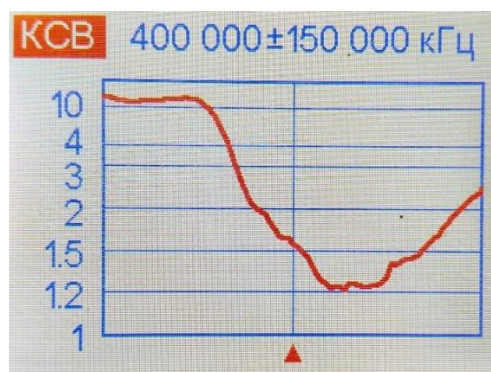


Рис. 6. Измеренная частотная характеристика КСВ

Как видно из рис. 6, у макета новой антенны значения КСВ не превышают 2 в полосе частот 370—530 МГц (абсолютное значение полосы 160 МГц), минимальное значение 1,2 отмечено на частоте порядка 440 МГц.

Особый интерес вызывает поведение характеристик антенны при удержании модели шасси радиостанции в модели кисти руки вблизи модели головы человека, рис. 7. Полученные при этом характеристики антенны иллюстрируются рис. 8—10.

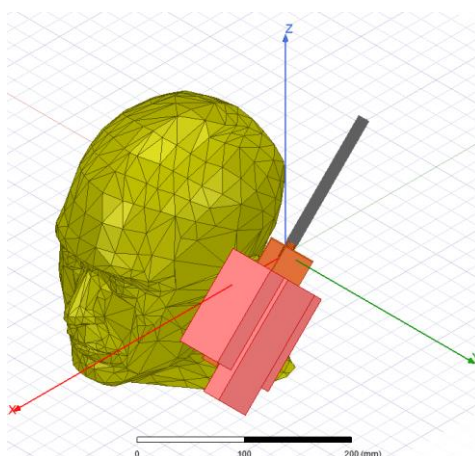


Рис. 7. Имитационная модель радиостанции с исследуемой антенной вблизи головы человека

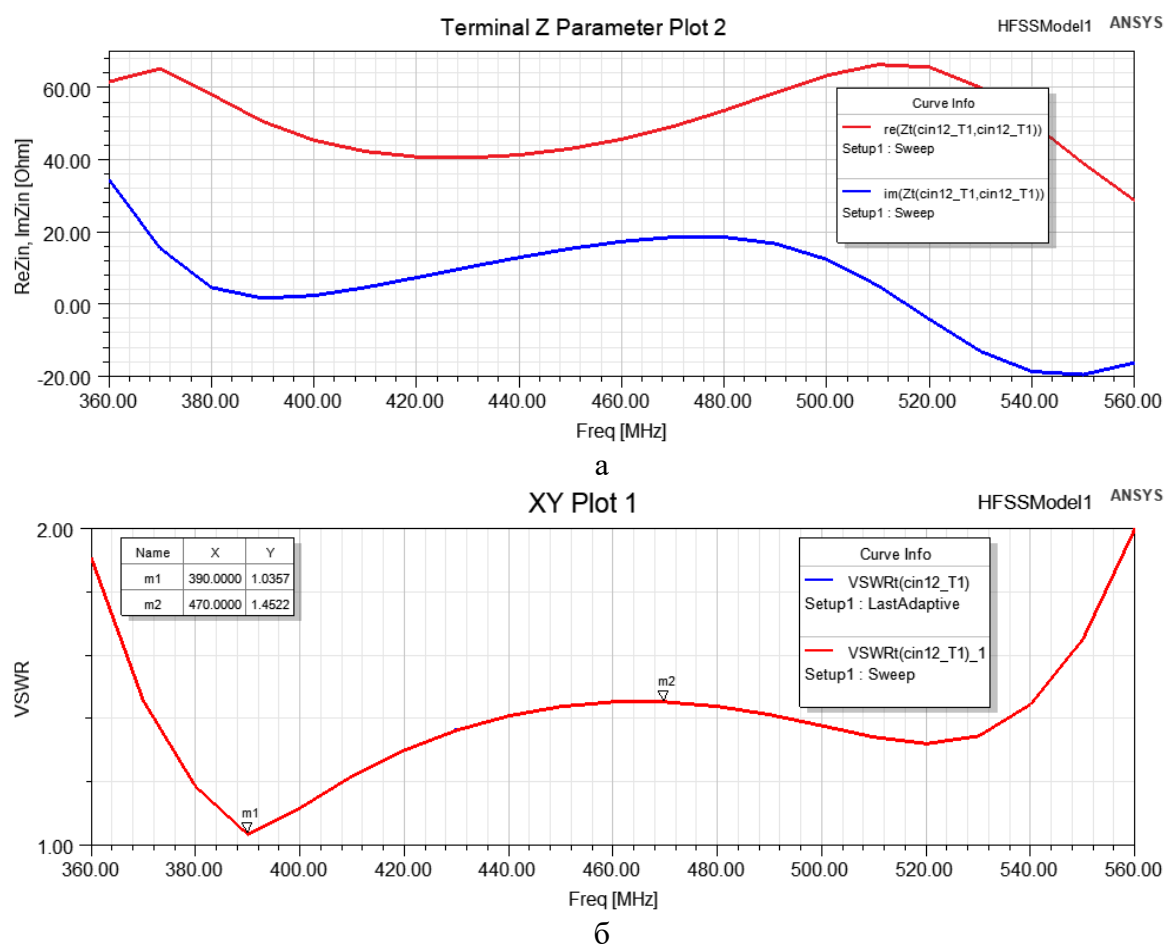


Рис. 8. Частотные характеристики входного сопротивления (а) и КСВ (б)

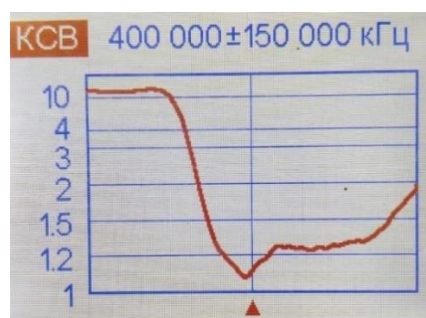


Рис. 9. Измеренная частотная характеристика КСВ

Измеренные значения КСВ (рис. 9) не превышают 2 в полосе частот 370 –550 МГц, при этом минимум КСВ=1,1 отмечен на частоте около 390 МГц, что удовлетворительно согласуется с результатами имитационного моделирования (рис. 8, б). На рис. 10 представлен пример азимутальных ДН антенны на частоте 430 МГц, полученной при имитационном моделировании.

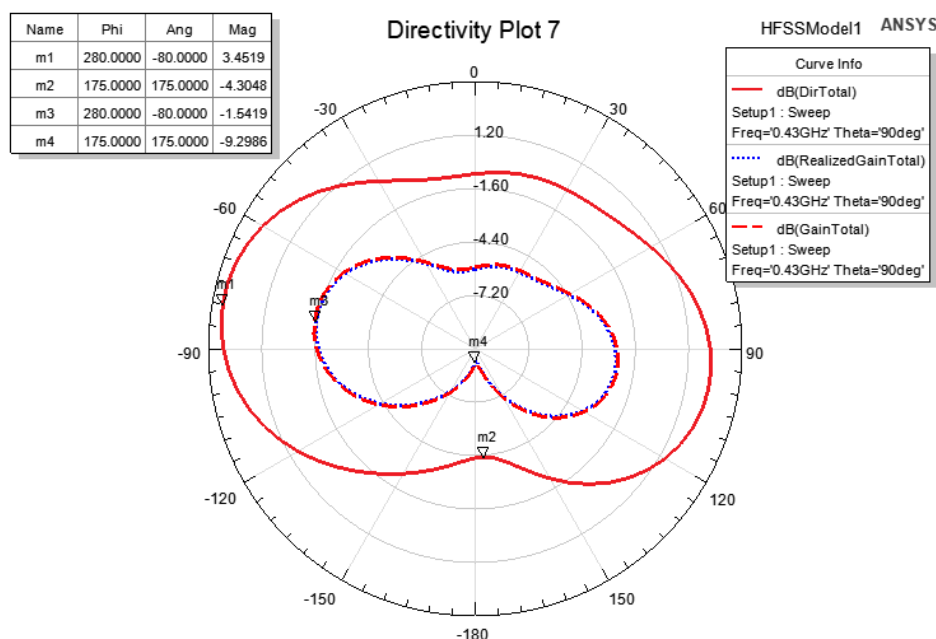


Рис. 10. Азимутальные ДН на частоте 430 МГц

Главный результат анализа ДН антенны состоит в том, что, как видно из рис. 10, новая антенна при расположении радиостанции вблизи головы человека обеспечивает максимальный реализуемый КУ = -1,5 дБ, при этом минимальный реализуемый КУ = -9,3 дБ, что выгодно отличает новую антенну от укороченных аналогов.

Таким образом, новая антенна, хотя и несколько более сложная в плане конструкции и технологии изготовления и имеющая длину, в среднем, в полтора раза большую длины укороченных аналогов, отличается более широкой полосой качественного согласования по входу и практически вдвое большим реализуемым КУ в реальных условиях эксплуатации. Антенна может использоваться на любых частотах в полосе 370—530 МГц в составе радиостанций систем связи стандартов TETRA, DMR и APCO-25, потенциально обеспечивая при одинаковых значениях выходной мощности радиопередатчика и чувствительности радиоприемника расширение зоны радиопокрытия. Полученные результаты в отношении поведения реальных коэффициентов усиления и изменения формы ДН антенны могут быть полезны для более точного расчета характеристик зон радиопокрытия подвижных систем и сетей радиосвязи.

Представленная в статье антенна может использоваться не только в составе носимых радиостанций систем подвижной радиосвязи диапазона УВЧ, но и в аппаратуре других радиосистем, в частности, радиоконтроля и радиоуправления.

ЛИТЕРАТУРА

1. Системы радиосвязи специального назначения / Н. С. Хохлов [и др.]. — Воронеж : Воронежский институт МВД России, 2017. — 99 с.
2. ГОСТ Р 56154-2014. Национальный стандарт Российской Федерации. Антенны приемопередающие для центровых (базовых) и мобильных радиостанций сухопутной подвижной радиосвязи и их характеристики. — URL: <https://docs.cntd.ru/document/1200113846>

3. Volakis J. L. Antenna Engineering Handbook. — McGraw-Hill, 2007. — 1755 p.
4. Andersen J. B., Hansen F. Antennas for VHF/UHF personal radio: A theoretical and experimental study of characteristics and performance // IEEE Transactions on Vehicular Technology. — 1977. — Vol. VT-26. — No. 4. — P. 349—357.
5. Balanis C. A. Antenna Theory: Analysis and Design. — Wiley-Interscience, 2005. — 1136 p.
6. Айзенберг Г. З., Ямпольский В. Г., Терешин О. Н. Антенны УКВ : в 2 ч. Ч. 1. — М. : Связь, 1977. — 384 с.
7. Hytera AN0435H13. — URL: <https://hytera-europe.com/accessories/an0435h13>.
8. Обзор характеристик антенны Hytera AN0435H13. — URL: <https://viva-telecom.org/16380/hytera/an0435h13/>
9. Wide-band helical antenna / US Patent Number: 4,772,895. Date of Patent: Sep. 20, 1988.
10. Compact Wide Band Double Helical Antenna for Public Safety VHF Band / DOI:10.34385/proc.35.3C19-3/.
11. Силин Р. А., Сазонов В. П. Замедляющие системы. — М. : Сов. радио, 1966. — 632 с.

REFERENCES

1. Sistemy` radiosvyazi special`nogo naznacheniya / N. S. Xoxlov [i dr.]. — Voronezh : Voronezhskij institut MVD Rossii, 2017. — 99 s.
2. GOST R 56154-2014. Nacional`ny`j standart Rossijskoj Federacii. Antenny` priemoperedayushhie dlya centrov`x (bazovy`x) i mobil`ny`x radiostancij suxoputnoj podvizhnoj radiosvyazi i ix xarakteristiki. — URL: <https://docs.cntd.ru/document/1200113846>
3. Volakis J. L. Antenna Engineering Handbook. — McGraw-Hill, 2007. — 1755 p.
4. Andersen J. B., Hansen F. Antennas for VHF/UHF personal radio: A theoretical and experimental study of characteristics and performance // IEEE Transactions on Vehicular Technology. — 1977. — Vol. VT-26. — No. 4. — P. 349—357.
5. Balanis C. A. Antenna Theory: Analysis and Design. — Wiley-Interscience, 2005. — 1136 p.
6. Ajzenberg G. Z., Yampol`skij V. G., Tereshin O. N. Antenny` UKV : v 2 ch. Ch. 1. — М. : Svyaz`, 1977. — 384 s.
7. Hytera AN0435H13. — URL: <https://hytera-europe.com/accessories/an0435h13>.
8. Obzor xarakteristik antenny` Hytera AN0435H13. — URL: <https://viva-telecom.org/16380/hytera/an0435h13/>
9. Wide-band helical antenna / US Patent Number: 4,772,895. Date of Patent: Sep. 20, 1988.
10. Compact Wide Band Double Helical Antenna for Public Safety VHF Band / DOI:10.34385/proc.35.3C19-3/.
11. Silin P. A., Sazonov V. P. Zamedlyayushhie sistemy`. — М. : Sov. radio, 1966. — 632 s.

СВЕДЕНИЯ ОБ АВТОРАХ

Белозерцев Юрий Васильевич. Заместитель генерального директора по научно-техническому развитию.

АО ВНИИ «Вера».

E-mail: belozertsev.yuriy@yandex.ru

Россия, 394026, Воронеж, Московский проспект, 7б.

Климов Александр Иванович. Профессор кафедры инфокоммуникационных систем и технологий.
Доктор технических наук, профессор.
Воронежский институт МВД России.
E-mail: alexserkos@inbox.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Петров Максим Сергеевич. Курсант.
Воронежский институт МВД России.
E-mail: maximpetrov172@gmail.com
Россия, 394065, Воронеж, проспект Патриотов, 53.

Belozertsev Yuriy Vasil'yevich. Deputy Director General for Scientific and Technical Development.
JSC Research Institute «Vega», Voronezh.
E-mail: belozertsev.yuriy@yandex.ru
Russia, 394026, Voronezh, Moskovsky Prospect, 7b.

Klimov Alexander Ivanovich. Professor of the chair of Infocommunication Systems and Technologies.
Doctor of Sciences (Radio Engineering), Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: alexserkos@inbox.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Petrov Maxim Sergeevich. Cadet.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: maximpetrov172@gmail.com
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: диапазон УВЧ; подвижная радиосвязь; антенна; диаграмма направленности; коэффициент стоячей волны напряжения.

Key words: UHF band; mobile radio communications; antenna; radiation pattern; voltage standing wave ratio.

УДК 621.396.67

Д. А. Ерошенко

А. И. Климов, доктор технических наук, профессор

Н. Е. Фомин

ПОЛОСКОВАЯ АНТЕННАЯ РЕШЕТКА ДИАПАЗОНА КВЧ

EHF-BAND STRIP ANTENNA ARRAY

В статье представлены результаты разработки и имитационного моделирования плоской полосковой антенной решетки вытекающей волны диапазона КВЧ. Антенна имеет размеры $90,4 \times 89,2 \times 4$ мм³, в полосе частот 60—60,5 ГГц обладает коэффициентом усиления 34—34,3 дБ и может быть использована в аппаратуре различных беспроводных систем, в том числе радиорелейных линий (радиомостов) повышенной помехозащищенности.

The article presents the results of the development and simulation of a flat strip leaky wave antenna array of EHF band. The antenna dimensions are $90,4 \times 89,2 \times 4$ mm³, has a gain of 34—34,3 dB in the frequency band 60—60,5 GHz and may be used in equipment of various wireless systems, including radio relay lines (radio bridges) with enhanced noise immunity.

В настоящее время в числе различных систем радиосвязи ОВД все шире используются системы беспроводного широкополосного доступа (БШД), например стандартов WiMax, а также наземные радиорелейные линии (РРЛ) прямой видимости, работающие в диапазонах УВЧ и СВЧ [1]. Вместе с тем значительные перспективы открываются при внедрении систем БШД и РРЛ (в том числе однопролетных РРЛ — радиомостов), работающих в диапазоне КВЧ, т. е. миллиметровых волн (ММВ). Такие системы отличаются компактностью радиоаппаратуры, существенно большей пропускной способностью — порядка нескольких Гбит/с, высокой помехоустойчивостью и при этом в гораздо меньшей степени обостряют проблему электромагнитной совместимости (ЭМС) радиоэлектронных средств (РЭС) благодаря применению остронаправленных антенн и использованию особенностей распространения ММВ в атмосфере [2—5]. Особого внимания заслуживают системы, работающие в окрестности частоты 60 ГГц (длина волны 5 мм), на которой радиоволны в силу резонансного поглощения энергии молекулами кислорода испытывают значительное погонное ослабление плотности потока мощности на приземной трассе распространения, достигающее 16 дБ/км (в так называемых «окнах прозрачности», например, в полосе частот 36—38 ГГц, погонное ослабление в чистой атмосфере не превышает десятых долей дБ/км) [6]. С одной стороны, такое ослабление ММВ на частоте 60 ГГц препятствует реализации протяженных (как в диапазонах УВЧ и СВЧ) наземных радиолиний прямой видимости с высокой пропускной способностью, но с другой — позволяет существенно повысить помехозащищенность радиолиний за счет повышения скрытности их работы и усложнения обнаружения техническими средствами радиораз-

ведки [4, 6, 7]. Радиолинии диапазона 60 ГГц перспективны и для построения помехозащищённых периметральных охранных систем, и различных радиолокационных устройств небольшого радиуса действия.

В отношении систем связи ОВД РФ системы диапазона 60 ГГц могут быть хорошим вариантом быстро развертываемых и достаточно высокоскоростных систем для использования на ограниченных площадях на расстояниях до сотен метров, например, в условиях проведения специальных операций при повышенных требованиях к помехозащищённости связи и защите передаваемой информации от несанкционированного доступа.

На сегодняшний день за рубежом и в России производится довольно много аппаратуры для РРЛ (радиомостов) диапазона КВЧ [8—11]. В большинстве случаев в составе радиорелейных станций (РРС) применяются довольно громоздкие, сложные и дорогостоящие зеркальные (иногда рупорно-линзовые) антенны [5, 8]. Очевидно, что их замена плоскими антеннами позволяет улучшить массогабаритные показатели и упростить конструкцию РРС. Однако такая замена требует решения проблемы построения плоских антенн с высокими коэффициентами полезного действия (КПД) и усиления (КУ), с диаграммами направленности (ДН) шириной 1—4 градуса и низким (не более –16...–18 дБ) уровнем боковых лепестков (УБЛ). Дело в том, что известные плоские антенны — антенные решетки (волноводно-щелевые, полосковые) диапазона КВЧ зачастую либо весьма сложны в изготовлении и имеют высокую стоимость, либо имеют невысокий КПД, не превышающий в среднем 30—50%, что, соответственно, не позволяет получить высокий (30—35 дБ) КУ и приводит к уменьшению дальности действия радиосистемы [12, 13]. Кроме того, многие известные плоские антенные решетки, имеющие КУ порядка 32—34 дБ, имеют ДН со слишком высоким (вплоть до –12...–10 дБ) УБЛ, что приводит к снижению помехоустойчивости и помехозащищённости соответствующей радиосистемы и обостряет проблему ЭМС РЭС.

Целью работы является разработка и исследование плоской полосковой антенной решетки с высоким коэффициентом усиления для аппаратуры РРЛ (радиомостов), работающих в окрестности частоты 60 ГГц.

Достижение поставленной цели потребовало решения следующих задач:

- анализа вариантов построения плоских антенных решеток линейной поляризации с высоким КУ и низким УБЛ ДН для полос частот в окрестности 60 ГГц;
- разработки конструкции новой антенны и исследования ее электрических характеристик.

В качестве плоских антенн диапазона КВЧ в настоящее время используются:

- волноводно-щелевые антенные решетки (ВЩАР);
- полосковые и микрополосковые антенные решетки (МΠΑР);
- плоские антенны вытекающей волны (ПАВВ).

В методических рекомендациях [13] представлены результаты анализа конструкций и электрических характеристик нескольких заслуживающих внимания образцов антенн названных типов.

Так, примером современной металлической ВЩАР служит антенна [17], имеющая довольно сложную трехслойную конструкцию с параллельной системой питания, построенную в виде реберно-щелевого распределителя мощности. Излучающая система выполнена в виде решетки из $16 \times 16 = 256$ щелей. В 16-процентной полосе частот (56—65,7 ГГц) КСВ на входе антенны не превышает 2, КПД не менее 70%, а КУ находится в пределах от 32,5 до 33,2 дБ. Этот и другие примеры [13] показывают, что металлические ВЩАР традиционных конструкций обладают высоким КПД и обеспечивают КУ, достигающий 30 и

более дБ, однако конструктивно сложны, нетехнологичны и поэтому имеют высокую стоимость.

Вместе с тем, многие современные ВЩАР изготавливаются по технологии SIW (Substrate Integrated Waveguide) — на основе металлодиэлектрических волноводов, интегрированных с подложкой. Известные варианты таких ВЩАР СВЧ и КВЧ на основе плоскопараллельного волновода с торцевым и центральным параллельно-последовательным питанием в режиме нормального излучения имеют КПД до 50—60% и КУ, достигающий 32 дБ [13].

Известны и МПАР с высокими КНД и КУ, превышающими 30 дБ. Однако такие МПАР, как и традиционные ВЩАР, имеют сложные многослойные конструкции [13]. Примером МПАР СВЧ с высоким КУ служит антенна [18], разработанная для применения в радиоаппаратуре беспилотных летательных аппаратов (БПЛА). Это антенна, разработанная для полосы частот 25,43—26,91 ГГц, имеет параллельную систему распределения мощности, содержит $32 \times 32 = 1024$ полосковых элемента, размещенных на подложке с размерами 232,6 мм ($20\lambda_0$) $\times$ 257 мм ($22,5\lambda_0$). Толщина конструкции антенны 1,664 мм ($0,14\lambda_0$). КПД антенны превышает 52 %, КУ составляет 30,71—32,8 дБ. Существенным недостатком антенны является высокий УБЛ ДН, в среднем составляющий – 14 дБ. В указанной выше полосе частот модуль коэффициента отражения по напряжению от входа антенны не превышает –10 дБ, что соответствует $K_{CB} \leq 2$, а КПД антенны находится в пределах от 50 % до 60 %.

Интересный пример МПАР диапазона КВЧ описан в [19]. Это антенна двухслойной конструкции, содержащая излучающую систему в виде $32 \times 32 = 1024$ полосковых элементов с параллельным распределителем мощности, построенном на основе волноводов, изготавливаемых по технологии SIW. В полосе рабочих частот 91—95 ГГц измеренные значения КУ антенны составили в среднем 30 дБ, однако при весьма низком КПД ~24 %.

Таким образом, многие современные МПАР уступают ВЩАР по значениям КПД и КУ.

В этой связи в качестве базовой для разработки новой плоской антенны линейной поляризации для РРС диапазона 60 ГГц в настоящей работе выбрана плоская антенна вытекающей волны (ПАВВ) СВЧ с большой площадью раскрыва, обеспечивающая получение КНД не менее 34 дБ, построенная в виде объединения четырех подрешеток вытекающей волны с помощью четырехканального параллельного сумматора / делителя мощности лучевого типа, разработанная ранее на кафедре инфокоммуникационных систем и технологий Воронежского института МВД России для полосы частот 24—24,25 ГГц. Базовая ПАВВ СВЧ имеет КПД более 90%, КУ ~34 дБ и обеспечивает формирование ДН с УБЛ не более –18 дБ [20].

Параметры конструкции антенны КВЧ для полосы частот 60—61 ГГц определены по методике, разработанной на кафедре ИКСиТ [13] с использованием хорошо известного в электродинамике и теории антенн принципа электродинамического подобия [21, 22].

Поэтому новая антенна для работы в окрестности частоты 60 ГГц представляет собой масштабную (уменьшенную в 2,5 раза) копию антенны для средней частоты 24 ГГц [20] и имеет соответственно уменьшенные размеры раскрыва $90,4 \times 89,2$ мм².

Внешний вид антенны показан на рис. 1.

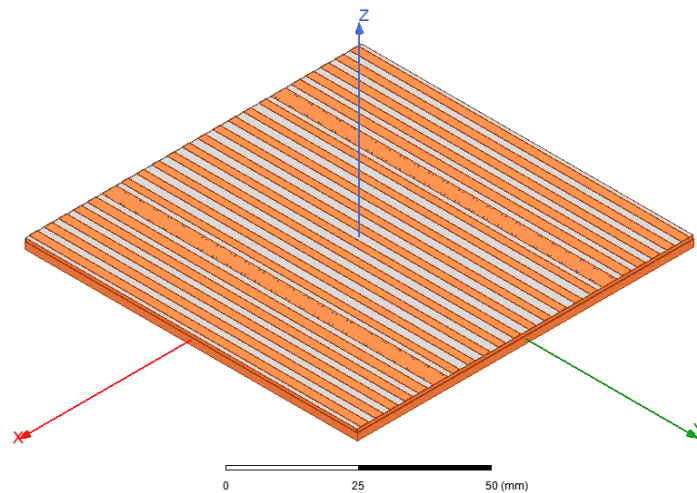


Рис. 1. ПАВВ диапазона 60 ГГц, составленная из четырех подрешеток

Основные электрические характеристики — частотная характеристика КСВ (VSWR), частотные характеристики КНД (D), КУ с учетом только тепловых потерь (G) и реализуемого КУ (GR) с учетом качества согласования по входу, а также пример ДН в Е- и Н-плоскостях на частоте 60,25 ГГц иллюстрируются рис. 2—4. Эти характеристики получены путем имитационного компьютерного моделирования разработанной антенны с помощью специализированной программы для анализа и синтеза устройств СВЧ и антенн ANSYS HFSS.

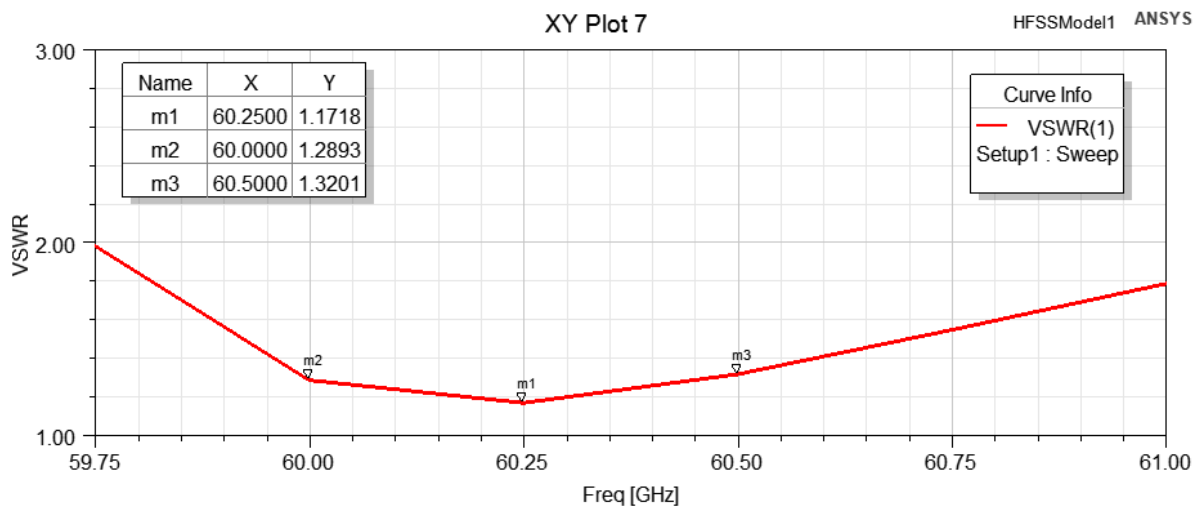


Рис. 2. Частотная характеристика КСВ

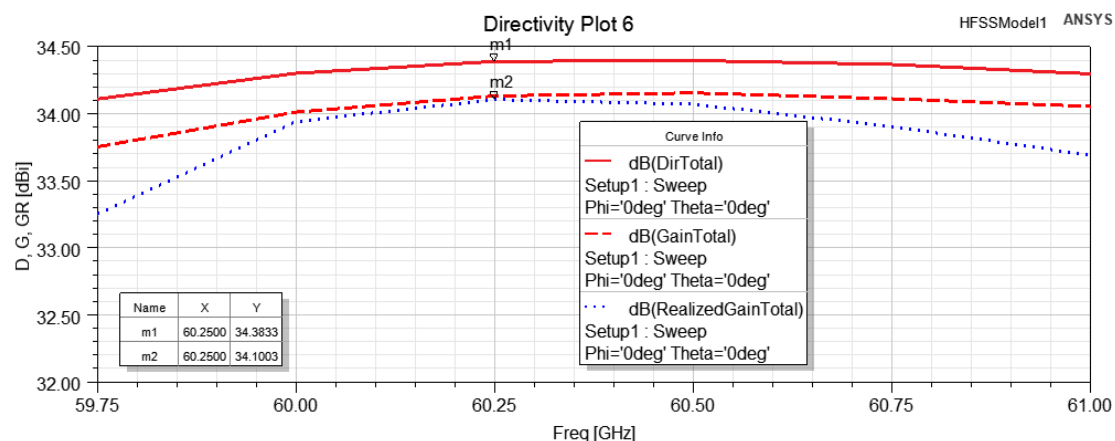


Рис. 3. Частотные характеристики КНД и КУ

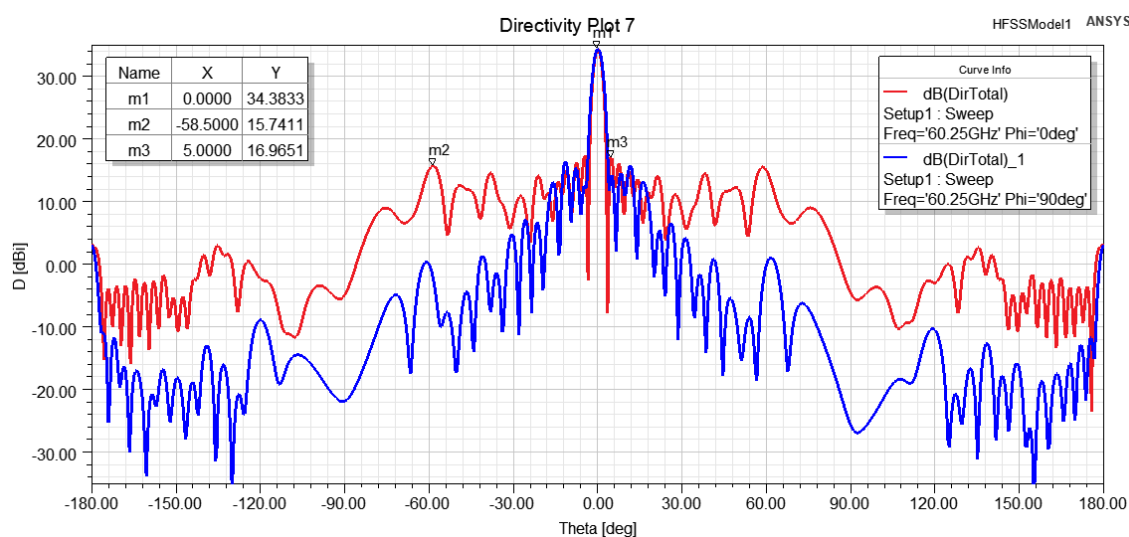


Рис. 4. ДН антенны в Е- и Н-плоскостях на частоте 60,25 ГГц

Для большей наглядности на рис. 5 показана пространственная ДН новой антенны в сферической системе координат в виде зависимости КНД от направления на частоте 60,25 ГГц.

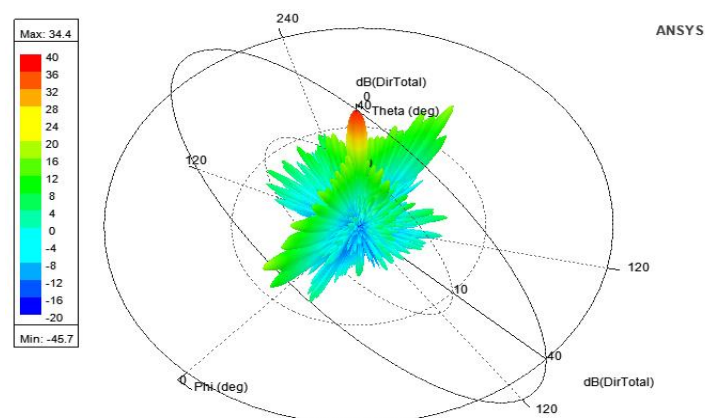


Рис. 5. Пространственная ДН на частоте 60,25 ГГц

Как видно из представленных на рис. 2 и 3 характеристик, в полосе частот 60—61 ГГц значения КСВ на входе антенны не превышают 2, причем в полосе 60—60,5 ГГц $\text{КСВ} \leq 1,32$; максимальный реализуемый КУ составил 34,1 дБ на частоте 60,25 ГГц, причем в полосе 59,75—60,75 ГГц КУ превышает 33,25 дБ.

Анализ ДН антенны в полосе частот 59,75—60,75 ГГц показал, что ее ширина по уровню -3 дБ в Е- и Н-плоскостях составляет 3 градуса, УБЛ в полосе частот 60—60,5 ГГц не превышает -17 дБ, в частности, на частоте 60,25 ГГц (рис. 4) составляет $-17,3$ дБ, что выгодно отличает данную антенну от многих известных плоских антенных решеток диапазона КВЧ, включая упомянутые выше.

Рассчитанное значение эффективности излучения антенны — произведения КПД и коэффициента использования поверхности, иными словами, отношения реализуемого КУ (34,1 дБ или 2570 в безразмерном выражении к максимально возможному КНД 36,1 дБ или 4100 в безразмерном выражении, рассчитанному для антенны с раскрытием такой же площади, но при КПД = 1 и КИП = 1) на частоте 60,25 ГГц составило 0,627, т. е. 62,7%. В полосе частот 60—60,5 ГГц эффективность излучения антенны оказывается не менее 61,7%, что также выгодно отличает новую ПАВВ от многих плоских МПАР.

Стоит отметить, что, судя по форме ДН, есть резерв увеличения КНД и, соответственно, КУ антенны до 34,5—35 дБ, а также дальнейшего снижения УБЛ ДН.

В отношении практического использования новой антенны возможны следующие варианты построения РРС и работы соответствующей РРЛ (радиомоста):

1. С одной антенной линейной поляризации (например, вертикальной), работа на передачу и прием ведется на одной частоте.
2. С двумя аналогичными антеннами линейной поляризации, размещенными в одной плоскости, при этом каждая антенна рассчитана на заданную полосу частот, работа на передачу и прием ведется на соответственно разнесенных частотах.
3. С двумя одинаковыми антеннами линейной поляризации, размещенными в одной плоскости, но развернутыми друг относительно друга на 90 градусов, так что работа ведется с ортогональными линейными поляризациями на одной частоте передачи и приема.
4. С двумя аналогичными антеннами линейной поляризации, размещенными в одной плоскости, но рассчитанными на различные полосы частот и развернутыми друг относительно друга на 90 градусов, так что работа на передачу и прием ведется с ортогональными линейными поляризациями на соответственно разнесенных частотах.

Выбор того или другого варианта зависит от требований к тактико-техническим характеристикам конкретной системы связи.

Учитывая, что полоса рабочих частот антенны, ограниченная качеством согласования и формы ДН, а также КУ $\geq 33,5$ дБ, превышает 500 МГц и в принципе достаточна для высокоскоростной передачи информации по РРЛ и радиомостам, полученные результаты позволяют сделать вывод о том, что разработанная антенна представляется перспективной альтернативой известным плоским антеннам в плане использования в аппаратуре помехозащищенных систем радиосвязи прямой видимости диапазона КВЧ и, в частности, диапазона 60 ГГц.

ЛИТЕРАТУРА

1. Организация радиосвязи в органах внутренних дел : учеб. пособие / О. И. Боква [и др.]. — Воронеж : Воронежский институт МВД России, 2016. — 106 с.

2. Кузнецов А. В. Многофункциональные унифицированные комплексы антенн для аппаратуры спецтехники и связи диапазона крайне высоких частот : дис. ... канд. техн. наук. — Воронеж : 2019. — 154 с.
3. Вишневский В., Фролов С., Шахнович И. Радиорелейные линии связи в миллиметровом диапазоне: новые горизонты скоростей // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. — 2010. — № 3. — С. 70—79.
4. Вишневский В. Миллиметровый диапазон как промышленная реальность // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. — 2011. — № 1. — С. 90—97.
5. Канавин С. В., Климов А. И. Радиорелейные и спутниковые системы передачи : учебное пособие. — Воронеж : Воронежский институт МВД России, 2016. — 230 с.
6. Bains A. S. An Overview of Millimeter Wave Communications for Military Applications // Defence Science Journal. — 1993. — Vol. 43. — No. 1. — P. 27—36.
7. Cotton Simon L., Scanlon William G. Millimeter-Wave Soldier-to-Soldier Communications for Covert Battle-field Operations // IEEE Communications Magazine. — 2009. — October. — P. 72—81.
8. Беспроводные системы связи. — URL: <http://dokltd.ru/products>
9. 60 GHz Millimeter Wave Wireless Communications Module. — URL: <https://mmwavetech.fujikura.jp/>
10. Radio bridge airFiber 60 HD. — URL: <https://ubiquiti.ru/airfiber-60-hd.html>
11. Radio bridge nRAYG-60adpair. — URL: https://mikrotik.su/product/mikrotik_nray_60g/
12. Климов А. И., Ерошенко Д. А. Методические рекомендации по проектированию однослойной плоской антенны вытекающей волны для радиоволновых двухпозиционных извещателей СВЧ и КВЧ диапазонов. — Воронеж : Воронежский институт МВД России, 2014. — 31 с.
13. Климов А. И., Никулин С. С. Полосковые антенные решетки СВЧ с высоким коэффициентом усиления : методические рекомендации. — Воронеж : Воронежский институт МВД России, 2025. — 67 с.
14. Об использовании радиоэлектронными средствами фиксированной службы полосы радиочастот 58,25—63,25 ГГц : решение ГКРЧ при Министерстве информационных технологий и связи Российской Федерации от 20 декабря 2011 года № 11-13-06-1.
15. Радиомост PPC-1000. — URL: <https://dokltd.ru/products/>
16. Твердотельные устройства СВЧ в технике связи / Л. Г. Гассанов [и др.]. — М. : Радио и связь, 1988. — 288 с.
17. Design and Fabrication of a High-Gain 60-GHz Corrugated Slot Antenna Ar-ray With Ridge Gap Waveguide Distribution Layer / D. Zarifi, A. Farahbakhsh, A. U. Zaman and P. -S. Kildal // IEEE Transactions on Antennas and Propagation. — 2016. — V. 64. — № 7. — P. 2905—2913. — Doi: 10.1109/TAP.2016.2565682.
18. Anim K., Lee J.-N., Jung Y.-B. High-Gain Millimeter-Wave Patch Array Antenna for Unmanned Aerial Vehicle Application // Sensors. — 2021. — № 21. — P. 3914. — URL : <https://doi.org/10.3390/s21113914>
19. Cheng Y., Guo Yong-xin, Guo Zhen. W-Band Large-Scale High-Gain Planar Integrated Antenna Array // IEEE Transactions on Antennas and Propagation. — 2014. — Vol. 62, I. 6. — P. 3370—3373.
20. Ерошенко Д. А., Галуза М. А., Климов А. И. Плоская антенна СВЧ с высоким коэффициентом усиления и низким уровнем боковых лепестков диаграммы направленности // Вестник Воронежского института МВД России. — 2022. — № 4. — С. 124—133.

21. Юдин В. И. Техническая электродинамика. Свободные электромагнитные волны : учеб. пособие. — Воронеж : ВПИ, 1988. — 159 с.

22. Климов А. И. Антенно-фидерные устройства : учеб. пособие. — Воронеж : Воронежский институт МВД России, 2012. — 260 с.

REFERENCES

1. Organizaciya radiosvyazi v organax vnutrennix del : ucheb. posobie / O. I. Bokova [i dr.]. — Voronezh : Voronezhskij institut MVD Rossii, 2016. — 106 s.

2. Kuznecov A. V. Mnogofunkcional'ny'e unificirovanny'e komplekсы` antenн dlya apparatury` specztekhniki i svyazi diapazona krajne vy`sokix chastot : dis. ... kand. texn. nauk. — Voronezh : 2019. — 154 s.

3. Vishnevskij V., Frolov S., Shaxnovich I. Radiorelejny`e linii svyazi v millimetrovom diapazone: novy`e gorizonty` skorostej // E`LEKTRONIKA: Nauka, Tekhnologiya, Biznes. — 2010. — № 3. — S. 70—79.

4. Vishnevskij V. Millimetrovy`j diapazon kak promy`shlennaya real`nost` // E`LEKTRONIKA: Nauka, Tekhnologiya, Biznes. — 2011. — № 1. — S. 90—97.

5. Kanavin S. V., Klimov A. I. Radiorelejny`e i sputnikovy`e sistemy` peredachi : uchebnoe posobie. — Voronezh : Voronezhskij institut MVD Rossii, 2016. — 230 s.

6. Bains A. S. An Overview of Millimeter Wave Communications for Military Applications // Defence Science Journal. — 1993. — Vol. 43. — No. 1. — P. 27—36.

7. Cotton Simon L., Scanlon William G. Millimeter-Wave Soldier-to-Soldier Communications for Covert Battle-field Operations // IEEE Communications Magazine. — 2009. — October. — P. 72—81.

8. Besprovodny`e sistemy` svyazi. — URL: <http://dokltd.ru/products>

9. 60 GHz Millimeter Wave Wireless Communications Module. — URL: <https://mmwa-vetech.fujikura.jp/>

10. Radio bridge airFiber 60 HD. — URL: <https://ubiquiti.ru/airfiber-60-hd.html>

11. Radio bridge nRAYG-60adpair. — URL: https://mikrotik.su/product/mikrotik_nray_60g/

12. Klimov A. I., Eroshenko D. A. Metodicheskie rekomendacii po proektirovaniyu odnoslojnoj ploskoj antenny` vy`tekayushhej volny` dlya radiovolnovy`x dvuxpozicionny`x izveshhatelej SVCh i KVCh diapazonov. — Voronezh : Voronezhskij institut MVD Rossii, 2014. — 31 s.

13. Klimov A. I., Nikulin S. S. Poloskovy`e antenny`e reshetki SVCh s vy`sokim koef`ficientom usileniya : metodicheskie rekomendacii. — Voronezh : Voronezhskij institut MVD Rossii, 2025. — 67 s.

14. Ob ispol`zovanii radioe`lektronny`mi sredstvami fiksirovannoj sluzhby` polosy` radiochastot 58,25—63,25 GGcz : reshenie GKRC h pri Ministerstve informacionny`x tekhnologij i svyazi Rossijskoj Federacii ot 20 dekabrya 2011 goda № 11-13-06-1.

15. Radiomost RRS-1000. — URL: [https:// dokltd.ru/products/](https://dokltd.ru/products/)

16. Tverdotel`ny`e ustrojstva SVCh v tekhnike svyazi / L. G. Gassanov [i dr.]. — M. : Radio i svyaz`, 1988. — 288 s.

17. Design and Fabrication of a High-Gain 60-GHz Corrugated Slot Antenna Ar-ray With Ridge Gap Waveguide Distribution Layer / D. Zarifi, A. Farahbakhsh, A. U. Zaman and P. -S. Kildal // IEEE Transactions on Antennas and Propagation. — 2016. — V. 64. — № 7. — P. 2905—2913. — Doi: 10.1109/TAP.2016.2565682.

18. Anim K., Lee J.-N., Jung Y.-B. High-Gain Millimeter-Wave Patch Array Antenna for Unmanned Aerial Vehicle Application // Sensors. — 2021. — № 21. — P. 3914. — URL : <https://doi.org/10.3390/s21113914>

19. Cheng Y., Guo Yong-xin, Guo Zhen. W-Band Large-Scale High-Gain Planar Integrated Antenna Array // IEEE Transactions on Antennas and Propagation. — 2014. — Vol. 62, I. 6. — P. 3370—3373.

20. Eroshenko D. A., Galuza M. A., Klimov A. I. Ploskaya antenna SVCh s vy`sokim koe`fficientom usileniya i nizkim urovnem bokovy`x lepestkov diagrammy` napravlenosti // Vestnik Voronezhskogo instituta MVD Rossii. — 2022. — № 4. — S. 124—133.

21. Yudin V. I. Texnicheskaya e`lektrodinamika. Svobodny`e e`lektromagnitny`e volny` : ucheb. posobie. — Voronezh : VPI, 1988. — 159 s.

22. Klimov A. I. Antenno-fiderny`e ustrojstva : ucheb. posobie. — Voronezh : Voronezhskij institut MVD Rossii, 2012. — 260 s.

СВЕДЕНИЯ ОБ АВТОРАХ

Ерошенко Денис Александрович. Начальник редакторского отделения редакционно-издательского отдела.

Воронежский институт МВД России.

E-mail: den1is_90@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Климов Александр Иванович. Профессор кафедры инфокоммуникационных систем и технологий. Доктор технических наук, профессор.

Воронежский институт МВД России.

E-mail: alexserkos@inbox.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Фомин Никита Евгеньевич. Курсант.

Воронежский институт МВД России.

E-mail: nikitafofmin2003@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Eroshenko Denis Aleksandrovich. Head of the Editorial Department of the Editorial and Publishing Department.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: den1is_90@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Klimov Alexander Ivanovich. Professor of the chair of Infocommunication Systems and Technologies. Doctor of Sciences (Radio Engineering), Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Fomin Nikita Evgen'evich. Cadet.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: nikitafofmin2003@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: полосковая антенная решетка; диапазон КВЧ; радиомост; помехозащищенность; коэффициент усиления; диаграмма направленности.

Key words: strip antenna array; EHF band; radio bridge; noise immunity; gain; radiation pattern.

УДК 621.396.67

С. А. Шерстюков, доктор технических наук, доцент

О. В. Толстых, кандидат технических наук

**АЛГОРИТМЫ И УСТРОЙСТВА
РАДИОЭЛЕКТРОННОГО ПРОТИВОДЕЙСТВИЯ
БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТАМ
С БОРТОВЫМИ АВТОМАТИЧЕСКИМИ
РАДИОПЕЛЕНГАТОРАМИ**

**ALGORITHMS AND DEVICES
FOR RADIOELECTRONIC COUNTERACTION
TO UNMANNED AERIAL VEHICLES
WITH ON-BOARD AUTOMATIC RADIO DIRECTION FINDERS**

Использование для защиты российских гражданских и военных объектов стационарных и мобильных комплексов противодействия беспилотным летательным аппаратам (БПЛА) на сегодняшний день является недостаточной мерой, поскольку сами комплексы, формирующие излучения, становятся целями для ударных БПЛА противника, на которых устанавливаются бортовые автоматические радиопеленгаторы. Представлены алгоритмы конфликтного взаимодействия российского наземного пункта управления БПЛА (российского наземного комплекса радиоэлектронного подавления) и украинского ударного БПЛА с бортовым автоматическим радиопеленгатором. Для размещения на платформе БПЛА разработана и исследована новая цифровая структурная схема, формирующая уводящие радиоэлектронные помехи на основе линейно-частотной модуляции шума.

Практическая реализация новых результатов позволит повысить качество радиоэлектронных шумовых помех, надежность радиоэлектронного подавления и изменить тактику противодействия БПЛА противника.

The use of stationary and mobile unmanned aerial vehicle (UAV) countermeasure systems for protecting Russian civilian and military facilities is currently an insufficient measure, since the systems themselves that generate the emissions become targets for enemy attack UAVs, which are equipped with onboard automatic radio direction finders. Algorithms for conflict interaction between a Russian UAV ground control post (a Russian ground-based electronic countermeasure system) and a Ukrainian attack UAV with an onboard automatic radio direction finder are presented. A new digital structural circuit that generates diverting electronic interference based on linear-frequency noise modulation has been developed and studied for placement on the UAV platform.

Practical implementation of the new results will improve the quality of electronic noise interference, the reliability of electronic suppression, and will change the tactics of countering enemy UAVs.

С целью изменения тактики противодействия БПЛА противника и повышения качества радиоэлектронных шумовых помех в статье решены следующие задачи: разработаны алгоритмы конфликтного взаимодействия российского наземного пункта управления БПЛА (и российского наземного комплекса радиоэлектронного подавления) и украинского ударного БПЛА с бортовым автоматическим радиопеленгатором; для размещения на платформе БПЛА разработана и исследована новая цифровая структурная схема, формирующая уводящие радиоэлектронные помехи на основе линейно-частотной модуляции шума.

Из анализа радиоэлектронного оборудования, использующегося в условиях проведения специальной военной операции (СВО), следует, что для прикрытия военных объектов и расположений личного состава от ударных и разведывательных беспилотных летательных аппаратов (БПЛА) противника в тактическом звене управления (до 30 км от линии боевого соприкосновения (ЛБС)) в основном используются относительно недорогие по стоимости отечественные и китайские комплексы противодействия БПЛА («окопный РЭБ»), состоящие из модулей обнаружения (МО) и модулей радиоэлектронного воздействия (МРВ) на БПЛА. С помощью МО (радиопеленгаторов) проводится радиомониторинг окружающего пространства в районе дислокации защищаемого объекта с целью обнаружения источников радиоизлучений (ИРИ), определения направления на ИРИ, пространственной селекции сигналов ИРИ, оценки основных параметров радиосигналов, излучаемых БПЛА, и других функций. В состав мобильных радиопеленгаторов, как правило, входят: блоки обнаружения сигналов каналов управления и передачи данных, треноги для размещения оборудования, комплекты антенн (направленных и всенаправленных), блоки питания, технологические автоматизированные рабочие места.

С помощью мобильных МРВ осуществляют противодействие БПЛА ближнего радиуса действия путем формирования шумовых радиоэлектронных помех (ШРП) и воздействия ими на каналы управления БПЛА и бортовые радиоприемники сигналов глобальных навигационных спутниковых систем (ГНСС) (GPS, Глонасс, Galileo, Beidou). Мобильные МРВ в основном отличаются друг от друга количеством одновременно формируемых ШРП на каналы управления и на приемники ГНСС, временем непрерывной работы комплексов от аккумуляторных батарей (АКБ), массой АКБ, мощностью излучений и другими параметрами. МРВ конструктивно изготавливаются в виде антидроновых ружей, радиопередатчиков с набором всенаправленных антенн, помеховых радиопередатчиков с антеннами с диаграммами направленности купольной формы и др. Для противодействия БПЛА также применяются комплексы кинетического поражения БПЛА и перехватчики БПЛА.

Общим недостатком указанных выше бюджетных систем противодействия является то, что они формируют помеховые радиосигналы, в основном, в стандартных, заранее известных диапазонах рабочих частот (ДРЧ) работы коммерческих БПЛА. При функционировании БПЛА противника на нестандартных полосах частот МРВ оказываются неэффективными. Кроме того, в силу статического положения МРВ существует опасность определения их местоположения радиопеленгаторами противника по излучаемым помеховым радиосигналам.

В основу технических мероприятий РЭП БПЛА военными профессиональными системами входят: постановка радиопомех системам управления и навигации, перехват разведывательной информации, противодействие средствам наблюдения и распознавания, установленным на БПЛА. На вооружении подразделений РЭБ стоят станции помех РП-377УВМ1Л «Лесочек» (рис. 1), Р-330Ж «Житель», Р-934БМВ или «Палантин-У»

(рис. 2), комплексы «Поле-21» (Поле-21 М) (рис. 3), «Силок-01» («Силок-02») (рис. 4), противодроновые ружья ЛПД-801 (ЛПД-802) и другие радиосредства.



Рис. 1. Размещение станции помех «Лесочек» на капоте автомобиля



Рис. 2. Комплекс РЭБ Р-934БМВ («Палантин-У»)



Рис. 3. Средства комплекса «Поле-21»: стойка с аппаратурой (слева), антенные модули (справа сверху) и пульт управления (справа внизу)



Рис. 4. Развертывание комплекса «Силок-01»

Вышеуказанные станции и комплексы помех в целях защиты личного состава и военных объектов в различных режимах работы осуществляют обнаружение и РЭП каналов управления и передачи данных с БПЛА (обратных каналов передачи данных и телеметрии с БПЛА) на разных расстояниях (от нескольких сотен метров до нескольких десятков километров) путем постановки прицельных по частоте и заградительных в заданных азимутальных секторах помех по главным и боковым лепесткам диаграмм направленности антенн БПЛА и наземных пунктов управления (НПУ), а также наземных терминалов потребителей информации.

Основными недостатками военных стационарных комплексов помех являются: малая мобильность и высокая радиозаметность в электромагнитном спектре. В связи с

этим после радиоэлектронного воздействия на средства противника, комплексы РЭБ должны оперативно проводить смену позиций, чтобы не попасть под ответное огневое поражение по результатам радиоэлектронной разведки (РЭР) противника.

С целью выявления и поражения российских НПУ БПЛА и модулей радиоэлектронного воздействия на БПЛА в настоящее время противником стали активно применяться ударные FPV-дроны со встроенными радиопеленгаторами, в состав которых входят комплекты направленных антенн и модули автоматического определения пеленгов на ИРИ. На рис. 5 показан снимок с экрана украинского пульта управления FPV-дроном с автоматическим модулем радиопеленгации ИРИ.

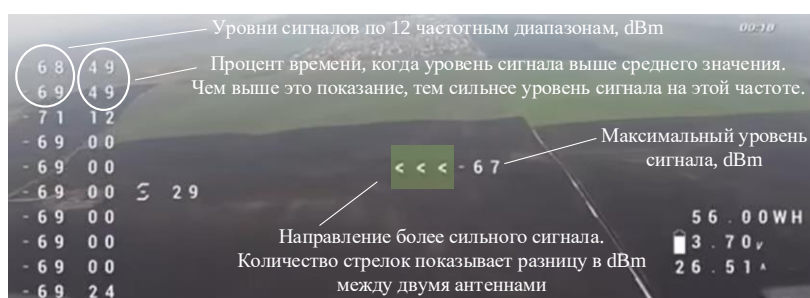


Рис. 5. Снимок с экрана украинского пульта управления FPV-дроном с автоматическим модулем радиопеленгации

На рис. 5 по центру экрана в заданной полосе частот в реальном режиме времени отображаются максимальные уровни сигналов, выраженные в dBm. Рядом с числовыми значениями показан индикатор, указывающий на направление более сильного (приоритетного) радиосигнала. С левой стороны экрана указаны значения уровней сигналов (в dBm) по 12 частотным диапазонам и процент времени, в течение которого уровень принимаемого радиосигнала находится выше среднего значения. Из анализа режимов работы бортового автоматического радиопеленгатора (БАРП) следует, что на выходе решающего устройства модуля автоматического определения пеленгов на ИРИ формируется управляющее напряжение, поступающее на полетный контроллер (ПК), который подстраивает траекторию движения БПЛА в направлении приоритетного ИРИ.

На рис. 6 для примера показан внешний вид отечественного БПЛА с БАРП и комплектом антенн в радиопрозрачном боксе.



Рис. 6. Внешний вид отечественного БПЛА с БАРП

Для выработки решений по защите объектов от поражения ударными украинскими БПЛА с бортовой системой самонаведения рассмотрим алгоритмы конфликтного взаимодействия российского наземного комплекса РЭП (РНК РЭП) и/или НПУ БПЛА с украинским ударным (УкУ) БПЛА, оснащенным БАРП ИРИ (рис. 7).

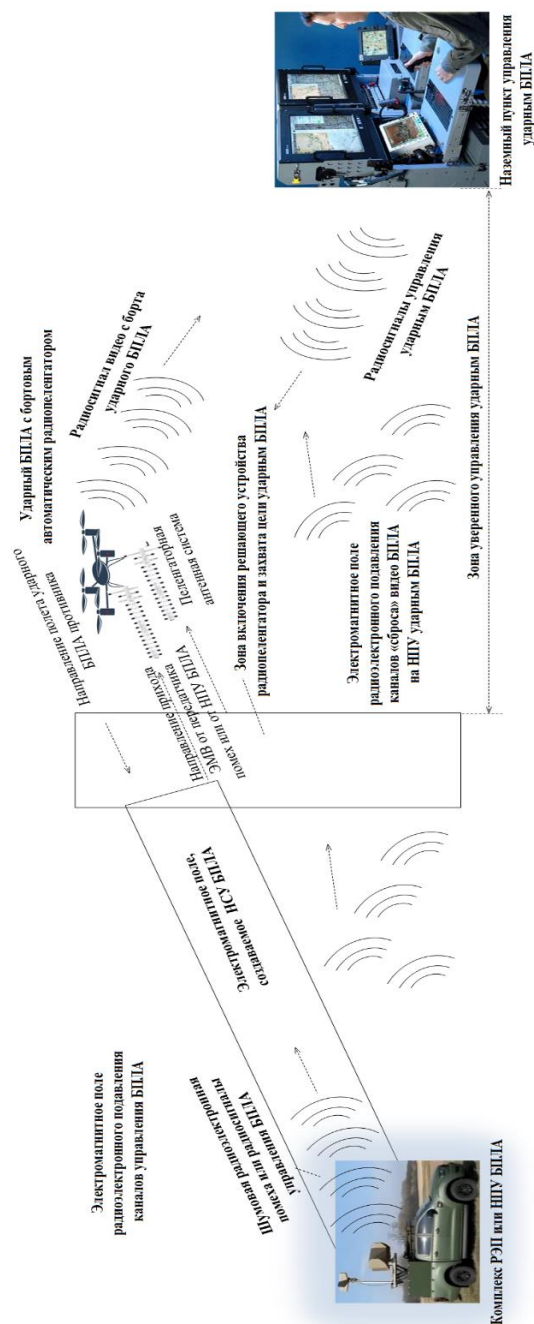


Рис. 7. Алгоритм конфликтного взаимодействия РНК РЭП и/или НПУ БПЛА с УкУ БПЛА

1. Алгоритм конфликтного взаимодействия российского НПУ БПЛА и УкУ БПЛА с БАРП

1.1. Российский НПУ БПЛА передает радиосигналы управления и принимает радиосигналы видеоизображения с курсовой видеокамеры БПЛА.

1.2. УкУ БПЛА, двигаясь в сторону предполагаемого излучения, принимает и обрабатывает с помощью БАРП радиосигналы управления с российского НПУ, одновременно принимает радиосигналы управления со своего НПУ и передает на свой НПУ радиосигналы видеоизображения с курсовой видеокамеры. БАРП УкУ БПЛА выполняет непрерывное сканирование в заданном радиочастотном диапазоне, помогая оператору УкУ БПЛА визуально определить наземную цель.

1.3. БАРП УкУ БПЛА в соответствии с заданным алгоритмом принимает радиосигнал управления от российского НПУ, определяет его как приоритетный сигнал, записывает параметры радиосигнала в оперативное запоминающее устройство (ОЗУ) и формирует напряжение управления для ПК БПЛА, который, в свою очередь, корректирует работу двигателей для направления движения БПЛА на ИРИ. Оператор управления УкУ БПЛА по радиоканалу передачи видео в процессе выполнения визуального контроля в оптическом диапазоне обнаруживает наземную цель (российский НПУ) и наводит на неё ударный БПЛА.

2. Алгоритм конфликтного взаимодействия РНК РЭП и УкУ БПЛА с БАРП

2.1. РНК РЭП излучает шумовые радиоэлектронные помехи в заданном диапазоне рабочих частот, подавляя радиоканалы управления, телеметрии, спутниковых навигационных систем и радиоканалы «сброса» видео с украинских БПЛА на НПУ.

2.2. УкУ БПЛА с БАРП, двигаясь в сторону предполагаемого излучения, постоянно находится в «слабом» электромагнитном поле, создаваемым РНК РЭП, принимает радиосигналы управления с украинского НПУ и одновременно передает на украинский НПУ радиосигналы видеоизображения с курсовой видеокамеры. БАРП выполняет непрерывное сканирование в заданном радиочастотном диапазоне, принимает помеховые радиосигналы от РНК РЭП, постепенно уводит ударный БПЛА в сторону излучения РНК РЭП, приближаясь к зоне «сильного» электромагнитного поля, создаваемого РНК РЭП.

2.3. В зоне «сильного» электромагнитного поля, создаваемого РНК РЭП, БАРП УкУ БПЛА, приняв и обработав самый высокий по уровню мощности помеховый радиосигнал, определяет его как приоритетный сигнал, записывает параметры радиосигнала в ОЗУ и формирует напряжение управления для ПК БПЛА, который, в свою очередь, корректирует работу двигателей для направления движения БПЛА на помеховый ИРИ. По мере продвижения УкУ БПЛА в зоне «сильного» электромагнитного поля, создаваемого РНК РЭП, соотношения «сигнал/шум» на входе радиоприемных устройств УкУ БПЛА и НПУ изменяются в пользу шума, в результате оператор украинского НПУ полностью теряет визуальный контроль и радиочастотное управление БПЛА.

2.4. В режиме полного отсутствия управления с НПУ УкУ БПЛА автоматически продолжает движение в направлении ИРИ, используя в качестве ориентира приоритетный помеховый радиосигнал, создаваемый РНК РЭП. По мере приближения УкУ БПЛА к источнику помехового радиосигнала на входе БАРП уровень сигнала увеличивается, повышая точность наведения УкУ БПЛА на наземную цель.

2.5. В случае выключения питания РНК РЭП при визуальном обнаружении приближения УкУ БПЛА вероятность поражения объекта, прикрываемого комплексом РЭП, остается высокой в силу высокой скорости полета УкУ БПЛА.

2.6. Постановка дополнительных заградительных и узкополосных шумовых помех повышенной мощности на каналы управления и каналы «сброса» видео УкУ с БАРП по результатам визуального обнаружения не решает проблему защиты объекта, прикрываемого РНК РЭП, по причине высокой скорости полета УкУ БПЛА, а также инерционности процесса вычисления пеленгов на ИРИ системой БАРП и формирования управляющих напряжений ПК БПЛА.

Таким образом, в данном случае воздействие ШРП на каналы видео, управления УкУ БПЛА и его бортовые радиоприемники сигналов ГНСС не решает задачу защиты объектов от поражения УкУ БПЛА, в связи с чем для защиты объектов от поражения ударными украинскими БПЛА с бортовой системой самонаведения в работе одновременно с РНК РЭП предлагается использование станции РЭП на базе БПЛА длительного применения с привязным питанием и управлением (рис. 8), формирует уводящие ШРП.

В состав структурной схемы на рис. 8 входят следующие функциональные блоки:

1) многофункциональная привязная высотная платформа длительного применения на базе БПЛА коптерного типа, оснащенного:

- широкодиапазонным возбудителем (ВО) ШРП;
- направленной антенной системой для работы передающей аппаратуры;
- оборудованием управления полетом;
- бортовой непрерывной системой видеонавигации;
- резервным аккумуляторным блоком;
- бортовым преобразователем напряжения;
- курсовой видеокамерой;
- подвесом видеокамеры;
- контроллером натяжения кабеля питания и управления;
- радиопередатчиком видеоизображения;

2) система привязного электропитания БПЛА, состоящая из: первичного источника питания, преобразователя напряжения, контроллера подачи питания, автоматической кабельной лебедки, блока управления катушкой лебедки;

4) широкодиапазонное сканирующее радиоприемное устройство;

5) автоматический диапазонный радиопеленгатор с комплектом антенн.

Принцип действия функциональной схемы заключается в следующем. БПЛА с установленным радиооборудованием и закрепленными направленными антенными системами за счет штатного аккумуляторного блока *на начальном этапе* поднимается оператором на высоту от 5 до 10 метров относительно земной поверхности, фиксируется в точке зависания с помощью бортовой системы позиционирования. Направленная антенная система (3 директорные антенны: 1 — расположена в горизонтальной плоскости; 2 — расположена под углом 45^0 вверх, 3 — расположена под углом 45^0 вниз) ориентируется в направлении возможного появления БПЛА противника за счет изменения положения коптера в азимутальном секторе. После окончания процедуры фиксации положения коптера (через 1-2 минуты) с наземного источника питания (НИП) по кабелю питания подается постоянное напряжение. Бортовая непрерывная система видеонавигации (БНСВН), основанная на ана-

лизе относительного смещения соседних кадров, обеспечивает точность определения положения БПЛА в пространстве над неизвестной местностью. После подачи напряжения с НИП и установления штатных режимов работы навесного радиооборудования коптер в соответствии с полетным алгоритмом, начинает медленно, со скоростью 1 метр в секунду, выполнять плавные боковые пролеты (10 метров влево, затем 10 метров вправо относительно исходной точки зависания). Выполнение указанного алгоритма полета необходимо для снижения вероятности обнаружения, физического и радиоэлектронного поражения коптера и оператора управления противником, в том числе при атаках УКУ БПЛА с БАРП.

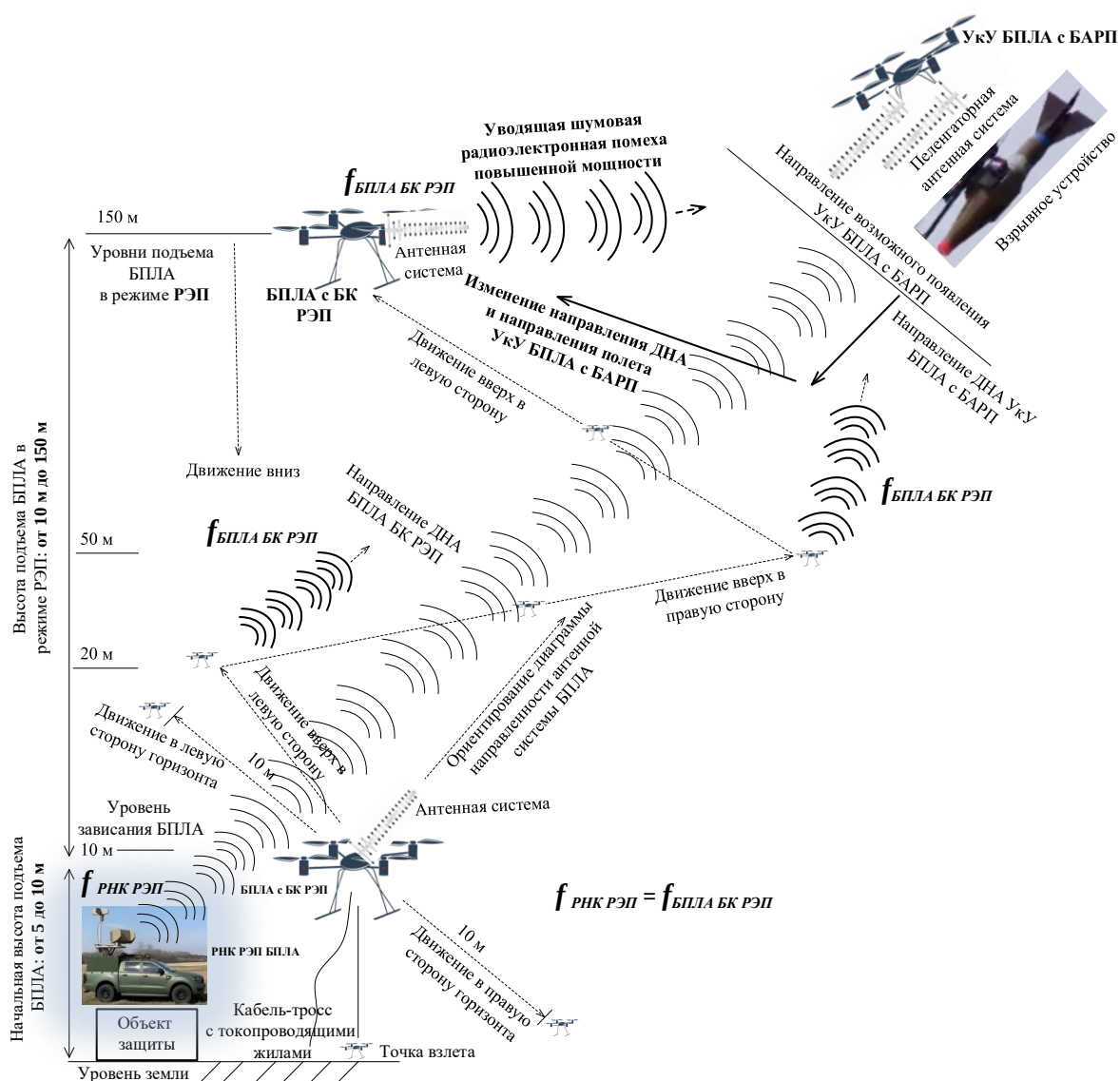


Рис. 8. Алгоритм радиоэлектронного противодействия РНК РЭП и УКУ БПЛА с БАРП

Наземный автоматический радиопеленгатор выполняет панорамный поиск радиоизлучений в круговом азимутальном секторе и в предполагаемом диапазоне рабочих частот (ДРЧ) БПЛА противника. При радиопеленговании сигналы, принимаемые элементами антенной системы, поступают на вход двухканального аналого-цифрового тракта пеленгования радиосигналов, который предназначен для реализации корреляционного интерферометрического пеленгования источников радиоизлучений (ИРИ) и технического анализа их сигналов в процессе пеленгования. В радиоприемном устройстве реализуется преобразование принятых радиосигналов в сигналы промежуточной частоты, их аналого-цифровое преобразование и цифровая фильтрация. Цифровые отсчеты сигнала подвергаются математической обработке с применением модуля интегрального измерителя, реализованного программным способом. Результаты измерений отображаются на экране ноутбука. Определение направления на ИРИ осуществляется в автоматизированном (по команде оператора) или автоматическом режимах (в соответствии с планом радиоконтроля) на основе доплеровского эффекта с отображением пеленга на электронной карте местности и собственной привязкой к географическим координатам.

При обнаружении ИРИ БПЛА противника производится их технический анализ, в результате которого определяются типы и модели БПЛА в соответствии с известной классификацией, и идентифицируются следующие параметры: частоты несущих колебаний; уровни радиосигналов; значения ширины полос частот; коэффициенты амплитудной модуляции; значения девиации частот; виды модуляции. Для цифровой модуляции дополнительно происходит оценка скорости передачи информации и частот манипуляции.

После сохранения параметров в ПЗУ результаты технического контроля в виде последовательного кода передаются по кабелю привязного питания на ВО ШРП, в котором по результатам технического анализа одновременно формируются помеховые радиосигналы для РЭП каналов видео- и телеметрии с бортов БПЛА на наземные пункты управления (НПУ) и сигналы с НПУ, поступающие на входы радиоприемных устройств FPV-дронов. При обнаружении радиопеленгатором нескольких радиосигналов управления одним БПЛА (в разных ДРЧ) возбудитель по командам управления одновременно формирует помеховые сигналы на соответствующих частотах.

Одновременно с результатами технического контроля от радиопеленгатора по кабелю привязного питания на БНСВН передаются команды, в соответствии с которыми БПЛА корректирует свое положение в пространстве, направляя максимумы диаграмм направленности антенн в сторону движения БПЛА противника.

Широкодиапазонный ВО ШРП находится в режиме ожидания команды на формирование помехового радиосигнала (излучение на выходе ВО отсутствует для обеспечения радионезаметности). Радиопередатчик помех выполнен на основе линейно-частотной модуляции шума (ЛЧМШ) (рис. 9) [1].

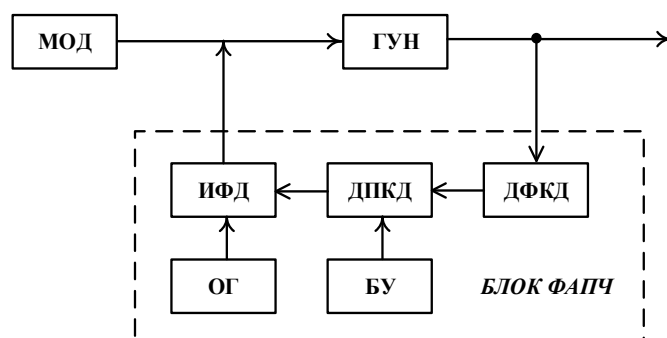


Рис. 9. Блок-схема формирования помехового сигнала на основе ЛЧМШ

Возбудитель состоит из следующих блоков: блока модулятора, блока ГУН, блока ФАПЧ, состоящего из блоков: ДФКД — делителя частоты с фиксированным коэффициентом деления, ДПКД — делителя частоты с переменным коэффициентом деления, ИФД — импульсно-фазового детектора, ОГ — опорного генератора и БУ — блока управления. Центральная частота ВО устанавливается системой ФАПЧ, высокочастотный (ВЧ) сигнал на которую подается с ГУН. Ширина спектра шумового сигнала определяется амплитудой пилообразного сигнала модуляции со случайным периодом следования. Модулирующий сигнал поступает на ГУН с блока модулятора, состоящего из источника шумового сигнала (сформированного шумовым диодом с последующим усилением) и генератора пилообразного напряжения (ГПН), частота которого изменяется по случайному закону. Эти сигналы суммируются в сумматоре и в зависимости от средней частоты модулирующей пилю ЛЧМШ-помеха может вырождаться в свипирующую помеху.

Модулирующий сигнал $m(t)$ представляет собой сумму шумового сигнала $n(t)$ и пилообразного сигнала $p(t)$:

$$m(t) = n(t) + p(t),$$

где $n(t)$ — белый шум с плотностью мощности $S_n(f)$,

$p(t)$ — пилообразный сигнал с амплитудой A_p и случайным периодом T_p .

Высокочастотный сигнал $s(t)$ генерируется ГУН и линейно модулируется сигналом $m(t)$:

$$s(t) = A_c \cos(2\pi f_c t + \varphi(t)),$$

где A_c — амплитуда несущего колебания, f_c — центральная частота колебания,

$\varphi(t)$ — фаза, зависящая от модулирующего сигнала: $\varphi(t) = k_m \int m(t) dt$,

где k_m — коэффициент модуляции.

Этот сигнал представляет собой колебания с высокой частотой f_c , которая медленно изменяется под воздействием интегрированного модулирующего сигнала $\int m(t)dt$.

Из-за пилообразной компоненты $m(t)$ частота $s(t)$ линейно изменяется в течение каждого периода пилообразного сигнала, что создает эффект свипа (линейного изменения частоты). Белый шум добавляет в $m(t)$ случайность к этому свипу. Временной график $s(t)$ представляет собой высокочастотные колебания, где частота медленно изменяется в соответствии с пилообразным сигналом. Эти изменения носят случайный характер из-за наличия шумовой компоненты.

Аналитически ЛЧМШ-сигнал представлен как

$$S_{\text{ЛЧМ}}(t) = A_c \cos(2\pi f_c t + k_m \int [n(t) + p(t) dt]).$$

Плотность спектральной мощности шумового сигнала $n(t)$ равномерна в широком диапазоне частот: $S_n(f) = N_0/2$.

В процессе модуляции шум приводит к расширению спектра несущего колебания.

Спектр пилообразного сигнала $p(t)$ имеет дискретный состав, состоящий из гармоник:

$$p(f) = \sum_{k=1}^{\infty} \frac{A_p}{k\pi} \sin\left(\frac{k\pi}{T_p}\right) e^{-jk\omega_p t}.$$

Спектральный состав содержит отдельные гармоники, расположенные с шагом $1/T_p$ вокруг нулевой частоты.

Описание спектра ЛЧМШ-сигнала, представляющего собой смесь спектров шумового и пилообразного сигналов, модулированных на несущей частоте:

- после модуляции высокочастотного сигнала $s(t)$ сигналом $m(t)$ спектр расширяется;
- энергия радиосигнала сосредоточена по обе стороны от частоты несущего колебания f_c ;
- ширина спектра определяется амплитудой пилообразного сигнала A_p и характеристиками шумового сигнала;
- на временном графике отображается широкополосный спектр, симметричный относительно f_c с более высокими значениями энергии вблизи f_c и постепенным затуханием по мере удаления от f_c .

На рис. 10 *вверху* показан временной вид модулирующего сигнала $m(t)$, состоящего из суммы шумового сигнала $n(t)$ и пилообразного сигнала $p(t)$, а на рис. 10 *внизу* — временной вид высокочастотного сигнала $s(t)$, который генерируется ГУН и линейно модулируется сигналом $m(t)$.

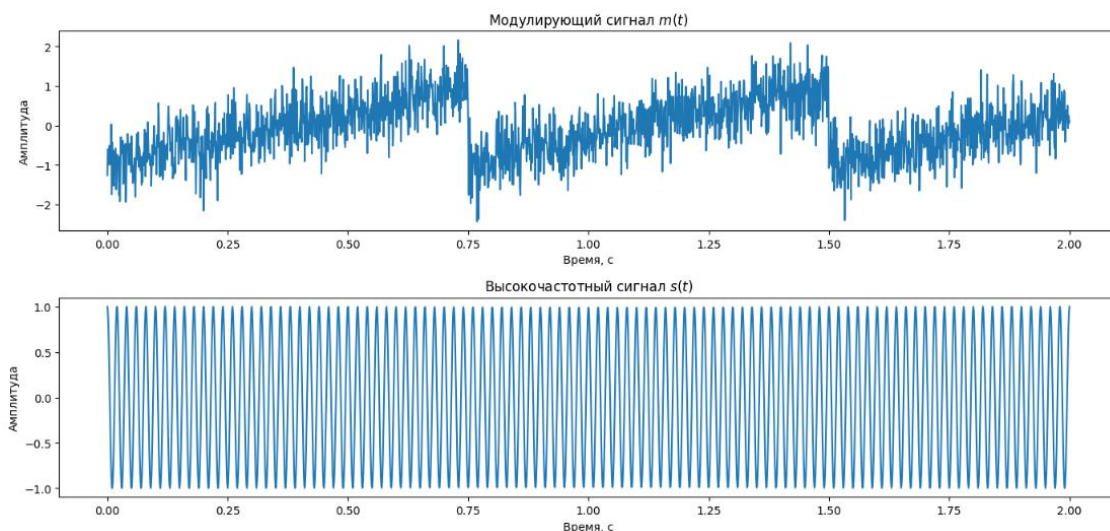


Рис. 10. Временные виды сигналов $m(t)$ и $s(t)$.

На рис. 10 *вверху* наблюдаются хаотичные колебания с периодическими «провалами» (эффект пилообразной модуляции). Очевидно, что частота плавно нарастает, но с

заметными искажениями из-за наличия в схеме аналоговых компонентов. Данные факторы влияют на качество ШРП и приводят к снижению коэффициента РЭП.

Для улучшения качества ЛЧМШ-помехи, формируемой схемой на рис. 9, требуется проведение ее модернизации путем замены на структурную схему, реализованную по SDR-технологии (рис. 11).

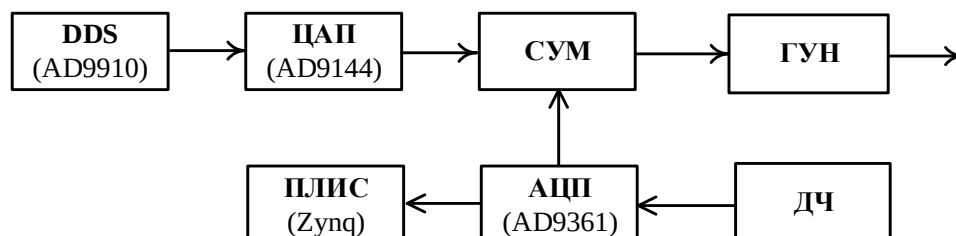


Рис. 11. Модернизированная структурная схема, реализованная по SDR-технологии

В состав модернизированной структурной схемы входят следующие компоненты:

- **DDS** (прямой цифровой синтезатор). Рекомендуемая модель чипа: AD9910 (Analog Devices); частота: до 1 ГГц; разрешение: 14-бит ЦАП. Особенности: встроенный генератор шума, SPI-интерфейс для управления. Альтернативы: микросхема AD9858 (до 200 МГц, 10-бит) — для бюджетных решений, микросхема HMC704 (до 6 ГГц) — для СВЧ-диапазонов;

- **ЦАП** (для шумового сигнала). Рекомендуемая модель чипа: AD9144 (Analog Devices); частота: до 2,8 ГГц; разрешение: 16 бит; интерфейс: JESD204B. Альтернативы: микросхема AD9767 (14 бит, 125 МГц) — для узкополосных систем;

- **ПЛИС** (для PID и цифровой обработки). Рекомендуемая модель чипа: Xilinx Zynq-7020; логика: 85K логических ячеек; ЦПУ: Dual-core ARM Cortex-A9. Особенности: встроенные АЦП/ЦАП-интерфейсы, поддержка VHDL/Verilog. Альтернативы: СБИС Intel Cyclone 10LP — для менее сложных задач;

- **АЦП**. Рекомендуемая модель чипа: AD9361;

- **СУМ** — сумматор;

- **ДЧ** — делитель частоты;

- **ГУН** — генератор, управляемый напряжением.

Данная схема формирует равномерные во временной области радиочастотные колебания без резких провалов в отличие от схемы на рис. 9. Линейное нарастание частоты пилообразного напряжения выглядит визуально гладко (рис. 12). При увеличении частоты ШИМ-модуляции пила до 1 МГц линейное нарастание частоты пила будет выглядеть как ровная «размазанная» синусоида. При этом ширина выходного спектра ЛЧМШ будет увеличиваться пропорционально увеличению частоты ШИМ-модуляции.

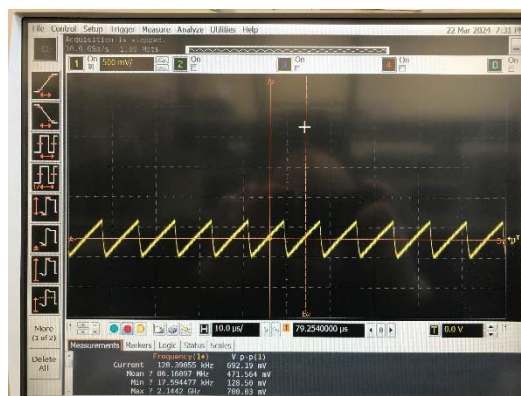


Рис. 12. Линейное нарастание частоты пилообразного напряжения

Замена аналогового шума на цифровой шум с гауссовским распределением осуществляется за счет использования DDS (прямого цифрового синтеза) по формуле

$$n_{\text{цифр}}[n] = \sum_{k=1}^M a_k \sin\left(2\pi \frac{f_k}{f_s} n + \varphi_k\right),$$

где a_k , φ_k — случайные амплитуда и фаза.

python

```
# Генерация цифрового шума (Python)
import numpy as np
fs = 100e6 # Частота дискретизации 100 МГц
noise = np.random.normal(0, 0.1, int(fs * 1e-3)) # Шум длительностью 1 мс
```

ШИМ-модуляция пила реализуется за счет генерации пила ШИМ с обратной связью через таймер MCU (STM32), частота регулируется от 1 кГц до 1 МГц.

Код для STM32:

```
// Настройка ШИМ (HAL)
TIM_HandleTypeDef htim;
htim.Instance = TIM2;
htim.Init.Prescaler = 0;
htim.Init.Period = 1000; // Частота 1 МГц / 1000 = 1 кГц
HAL_TIM_PWM_Start(&htim, TIM_CHANNEL_1);
```

Реализация адаптивной ФАПЧ с PID производится с использованием цифровой ФАПЧ на базе ПЛИС (Xilinx Zynq) с PID-регулятором.

Коэффициенты: $K_p = 0,5$, $K_i = 0,01$, $K_d = 0,001$.

Уравнение PID:

$$\Delta f(t) = k_p \Delta \varphi(t) + k_i \int \Delta \varphi dt + k_d \frac{d\Delta \varphi}{dt}.$$

Реализация на Verilog:

```

verilog

module PID (
    input clk, input signed [15:0] error,
    output reg signed [15:0] control
);
    reg signed [15:0] integral, prev_error;
    always @(posedge clk) begin
        integral <= integral + error;
        control <= (error * 50) + (integral / 100) + ((error - prev_error) / 1000);
        prev_error <= error;
    end
endmodule

```

Сравнение характеристик схемных решений:

Параметр	Аналоговая схема	Цифровая схема
Полоса частот	1–10 МГц	0,1–100 МГц
Стабильность частоты	± 1 кГц	± 10 Гц
Уровень шума	-60 дБ/Гц	-90 дБ/Гц
Время установления	10 мс	0,1 мс

Заключение. Из сравнительных оценок характеристик схемных решений следует, что в аналоговой схеме (рис. 9) ширина полосы выходного спектра регулируется от 1 до 10 МГц, неравномерность составляет ± 3 дБ (из-за аналоговых искажений), а уровень шума достигает высокого значения -60 дБ/Гц.

В цифровой модернизированной схеме (DDS + PID) ширина полосы частот регулируется от 0,1 до 100 МГц (расширена в 10 раз), неравномерность составляет $\pm 0,5$ дБ, а уровень шума равен -90 дБ/Гц (почти нет паразитных гармоник).

В результате применения модернизации аналоговой схемы выходной ЛЧМШ носит стабильный характер, флуктуации амплитуды отсутствуют, при этом точность амплитуды составляет $\pm 0,1\%$ (в отличие от $\pm 5\%$ у аналогового диода), а ширина полосы частот достигает 100 МГц (это значение ограничено только ЦАП), реализация ШИМ-модуляции пила регулируется с точностью до 1 Гц (вместо 100 Гц).

На рис. 13 представлены выходные спектры ЛЧМШ, реализуемые с помощью модернизированной структурной схемы на рис. 11.

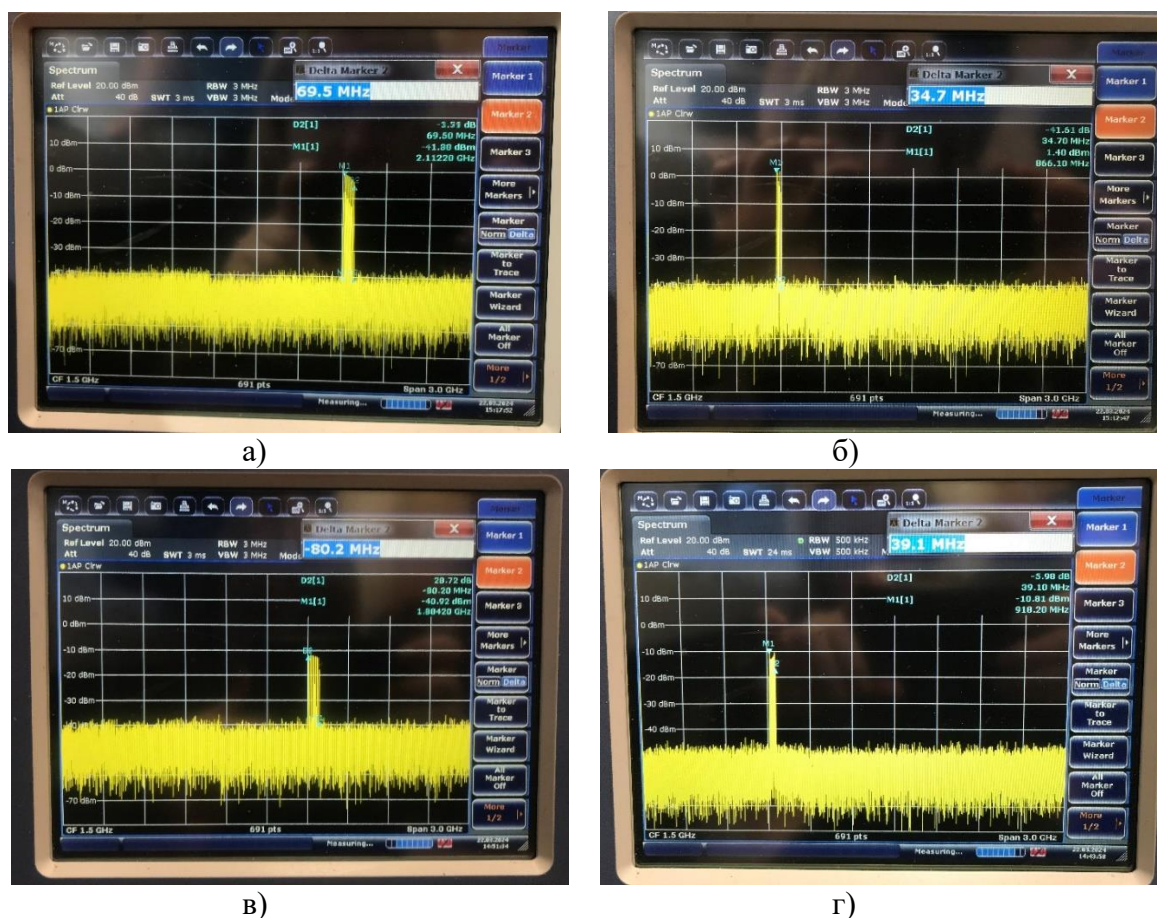


Рис. 13 Выходные спектры ЛЧМШ, формируемые с помощью SDR для РЭП систем: а) – 3G; б) – CDMA; в) – DCS; г) – GSM

Из анализа выходных спектров на рис. 13 следует, что их спектральные маски приближены к прямоугольным (идеальным) формам, свидетельствующим о высоком качестве формирования ЛЧМШ с помощью модернизированной схемы. Для достижения цифровой схемой достаточных для надежного РЭП энергетических показателей на выходе ГУН необходимо (обязательно) реализовывать широкополосные тракты усиления и антенно-фидерные тракты с точки зрения размещения их на БПЛА.

ЛИТЕРАТУРА

1. Пространственные и вероятностно-временные характеристики эффективности станций ответных помех при подавлении систем радиосвязи / В. И. Борисов, В. М. Зинчук, А. Е. Лимарев [и др.] ; под ред. В. И. Борисова. — М. : РадиоСофт, 2008. — 362 с.

REFERENCES

1. Prostranstvenny`e i veroyatnostno-vremenny`e karakteristiki e`ffektivnosti stancij otvetny`x pomex pri podavlenii sistem radiosvyazi / V. I. Borisov, V. M. Zinchuk, A. E. Limarev [i dr.] ; pod red. V. I. Borisova. — M. : RadioSoft, 2008. — 362 s.

СВЕДЕНИЯ ОБ АВТОРЕ

Шерстюков Сергей Анатольевич. Профессор кафедры инфокоммуникационных систем и технологий. Доктор технических наук, доцент.

Воронежский институт МВД России.

E-mail: sherserge@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Толстых Ольга Владимировна. Доцент кафедры радиотехнических систем и комплексов охранного мониторинга. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: tov48@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Sherstyukov Sergey Anatolyevich. Professor of the chair of Infocommunication Systems and Technologies. Doctor of Technical Sciences, Assistant Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: sherserge@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tolstykh Olga Vladimirovna. Associate Professor of the chair of Radio Technical Systems and Security Monitoring Complexes. Candidate of Technical Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: tov48@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: бортовой автоматический радиопеленгатор; шумовая радиоэлектронная помеха; линейно-частотная модуляция шума.

Key words: on-board automatic radio direction finder; noise electronic interference; linear-frequency noise modulation.

УДК 621.396.62

В. И. Калинин, кандидат технических наук
А. Д. Лунёв, кандидат технических наук
А. Г. Чернышов, кандидат технических наук
Д. А. Попов

АЛГОРИТМ СОВМЕСТНОЙ АДАПТАЦИИ ПО МОЩНОСТИ ИЗЛУЧЕНИЯ ПЕРЕДАТЧИКОВ И СКОРОСТИ ПЕРЕДАЧИ СООБЩЕНИЙ В РАДИОЛИНИЯХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

ALGORITHM FOR JOINT ADAPTATION IN TRANSMITTER RADIATION POWER AND MESSAGE TRANSMISSION RATE IN RADIO LINKS SPECIAL PURPOSE

В статье описывается алгоритм совместной автоматической регулировки мощности и скорости передачи сообщений в радиолиниях специального назначения. Особенностью таких радиолиний может являться условие передвижения радиостанции одного или обоих корреспондентов, что говорит о различных статистических свойствах канала в зависимости от состояния объекта. В связи с этим при разработке алгоритма в работе предложено определять пороговые (требуемые) значения отношения сигнал/помеха в зависимости от того, находится радиостанция на стоянке либо в движении.

This article describes an algorithm for joint automatic adjustment of power and transmission speed in radio links. A feature of radio links may be the condition of movement of the radio station of one or both correspondents, which indicates different statistical properties of the channel depending on the state of the object. In this regard, when developing the algorithm in the work, it is proposed to determine the threshold (required) values of the signal/interference ratio depending on whether the radio station is stationary or moving.

Введение. Известно, что радиолиния зачастую может обладать избыточным энергетическим потенциалом за счет превышения уровня сигнала над уровнем помех больше требуемого значения. Этот потенциал можно использовать для улучшения других характеристик радиолинии путем применения в ней автоматического регулирования мощности излучения передатчиков (АРМ) и автоматического регулирования скорости передачи сообщений (АРС).

Характеристики, которые могут быть при этом улучшены:
при применении АРМ:

- снижение энергетических затрат,
- повышение разведзащищенности,
- улучшение электромагнитной совместимости;

при применении АРС:

- повышение своевременности передачи сообщений,
- снижение энергетических затрат,

- повышение разведзащищенности.

При этом АРМ фактически представляет собой адаптацию по мощности, а АРС — по скорости.

Основная часть. Несмотря на то что в коммерческих системах радиосвязи подобные технологии используются уже достаточно давно, в системах радиосвязи специального назначения АРМ и АРС до сих пор не применяется.

Отметим, что решаемая в работе задача применима к дискретным сообщениям, к которым можно отнести сигналы управления и оповещения, подтверждения и донесения по принятым сигналам о выполненных мероприятиях, графические сообщения, данные, видеокадры (стоп-кадры), мультимедийные сообщения.

Подобные задачи решались ранее такими учеными, как В. П. Постюшков, А. Ю. Гужва, А. В. Тихонов, например в работах [1, 2]. Однако в указанных работах задачи по АРС и АРМ решались независимо, отдельно друг от друга. В настоящей работе предлагается алгоритм совместного управления скоростным и энергетическим ресурсами радиолинии специального назначения.

Результатом функционирования предлагаемого алгоритма является обеспечение передачи сообщений в радиолинии с максимально возможной скоростью при минимальных энергетических затратах.

На рис. 1—3 изображена блок-схема алгоритма, использующего совместное автоматическое регулирование мощности излучения передатчиков и автоматическое регулирование скорости передачи сообщений в радиолинии. Опишем его работу, при этом будем считать, что первый служебный сигнал (тестовый) будет передан радиостанцией А, на его основе будет выработан первый управляющий сигнал радиостанцией Б.

В блоке 1 показан ввод всех значений допустимого превышения уровня сигнала над уровнем помехи $z_{\text{доп}}$, ($P_i = 1 \dots I$, $V_n = 1 \dots N$). Эти значения могут быть рассчитаны заранее в зависимости от вида сигнала, модели канала, заданной вероятности ошибки и используемого числа градаций I мощности P_i и градаций N скорости V_n . Соответственно, в системе где эти значения фиксированы, никакого ввода $z_{\text{доп}}$ производиться не будет, а блок 1 в алгоритме будет отсутствовать.

Блок 2 показывает, что алгоритм начинает свою работу при значениях мощности излучения обоих передатчиков радиолинии и скорости передачи сообщений, равных максимальным величинам, $P_i = P_{\text{max}}$; $V_n = V_{\text{max}}$.

В блоке 3 скрыт процесс вхождения в связь двух корреспондентов. Именно в нём должно осуществляться управление ресурсами радиолинии по возмущениям (ИК-управление). В настоящей работе данный процесс подробно не рассматривается.

Для того чтобы определить используемую модель канала, статическую или динамическую, необходимо провести ряд статистических измерений, на основе которых будут проведены расчеты, результаты которых позволят определить тип модели канала. Этому посвящены действия блоков 4—15.

Блок 4 — условный. Если осуществляется передача тест-сигнала радиостанцией А, работа алгоритма переходит к 5-му, а затем 6-му блокам.

В блоке 5 происходит процесс приёма тест-сигнала от радиостанции А радиостанцией Б.

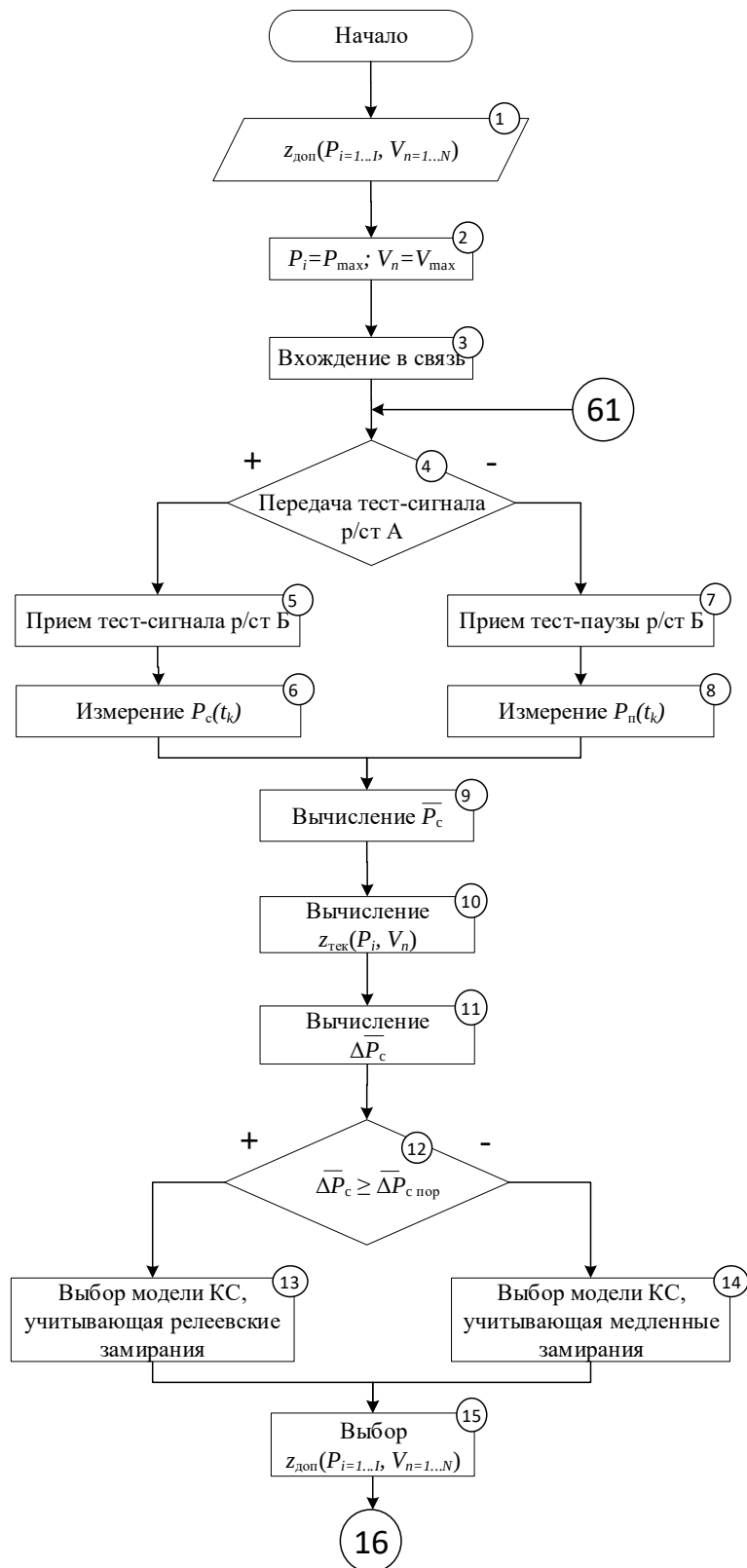


Рис. 1. Блок-схема алгоритма совместного управления энергетическим и скоростным ресурсами радиолинии (начало)

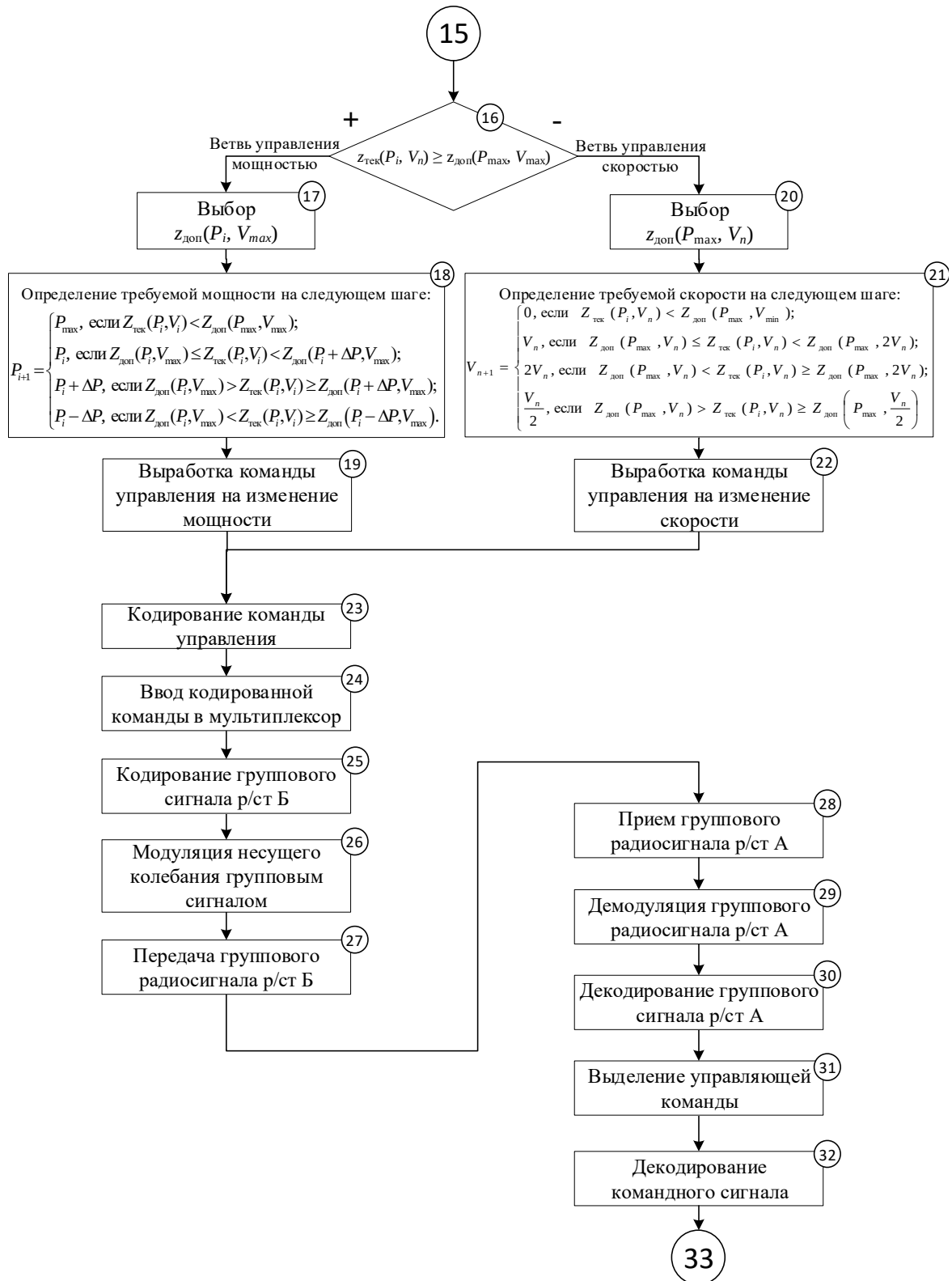


Рис. 2. Блок-схема алгоритма совместного управления энергетическим и скоростным ресурсами радиолинии (продолжение)

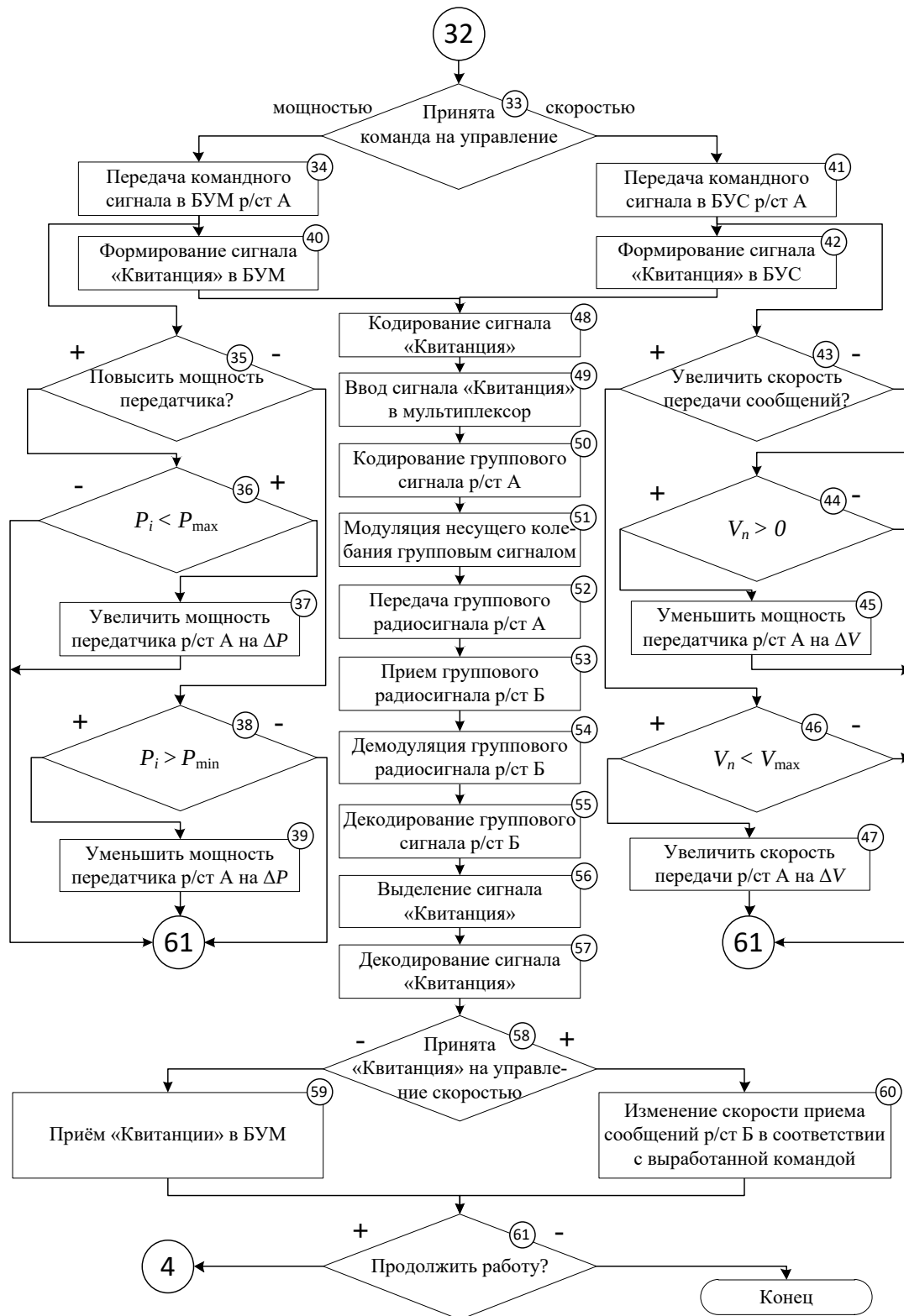


Рис. 3. Блок-схема алгоритма совместного управления энергетическим и скоростным ресурсами радиолинии (окончание)

Затем в блоке 6 измеряется уровень мощности этого сигнала P_c в момент времени t_k . Измерения производятся через интервалы времени $\Delta t \ll T_{\text{изм}}$. Время измерений составляет $T_{\text{изм}}$.

В случае если передача тест-сигнала радиостанцией А не осуществляется, работа алгоритма переходит к 7-му, а затем 8-му блокам.

В блоке 7 происходит процесс приёма тест-паузы радиостанцией Б.

Во время неё в блоке 8 измеряется уровень мощности помех P_n .

В блоке 9 по результатам $k = 1 \dots K$ измерений, произведенных в блоках 5 и 6, вычисляется среднее значение мощности сигнала:

$$\bar{P}_c = \frac{1}{K} \sum_{k=1}^K P_c(t_k).$$

В блоке 10 на основании текущих измерений, произведенных в блоках 5 и 7, вычисляется текущее значение превышения уровня сигнала над уровнем помехи при работе на i -й градации мощности и n -й градации скорости:

$$z_{\text{тек}}(P_i, V_n) = 10 \lg h_{i,n}^2 = 10 \lg h_{\text{тек}}^2 = 10 \lg \left(\frac{P_{ci}(t_k) \cdot \Delta f_c}{P_n \cdot V_n} \right),$$

где Δf_c — ширина спектра сигнала при работе радиолинии на V_n .

В блоке 11 вычисляется изменение мощности сигнала:

$$\Delta \bar{P}_c = \frac{1}{K} \sum_{k=1}^K |P_c(t_k) - \bar{P}_c|.$$

В блоке 12 полученное значение $\Delta \bar{P}_c$ сравнивается с пороговым $\Delta \bar{P}_{c \text{ пор}}$. В случае если выполняется условие $\Delta \bar{P}_c \geq \Delta \bar{P}_{c \text{ пор}}$, алгоритм переходит к блоку 13, в противном случае — к блоку 14.

В блоке 13 осуществляется выбор модели канала связи, учитывающей релеевские замирания, т. е. динамической модели.

В блоке 14 осуществляется выбор модели канала связи, учитывающей только медленные замирания, т. е. статической модели.

В блоке 15, исходя из выбранной модели канала, осуществляется выбор значений $z_{\text{доп}}(P_i = 1 \dots I, V_n = 1 \dots N)$ из множества, определенного в блоке 1.

В блоке 16 происходит сравнение текущего значения $z_{\text{тек}}(P_i, V_n)$, полученного в блоке 10, со значением $z_{\text{доп}}$ из множества, определенного в блоке 15, при котором $P_i = P_{\text{max}}; V_n = V_{\text{max}}$. В случае выполнения условия $z_{\text{тек}}(P_i, V_n) \geq z_{\text{доп}}(P_{\text{max}}, V_{\text{max}})$ алгоритм переходит к ветви управления мощностью (блоки 17-19). В противном случае — к ветви управления скоростью (блоки 20—22).

Здесь следует отметить, что выполнение данного условия означает, что в радиолинии, даже при работе на максимальной скорости, присутствует избыточный энергетический запас, и, соответственно, есть возможность снизить мощность излучения. Но при этом не стоит забывать про требования по достоверности передачи сообщений, что как раз и реализуется в ветви управления мощностью.

Если же $z_{\text{тек}}(P_i V_n) < z_{\text{доп}}(P_{\text{max}} V_{\text{max}})$, то даже на максимальной мощности передача сообщений с заданной достоверностью невозможна. В этом случае обмен сообщениями с заданной достоверностью возможно обеспечить, снизив скорость их передачи. Это объясняется тем, что при снижении скорости элементарной посылке выделяется бóльшая энергетика, что, в свою очередь, обеспечивает повышение помехоустойчивости передачи.

В блоке 17 из множества значений $z_{\text{доп}}(P_i = 1 \dots I, V_n = 1 \dots N)$, определенных в блоке 15, выбираются только те $z_{\text{доп}}(P_i, V_{\text{max}})$, при которых скорость имеет максимальное значение V_{max} .

Блоки 18 и 21 являются ядрами алгоритма, каждый своей ветви управления. Именно в них вырабатывается управляющее решение по соответствующему изменению скорости или мощности.

Итак, в блоке 18 сравнивается текущее значение $z_{\text{тек}}(P_i V_n)$, определенное в блоке 10, со множеством допустимых значений, определенных в блоке 17. Решение о соответствующем изменении уровня мощности принимается согласно условию

$$P_{i+1} = \begin{cases} P_{\text{max}}, & \text{если } Z_{\text{тек}}(P_i, V_i) < Z_{\text{доп}}(P_{\text{max}}, V_{\text{max}}); \\ P_i, & \text{если } Z_{\text{доп}}(P_i, V_{\text{max}}) \leq Z_{\text{тек}}(P_i, V_i) < Z_{\text{доп}}(P_i + \Delta P, V_{\text{max}}); \\ P_i + \Delta P, & \text{если } Z_{\text{доп}}(P_i, V_{\text{max}}) > Z_{\text{тек}}(P_i, V_i) \geq Z_{\text{доп}}(P_i + \Delta P, V_{\text{max}}); \\ P_i - \Delta P, & \text{если } Z_{\text{доп}}(P_i, V_{\text{max}}) < Z_{\text{тек}}(P_i, V_i) \geq Z_{\text{доп}}(P_i - \Delta P, V_{\text{max}}). \end{cases}$$

Таким образом, мощность на следующем шаге управления устанавливается равной максимальному значению в том случае, если текущее отношение сигнал/помеха меньше допустимого при P_{max} .

Мощность на следующем шаге управления остаётся неизменной, если текущее отношение сигнал/помеха больше допустимого при текущем уровне мощности P_i , но меньше допустимого при повышенном на одну дискрету $P_i + \Delta P$.

Мощность на следующем шаге управления повышается на одну дискрету, если текущее отношение сигнал/помеха меньше допустимого при текущем уровне мощности P_i , но больше допустимого при повышенном на одну дискрету $P_i + \Delta P$.

Мощность на следующем шаге управления уменьшается на одну дискрету, если текущее отношение сигнал/помеха больше допустимого при текущем уровне мощности P_i , и больше допустимого при пониженном на одну дискрету $P_i - \Delta P$.

При этом все эти решения принимаются при уровне скорости, жестко установленном на максимуме V_{max} . То есть целесообразность АРМ существует только при условии обеспечения максимальной скорости передачи сообщений.

В блоке 19 формируется команда управления на изменение мощности в соответствии с решением, принятым в блоке 18.

Теперь рассмотрим ветвь управления скоростью.

В блоке 20 из множества значений $z_{\text{доп}}(P_i = 1 \dots I, V_n = 1 \dots N)$, определенных в блоке 15, выбираются только те $z_{\text{доп}}(P_{n_{\text{max}}})$, при которых мощность имеет максимальное значение P_{max} .

В блоке 21 сравнивается текущее значение $z_{\text{тек}}(P_i, V_n)$, определенное в блоке 10, со множеством допустимых значений, определенных в блоке 20. Решение о соответствующем изменении скорости передачи сообщений принимается согласно условию

$$V_{n+1} = \begin{cases} 0, & \text{если } Z_{\text{тек}}(P_i, V_n) < Z_{\text{доп}}(P_{\text{max}}, V_{\text{min}}); \\ V_n, & \text{если } Z_{\text{доп}}(P_{\text{max}}, V_n) \leq Z_{\text{тек}}(P_i, V_n) < Z_{\text{доп}}(P_{\text{max}}, 2V_n); \\ 2V_n, & \text{если } Z_{\text{доп}}(P_{\text{max}}, V_n) < Z_{\text{тек}}(P_i, V_n) \geq Z_{\text{доп}}(P_{\text{max}}, 2V_n); \\ \frac{V_n}{2}, & \text{если } Z_{\text{доп}}(P_{\text{max}}, V_n) > Z_{\text{тек}}(P_i, V_n) \geq Z_{\text{доп}}\left(P_{\text{max}}, \frac{V_n}{2}\right). \end{cases}$$

То есть скорость на следующем шаге управления устанавливается равной нулю в том случае, если текущее отношение сигнал/помеха меньше допустимого при V_{min} . В этом случае фактически передача будет отсутствовать, поскольку сообщение с такими параметрами качества канала принято не будет. В этом есть и плюс, который состоит в том, что в момент наиболее худшего канала не будет излучения радиостанции, что повышает не только разведзащищенность, но и экономию энергии.

Скорость на следующем шаге управления остаётся неизменной, если текущее отношение сигнал/помеха больше допустимого при текущем уровне скорости V_n , но меньше допустимого при повышенном $2V_n$.

Скорость на следующем шаге управления увеличивается в два раза, если текущее отношение сигнал/помеха больше допустимого при текущем уровне скорости V_n и больше допустимого при повышенном $2V_n$.

Скорость на следующем шаге управления снижается в два раза, если текущее отношение сигнал/помеха меньше допустимого при текущем уровне скорости V_n , но больше допустимого при уменьшенном вдвое $V_n / 2$.

При этом все эти решения принимаются при уровне мощности, жестко установленном на максимуме P_{max} . То есть целесообразность АРС существует только тогда, когда даже максимальный уровень мощности не может обеспечить передачу сообщений с требуемой достоверностью.

В блоке 22 формируется команда управления на изменение скорости в соответствии с решением, принятым в блоке 21.

Блоки 23—32 работают независимо от того, какая команда, на управление мощностью или скоростью, была сформирована.

В блоке 23 производится кодирование команды управления (в случае введения избыточности).

В блоке 24 осуществляется ввод сигнала кодированной команды управления в мультиплексор передачи.

В блоке 25 происходит кодирование группового сигнала радиостанции Б.

В блоке 26 несущее колебание передатчика модулируется сформированным групповым сигналом в передатчике корреспондента *Б*.

В блоке 27 групповой радиосигнал передается радиостанцией корреспондента *Б* в эфир.

В блоках 28 и 29 корреспондентом *А* осуществляется его прием и демодуляция, соответственно.

В блоке 30 осуществляется декодирование принятого группового сигнала.

В блоке 31 осуществляется выделение в демультимплексоре управляющей команды из группового сигнала.

В блоке 32 (в случае введения избыточности в командный сигнал) происходит его декодирование.

В блоке 25 производится передача командного сигнала на вход блока управления скоростью передачи, в блоке 26 — ее прием.

В блоке 33 происходит анализ этой команды. Если принята команда на изменение мощности, будет работать соответствующая ветвь алгоритма (блоки 34—40). Если принята команда на управление скоростью, то будет работать соответствующая ей ветвь (блоки 41—47).

Итак, если принята команда на управление мощностью, то алгоритм переходит к блоку 34, в котором осуществляется передача командного сигнала в блок управления мощностью (БУМ) радиостанции корреспондента *А*.

В блоке 35 происходит анализ этой команды. В случае если была принята команда на повышение мощности передатчика, алгоритм переходит к блоку 36, в противном случае — к блоку 38.

В блоке 36 сравнивается текущее значение мощности P_i с максимальным $P_{\max}$. В том случае, если $P_i < P_{\max}$, алгоритм переходит к блоку 37, в котором осуществляется повышение мощности передатчика радиостанции *А* на одну дискрету ΔP . Если же условие не выполняется, т. е. фактически $P_i = P_{\max}$, то повышать мощность уже нет возможности и алгоритм переходит сразу к блоку 61.

После того как в блоке 37 была повышена мощность передатчика радиостанции *А*, алгоритм также переходит к блоку 61.

Вернемся к блоку 35. Если команда на управление мощностью не была связана с её повышением, то алгоритм переходит к блоку 38, в котором сравнивается текущее значение мощности P_i с минимальным $P_{\min}$. В случае если $P_i > P_{\min}$, алгоритм переходит к блоку 39. Если же условие не выполняется, т. е. фактически $P_i = P_{\min}$, то снижать мощность уже нет возможности и алгоритм переходит сразу к блоку 61.

В блоке 39 осуществляется уменьшение мощности передатчика радиостанции *А* на одну дискрету ΔP , а затем алгоритм переходит к блоку 61.

Параллельно с выполнением действий блоков 35—39, в БУМ формируется сигнал «Квитанция» (блок 40), который затем подается в тракт передачи радиостанции *А* (блоки 48—52), действия в котором рассмотрим позже. Сигнал «Квитанция» сообщает корреспонденту *Б* о том, что его команда была получена.

Если блок 33 определил, что была принята команда на управление скоростью, работает блок 41, в котором осуществляется передача командного сигнала в блок управления скоростью (БУС) радиостанции корреспондента *А*.

После этого в блоке 42 формируется сигнал «Квитанция», который предназначен для сообщения корреспонденту Б того, что его команда была получена. Параллельно с этим работает ветвь управления скоростью (блоки 43—47).

В блоке 43 определяется, какая команда была получена. Если это команда на увеличение скорости передачи сообщений, то алгоритм переходит к блоку 46. В противном случае — к блоку 44.

В блоке 44 происходит сравнение текущего значения скорости V_n с минимальным $V = 0$. Если $V_n > 0$, то скорость возможно уменьшить и алгоритм переходит к блоку 45. В противном случае, когда фактически $V_n = 0$, снижать скорость невозможно, передачи нет, алгоритм переходит к блоку 61.

В блоке 45 скорость передачи сообщений снижается, а действие алгоритма отправляется к блоку 61.

Если же после блока 43 алгоритм перешел к блоку 46, то текущее значения скорости V_n сравнивается с максимальным $V_{\max}$. В случае если $V_n < V_{\max}$, увеличение скорости возможно и алгоритм переходит к блоку 47. В противном случае, когда $V_n = V_{\max}$, возможности увеличить скорость нет и алгоритм переходит к блоку 61.

В блоке 47 осуществляется увеличение скорости передачи сообщений, затем алгоритм переходит к блоку 61.

После выполнения действий в блоках 40 или 42, параллельно с работой ветвей 35—39 или 43—47 соответственно, алгоритм переходит к блоку 48.

В блоке 48 сигнал «Квитанция» кодируется (в случае введения избыточности).

В блоке 49 осуществляется ввод сигнала «Квитанция» в мультиплексор передачи.

В блоке 50 осуществляется кодирование группового сигнала с выхода мультиплексора.

В блоке 51 несущее колебание передатчика модулируется сформированным групповым сигналом в передатчике корреспондента А.

В блоке 52 групповой радиосигнал передается радиостанцией корреспондента А в эфир.

В блоках 53 и 54 корреспондентом Б осуществляется прием и демодуляция группового сигнала соответственно.

В блоке 55 осуществляется его декодирование.

В блоке 56 осуществляется выделение сигнала «Квитанция» в демультиплексоре.

В блоке 57 происходит декодирование сигнала «Квитанция» (в случае введения в нее избыточности в радиостанции корреспондента А).

В блоке 58 определяется, на какую команду была получена «Квитанция». Если это «Квитанция» на команду об управлении скоростью, то алгоритм переходит к блоку 60, в противном случае (на управление мощностью) — к блоку 59.

В блоке 59 осуществляется прием сигнала «Квитанция» в БУМ радиостанции корреспондента Б, который свидетельствует о выполнении управляющей команды аппаратурой радиостанции корреспондента А.

В блоке 60 осуществляется прием сигнала «Квитанция» в БУС радиостанции корреспондента Б, который свидетельствует о выполнении управляющей команды аппаратурой радиостанции корреспондента А. Затем исполняется команда на изменение скорости приема сообщений в соответствии с ранее выработанной командой.

Из блоков 59 и 60, а также блоков 36, 37, 38, 39, 44, 45, 46, 47 действие алгоритма переходит к блоку 61.

В блоке 61 принимается решение о дальнейшем продолжении работы радиолинии и осуществлении в ней автоматической регулировки мощности и автоматической регулировки скорости передачи. В случае положительного принятия решения действие алгоритма возвращается к блоку 4. В противном случае алгоритм прекращает свою работу.

Вывод. Таким образом, в результате работы предложенного алгоритма осуществляется циклическое управление мощностью излучения передатчиков и скоростью передачи сообщений по принципу увеличения либо уменьшения скорости на величину единичной дискреты в соответствии с состоянием объекта (моделью канала связи).

ЛИТЕРАТУРА

1. Гужва А. Ю. Способы регулирования мощности передатчиков в системах связи с подвижными объектами // XI Межвузовская НТК «Военная радиоэлектроника: опыт использования и проблемы, подготовка специалистов» : тезисы докладов. — Петродворец : ВМИРЭ, 2000. — С. 207.

2. Тихонов А. В. Способы управления скоростью передачи в радиолиниях системы связи с подвижными объектами // Военно-техническая конференция, посвященная 109-летию изобретения радио : тезисы докладов. — СПб : Военно-транспортный университет ЖДВ РФ. — 2004.

REFERENCES

1. Guzhva A. Yu. Sposoby` regulirovaniya moshhnosti peredatchikov v sistemax svyazi s podvizhny`mi ob`ektami // XI Mezhvuzovskaya NTK «Voennaya radioe`lektronika: opy`t ispol`zovaniya i problemy`, podgotovka specialistov» : tezisы` dokladov. — Petrodvorecz : VMIRE`, 2000. — S. 207.

2. Tixonov A. V. Sposoby` upravleniya skorost`yu peredachi v radioliniyax sistemy` svyazi s podvizhny`mi ob`ektami // Voenno-texnicheskaya konferenciya, posvyashhennaya 109-letiyu izobreteniya radio : tezisы` dokladov. — SPb : Voenno-transportny`j universitet ZhDV RF. — 2004.

СВЕДЕНИЯ ОБ АВТОРАХ

Калинин Владимир Игоревич. Старший преподаватель кафедры радиосвязи. Кандидат технических наук.

Военная академия связи им. С. М. Будённого.

E-mail: zursmansor@mail.ru

Россия, 194064, Санкт-Петербург, Тихорецкий пр., 3.

Лунёв Артём Дмитриевич. Доцент кафедры радиоэлектроники и телекоммуникаций. Кандидат технических наук.

Уральский федеральный университет им. первого президента России Б. Н. Ельцина.

E-mail: a.d.lunev@urfu.ru

Россия, 620002, Екатеринбург, ул. Мира, 19.

Чернышов Артём Геннадьевич. Старший преподаватель кафедры радиосвязи. Кандидат технических наук.

Военная академия связи им. С. М. Будённого.

E-mail: chernyshov.ag09@gmail.com

Россия, 194064, Санкт-Петербург, Тихорецкий пр., 3.

Попов Денис Александрович. Старший преподаватель кафедры специальной подготовки.

Уральский федеральный университет им. первого президента России Б. Н. Ельцина.

E-mail: d.a.popov@urfu.ru

Россия, 620002, Екатеринбург, ул. Мира, 19.

Kalinin Vladimir Igorevich. Senior lecturer of the chair of Radio Communications. Candidate of Technical Sciences.

Military Academy of Communications named after S. M. Budyonny.

E-mail: zursmansor@mail.ru

Russia, 194064, Saint Petersburg, Tikhoretsky pr., 3.

Lunev Artem Dmitrievich. Associate Professor of the chair of Radio Electronics and Telecommunications. Candidate of Technical Sciences.

Ural Federal University named after the first President of Russia B. N. Yeltsin.

E-mail: a.d.lunev@urfu.ru

Work address: Russia, 620002, Yekaterinburg, Mira Str., 19.

Chernyshov Artyom Gennadievich. Senior lecturer of the chair of Radio Communications. Candidate of Technical Sciences.

Military Academy of Communications named after S. M. Budyonny.

E-mail: chernyshov.ag09@gmail.com

Russia, 194064, Saint Petersburg, Tikhoretsky pr., 3.

Popov Denis Alexandrovich. Senior lecturer of the chair of Special Training.

Ural Federal University named after the first President of Russia B. N. Yeltsin.

E-mail: zursmansor@mail.ru

Work address: Russia, 620002, Yekaterinburg, Mira Str., 19.

Ключевые слова: управление мощностью передатчика; управление скоростью передачи сообщения; достоверность; алгоритм управления.

Keywords: transmitter power control; message rate control; reliability of communication; control algorithm.

УДК 621.396

И. В. Лазарев, кандидат технических наук, доцент

СИНТЕЗ МОДЕЛИ НАДЕЖНОСТИ МНОГОРУБЕЖНЫХ ПЕРИМЕТРИЧЕСКИХ ОХРАННЫХ СИСТЕМ РАСПРЕДЕЛЁННЫХ ОБЪЕКТОВ

SYNTHESIS OF A RELIABILITY MODEL FOR MULTI-BORDER PERIMETER SECURITY SYSTEMS OF DISTRIBUTED FACILITIES

С использованием методологии вероятностного анализа применительно к структуре многорубежной, многодатчиковой периметрической охранной системы распределённых объектов рассмотрена математическая модель и предложен подход к оценке показателя надёжности технических средств. На основе «дерева» надёжности обсуждаются составляющие показателя синтезированных структур. Приводятся аналитические выражения, позволяющие производить оценку надёжности охранной системы с учетом эксплуатационных характеристик используемой элементной базы. Рассматривается формулировка задачи оптимизации структуры многорубежной многодатчиковой периметрической охранной системы с учётом ограниченных ресурсных затрат.

Using the methodology of probabilistic analysis in relation to the structure of a multi-border, multi-sensor perimeter security system of distributed objects, a mathematical model is considered and an approach to assessing the reliability of technical means is proposed. Based on the reliability "tree", the components of the indicator of synthesized structures are discussed. Analytical expressions are given that make it possible to assess the reliability of the security system, taking into account the operational characteristics of the element base used. The paper considers the formulation of the problem of optimizing the structure of a multi-border, multi-sensor perimeter security system, taking into account limited resource costs.

Введение. В современных условиях необходимо отметить тот факт, что объекты различной формы собственности подлежат охране с применением различного набора технических средств. Следует отметить, что наибольшее проявление преступных посягательств направлено на инфраструктуры, имеющие важное значение с точки зрения как оборонного характера, так и народно-хозяйственного. Представителями таких объектов выступают: военные склады, аэропорты, предприятия водоснабжения, энергетики и пр.

Охрана данных объектов осуществляется путем создания по периметру сигнализационных зон (СЗ). При этом СЗ оснащаются набором технических средств, обеспечивающих наблюдение за наземной обстановкой. Вместе с тем, учитывая большую протяженность СЗ, при ее оснащении используется несколько датчиков, которые в своей совокупности образуют рубежи периметрической охранной системы. В этом случае охранная система применительно к распределённым объектам приобретает тип многорубежной многодатчиковой периметрической охранной системы (ММП ОС).

При попытке совершения внешним нарушителем действия, направленного на проникновение в СЗ ММПОС, с использованием технических средств осуществляется многоэтапная обработка данных, поступающих с различных датчиков. Так, на первом этапе осуществляется пространственное обнаружение объекта (цели) на рубеже периметрической охранной системы. Последующим этапом обеспечивается решение задачи, направленной на формирование обобщенного сигнала тревоги. Наличие данного сигнала в системе охраны свидетельствует о необходимости реагирования со стороны дежурной смены, направленного на противодействие внешнему нарушителю [1].

Следует отметить, что применение ММПОС распределенных объектов влечет за собой необходимость при проектировании охранных систем решения дилеммы. С одной стороны, архитектура ММПОС направлена на обеспечение повышенной вероятности обнаружения объекта, а с другой — влечет усложнение аппаратной реализации охранных систем и, как следствие, влияет на структурную надежность при использовании технических средств.

Как показано в работах [2—4], вопросы, связанные с проведением оценки по обнаружительной способности ММПОС, рассматривались на основе вероятностных характеристик, в частности суммарной вероятности полной ошибки.

Следовательно, следующим этапом является рассмотрение второй составляющей дилеммы в части анализа надежности ММПОС распределенных объектов.

В данной статье рассматриваются вопросы, обусловленные заданием функции-модели надежности ММПОС распределенных объектов, получением аналитических выражений для характеристик надежности их структур и формулировки задачи оптимизации.

Основная часть. Исходя из подходов, приведенных в [5], архитектура ММПОС распределенных объектов содержит признаки иерархической структуры. Поэтому при обработке информации в ММПОС распределенных объектов взаимодействие в структуре возможно на основе нескольких связанных между собой операций. В частности, к ним следует отнести: первичную, вторичную и третичную обработку информации. Структурная схема устройства, осуществляющего указанные операции, представлена системами обработки в структуре ММПОС (рис. 1).

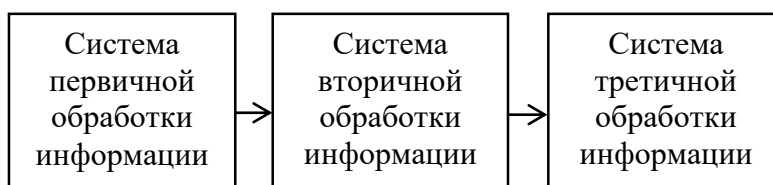


Рис. 1. Структурная схема обработки информации ММПОС

Первичная обработка включает операции, связанные с пространственным обнаружением объекта (цели), которое проводится с использованием технических средств. В частности, в ММПОС распределенных объектов осуществляется конечным набором первичных датчиков.

Вторичная обработка направлена на вынесение решения о складывающейся обстановке в СЗ и основывается на использовании совокупности анализа бинарной информации от первичных датчиков устройством обработки информации. При этом результат работы устройства обработки информации выступает в качестве вторичного датчика для последующей обработки.

В процессе третичной обработки осуществляется анализ данных, поступающих с вторичных датчиков, принадлежащих различным рубежам. Результатом работы является формирование окончательного решения, свидетельствующего о попытке проникновения внешнего нарушителя в СЗ ММПОС распределенных объектов.

Следует отметить, что вторичная и третичная обработка информации может осуществляться на основе применения аппаратных и аппаратно-программных средств, в частности микропроцессоров и компьютерной техники (ЭВМ). Применение ЭВМ позволяет вести наблюдение в охраняемой зоне силам реагирования в автоматическом или автоматизированном режимах, используя экран ЭВМ.

С учетом вышеизложенного следует отметить, что в интересах информирования задействованных подразделений при выполнении поставленных задач типовой вариант структуры ММПОС распределенных объектов включает в себя технические средства, отражающие взаимодействие систем обработки информации (рис. 1) и устройства отображения информации, представленные пультом централизованного наблюдения (ПЦН) (рис. 2).

Функционирование структуры ММПОС (рис. 2) состоит в следующем.

Рубежи, представляющие собой систему первичной обработки информации, содержат в себе типовой набор первичных датчиков в общем случае ($D_1 \dots D_K$) [6]. При появлении внешнего нарушителя в сигнализационной зоне первичные датчики направлены на решение задачи обработки путем формирования информационного, бинарного сигнала по типу «да» или «нет». Затем данная информация с использованием K каналов связи ($KC_1 \dots KC_K$) поступает на входы устройства обработки информации (УОИ).

В устройстве обработки информации осуществляется вторичная обработка информации путем объединения данных в соответствии, например, с решающим правилом [6]. В результате формируется сигнал, свидетельствующий о наличии тревожного сообщения, обработанного с использованием вторичных датчиков СЗ.

Аналогичным образом обработка информации осуществляется на других рубежах. Затем информация с вторичных датчиков рубежей поступает на узел совместной обработки (УСО). В УСО функционирование направлено на формирование окончательного решения о тревожном извещении. Решение выносится на основе алгоритма объединения информации с вторичных датчиков.

Объединение информации с вторичных датчиков в УСО может осуществляться двояко. Во-первых, путем применения алгоритмов, основанных на использовании статистических подходов к объединению данных при формировании обобщенного тревожного сообщения т. е. оптимальных, характер которых направлен, например, на минимизацию суммарной вероятности полной ошибки [3]. Во-вторых, квазиоптимальных, когда решение о формировании обобщенного тревожного сообщения осуществляется, к примеру, на основе использования логических правил. Таковыми могут выступать правила вида: все вторичные датчики на рубежах вынесли решение о его наличии либо обобщенное тревожное сообщение формируется, в случае когда хотя бы вторичные датчики одного рубежа из M вынесли решение о его наличии.

Сформированное таким образом обобщенное тревожное сообщение по линии связи поступает на приемно-контрольный прибор (ПКП) ПЦН, а в дальнейшем высвечивается на устройстве отображения (УО). В качестве УО может выступать монитор приемляемой ЭВМ.

При оценке функционирования качества охранных систем рассматриваемого типа в научно-технической литературе рассматривались различные подходы [7—10]. Однако следует отметить, что они не применимы в полной мере к анализу надежности ММПОС распределенных объектов (рис. 2).

При проектировании охранной системы заказчик руководствуется тем, что надежность структур ММПОС распределенных объектов должна удовлетворять соотношению вида

$$H_{oc} \geq H_{oc}^{тр}, \quad (1)$$

где $H_{oc}^{тр}$ — требуемая надежность ММПОС.

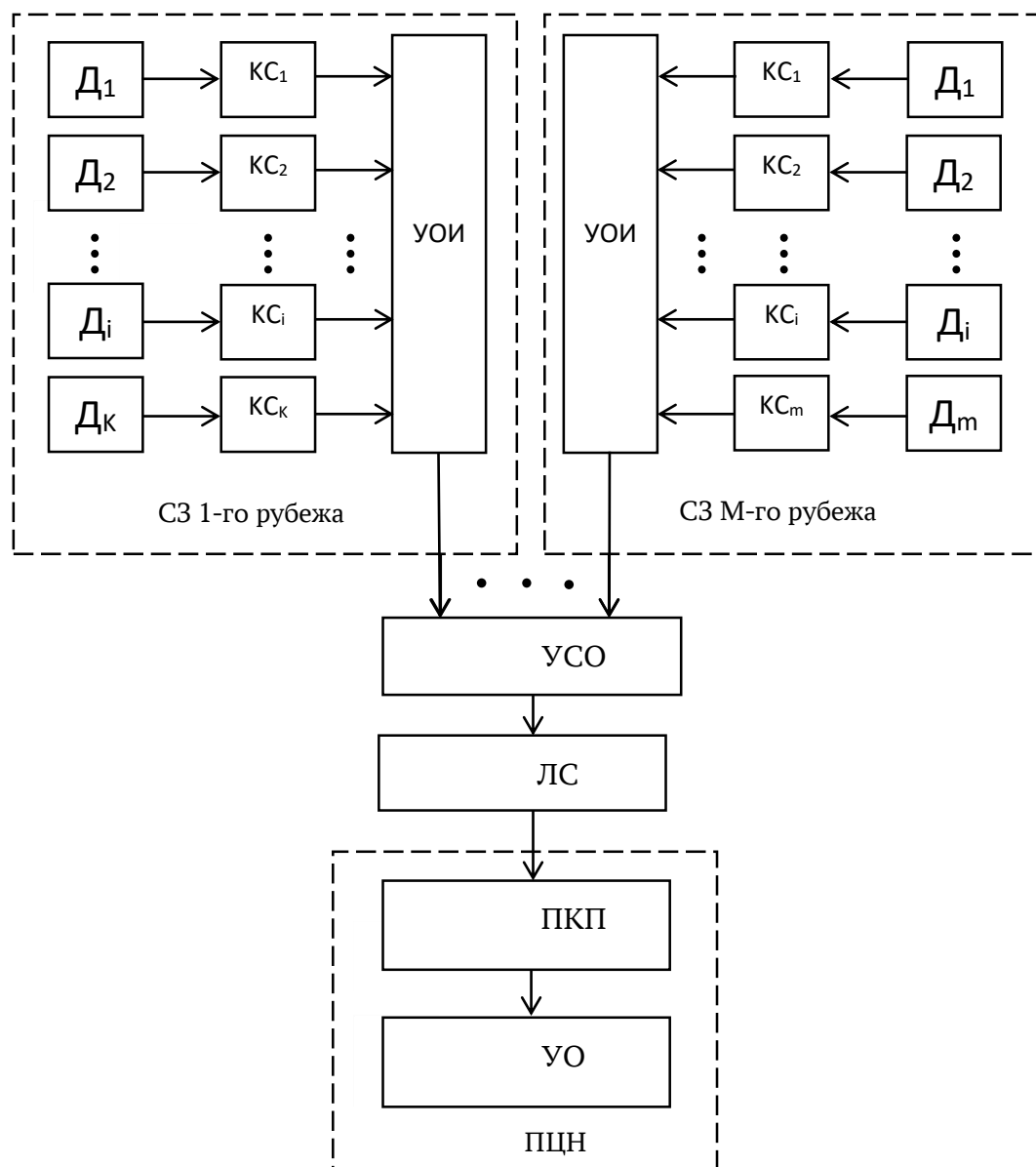


Рис 2. Структурная схема ММПОС

Исходя из принципов функционирования ММПОС распределенных объектов, следует отметить, что структура (рис. 2) содержит ряд взаимодействующих систем. Поэтому при оценке надежности необходимо рассматривать частные и обобщенные показатели. Для этого, опираясь на подходы, приведенные в [7], представим ММПОС посредством «дерева» показателей охранной системы (рис. 3).

Исходя из структуры рис. 3, следует заключить, что оценку надежности необходимо производить исходя из структурирования «дерева» по уровням иерархии.

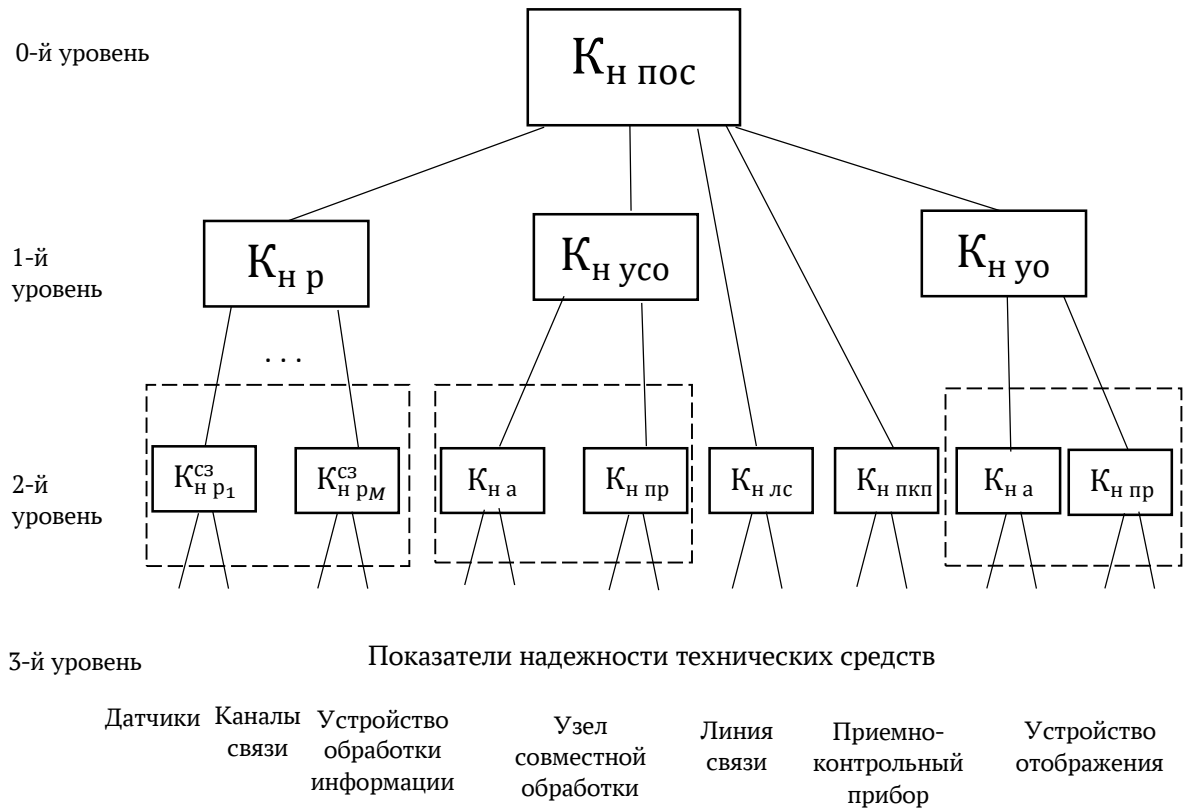


Рис. 3. «Дерево» показателей надежности многорубежной многодатчиковой охранной системы

Рассматривая показатели второго уровня $K_{n p_1}^{cs}$ и $K_{n p_m}^{cs}$, следует заключить, что они отражают обобщенные показатели технических средств СЗ на 1-м и М-м рубеже соответственно.

При реализации УСО с использованием микропроцессора оперируют показателями надежности вида $K_{на}$ и $K_{пр}$. Данные показатели обусловлены необходимостью взаимодействия аппаратурной и программной частью в процессе выполнения решающего правила, направленного на объединение информации с рубежей ММПОС.

Показатели надежности вида $K_{лс}$ и $K_{пкп}$ представляют собой обобщающие показатели, характеризующие надежностные свойства линий связи и ПКП соответственно.

Для оперативного отображения информации на ПЦН в качестве УО в большинстве случаев применяют ЭВМ. При использовании ЭВМ для описания надежности следует ввести

два вида показателей: $K_{на}$ и $K_{пр}$. Данные показатели отражают двухстороннюю надежность, а именно, с одной стороны, задействованной аппаратурной частью, а с другой — программной частью.

Показатели $K_{пр}$, $K_{нuso}$ и $K_{нуo}$ характеризуют в структуре «дерева» надежности возможности, обусловленные использованием в структуре ММПОС технических средств, связанных с решением задач на этапе первичной, вторичной, третичной обработки и УО соответственно.

Нулевой уровень «дерева» надежности представлен показателем $K_{нпoc}$, свидетельствующим о возможности задействованных технических средств ММПОС распределенных объектов качественно решать задачи, обусловленные обнаружением АНФП нарушителя в СЗ несколькими рубежами в рамках выполняемых охранных мероприятий.

Третий уровень «дерева» содержит показатели типовых информационных элементов, входящих в оснащение СЗ рубежей, и надёжностные показатели, характеризующие объединительные возможности рубежей, линии связи, ПКП и УО, обусловленные используемым набором технических средств ММПОС.

Анализ «дерева» показателей ММПОС распределенных объектов свидетельствует о возможности проведения оценки надежности технических средств в процессе их функционирования. Данный подход обуславливает введение векторного показателя

$$Y_T^{ММПОС} = \|Y_1, Y_2, Y_3, Y_4, Y_5, Y_6\|, \quad (2)$$

где Y_1 — показатель, отражающий безотказность линейки технических средств СЗ;
 Y_2 — показатель, отражающий безотказность вторичных датчиков системы вторичной обработки информации;
 Y_3 — показатель, отражающий безотказность технических средств УСО;
 Y_4 — показатель, отражающий безотказность технических средств, представленных линией связи;
 Y_5 — показатель, отражающий безотказность технических средств ПКП;
 Y_6 — показатель, отражающий безотказность технических средств УО.

Комплексное использование при построении ММПОС аппаратурных и аппаратно-программных средств позволяет рассматривать ее качество в рамках вероятностно-статистической теории надежности. При данном подходе необходимо оперировать рядом характеристик. На основе анализа [11—13] на стадии оценки надежности структур ММПОС следует оперировать характеристиками вида: вероятность безотказной работы технических средств и вероятность безотказной работы программы; интенсивность отказов технических средств и параметр потока отказов программы; средняя наработка до отказа технических средств и период средней наработки программы на отказ; вероятность отказа; коэффициент готовности.

Следует отметить, что при анализе работоспособности радиоэлектронной аппаратуры на этапе ее эксплуатации необходимо принимать во внимание тот факт, что технические средства ММПОС подвержены, как правило, внезапным отказам.

Исходя из вышесказанного и с учетом детализации структуры СЗ, архитектуру построения ММПОС можно охарактеризовать вероятностью безотказной работы и векторный показатель (2) представить как

$$Y_T^{ММПОС} = \|P_{брд}, P_{бркс}, P_{бруoi}, P_{брусo}, P_{брлс}, P_{брпкп}, P_{бруo}\|, \quad (3)$$

где

$P_{брд}$ — вероятность безотказной работы первичных датчиков СЗ;

$P_{брКС}$ — вероятность безотказной работы канала связи СЗ;

$P_{брУОИ}$ — вероятность безотказной работы УОИ рубежа СЗ;

$P_{брУСО}$ — вероятность безотказной работы УСО;

$P_{брЛС}$ — вероятность безотказной работы линии связи;

$P_{брПКП}$ — вероятность безотказной работы ПКП;

$P_{брУО}$ — вероятность безотказной работы УО.

Исходя из рассмотренной модели, внезапный отказ приводит к нарушению работоспособности ММПОС распределенных объектов. Например, при выходе из строя первичных датчиков ограничиваются операции первичной обработки. При возникновении отказа вторичных датчиков не обеспечивается качественное выполнение операций, предусмотренных на этапе вторичной обработки. При возникновении отказа в УСО не обеспечивается качественное выполнение операций в процессе третичной обработки. Кроме того, при отказе любого элемента по трафику «линия связи — ПКП — УО» не обеспечивается доведение обобщенного тревожного сообщения до сил реагирования, а следовательно, ограничивается возможность по своевременному противодействию, направленному на пресечение акта незаконного физического проникновения (АНФП), совершаемого внешним нарушителем.

Следовательно, при учете и анализе вероятностных показателей, представленных выражением (3), необходимо исходить из того, что каждый из задействованных компонентов структуры ММПОС распределенных объектов необходим при обеспечении нормального функционирования охранной системы.

При анализе надежности радиотехнических устройств применяются подходы, основанные на методах последовательного, параллельного и последовательно-параллельного соединения элементов их архитектуры. Применительно к решаемой задаче следует применить мультипликативный подход при комплексировании показателей (рис. 3). В этом случае описание выражения (3) может быть введено соотношением вида

$$Y_T^{ММПОС} = P_{брд} \times P_{брКС} \times P_{брУОИ} \times P_{брУСО} \times P_{брЛС} \times P_{брПКП} \times P_{брУО}. \quad (4)$$

Анализ рассмотренной модели (4) позволяет предложить несколько типовых вариантов при оценке надежности ММПОС распределенных объектов, исходя из характеристик качества рассматриваемой архитектуры.

Предположим, что в рассматриваемой структуре (рис. 2) система первичной обработки информации (СПОИ) представлена набором датчиков, в основе которых реализован принцип действия различной физической природы. Каналы связи — разнотипные, а УОИ выполнено, например, на основе использования разнотипного набора радиокомпонентов. Это обуславливает, что вероятности безотказной работы i -го датчика, i -го канала связи, i -го устройства обработки информации на рубежах различны. Вероятности безотказной работы УСО, выполненного на базе микропроцессора (МП), различны в зависимости от количества рубежей. Число рубежей при проектировании охранной си-

системы можно допустить приемлемым из ряда $j = 2, \dots, M$. В дальнейшем считаем, что количество рубежей не менее двух. При этом количество датчиков на рубежах n_j СЗ различно.

В этом случае, возвращаясь к выражению (4), и на основе «дерева» показателя надежности охранной системы (рис. 3) следует заключить, что показатель надежности технических средств ММПОС распределенных объектов возможно представить в виде:

$$P_{\text{брр}}^{\text{ММПОС}} = [\prod_{j=1}^M (\prod_{i=1}^{n_j} P_{\text{брД}_i}^{(j)} \times P_{\text{брКС}_i}^{(j)} \times P_{\text{брУОИ}_i}^{(j)})] \times P_{\text{брМП}}^{(M)} \times P_{\text{брЛС}} \times P_{\text{брПКП}} \times P_{\text{брЭВМ}}. (5)$$

В выражении (5) вновь введенные обозначения имеют следующий смысл:

$P_{\text{брД}_i}^{(j)}$ — вероятность безотказной работы i -го первичного датчика СПОИ j -го рубежа;

$P_{\text{брКС}_i}^{(j)}$ — вероятность безотказной работы i -го канала связи СЗ j -го рубежа;

$P_{\text{брУОИ}_i}^{(j)}$ — вероятность безотказной работы i -го вторичного датчика СЗ j -го рубежа;

$P_{\text{брМП}}^{(M)}$ — вероятность безотказной работы технических средств системы третичной обработки при использовании M рубежей;

$P_{\text{брЭВМ}}$ — вероятность безотказной работы технических средств УО, реализованного на базе ЭВМ.

Рассмотрим случай, когда следует учесть, что количество рубежей ММПОС задано и равно, например, M . Кроме того, для структуры (рис. 2) характерно то, что вероятности безотказной работы i -го первичного датчика, i -го канала связи одинаковы, то есть $P_{\text{брД}_i}^{(j)} = P_{\text{брД}}^{(j)}$ и $P_{\text{брКС}_i}^{(j)} = P_{\text{брКС}}^{(j)}$. Это свойственно для структуры в случае, когда технические средства, отражающие СЗ рубежей, представлены набором однотипных первичных датчиков и каналов связи. Устройство обработки информации выполнено, например, на основе использования технических средств на рубежах СЗ, исходя из различного набора радиоэлементов. Вероятности безотказной работы j -го УОИ на рубежах следует положить различными. Как и ранее, полагаем, что количество датчиков на рубежах СЗ различно.

В этом случае, воспользовавшись выражением (5), показатель надежности технических средств ММПОС распределенных объектов следует представить как:

$$P_{\text{брор1}}^{\text{ММПОС}} = [\prod_{j=1}^M (P_{\text{брД}}^{(j)} \times P_{\text{брКС}}^{(j)})^{n_j} \times P_{\text{брУОИ}}^{(j)}] \times P_{\text{брМП}}^{(M)} \times P_{\text{брЛС}} \times P_{\text{брПКП}} \times P_{\text{брЭВМ}}. (6)$$

Предположим, как и ранее, количество рубежей при проектировании ММПОС наперед задано и равно, как и прежде, M . Рассматриваемая структура (рис. 2) характеризуется тем, что вероятности безотказной работы i -го первичного датчика, i -го канала связи на рубежах одинаковы. Устройство обработки информации выполнено, например, на основе использования однотипного набора радиокомпонентов. Кроме того, предположим, что количество датчиков на рубежах СЗ одинаково, следовательно, $n_j = n$. Поэтому вероятности безотказной работы j -го УОИ на рубежах следует рассматривать одинаковыми, то есть $P_{\text{брУОИ}_i}^{(j)} = P_{\text{брУОИ}}^{(j)}$.

В этих условиях, основываясь на учете выражения (6), показатель надежности технических средств ММПОС распределенных объектов следует представить как:

$$P_{\text{брор2}}^{\text{ММПОС}} = \left(P_{\text{брД}}^{(j)} \times P_{\text{брКС}}^{(j)} \right)^{M \times n} \times P_{\text{бруОИ}}^M \times P_{\text{брМП}}^{(M)} \times P_{\text{брЛС}} \times P_{\text{брПКП}} \times P_{\text{брЭВМ}}. \quad (7)$$

При проектировании ММПОС с использованием широкого выбора элементной базы, представленной на рынке охранных услуг, возможны построения различных вариантов их структур. Поэтому перед заказчиками возникает задача внедрения наилучшей ММПОС распределенных объектов, которая может быть в условиях ресурсных ограничений представлена соотношением вида

$$\omega_p^* = \operatorname{argmax} Y_T^{\text{ММПОС}}(\omega_p) \quad (8)$$

при $\omega_m \in \Omega$, $\Omega = \{\omega_1, \omega_2, \dots, \omega_p\}$, $m = 1, \dots, p$.

В выражении (8) технические средства ММПОС представлены количеством информационных элементов ω_p . При этом информационные элементы удовлетворяют соотношению (1).

Дальнейшее исследование может быть направлено на проведение оценивания показателей при использовании выражений (5), (6) и (7).

Заключение. В статье применительно к системе охраны распределенных объектов синтезирована структурная схема ММПОС. Рассмотрено функционирование ММПОС распределенных объектов применительно к трем этапам обработки информации, а именно: первичной, вторичной и третичной. Применительно к различным вариантам используемой при построении ММПОС распределенных объектов элементной базы получены аналитические выражения для оценки векторного показателя надежности по параметру вероятности безотказной работы. Предложенная модель надежности ММПОС распределенных объектов, полученные аналитические выражения и сформулированный подход к постановке оптимизационной задачи позволяют производить оценку вариантов построения охранных систем и выбирать среди них наилучший с учетом ограниченных ресурсов.

ЛИТЕРАТУРА

1. Организация деятельности подразделений вневедомственной охраны : курс лекций / С. А. Винокуров [и др.] Ч.1. — Воронеж : Воронежский институт МВД России, 2010 — 171 с.
2. Парфенов В. И., Ле В. Д. Анализ показателей эффективности алгоритмов обработки информации в беспроводных сенсорных сетях // XXV Международная научно-техническая конференция «Радиолокация, навигация, связь» : сборник трудов. — М., 2019. — Т.1. — С. 63—70.
3. Лазарев И. В. К вопросу оценки показателя эффективности многорубежной периметрической охранной системы распределенных объектов // Вестник Воронежского института МВД России. — 2023. — № 3. — С. 216—224.

4. Лазарев И. В., Сорокин П. М. Анализ показателей структур периметрической охранной системы распределенных объектов // Вестник Воронежского института МВД России. — 2024. — № 4. — С. 148—155.
5. Балашов Е. П., Пузанков Д. В. Проектирование информационно-управляющих систем. — М. : Радио и связь, 1987. — 256 с.
6. Лазарев И. В. Синтез алгоритма обработки информации в сигнализационной зоне периметрических охранных систем распределенных объектов // Вестник Воронежского института МВД России. — 2022. — № 4. — С. 91—98.
7. Лазарев И. В., Анисимов С. Л. О показателе эффективности системы первичной обработки информации периметрических охранных систем распределенных объектов // Вестник Воронежского института МВД России. — 2023. — № 1. — С. 118—127.
8. Булгаков О. М., Удалов В. П. Анализ модели надежности охранно-пожарной сигнализации // Вестник Воронежского института МВД России. — 2012. — № 2. — С. 5—12.
9. Никулин С. С., Лазарев И. В., Печенин Е. А. К вопросу об оценке надежности эргатических охранных систем // Вестник Воронежского института ФСИН России. — 2021. — № 2. — С. 68—73.
10. Лазарев И. В. К вопросу оценки показателя надежности системы первичной обработки информации периметрических охранных систем распределенных объектов // Вестник Воронежского института МВД России. — 2024. — № 1. — С. 127—137.
11. Баранова А. В., Ямпурин Н. П. Основы надежности электронных средств. — М. : Академия, 2010. — 234 с.
12. Острейковский В. А. Теория надежности. — М. : Высшая школа, 2003. — 457 с.
13. Надежность информационных систем : учебное пособие / Ю. Ю. Громов, О. Г. Иванов, Н. Г. Мосягин, К. А. Набатов. — Тамбов : Изд-во ГОУ ВПО ТГТУ, 2010. — 160 с.

REFERENCES

1. Organizaciya deyatel`nosti podrazdelenij vnevedomstvennoj ohrany` : kurs lekcij / S. A. Vinokurov [i dr.] Ch.1. — Voronezh : Voronezhskij institut MVD Rossii, 2010 — 171 s.
2. Parfenov V. I., Le V. D. Analiz pokazatelej e`ffektivnosti algoritmov obrabotki informacii v besprovodny`x sensory`x setyax // XXV Mezhdunarodnaya nauchno-texnicheskaya konferenciya «Radiolokaciya, navigaciya, svyaz`» : sbornik trudov. — M., 2019. — T.1. — S. 63—70.
3. Lazarev I. V. K voprosu ocenki pokazatelya e`ffektivnosti mnogorubezhnoj perimetriceskoj oxrannoj sistemy` raspredelenny`x ob`ektov // Vestnik Voronezhskogo instituta MVD Rossii. — 2023. — № 3. — S. 216—224.
4. Lazarev I. V., Sorokin P. M. Analiz pokazatelej struktur perimetriceskoj oxrannoj sistemy` raspredelenny`x ob`ektov // Vestnik Voronezhskogo instituta MVD Rossii. — 2024. — № 4. — S. 148—155.
5. Balashov E. P., Puzankov D. V. Proektirovanie informacionno-upravlyayushhix sistem. — M. : Radio i svyaz`, 1987. — 256 s.
6. Lazarev I. V. Sintez algoritma obrabotki informacii v signalizacionnoj zone perimetriceskix oxranny`x sistem raspredelenny`x ob`ektov // Vestnik Voronezhskogo instituta MVD Rossii. — 2022. — № 4. — S. 91—98.

7. Lazarev I. V., Anisimov S. L. O pokazatele e`ffektivnosti sistemy` pervichnoj obrabotki informacii perimetricheskix ohranny`x sistem raspredelenny`x ob`ektov // Vestnik Voronezhskogo instituta MVD Rossii. — 2023. — № 1. — S. 118—127.

8. Bulgakov O. M., Udalov V. P. Analiz modeli nadezhnosti ohranno-pozharnoj signalizacii // Vestnik Voronezhskogo instituta MVD Rossii. — 2012. — № 2. — S. 5—12.

9. Nikulin S. S., Lazarev I. V., Pechenin E. A. K voprosu ob ocenke nadezhnosti e`rgaticheskix ohranny`x sistem // Vestnik Voronezhskogo instituta FSIN Rossii. — 2021. — № 2. — S. 68—73.

10. Lazarev I. V. K voprosu ocenki pokazatelya nadezhnosti sistemy` pervichnoj obrabotki informacii perimetricheskix ohranny`x sistem raspredelenny`x ob`ektov // Vestnik Voronezhskogo instituta MVD Rossii. — 2024. — № 1. — S. 127—137.

11. Baranova A. V., Yampurin N. P. Osnovy` nadezhnosti e`lektronny`x sredstv. — M. : Akademiya, 2010. — 234 s.

12. Ostrejkovskij V. A. Teoriya nadezhnosti. — M. : Vy`sshaya shkola, 2003. — 457 s.

13. Nadezhnost` informacionny`x sistem : uchebnoe posobie / Yu. Yu. Gromov, O. G. Ivanov, N. G. Mosyagin, K. A. Nabatov. — Tambov : Izd-vo GOU VPO TGTU, 2010. — 160 s.

СВЕДЕНИЯ ОБ АВТОРЕ

Лазарев Иван Владимирович. Доцент кафедры физики и радиоэлектроники. Кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: vorhmscl@comch.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Lazarev Ivan Vladimirovich. Associate Professor of the chair of Physics and Radioelectronics. Candidate of Technical Sciences, Associate 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: многорубежное устройство охраны; надежность; показатели.

Key words: multiborder security device; reliability; performance.

УДК 621.396

ЮРИДИЧЕСКИЕ НАУКИ

В. С. Латыпов, доктор юридических наук, доцент

Б. А. Галлямов

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ: ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ

USING ARTIFICIAL INTELLIGENCE IN CRIMINAL PROCEEDINGS: REGULATORY ISSUES

В статье рассматриваются правовые и практические проблемы применения технологий искусственного интеллекта в уголовном судопроизводстве России. Отмечается правовой пробел в части процессуального закрепления механизмов использования ИИ, отсутствие единых стандартов сертификации, контроля, допустимости доказательств, полученных с его помощью. Авторы предлагают конкретные изменения в УПК РФ, включая закрепление статуса ИИ как технического средства, создание реестра сертифицированных систем, определение модели ответственности, а также запрет на автоматическое принятие решений, затрагивающих права личности. Делается вывод о необходимости сбалансированного подхода, обеспечивающего эффективность и правовую безопасность применения ИИ в рамках уголовной юстиции.

The article discusses the legal and practical problems of the use of artificial intelligence technologies in criminal proceedings in Russia. There is a legal gap in terms of the procedural consolidation of the mechanisms for using AI, the lack of uniform standards for certification, control, and the admissibility of evidence obtained with its help. The authors propose specific changes to the Criminal Procedure Code of the Russian Federation, including consolidating the status of AI as a technical tool, creating a register of certified systems, defining a model of responsibility, and prohibiting automatic decision-making affecting individual rights. It is concluded that there is a need for a balanced approach to ensure the effectiveness and legal security of the use of AI in criminal justice.

Развитие цифровых технологий оказывает растущее влияние на сферу уголовного судопроизводства, изменяя методы выявления, расследования и доказывания преступлений. Искусственный интеллект (далее — ИИ), как один из самых значимых инструментов современной цифровизации, уже применяется в ряде процедур, включая распознавание лиц, анализ данных, оценку доказательств и прогнозирование преступлений.

В условиях цифровых изменений правоохранительной деятельности встает вопрос о правомерности, допустимости и границах использования таких технологий, особенно когда они способны повлиять на права и свободы личности. Полагаем, что особое значение технологии ИИ могут иметь при внедрении электрон-

ного документооборота в современное уголовное судопроизводство, закономерное развитие которого видится в поэтапном переходе бумажного уголовного дела в электронное. В настоящее время в доктрине уголовно-процессуального права наиболее детализированной и заслуживающей поддержки видится представленная С. В. Зуевым и Н. А. Моругиной теоретическая модель электронного уголовного дела, структурно состоящая из восьми взаимосвязанных блоков [1].

В свою очередь, российская правовая система сталкивается с отсутствием системного подхода к регулированию ИИ в уголовном процессе, что порождает неопределенность как в теоретико-правовом, так и в практических аспектах.

На сегодняшний день в Уголовно-процессуальном кодексе Российской Федерации (далее — УПК РФ) отсутствуют нормы, регулирующие применение ИИ. Использование технических средств допускается лишь в общих формулировках, не учитывающих специфику алгоритмических решений и рисков [2], связанных с их непрозрачностью, ограничениями точности и возможной коррупционной составляющей. Между тем, согласно проведенному в 2025 г. в рамках настоящего исследования опросу сотрудников правоохранительных органов, их правоприменительная деятельность уже включает в себя применение ИИ-систем. Так, из числа 63 опрошенных сотрудников следственных подразделений ОВД и сотрудников органа дознания, осуществляющих свою деятельность на территории Республики Башкортостан, Оренбургской и Челябинской областей большинство респондентов отметило, что хотя бы раз обращалось к технологиям ИИ — 74,6% (47 человек). Обращение к данным технологиям было вызвано необходимостью: формулирования отдельных фрагментов процессуальных документов — 65,95% (31 человек); решения правовой ситуации — 61,7% (29 человек); подготовки ответов на ходатайства и жалобы участников уголовного судопроизводства — 78,72% (37 человек).

Актуальность исследования обусловлена необходимостью выработки урегулированного правового режима, который, с одной стороны, позволит использовать возможности ИИ для повышения эффективности уголовного судопроизводства [3], а с другой — обеспечит защиту конституционных прав и законных интересов участников процесса. Правоприменительная практика и доктрина уголовно-процессуального права все чаще поднимают вопросы допустимости ИИ как доказательства, возможности наделения его субъектным статусом, а также определения ответственности за ошибки и ущерб, причиненный в результате применения интеллектуальных систем.

В настоящее время растет количество исследований различного уровня, посвященных анализу применения ИИ в уголовном судопроизводстве, выявлению возможных проблем и поиску путей их решения [4, 5, 6, 7].

Кроме того, прослеживается тенденция, когда научное сообщество, практикующие юристы, интересующиеся вопросами цифрового правосудия, в том числе возможностями внедрения технологий ИИ в уголовный процесс, объединяются в научно-практические группы, как правило возглавляемые ведущими специалистами в указанной сфере. Ярким примером такого объединения является созданная профессором С. В. Зуевым Telegram-

группа «Развитие информационных технологий в уголовном судопроизводстве» (РИТВУС) [8].

В рамках настоящего исследования предпринята попытка проанализировать правовые проблемы, связанные с применением ИИ в уголовном процессе, а также сформулировать предложения по совершенствованию законодательства в указанной сфере.

В настоящее время в российском уголовно-процессуальном законодательстве отсутствуют специальные нормы, регулирующие порядок применения ИИ в ходе предварительного расследования и судебного разбирательства. Вместе с тем ч. 6 ст. 164 УПК РФ допускает использование технических средств при проведении следственных действий, однако понятие «технические средства» трактуется чрезвычайно широко [9] и не охватывает специфики программных решений на базе машинного обучения. Более того, алгоритмы, используемые в системах ИИ, не проходят обязательную государственную сертификацию, не подлежат обязательному контролю на предмет точности, объективности, воспроизводимости, что создает риски использования недостоверных данных.

В результате этого возникает закономерный вопрос о допустимости результатов, полученных с помощью ИИ [10], в качестве доказательств по уголовному делу, поскольку в соответствии со ст. 75 УПК РФ недопустимыми признаются доказательства, полученные с нарушением закона. Если алгоритм не зарегистрирован, его работа не протоколирована, а сам процесс применения не отражен в материалах дела, велика вероятность признания полученной информации недопустимой.

Таким образом, полагаем, что ключевой проблемой является отсутствие четких процессуальных рамок использования ИИ, которые бы включали определение терминологии, условия допустимости, порядок протоколирования, обязательность оценки результатов человеком и ответственность за искажения.

Для устранения правового пробела и обеспечения легитимного использования ИИ в уголовном процессе представляется необходимым внести в УПК РФ ряд изменений, направленных на системную регламентацию порядка применения интеллектуальных технологий. В первую очередь требуется закрепить в законодательстве определение понятия «искусственный интеллект» применительно к целям уголовного судопроизводства. Это определение должно учитывать как техническую природу систем, основанных на машинном обучении, так и их функциональное назначение — помощь в сборе, обработке, анализе и визуализации информации, связанной с расследованием преступлений.

Анализ действующего уголовно-процессуального законодательства позволяет утверждать, что в настоящее время отсутствует легальное определение понятия искусственного интеллекта. Единственным нормативным актом, раскрывающим сущность и значение этой технологии, является изданный 5 лет назад Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» [11], следует отметить, что схожее определение содержится также в Федеральном законе от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона „О персональных данных“» [12]. Вместе с тем предложенные в данных нормативных правовых актах определения не позволяют их использовать в уголовно-процессуальной сфере и нуждаются, на наш взгляд, в соответствующей адаптации и обязательном закреплении в действующем УПК РФ.

Ранее В. С. Латыповым определена необходимость отражения в ст. 5 УПК РФ данного понятия в следующем виде: «Искусственный интеллект — технологии, применяемые в рамках уголовного судопроизводства, предназначенные для анализа, обработки информации, способные к обучению, выявлению закономерностей, построению прогнозов и принятию решений на основе полученной информации», а также нормативного закрепления возможности использования в уголовном судопроизводстве информационных технологий в ст. 19.2 УПК РФ [13]. В целом подтверждая высказанную позицию, полагаем, что оптимальным решением также будет являться введение в УПК РФ новой статьи 164.2 «Применение систем искусственного интеллекта при производстве по уголовному делу». Предполагается, что указанная норма должна содержать положения о возможности использования ИИ при условии его сертификации; обязательную фиксацию каждого случая применения ИИ в процессуальных документах (протоколах следственных действий, судебных заседаний и др.); требование обязательной оценки результатов ИИ должностным лицом — следователем, прокурором, судьёй; признание результатов ИИ допустимыми доказательствами только при наличии подтвержденной достоверности и соответствия установленным стандартам; определение последствий нарушения этих правил (например, признание доказательств недопустимыми, дисциплинарная или иная ответственность).

Кроме того, считаем, что необходимым условием является создание государственной системы сертификации ИИ-систем, предназначенных для использования в уголовном процессе. Такая система должна включать: государственный реестр сертифицированных ИИ-средств; процедуру технической и правовой экспертизы, подтверждающей корректность работы алгоритма, защиту персональных данных, объяснимость логики принятия решений и устойчивость к манипуляциям; обязательную идентификацию и маркировку систем, допущенных к применению в правоприменительной деятельности; возможность общественного и научного контроля за процедурой сертификации.

Аналогичные подходы уже реализуются в других отраслях: например, в сфере медицины допускается использование только зарегистрированных диагностических приборов, прошедших государственную проверку [14]. Применительно к ИИ участие сертифицированных систем в процессе должно быть допустимо на тех же основаниях.

Кроме того, в ст. 88 УПК РФ, регламентирующей правила оценки доказательств, целесообразно зафиксировать, что результаты ИИ не имеют заранее установленной силы и подлежат обязательной проверке в соответствии со ст. 87 УПК РФ.

Применение технологий ИИ должно находить обязательное отражение в процессуальных документах. В ст. 166 УПК РФ, регулирующей правила составления протоколов следственных действий, следует указать, что использование ИИ подлежит отражению с указанием конкретного алгоритма, версии, условий и результата работы. Подобные требования необходимо ввести и в отношении протоколов судебных заседаний (ст. ст. 259, 260 УПК РФ).

Таким образом, законодательное оформление применения ИИ должно базироваться на принципах допустимости, верифицируемости и ответственности. Лишь при наличии таких механизмов возможно законное и безопасное использование интеллектуальных технологий в уголовном процессе.

Одной из центральных проблем правового регулирования ИИ является вопрос о распределении ответственности за последствия использования интеллектуальных систем. В уголовном процессе последствия могут быть критическими — от нарушения прав граждан до вынесения незаконных решений. В связи с этим требуется юридически закреплённая модель, определяющая, кто и в каком объёме несет ответственность за ошибки, сбои или предвзятые решения, сгенерированные ИИ.

Предлагаем рассмотреть несколько моделей распределения ответственности:

Первая модель предполагает, что вся ответственность ложится на должностное лицо, принявшее процессуальное решение. В рамках этой концепции ИИ рассматривается исключительно как вспомогательный инструмент [15], а субъектом действия и носителем ответственности всегда выступает должностное лицо — следователь, прокурор или судья. Такой подход соответствует принципу личной ответственности и уже закреплён в УПК РФ. Однако его слабое место — неспособность привлечь к ответственности разработчиков, допустивших системную ошибку в программном обеспечении, а также отсутствие механизмов компенсации вреда пострадавшему за счёт производителя ИИ.

Вторая модель строится на признании ИИ продуктом, аналогичным техническому устройству, используемому в медицине, транспорте или строительстве. В этом случае действует принцип ответственности за дефект товара [16]. Если интеллектуальная система с ошибкой повлияла на процесс и привела к нарушению прав гражданина, ответственность может нести разработчик. Такой подход требует нормативного закрепления дефекта как основания гражданско-правовой ответственности (например, по правилам гл. 59 Гражданского кодекса Российской Федерации «Обязательства вследствие причинения вреда»). Дополнительно может быть предусмотрено обязательное страхование ответственности разработчиков, особенно на стадии внедрения и экспериментального применения технологий.

Третья модель — комбинированная. Она предполагает, что ответственность несёт лицо, применившее ИИ в процессе, но в случае установления технологического сбоя или ошибки — к ответственности может привлекаться и разработчик [17]. В таком случае возникает право регрессного иска со стороны государства или должностного лица к производителю технологии. Для реализации такой модели необходимо создать комиссии по расследованию инцидентов, связанных с ИИ, и предусмотреть правовые процедуры определения источника ошибки.

Комбинированная модель видится наиболее сбалансированной. Она позволяет сохранить принцип личной ответственности, стимулирует должностных лиц проверять и критически оценивать алгоритмические выводы, но в то же время не исключает привлечения к ответственности разработчиков и поставщиков технологий. Это особенно актуально в условиях, когда ИИ-системы внедряются в рамках экспериментальных правовых режимов, где нормативная база ещё формируется.

В целях повышения гарантий лиц и организаций предлагается закрепить в УПК РФ норму 164.3 следующего содержания: «Использование технологий искусственного интеллекта не освобождает должностных лиц от ответственности за соблюдение закона при сборе доказательств и принятии решений. Вред, причинённый в результате применения ИИ, подлежит возмещению в порядке, установленном законодательством. Государственные органы, осуществляющие уголовное судопроизводство, вправе предъявить регрессное требование к разработчику ИИ-системы, если будет установлено, что ошибка обусловлена её техническим дефектом».

Закрепление такой нормы обеспечит правовую определенность, создаст систему стимулов для надёжного проектирования ИИ и повлияет на качество цифровых решений, применяемых в уголовной юстиции.

Искусственный интеллект представляет собой мощный инструмент, способный существенно трансформировать уголовное судопроизводство. Он уже оказывает влияние на стадии сбора доказательств, анализа информации и подготовки процессуальных решений. Однако без надлежащего правового регулирования его использование сопряжено с рисками нарушения прав личности, снижения качества доказывания и подрыва легитимности судебных актов.

Проведённый анализ показывает, что в действующем российском законодательстве отсутствуют чёткие нормы, регламентирующие применение ИИ в уголовном процессе. Это создает правовую неопределенность, ведет к спорной практике и ограничивает возможности использования технологий. В связи с этим требуется системная законодательная реформа, которая должна предусматривать: включение в УПК РФ терминологии и специальных норм о применении ИИ; создание государственной системы сертификации ИИ-систем и ведение публичного реестра допущенных к использованию алгоритмов; обязательную фиксацию всех случаев использования ИИ в материалах уголовного дела; признание допустимости доказательств, полученных с применением ИИ, только при соблюдении условий верификации, протоколирования и экспертной оценки человеком; закрепление модели распределения ответственности, предусматривающей возможность привлечения к ответственности как должностных лиц, так и разработчиков систем в случае технологического сбоя; соблюдение базовых принципов: приоритет человека, прозрачность алгоритмов, объяснимость решений, возможность обжалования, защита персональных данных.

Таким образом, эффективное и безопасное внедрение ИИ в уголовное судопроизводство в

России возможно только при условии нормативного закрепления правил его применения, создания процедур сертификации и контроля, а также обеспечения механизмов защиты прав

граждан. Это позволит использовать технологический потенциал ИИ без ущерба для фундаментальных принципов правосудия и прав личности.

ЛИТЕРАТУРА

1. Зуев С. В., Моругина Н. А. Электронное уголовное дело: теоретическая модель // Вестник Казанского юридического института МВД России. — 2024. — Т. 15, № 3 (57). — С. 83—94.

2. Моругина Н. А. Электронное уголовное дело: понятие, история, зарубежный опыт, перспективы // Правопорядок: история, теория, практика. — 2025. — № 1 (44). — С. 84—89.

3. Чурикова А. Ю. Использование информационных технологий и систем в уголовном судопроизводстве: возможности, риски, правовое регулирование : дис. ... д-ра юрид. наук. — Саратов, 2025. — 498 с.

4. Правовые и организационно-технологические гарантии цифрового уголовного судопроизводства / Д. В. Бахтеев, Е. А. Буглаева, В. Б. Вехов [и др.]. — М. : Юрлитинформ, 2025. — 312 с.

5. Гладышева О. В., Семенцов В. А., Лошкобанова Я. В. Искусственный интеллект и цифровые (электронные) доказательства в уголовном судопроизводстве // Юридический вестник Кубанского государственного университета. — 2024. — № 1. — С. 89—99.

6. Чурикова А. Ю. Искусственный интеллект в уголовном процессе: возможные риски использования // Информационное право. — 2023. — № 4 (78). — С. 22—25.

7. Латыпов В. С., Гуськова А. Б. Примирение сторон в уголовном судопроизводстве с применением технологий искусственного интеллекта // Закон и право. — 2024. — № 2. — С. 264—267.

8. Развитие информационных технологий в уголовном судопроизводстве. — URL: <https://t.me/+mNhc11bBMj42NjYy> (дата обращения: 23.04.2025).

9. Щедрин Д. Н. Немного о технических средствах в уголовном процессе // Применение специальных познаний в правоприменительной и экспертной деятельности : материалы межвузовской научно-практической конференции, Красноярск, 27 мая 2020 года. — Красноярск : Красноярский государственный аграрный университет, 2020. — С. 73—75.

10. Виртуальный следователь: помогут ли нейросети распознать маньяка // URL:

<https://legalacademy.ru/sphere/post/> (дата обращения: 24.04.2025).

11. О развитии искусственного интеллекта в Российской Федерации : указ Президента РФ от 10 октября 2019 № 490 (ред. от 15.02.2024) (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Собрание законодательства РФ. — 2019. — № 41. — Ст. 5700.

12. О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» : Федеральный закон от 24.04.2020 № 123-ФЗ // Собрание законодательства РФ. — 2020. — № 17. — Ст. 2701.

13. Латыпов В. С. Вопросы интеграции технологий искусственного интеллекта в деятельность по оказанию содействия уголовному правосудию: тезисы // Уголовное судопроизводство России и зарубежных государств: проблемы и перспективы развития : материалы международной научно-практической конференции, Санкт-Петербург, 29 ноября 2024 года. — СПб. : Санкт-Петербургский университет МВД России, 2024. — С. 158—162.

14. Об утверждении Правил государственной регистрации медицинских изделий : постановление Правительства РФ от 30.11.2024 № 1684 // Собрание законодательства РФ. — 2024. — № 50. — Ст. 7744.

15. Литвин И. И. К вопросу о правосубъектности искусственного интеллекта в уголовном судопроизводстве // Advances in Law Studies. — 2022. — Т. 10, № 2. — С. 26—30.

16. Коновалов А. Кто в ответе за «искусственный интеллект»? // URL: <https://www.advgazeta.ru/mneniya> (дата обращения: 24.04.2025).

17. Разработчики ИИ будут обязаны страховать ответственность за возможный вред жизни // URL: <https://dumatv.ru/news> (дата обращения: 24.04.2025).

REFERENCES

1. Zuev S. V., Morugina N. A. Elektronnoe ugovnoe delo: teoreticheskaya model' // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii. — 2024. — T. 15, № 3 (57). — S. 83—94.
2. Morugina N. A. Elektronnoe ugovnoe delo: ponyatie, istoriya, zarubezhnyj opyt, perspektivy // Pravoporyadok: istoriya, teoriya, praktika. — 2025. — № 1 (44). — S. 84—89.
3. Churikova A. Yu. Ispol'zovanie informacionnyh tekhnologij i sistem v ugovnom sudoproizvodstve: vozmozhnosti, riski, pravovoe regulirovanie : dis. ... d-ra yurid. nauk. — Saratov, 2025. — 498 s.
4. Pravovyie i organizacionno-tekhnologicheskie garantii cifrovogo ugovnogo sudoproizvodstva / D. V. Bahteev, E. A. Buglaeva, V. B. Vekhov [i dr.]. — M. : Yurлитinform, 2025. — 312 s.
5. Gladysheva O. V., Semencov V. A., Loshkovanova Ya. V. Iskusstvennyj intellekt i cifrovye (elektronnye) dokazatel'stva v ugovnom sudoproizvodstve // Yuridicheskij vestnik Kubanskogo gosudarstvennogo universiteta. — 2024. — № 1. — S. 89—99.
6. Churikova A. Yu. Iskusstvennyj intellekt v ugovnom processe: vozmozhnye riski ispol'zovaniya // Informacionnoe pravo. — 2023. — № 4 (78). — S. 22—25.
7. Latypov V. S., Gus'kova A. B. Primirenie storon v ugovnom sudoproizvodstve s primeneniem tekhnologij iskusstvennogo intellekta // Zakon i pravo. — 2024. — № 2. — S. 264—267.
8. Razvitie informacionnyh tekhnologij v ugovnom sudoproizvodstve. — URL: <https://t.me/+mNhc11bBMj42NjYy> (data obrashcheniya: 23.04.2025).
9. Shchedrin D. N. Nemnogo o tekhnicheskikh sredstvakh v ugovnom processe // Primenenie special'nyh poznanij v pravoprimenitel'noj i ekspertnoj deyatel'nosti : materialy mezhvuzovskoj nauchno-prakticheskoy konferencii, Krasnoyarsk, 27 maya 2020 goda. — Krasnoyarsk : Krasnoyarskij gosudarstvennyj agrarnyj universitet, 2020. — S. 73—75.
10. Virtual'nyj sledovatel': pomogut li nejroseti raspoznat' man'yaka // URL: <https://legalacademy.ru/sphere/post/> (data obrashcheniya: 24.04.2025).
11. O razvitii iskusstvennogo intellekta v Rossijskoj Federacii : ukaz Prezidenta RF ot 10 oktyabrya 2019 № 490 (red. ot 15.02.2024) (vmeste s «Nacional'noj strategiej razvitiya iskusstvennogo intellekta na period do 2030 goda») // Sobranie zakonodatel'stva RF. — 2019. — № 41. — St. 5700.
12. O provedenii eksperimenta po ustanovleniyu special'nogo regulirovaniya v celyah sozdaniya neobhodimyh uslovij dlya razrabotki i vnedreniya tekhnologij iskusstvennogo intellekta v sub"ekte Rossijskoj Federacii — gorode federal'nogo znacheniya Moskve i vnesenii izmenenij v stat'i 6 i 10 Federal'nogo zakona «O personal'nyh dannyh» : Federal'nyj zakon ot 24.04.2020 № 123-FZ // Sobranie zakonodatel'stva RF. — 2020. — № 17. — St. 2701.
13. Latypov V. S. Voprosy integracii tekhnologii iskusstvennogo intellekta v deyatel'nost' po okazaniyu sodejstviya ugovnomu pravosudiyu: tezisy // Ugovnoe sudoproizvodstvo Rossii i zarubezhnyh gosudarstv: problemy i perspektivy razvitiya : materialy mezhdunarodnoj nauchno-prakticheskoy konferencii, Sankt-Peterburg, 29 noyabrya 2024 goda. — SPb. : Sankt-Peterburgskij universitet MVD Rossii, 2024. — S. 158—162.
14. Ob utverzhdenii Pravil gosudarstvennoj registracii medicinskih izdelij : postanovlenie Pravitel'stva RF ot 30.11.2024 № 1684 // Sobranie zakonodatel'stva RF. — 2024. — № 50. — St. 7744.
15. Litvin I. I. K voprosu o pravosub"ektnosti iskusstvennogo intellekta v ugovnom sudoproizvodstve // Advances in Law Studies. — 2022. — T. 10, № 2. — S. 26—30.
16. Konovalov A. Kto v otvete za «iskusstvennyj intellekt»? // URL: <https://www.advgazeta.ru/mneniya> (data obrashcheniya: 24.04.2025).
17. Razrabotchiki II budut obyazany strahovat' otvetstvennost' za vozmozhnyj vred zhizni // URL: <https://dumatv.ru/news> (data obrashcheniya: 24.04.2025).

СВЕДЕНИЯ ОБ АВТОРАХ

Латыпов Вадим Сагитьянович. Начальник кафедры уголовного процесса. Доктор юридических наук, доцент.

Уфимский юридический институт МВД России.

E-mail: vadi-latypov@yandex.ru

Россия, 450103, Уфа, ул. Муксинова, 2.

Галлямов Булат Азаматович. Курсант.

Уфимский юридический институт МВД России.

E-mail: gallyamov.bulat@bk.ru

Россия, 450103, Уфа, ул. Муксинова, 2.

Latypov Vadim Sagityanovich. Head of the Chair of Criminal Procedure. Doctor of Law, Associate Professor.

Ufa Law Institute of the Ministry of Internal Affairs of Russia.

E-mail: vadi-latypov@yandex.ru

Work address: Russia, 450103, Ufa, Muksinova Str., 2.

Gallyamov Bulat Azamatovich. Cadet.

Ufa Law Institute of the Ministry of Internal Affairs of Russia.

E-mail: gallyamov.bulat@bk.ru

Work address: Russia, 450103, Ufa, Muksinova Str., 2.

Ключевые слова: искусственный интеллект; уголовное судопроизводство; нормативное регулирование; досудебное производство; процессуальное решение; доказывание.

Key words: artificial intelligence; criminal proceedings; regulatory regulation; pre-trial proceedings; procedural decision; proof.

УДК 343.13

И. А. Насонова, доктор юридических наук, профессор

Т. А. Красноручкая, кандидат юридических наук

О ДОЗНАВАТЕЛЕ КАК УЧАСТНИКЕ ОТЕЧЕСТВЕННОГО УГОЛОВНОГО СУДОПРОИЗВОДСТВА И НЕОБХОДИМОСТИ КОРРЕКЦИИ НОРМАТИВНОГО ОПРЕДЕЛЕНИЯ, ЕМУ ПОСВЯЩЕННОГО

ON THE INTERROGATOR AS A PARTICIPANT IN DOMESTIC CRIMINAL PROCEEDINGS AND THE NEED TO CORRECT THE NORMATIVE DEFINITION DEVOTED TO HIM OR HER

В работе показано место дознавателя в системе участников уголовного судопроизводства. Раскрывается его значимость для успешного осуществления предварительного расследования в форме дознания. Анализируется уголовно-процессуальная деятельность дознавателя. Критически оценивается существующее в действующем законодательстве нормативное определение дознавателя.

The paper shows the place of the inquirer in the system of participants of criminal proceedings. His importance for the successful implementation of preliminary investigation in the form of inquiry is revealed. The criminal procedural activity of the inquirer is analyzed. The normative definition of the inquirer existing in the current legislation is critically evaluated.

На сегодняшний день уголовно-процессуальное законодательство России определяет дознание как форму предварительного расследования, которая реализуется дознавателем (следователем) по уголовному делу, по которому производство предварительного следствия необязательно (п. 8 ст. 5 Уголовно-процессуальный кодекс Российской Федерации) [1]. Заметим, как форма предварительного расследования дознание существовало не всегда. Изначально оно выходило за рамки уголовно-процессуального законодательства, поскольку носило административный характер и реализовывалось полицией.

Лишь после Судебной реформы 1860 года дознание приблизилось к предварительному расследованию и уже понималось как деятельность по собиранию предварительных сведений для расследования уголовных дел. В процессе дальнейшего реформирования уголовно-процессуального законодательства возникает дознание в двух формах: по делам, по которым проводились неотложные следственные действия (предварительное следствие в этой ситуации было обязательно), и по делам, по которым расследование в форме дознания осуществилось полностью (предварительное следствие применительно к указанному случаю было необязательно).

Как участник уголовного процесса дознаватель появился лишь с принятием УПК РФ в

2001 г. Ранее он фигурировал в уголовно-процессуальном законодательстве как «лицо, производящее дознание». Правда, обязанности дознавателя были закреплены еще в 1992 году. В этом году был утвержден приказ МВД России № 368 «О мерах по укреплению подразделений дознания и совершенствованию раскрытия преступлений, по которым предварительное следствие не обязательно» [2], согласно которому начали функционировать специализированные подразделения.

В 2001 году закрепляется правовое положение дознавателя на законодательном уровне. Дознаватель возводится в статус участника уголовного судопроизводства.

Следует отметить, что дознаватель обладает общими признаками участника уголовного судопроизводства, на которые не раз обращалось внимание в литературе. Среди них: наличие процессуального статуса (прав и обязанностей); способность осуществлять уголовно-процессуальную деятельность; способность вступать в уголовно-процессуальные отношения с иными участниками процесса [3. — С. 15—17].

Говоря о процессуальном статусе дознавателя, следует отметить, что круг полномочий, предоставленных ему для расследования уголовного дела, определяется уголовно-процессуальным законом. Среди них возможность самостоятельно производить следственные и иные процессуальные

действия и принимать процессуальные решения; обжаловать решения прокурора о возвращении уголовного дела для производства дополнительного дознания и другие (ч. 3 ст. 41 УПК РФ).

Предоставленные дознавателю права и обязанности образуют содержание уголовно-процессуальных отношений, в которые вступает дознаватель. Именно они связывают участников уголовного судопроизводства. Дознаватель вступает в отношения как с властными субъектами (например, с прокурором, начальником органа дознания, начальником подразделения дознания), так и с невластными участниками уголовного судопроизводства (например, с потерпевшим, подозреваемым).

Отношения с начальником органа дознания и начальником подразделения дознания строятся на основе подчиненности. Начальник подразделения дознания осуществляет промежуточный контроль по отношению к находящимся в его подчинении дознавателям. Начальник органа дознания отвечает за итоговые процессуальные решения по уголовному делу о преступлениях, расследуемых в форме дознания.

Указанные должностные лица руководят деятельностью дознавателя, причем делают это активно. В определенной мере это связано с изменениями, которые произошли в уголовно-процессуальном законодательстве в 2007 году. Именно тогда появился новый участник уголовного судопроизводства — начальник подразделения дознания, на которого была возложена обязанность осуществлять ведомственный процессуальный контроль за дознанием. Представляется, что данный шаг является необходимым для повышения эффективности дознания как формы предварительного расследования. Ведомственный процессуальный контроль, осуществляемый начальником подразделения дознания, особенно важен для сокращенной формы дознания, поскольку сопровождающая ее система гарантий является более уязвимой. Последнее обстоятельство может негативно сказаться не только на качестве расследования по уголовному делу, но и на обеспечении прав лиц, вовлекаемых в него (например, подозреваемого).

Отношения дознавателя с субъектами ведомственного процессуального контроля дополняются отношениями дознавателя с прокурором. Полномочия последнего в отношении дознавателя весьма широки. Решение ряда ключевых вопросов на предварительном расследовании, осуществляемом в форме дознания, завязано на прокуроре. К таким вопросам относится и избрание некоторых мер пресечения (заключение под стражу, домашний арест и др.), и производство отдельных следственных действий (например,

обыска в жилище). Прокурор дает согласие дознавателю на обращение в суд с ходатайством по указанным вопросам (п. 5 ч. 2 ст. 37 УПК РФ). Дознаватель, обращаясь в суд с одобренным прокурором ходатайством, вступает в уголовно-процессуальные отношения с судом, который, в отличие от прокурора, начальника органа дознания и начальника подразделения дознания, выполняет иную уголовно-процессуальную функцию — функцию разрешения уголовного дела.

В рамках упомянутых правоотношений дознаватель осуществляет уголовно-процессуальную деятельность. При этом дознаватель обязан строго соблюдать уголовно-процессуальный закон и выполнять требования ведомственных нормативных правовых актов.

Способность дознавателя осуществлять уголовно-процессуальную деятельность тесно связана с его функциональной характеристикой, позволяющей определить, носителем какой функции является данный участник уголовного судопроизводства. В пользу выполнения дознавателем функции обвинения свидетельствует ряд обстоятельств.

Во-первых, законодатель разместил указанного участника в главе 6 УПК РФ, посвященной участникам со стороны обвинения. Кроме этого дознаватель упоминается и в п. 47 ст. 5 УПК РФ, как субъект со стороны обвинения, и в ст. 21 УПК РФ, как лицо, осуществляющее уголовное преследование. И это не случайно, поскольку дознаватель, являясь субъектом обвинения, должен реализовывать обвинительную деятельность в форме уголовного преследования. А если рассматривать уголовное преследование, осуществляемое в ходе предварительного расследования, как форму проявления обвинительной деятельности дознавателя, то значимость расследования для данного участника уголовного судопроизводства как носителя функции обвинения несколько не уменьшается.

Во-вторых, предварительное расследование — это одна из досудебных стадий уголовного судопроизводства. Поэтому именовать идентичным образом еще и уголовно-процессуальную функцию вряд ли будет правильным.

В-третьих, в пользу выполнения дознавателем функции обвинения в определенной мере свидетельствует и характер процессуальных документов, изготавливаемых им в ходе предварительного расследования. А они в основном носят обвинительный характер (например, постановление об избрании меры пресечения, обвинительный акт, обвинительное постановление).

Обвинительная деятельность дознавателя может быть реализована в двух формах: непосредственная и опосредованная. Непосредственная

форма характерна для дознавателя в ситуации, когда он самостоятельно расследует уголовное дело в полном объеме (ч. 2 ст. 40.1 УПК РФ). При этом обвинительная деятельность дознавателя имеет как практическую сторону, так и мыслительную. Результатом мыслительной деятельности являются суждения по расследуемому уголовному делу, отражаемые в таких итоговых документах, как обвинительный акт и обвинительное постановление.

Опосредованная форма обвинительной деятельности востребована в том случае, когда дознаватель дает поручение органу дознания о проведении оперативно-розыскных мероприятий, о производстве отдельных следственных действий, об исполнении постановлений о задержании, приходе, заключении под стражу и о производстве иных процессуальных действий (п.1.1 ч. 3 ст. 41 УПК РФ).

Выполняя функцию обвинения, дознаватель осуществляет не только процессуальную, но также организационную и профилактическую деятельность. Указанные виды деятельности удачно дополняют друг друга.

Организационная деятельность дознавателя связана с организацией расследования по уголовному делу. В пользу существования указанного вида деятельности свидетельствует, например, закрепленное в п.1.1 ч. 3 ст. 41 УПК РФ полномочие дознавателя давать органу дознания письменные поручения о проведении оперативно-розыскных мероприятий и другие (п.1.1 ч. 3 ст. 41 УПК РФ).

Профилактическая деятельность дознавателя касается проведения мероприятий, носящих предупредительный характер, и предполагает обнаружение и устранение обстоятельств, которые способствуют совершению преступления. В ходе нее указанный участник уголовного судопроизводства нередко выносит представление о принятии мер по устранению обстоятельств, способствующих совершению преступления (ч. 2 ст. 158 УПК РФ). Данный документ выносится по уголовному делу, находящемуся в производстве дознавателя.

Процессуальная деятельность дознавателя связана с производством предварительного расследования, сопровождающимся применением процессуальных средств для установления обстоятельств, имеющих значение. Указанный вид деятельности многогранен. С одной стороны, дознаватель осуществляет от имени государства уголовное преследование, с другой — обеспечивает права лиц, вовлекаемых в дознание по конкретному уголовному делу. Необходимость осуществления правообеспечительной деятельности дознавателя вытекает из его обязанности участвовать в

достижении назначения уголовного судопроизводства, магистральным направлением которого является забота о правах потерпевшего, обвиняемого и других участников уголовного судопроизводства. Недаром в части первой статьи 6 УПК РФ обращается внимание на необходимость защиты в уголовном судопроизводстве прав и законных интересов лиц, вовлекаемых в него.

В силу важности задач, стоящих перед дознавателем, возникает вопрос о том, насколько обоснованно отнесение законодателем к числу дознавателей не только должностного лица органа дознания, правомочного по закону осуществлять предварительное расследование в форме дознания, но и лица, уполномоченного начальником органа дознания осуществлять такое расследование. На данный вопрос авторы отвечают по-разному.

Одни поддерживают законодателя и считают, что дознавателем необходимо считать любое должностное лицо, которому были делегированы конкретные процессуальные полномочия. Так, по мнению М. М. Куземаевой, распространение понятия «дознаватель» на должностных лиц, имеющих различный объем процессуальных полномочий, является верным, поскольку позволяет усовершенствовать архитектуру института дознания [4. — С. 12—13].

Другие ученые полагают, что должностное лицо, правомочное осуществлять дознание, и лицо, уполномоченное начальником органа дознания осуществлять такое расследование, — это разные процессуальные фигуры, не одинаково получающие свой процессуальный статус.

Действительно, согласно п. 7 ст. 5 УПК РФ статус первого уже имеется по закону. Данное лицо, находясь на штатной должности дознавателя, является правомочным осуществлять расследование в форме дознания. Статус второго приобретает при условии возложения на него начальником органа дознания обязанности осуществлять предварительное расследование в форме дознания. Такое должностное лицо органа дознания (например, участковый уполномоченный или оперуполномоченный), не состоящее в штате подразделения дознания, обладает всеми предусмотренными в законе процессуальными полномочиями дознавателя до тех пор, пока действует его уполномочивание на это от начальника органа дознания.

Данное обстоятельство позволяет задуматься над тем, сможет ли лицо, уполномоченное начальником органа дознания на осуществление расследования, выполнять свои обязанности так же качественно, как и штатный дознаватель. Ряд авторов не склонны давать положительный ответ на данный вопрос.

Так, А. И. Цыреторов и А. Г. Анисимов, учитывая высокую значимость защиты прав и свобод человека и гражданина в ходе дознания, полагают, что наделение статусом дознавателя любого сотрудника органа дознания недопустимо, поскольку это может способствовать злоупотреблению и произволу с его стороны. Кроме того, ученые обращают внимание на двойственное подчинение указанного сотрудника, что также крайне нежелательно. Так, участковый уполномоченный полиции, наделенный процессуальным статусом дознавателя, будет одновременно подчиняться и непосредственному руководителю — начальнику участковых уполномоченных полиции (организационное подчинение), и начальнику подразделения дознания (процессуальное подчинение) в соответствии с ч. 4 ст. 40.1 УПК РФ [5. — С. 149].

Приведенная позиция является обоснованной, особенно если учесть, что во-первых, дознание может осуществляться не только в отношении взрослых лиц, но и несовершеннолетних — самой уязвимой части населения, нуждающейся в особой охране своих прав [6. — С. 223]; во-вторых, дознание может сопровождаться применением уголовно-процессуального принуждения, предполагающего осуществление действий, ограничивающих права лица (хотя и на законном основании) и тем самым затрудняющих ему реализацию права на защиту (например, применение заключения под стражу) [7. — С. 249]; в-третьих, в ходе дознания могут приноситься жалобы, требующие грамотного и обоснованного ответа [8. — С. 36].

Я. А. Шараева также полагает, что сотрудников других служб и подразделений не следует наделять полномочиями дознавателя. В связи с

этим под дознавателем, по мнению автора, следует понимать «должностное лицо органа дознания, правомочное осуществлять предварительное расследование в форме дознания и иные полномочия УПК РФ» [9. — С. 130].

Отдельные авторы и вовсе предлагают закрепить в законе нормативное определение должностного лица органа дознания (путем дополнения статьи 5 пунктом 7.1) [9. — С. 130; 10. — С. 54].

Представляется, что приведенные точки зрения в пользу того, что дознание должно осуществляться штатным дознавателем, подчиненным непосредственно начальнику подразделения дознания, являются весьма убедительными. С учетом сказанного нормативная дефиниция дознавателя, предназначенная для размещения в п. 7 ст. 5 УПК РФ, может выглядеть следующим образом: «дознаватель — должностное лицо специализированного подразделения дознания, предназначенного для осуществления предварительного расследования в форме дознания, правомочное осуществлять расследование по уголовному делу».

Думается, что корректировка действующего нормативного определения дознавателя имеет важное значение. Она позволяет возлагать полномочия дознавателя только на лицо, занимающее указанную должность, а значит, изначально ориентированное не только на качественное осуществление предварительного расследования, но и на выполнение своих обязанностей по обеспечению прав и законных интересов лиц, вовлекаемых в дознание. Причем направленность дознавателя к достижению указанных целей зачастую базируется на уголовно-процессуальной ответственности, которой он может быть подвергнут.

ЛИТЕРАТУРА

1. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 20.03.2025) // Собрание законодательства РФ. — 2001. — № 52 (ч. I). — Ст. 4921.

2. О мерах по укреплению подразделений дознания и совершенствованию раскрытия преступлений, по которым предварительное следствие не обязательно : приказ МВД РФ от 16 октября 1992 года № 368. — Утратил силу // СПС «Консультант Плюс».

3. Кокорев Л. Д. Положение личности в советском уголовном судопроизводстве : дис. ... д-ра юрид. наук. — Воронеж, 1975. — 429 с.

4. Куземаева М. М. Функциональная характеристика деятельности дознавателя и органа дознания в уголовном процессе : автореф. дис. ... канд. юрид. наук. — Омск, 2006. — 22 с.

5. Цыреторов А. И., Анисимов А. Г. Должностное лицо органа дознания, не являющееся дознавателем // Пробелы в российском законодательстве. — 2020. — Т. 13. — № 7. — С. 146—150.

6. Насонов А. А. Меры уголовно-процессуального принуждения, применяемые к лицу, запрашиваемому к выдаче для уголовного преследования // Вестник Воронежского института МВД России. — 2017. — № 1. — С. 221—225.

7. Насонов А. А. Основания появления в российском уголовном процессе лица, выдача которого запрашивается для уголовного преследования // Вестник Воронежского государственного университета. Серия : Право. — 2016. — № 1 (24). — С. 241—250.

8. Насонова И. А. Ходатайства, жалобы, отводы: сходства и различия // Вестник Воронежского института МВД России. — 2011. — № 1. — С. 34—38.

9. Шараева Я. А. Процессуальный статус дознавателя: мифы и реальность // Философия права. — 2001. — № 3 (98). — С.127—131.

10. Гарипов Т. И. Вопросы совершенствования

правовой регламентации процессуального статуса органа дознания в уголовном процессе России // Ученые записки Казанского юридического института МВД России. — 2019. — Т. 4. — № 4 (28). — С. 51—54.

REFERENCES

1. Ugolovno-processual'ny'j kodeks Rossijskoj Federacii ot 18 dekabrya 2001 g. № 174-FZ (red. ot 20.03.2025) // Sobranie zakonodatel'stva RF. — 2001. — № 52 (ch. I). — St. 4921.

2. O merax po ukrepleniyu podrazdelenij doznanija i sovershenstvovaniyu raskry'tiya prestuplenij, po kotory'm predvaritel'noe sledstvie ne obyazatel'no : prikaz MVD RF ot 16 oktyabrya 1992 goda № 368 // Utratil silu. — SPS «Konsul'tant Plus».

3. Kokorev L. D. Polozhenie lichnosti v sovetском уголовном судопроизводстве : dis. ... d-ra yurid. nauk. — Voronezh, 1975. — 429 s.

4. Kuzembaeva M. M. Funkcional'naya karakteristika deyatel'nosti doznatelya i organa doznanija v уголовном процессе : avtoref. dis. ... kand. yurid. nauk. — Omsk, 2006. — 22 s.

5. Cyretorov A. I., Anisimov A. G. Dolzhnostnoe liczo organa doznanija, ne yavlyayushheesya doznatelyem // Probely' v rossijskom zakonodatel'stve. — 2020. — T. 13. — №7. — S. 146—150.

6. Nasonov A. A. Mery' ugolovno-processual'nogo prinuzhdeniya, primenyaemy'e k liczu, zaprashivaemomu k vy'dache dlya ugolovnogo presledovaniya // Vestnik Voronezhskogo instituta MVD Rossii. — 2017. — № 1. — S. 221—225.

7. Nasonov A. A. Osnovaniya pojavleniya v rossijskom уголовном процессе licza, vy'dacha kotorogo zaprashivaetsya dlya ugolovnogo presledovaniya // Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya : Pravo. — 2016. — № 1 (24). — S. 241—250.

8. Nasonova I. A. Xodatajstva, zhaloby', otvody': sxodstva i razlichiya // Vestnik Voronezhskogo instituta MVD Rossii. — 2011. — № 1. — S. 34—38.

9. Sharaeva Ya. A. Processual'ny'j status doznatelya: mify' i real'nost' // Filosofiya prava. — 2001. — № 3 (98). — S. 127—131.

10. Garipov T. I. Voprosy' sovershenstvovaniya pravovoj reglamentacii processual'nogo statusa organa doznanija v уголовном процессе Rossii // Ucheny'e zapiski Kazanskogo yuridicheskogo instituta MVD Rossii. — 2019. — T. 4. — № 4 (28). — S. 51—54.

СВЕДЕНИЯ ОБ АВТОРАХ

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.

Красноруцкая Татьяна Александровна. Доцент кафедры административного права. Кандидат юридических наук.

Воронежский институт МВД России.

E-mail: s.tatjana020382@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Nasonova Irina Alexandrovna. Professor of the chair of Criminal Procedure. 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.

Krasnorutskaya Tatiana Alexandrovna. Associate Professor of the chair of Administrative Law. Candidate of Law.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: s.tatjana020382@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: дознаватель; начальник подразделения дознания; начальник органа дознания; уголовное преследование; правообеспечительная деятельность; предварительное расследование; дознание.

Key words: inquirer; head of inquiry unit; head of inquiry body; criminal prosecution; law enforcement activity; preliminary investigation; inquiry.

УДК 343.13

У. Н. Ахмедов, кандидат юридических наук, доцент

А. В. Кретинин

**ТИПОВЫЕ ПРОЦЕССУАЛЬНЫЕ НАРУШЕНИЯ (ОШИБКИ),
ВСТРЕЧАЮЩИЕСЯ ПРИ ВЫНЕСЕНИИ ОРГАНОМ ДОЗНАНИЯ
РЕШЕНИЯ ОБ ОТКАЗЕ В ВОЗБУЖДЕНИИ УГОЛОВНОГО ДЕЛА
(НА ПРИМЕРЕ АНАЛИЗА ПРОКУРОРСКОЙ
ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ)**

**TYPICAL PROCEDURAL VIOLATIONS (ERRORS)
ENCOUNTERED WHEN THE BODY OF INQUIRY MAKES
A DECISION TO REFUSE TO INITIATE CRIMINAL PROCEEDINGS
(USING THE EXAMPLE OF AN ANALYSIS
OF PROSECUTORIAL LAW ENFORCEMENT PRACTICE)**

Анализ правоприменительной практики в части проведения предварительной проверки постановлений и вынесения по ним процессуальных решений показал, что наибольшее количество решений принимается об отказе в возбуждении уголовного дела. Наибольшее количество решений об отказе в возбуждении уголовного дела принимается органом дознания. В ходе проведенного исследования нам удалось выделить и систематизировать типовые процессуальные нарушения или ошибки, которые встречаются в обосновании решения об отмене постановления об отказе в возбуждении уголовного дела, вынесенного органом дознания.

An analysis of law enforcement practice in terms of conducting preliminary inspections and making procedural decisions on them has shown that the largest number of decisions are made to refuse to initiate criminal proceedings. The largest number of decisions on the refusal to initiate criminal proceedings is made by the body of inquiry. In the course of the conducted research, we were able to identify and systematize typical procedural violations or errors that occur in the justification of the decision to cancel the decision to refuse to initiate criminal proceedings issued by the body of inquiry.

По результатам рассмотрения сообщения о преступлении орган дознания, дознаватель, следователь, руководитель следственного органа вправе принимать решение об отказе в возбуждении уголовного дела. Кроме того, в ст. 148 УПК РФ содержится требование к отказу в возбуждении уголовного дела. В ней указаны субъекты, уполномоченные принимать решение об отказе в возбуждении уголовного дела. Уголовно-процессуальный кодекс Российской Федерации [1] содержит самостоятельную главу 4, которая называется «Основания отказа в возбуждении уголовного дела, прекращения уголовного дела и уголовного преследования».

Полагаем, в законодательстве содержится противоречие относительно полномочий участников на вынесение аналогичного решения. Как

верно указывает С. С. Шестало, решение принимается дознавателем, начальником подразделения дознания, начальником органа дознания, следователем, руководителем следственного органа [2]. В данном случае речь должна идти о полномочии конкретных должностных лиц на принятие решения об отказе в возбуждении уголовного дела. Полагаем, следует рассмотреть данный вопрос несколько шире.

Согласно п. 1 ч. 2 ст. 38 УПК РФ следователь уполномочен возбуждать уголовное дело. Но в данной норме не регламентировано положение о полномочии следователя на отказ в возбуждении уголовного дела. При этом п. 6 ч. 2 ст. 38 УПК РФ наделяет следователя иными полномочиями, которые предусмотрены УПК РФ. Иные полномочия следователя в целом позволяют нам ссылаться на другие нормы УПК РФ, где закреплено

право на вынесение решения от отказа в возбуждении уголовного дела.

Согласно ч. 2 ст. 39 УПК РФ руководитель следственного органа вправе возбудить уголовное дело. Полномочий по отказу в возбуждении уголовного дела законодатель в данной статье за ним не закрепляет. Но процессуальное законодательство наделяет руководителя аналогичными полномочиями, свойственными следователю.

Согласно п. 1 ч. 1 ст. 40.1 УПК РФ начальник подразделения дознания уполномочен поручать дознавателю проверку сообщения о преступлении, принимать по нему решение (ст. 145 УПК РФ). Он п. 4 ч. 1 ст. 40.1 УПК РФ уполномочивается на вынесение ходатайства об отмене процессуальных решений, адресованного прокурору.

Дознаватель согласно ст. 41 УПК РФ наделен рядом полномочий на осуществление процессуальных действий и принятие процессуальных решений в рамках предварительного расследования. При этом в указанной статье не закреплено полномочие на возбуждение уголовного дела или отказа в возбуждении уголовного дела. Указанное полномочие реализуется посредством ссылки на п. 1 ч. 2 ст. 40 УПК РФ.

Анализ практики показал, что наиболее часто прокурором отменяются постановления об отказе в возбуждении уголовного дела, внесенные органом дознания. По этой причине мы обратили внимание на типовые нарушения и ошибки, являющиеся основаниями для признания указанных постановлений незаконными и последующей их отмены.

Согласно требованию ст. 148 УПК РФ при отсутствии основания для возбуждения уголовного дела руководитель следственного органа, следователь, орган дознания или дознаватель выносит постановление об отказе в возбуждении уголовного дела. Отказ в возбуждении уголовного дела по основанию, предусмотренному п. 2 ч. 1 ст. 24 УПК РФ, — отсутствие в деянии состава преступления, допускается лишь в отношении конкретного лица.

Отказ в возбуждении уголовного дела, вынесенный в рамках проверки сообщения, может обжаловаться определенным участникам уголовного судопроизводства. К ним УПК РФ причисляет прокурора, руководителя следственного органа и суд. Указанные субъекты уполномочены принимать решение об отмене постановления об отказе в возбуждении уголовного дела. Статья 148 УПК РФ содержит императивное требование, заключающееся в том, что в случае признания постановления органа дознания, дознавателя об отказе в возбуждении уголовного дела незаконным

или необоснованным прокурор как уполномоченное должностное лицо обязан отменить его. В последующем он обязан направить вынесенное постановление начальнику органа дознания. В этом постановлении он дает конкретные указания на проведение дополнительных процессуальных действий, устанавливает конкретный срок на их исполнение.

Таким образом, вышеуказанные должностные лица, прежде чем выносить постановление об отмене постановления об отказе в возбуждении уголовного дела, должны признавать его незаконным или необоснованным. Примером является постановление прокурора района об отмене постановления об отказе в возбуждении уголовного дела по факту хищения бюджетных денежных средств должностными лицами ООО «...» при выполнении государственного контракта. В описательно-мотивировочной части постановления прокурора было установлено, что 29.01.2025 в ОМВД России по К району субъекта Федерации из 2 отдела УЭБиПК ГУ МВД России по субъекту Федерации по подследственности поступил материал проверки Контрольно-счетной палаты субъекта Федерации по факту выявленных в ходе контрольных мероприятий нарушений при исполнении государственных контрактов. 07.02.2025 оперуполномоченным ГЭБиПК ОМВД России по К району субъекта Федерации Г. принято решение об отказе в возбуждении уголовного дела на основании п. 2 ч. 1 ст. 24 УПК РФ, за отсутствием состава преступления, предусмотренного ч. 3 ст. 159 УК РФ, в действиях должностных лиц ООО «...».

Прокурор района признал вышеуказанное решение незаконным и подлежащим отмене, поскольку посчитал, что были нарушены ст. ст. 7 и 21 УПК РФ и решение об отказе в возбуждении уголовного дела было принято по результату неполно проведенной процессуальной проверки. Так, в рамках проведенной процессуальной проверки прокурор указал, что не произведен опрос должностных лиц ООО «...», представителя заказчика контракта Министерства строительства субъекта Федерации, а также руководства БУЗ СФ «...». Кроме того, указал, что к материалу проверки не приобщена копия государственного контракта, заключенного для выполнения подрядных работ по разработке рабочей документации и строительству объекта здравоохранения в с. НК К района субъекта Федерации.

Помимо этого, к материалу проверки, по мнению прокурора, не были приобщены правоустанавливающие и учредительные документы на ООО «...» (копия устава, выписка из ЕГРН и пр.), копия акта контрольного мероприятия «...», проведенного КСП субъекта Федерации, или выписка

из него. Также к материалу необходимо приобщить ответ на направленный запрос в БУЗ СФ «...» на предоставление заверенных копий документов, касающихся исполнения вышеуказанного контракта. Прокурор также указал на необходимость произведения с участием специалиста сверки фактических объемов работ и затраченных материалов. Кроме того, прокурор обратил внимание на то, что материал проверки поступил в прокуратуру района с ходатайством об отмене незаконного (необоснованного) постановления об отказе в возбуждении уголовного дела.

Таким образом, на примере данного решения прокурора становится понятным, что для признания процессуального решения незаконным он руководствуется положением УПК РФ (ст. 7 УПК РФ — законность при производстве по уголовному делу), а также требованиями других нормативных правовых актов. При этом должностное лицо, вынесшее решение об отказе в возбуждении уголовного дела, может не согласиться с решением прокурора и обжаловать его в установленном порядке.

Следует согласиться с Е. В. Коломеец в том, что «проблема незаконных отказов в возбуждении уголовного дела не менее актуальна и для органов дознания, поскольку наибольшее число процессуальных решений об отказе в возбуждении уголовного дела принимается именно данными органами» [3]. Действительно, сравнительный анализ отмененных постановлений об отказе в возбуждении уголовного дела, вынесенных различными субъектами процессуальной проверки, показал, что в связи с относительно высоким качеством проведения предварительной проверки следователями и двойным контролем принятых решений, как со стороны руководителя, так и прокурора, процессуальные решения, вынесенные следователями, в большей части подробно обосновываются и выполняются качественно.

Процессуальные решения об отказе в возбуждении уголовного дела, вынесенные органом дознания, можно характеризовать как формальные, в большей части низкие по качеству. Как верно отмечает Н. Н. Лунина, «постановления об отказе в возбуждении уголовного дела с формулировкой "опросить гражданина, названного заявителем в качестве лица, совершившего преступление, не представилось возможным, в связи с чем оснований к возбуждению уголовного дела не имеется" нельзя признать законными и обоснованными, но именно к таким доводам в настоящее время прибегают должностные лица для вынесения процессуального решения в установленный уголовно-процессуальным законом срок» [4]. Действительно, изучение большого количества постановлений прокуроров об отмене постановлений об

отказе в возбуждении уголовного дела показало наличие общих, типовых формулировок. Например, 12.12.2024 в ОМВД России по К району субъекта Федерации поступило заявление Н. с просьбой провести проверку по факту сокрытия места нахождения уставных документов и сервера с электронным оборотом документации ООО «...», а также печати, договоров и бухгалтерской документации, которые находились по адресу. 08.02.2025 старшим участковым уполномоченным ОУУП и ПДН ОМВД России по К району С принято решение об отказе в возбуждении уголовного дела на основании п. 1 ч. 1 ст. 24 УПК РФ, т. е. в связи с отсутствием события преступления. Прокурор пришел к выводу, что нарушены статьи 7 и 21 УПК РФ, решение органа дознания признал незаконным, принятым по результату неполной проведенной процессуальной проверки и подлежащим отмене по ряду оснований. По мнению прокурора, по материалу проверки должны были быть опрошены по существу произошедшего Г., Б., О., С., И., должны были быть приняты меры о направлении отдельного поручения в подразделения органов внутренних дел на установление и опрос вышеуказанных граждан. С целью установления лиц, осуществивших вывоз документации и компьютерного оборудования, должен был быть опрошен собственник здания, предоставивший в аренду помещение, а также сотрудники торговой точки, расположенной на первом этаже здания. Данный пример является типичным для постановлений прокуроров об отмене постановлений об отказе в возбуждении уголовного дела и направлении для проведения дополнительной проверки.

Таким образом, на сегодняшний день сложилась ситуация, вынуждающая нас согласиться с теми учеными-процессуалистами, которые считают, что значительную часть отменяемых прокурором процессуальных решений составляют постановления об отказе в возбуждении уголовного дела. Их особенность связана с тем, что они носят характер окончательных [3]. В случае незаконности они препятствуют доступу потерпевших от преступлений к правосудию, так как прекращают проверочные мероприятия [5].

Обобщение постановлений об отмене постановлений об отказе в возбуждении уголовного дела позволило нам установить некоторые типовые недостатки (ошибки). Их можно систематизировать следующим образом:

1. *Признание постановлений об отказе в возбуждении уголовного дела незаконными.* Признав незаконным постановление об отказе в возбуждении уголовного дела, прокурор, руководитель следственного органа или суд обязаны его отменить. При этом, как было указано выше, некоторые постановления из изученных нами должны

были отменяться в связи с их необоснованностью. Данное утверждение может подтверждаться следующим примером из правоприменительной деятельности. Прокурор района принял решение об отмене постановления об отказе в возбуждении уголовного дела. Изучение содержания постановления прокурора об отмене показало, что постановление органа дознания следовало бы отменить в связи с его необоснованностью. В частности, органом дознания было установлено, что 06.09.2024 в ОМВД России по К району субъекта Федерации по телефону поступило сообщение П. о том, что соседка К. выбила стену. 08.02.2025 участковым уполномоченным ОУУП и ПДН ОМВД России по К району Л. принято решение об отказе в возбуждении уголовного дела на основании п. 2 ч. 1 ст. 24 УПК РФ — за отсутствием состава преступления, предусмотренного ч. 1 ст. 167 УК РФ, в действиях К.

Прокурор посчитал данное решение органа дознания незаконным и отменил его. В обоснование принятого решения прокурор указал, что по материалу проверки не установлен размер ущерба, причиненного действиями К., результаты товароведческой судебной экспертизы к материалу проверки до настоящего времени не приобщены. Потребовал также к материалу проверки приобщить сведения о записях актов гражданского состояния К. (сведения о смерти, а также сведения о близких родственниках).

По нашему мнению, в этом случае следовало признать решение органа дознания необоснованным и незаконным. Не вдаваясь в дискуссию относительно правовой сущности и значения термина «необоснованное решение», укажем, что нами необоснованное решение понимается как решение, вынесенное надлежащими субъектами, но в котором неверно определены или не в полном объеме установлены фактические обстоятельства, являющиеся предметом познания. При этом, по нашему мнению, необоснованное решение, вынесенное надлежащим субъектом процессуальной проверки, должно признаваться незаконным. Но внимание следует акцентировать на законодательном требовании об уточнении характера допущенного нарушения. В данном случае существует огромное поле для дискуссии теоретиков и практиков, так или иначе причастных к разрешению проблем досудебного производства по уголовному делу.

2. Неполно проведенная процессуальная проверка. Наиболее распространённое основание для отмены прокурором постановления об отказе в возбуждении уголовного дела. В частности, обобщение прокурорской практики показало, что к основаниям признания процессуального решения подлежащим отмене в связи с неполно проведенной процессуальной проверкой

относятся следующие недостатки: по материалу проверки по существу произошедшего не опрашиваются заявители; достоверно не устанавливаются места произошедшего события; не опрашиваются надлежащие лица; документально не подтверждается стоимость приобретенных предметов и товаров; не приобщаются надлежащие документы; не истребуются материалы исполненного поручения, направленные в органы внутренних дел, и не приобщаются к материалам проверки и т. п. Примером может служить постановление прокурора об отмене постановления об отказе в возбуждении уголовного дела и о возвращении материалов для дополнительной проверки, вынесенное 18.02.2025. Согласно содержанию данного постановления, 04.02.2025 в ОМВД России по К району субъекта Федерации поступило заявление З., в котором он просит оказать помощь в передаче имущества, принадлежащего ООО «...», согласно решению Арбитражного суда от 25.01.2025, в дальнейшем распоряжение. 13.02.2025 старшим участковым уполномоченным ОУУП и ПДН ОМВД России по К району Ч. принято решение об отказе в возбуждении уголовного дела на основании п. 2 ч. 1 ст. 24 УПК РФ в связи с отсутствием в действиях Г. признаков преступления, предусмотренного ч. 1 ст. 330 УК РФ. Прокурором было установлено нарушение ст. ст. 7, 21 УПК РФ и, соответственно, решение участкового было признано незаконным. Прокурор указал, что решение об отказе в возбуждении уголовного дела принято по результату неполно проведенной процессуальной проверки и подлежит отмене по следующим основаниям: по материалу проверки не опрошен по существу произошедшего Г., меры по установлению его местонахождения не приняты; материал проверки содержит не относящееся к делу объяснение гражданина К., в связи с чем его необходимо из материала проверки изъять и приобщить к соответствующему материалу; не произведен осмотр места происхождения по адресу ..., а также не установлены и не опрошены лица, препятствовавшие доступу З. на вышеуказанный объект. Кроме того, прокурор отметил, что участковым не дана правовая оценка действиям гражданина Г. по ч. 1 ст. 315 УК РФ, в связи с чем на основании п. 4 ч. 3 ст. 151 УПК РФ необходимо выделение материала в отдельное производство и направление его для проведения дальнейшей проверки в порядке ст. ст. 144-145 УПК РФ в ОСП по К району УФССП России по субъекту Федерации.

3. Постановление об отказе в возбуждении уголовного дела выносится ненадлежащим должностным лицом. Наглядным примером является следующее решение. Проверив постановление об

отказе в возбуждении уголовного дела, прокурор района принял решение его отменить по причине того, что данное постановление вынесено незаконно. Основанием признания его незаконным явились следующие обстоятельства. Прокурором было установлено, что 31.01.2025 в ОМВД России по К. району из МСО СУ СК России по Воронежской области поступил материал проверки по факту незаконного отчуждения гражданкой С. автомобиля ВАЗ-21114, государственный регистрационный знак О111ОО11. 09.02.2025 старшим участковым уполномоченным ОУУП и ПДН ОМВД России по К району Ч. принято решение об отказе в возбуждении уголовного дела на основании п. 2 ч. 1 ст. 24 УПК РФ, за отсутствием состава преступления, предусмотренного ч. 1 ст. 312 УК РФ, в действиях С. Вышеуказанное решение прокурором было признано незаконным и отменено в силу того, что оно принято в нарушение требований ст. 151 УПК РФ, т. е. подследственности. По нашему мнению, прокурор принял законное и обоснованное решение, указав, что согласно положениям п. 4 ч. 3 ст. 151 УПК РФ по уголовным делам о преступлениях, предусмотренных ст. 312 УК РФ, дознание проводится дознавателями органов принудительного исполнения Российской Федерации, в связи с чем указанный материал проверки необходимо передать для проведения дальнейшей проверки в ОСП по К району УФССП России по соответствующему субъекту.

4. Отсутствие в постановлениях об отказе в возбуждении уголовного дела выводов о достоверности сведений, предоставленных во время проведения проверки сообщения о преступлении. Примером данного недостатка является постановление прокурора, в котором, было установлено, что 03.02.2025 в ОМВД России по К району субъекта Федерации поступило заявление представителя ООО «...» А. о совершении мошеннических действий гражданкой П. 12.02.2025 старшим участковым уполномоченным ОУУП и ПДН ОМВД России по К району субъекта Федерации Ч. принято решение об отказе в возбуждении уголовного дела на основании п. 2 ч. 1 ст. 24 УПК РФ за отсутствием состава преступления, предусмотренного ч. 1 ст. 159.1 УК РФ, в действиях П. Данное решение было признано прокурором незаконным. Постановление об отказе в возбуждении уголовного дела не содержало выводов о достоверности сведений, предоставленных П. в кредитную организацию при оформлении договора кредитования.

5. Ненадлежащая правовая оценка действий лиц со стороны должностного лица, осуществляющего процессуальную проверку по сообщению о

преступлении. Примером такого решения выступает постановление прокурора об отмене постановления об отказе в возбуждении уголовного дела, вынесенного 13.02.2025, и о возвращении материалов для дополнительной проверки. Прокурором установлено, что 16.12.2023 в ОМВД России по К району субъекта Федерации поступило сообщение Ф. о том, что мужчина по имени Г. не исполняет договорные обязательства по ремонту крыши в домовладении по адресу ... 08.02.2025 участковым уполномоченным ОУУП и ПДН ОМВД России по К району субъекта Федерации Л. принято решение об отказе в возбуждении уголовного дела на основании п. 1 ч. 1 ст. 24 УПК РФ, за отсутствием события преступления, предусмотренного ч. 1 ст. 159 УК РФ. Более того, заявителю разъяснено, что в данном случае он может подавать исковое заявление в порядке гражданского судопроизводства, так как указанные отношения являются гражданско-правовыми.

Прокурор посчитал решение участкового незаконным и отменил его. Незаконность отказа в возбуждении дела обосновал принятием по результату неполно проведенной процессуальной проверки.

6. Неверная правовая оценка и определение основания отказа в возбуждении уголовного дела. Данный вывод нами сформулирован в результате анализа совокупности изученных постановлений об отмене постановления об отказе в возбуждении уголовного дела, так как надзирающие и контролирующие лица практически не оспаривали основание прекращения уголовного дела, хотя верное определение такого основания имеет существенное практическое значение, в том числе для разрешения вопросов о реабилитации участников уголовного судопроизводства (подозреваемого, обвиняемого, осужденного) и возмещении вреда в порядке гражданского судопроизводства. Примером данного утверждения может являться следующее решение прокурора, выраженное в отмене постановления об отказе в возбуждении уголовного дела и о возвращении материалов для дополнительной проверки. Проверкой было установлено, что 08.10.2024 в ОМВД России по К району субъекта Федерации поступило заявление Х., в котором она просит привлечь к ответственности гражданина С., который повредил принадлежащую ей беседку. 30.01.2025 участковым уполномоченным ОУУП и ПДН ОМВД России по К району субъекта Федерации Б. принято решение об отказе в возбуждении уголовного дела на основании п. 2 ч. 1 ст. 24 УПК РФ, т. е. за отсутствием составов преступлений, предусмотренных ч. 1 ст. 119, ч. 1 ст. 167 УК РФ, в действиях С.

Прокурор посчитал данное решение незаконным и подлежащим отмене в связи с неполной

процессуальной проверкой. А именно, по его мнению, в рамках проведенной процессуальной проверки не установлена стоимость восстановительного ремонта поврежденной беседки, в связи с чем необходимо истребовать и приобщить заключение товароведческой судебной экспертизы, назначенной 30.01.2025, производство которой поручено экспертам ФБУ «...» Министерства юстиции Российской Федерации.

По нашему мнению, в данном случае следовало указать, что основанием отказа в возбуждении уголовного дела является п. 1 ч. 1 ст. 24 УПК РФ, т. е. отсутствие самого события преступления, а не п. 2 ч. 1 ст. 24 УПК РФ (отсутствие в деянии состава преступления).

Обратным примером прокурорской практики является следующее решение об отмене постановления об отказе в возбуждении уголовного дела и о возвращении материалов для дополнительной проверки. Прокурор К района субъекта Федерации, рассмотрев материалы проверки по обращению Д. установил, что 14.11.2024 в ОМВД России по К району субъекта Федерации из прокуратуры района поступило обращение Д. о хищении принадлежащего ей имущества с территории домовладения по адресу... 08.02.2025 участковым уполномоченным ОУУП и ПДН ОМВД России по К району субъекта Федерации Л. принято решение об отказе в возбуждении уголовного дела на основании п. 1 ч. 1 ст. 24 УПК РФ, за отсутствием события преступления, предусмотренного ч. 1 ст. 158 УК РФ. Прокурор посчитал указанное решение незаконным и подлежащим отмене, указав, что допущено нарушение ст. ст. 7, 21 УПК РФ, т. е. участковым решением принято по результату неполно проведенной процессуальной проверки.

По мнению прокурора, в таком случае по материалу проверки необходимо было определить точный перечень похищенного имущества, установить размер причиненного заявителю ущерба, а также его значительность. Кроме того, необходимо было произвести осмотр места происшествия.

В целом, соглашаясь с решением прокурора, полагаем, что необходимо было указать и на спорность основания прекращения уголовного дела по п. 1 ч. 1 ст. 24 УПК РФ, за отсутствием события преступления, предусмотренного ч. 1 ст. 158 УК РФ. В данном случае присутствует основание для прекращения уголовного дела по п. 2 ч. 1 ст. 24 УПК РФ, за отсутствием состава преступления, предусмотренного ч. 1 ст. 158 УК РФ.

7. *Нарушение разумности сроков уголовного судопроизводства.* Практически по всем постановлениям, вынесенным прокурором в рамках отказа в возбуждении уголовного дела, были установлены сроки дополнительной проверки в пределах от 25

до 30 суток. Указанный срок отводится на устранение нарушений норм УПК РФ, перечисленных в постановлении прокурора об отмене постановления органа дознания об отказе в возбуждении уголовного дела. В изученных постановлениях мы выявили небольшое количество указаний для проведения дополнительной проверки. Целесообразно ли устанавливать 30 суток для проведения одного или двух процессуальных действий, заключающихся, например, в проведении опроса какого-либо лица? Примером может служить следующее решение прокурора об отмене постановления органа дознания об отказе в возбуждении уголовного дела. Рассмотрев материалы проверки по обращению З., прокурор К района установил, что 31.05.2024 в ОМВД России по К району субъекта Федерации поступил рапорт старшего участкового уполномоченного ОУУП и ПДН ОМВД России по К району Р. о поступившем к нему обращении гражданки З. о неправомерных действиях сотрудников кредитной организации при рефинансировании кредита. 06.06.2024 старшим участковым уполномоченным ОУУП и ПДН ОМВД России по К району Р. принято решение об отказе в возбуждении уголовного дела на основании п. 1 ч. 1 ст. 24 УПК РФ, за отсутствием события преступления, предусмотренного ч. 1 ст. 159.1 УК РФ.

Прокурор, признав данное решение незаконным, принял решение о его отмене, посчитав нарушенными ст. ст. 7, 21 УПК РФ. Свое решение прокурор обосновал проведением органом дознания неполной процессуальной проверки. Указал, что по материалу проверки об обстоятельствах проведенного рефинансирования кредита, представленного З., а также изменения процентной ставки в сторону увеличения необходимо опросить представителя АО «...» с обязательным предъявлением документов. При этом, отменив постановление об отказе в возбуждении уголовного дела от 06.06.2024, вынесенное старшим участковым уполномоченным ОУУП и ПДН ОМВД России по К району Р., прокурор установил срок дополнительной проверки 30 суток. Тем самым фактически на проведение одного процессуального действия в виде опроса необоснованно им был отведен длительный временной промежуток, что способствует искусственному затягиванию срока повторной проверки сообщения о преступлении и нарушению разумности срока уголовного судопроизводства.

В заключение хотелось бы добавить, что в процессуальном законодательстве не упоминается кратность принятия органом дознания процессуального решения об отказе в возбуждении уголовного дела, что позволяет ему неоднократно выносить такое постановление, в том числе после проведенной по указанию прокурора дополнительной

процессуальной проверки. Признав это законодательным недостатком, полагаем, что законодатель должен проявить категоричность в данном вопросе — внести соответствующие изменения в содержание УПК РФ относительно принудительного воз-

буждения уголовного дела надзирающим должностным лицом, в частности прокурором, в случае, если обнаруживаются признаки злоупотребления органом дознания полномочием на отказ в возбуждении уголовного дела.

ЛИТЕРАТУРА

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 28.12.2024) (с изм. и доп., вступ. в силу с 05.02.2025) // Собрание законодательства РФ. — 2001. — № 52 (ч. I). — Ст. 4921.

2. Шестало С. С. Порядок обжалования постановлений о возбуждении уголовного дела и об отказе в возбуждении уголовного дела // СПС «КонсультантПлюс». 2025.

3. Коломеец Е. В. Обеспечение законности решений об отказе в возбуждении уголовного дела средствами прокурорского реагирования // Вестник Омской юридической академии. — 2018. — № 3. — С. 314—318.

4. Лунина Н. Н. Стадия возбуждения уголовных дел: необходимость совершенствования очевидна // Российский судья. — 2023. — № 11. — С. 23—28.

5. По делу о проверке конституционности положений частей второй и четвертой статьи 20, части шестой статьи 144, пункта 3 части первой статьи 145, части третьей статьи 318, частей первой и второй статьи 319 Уголовно-процессуального кодекса Российской Федерации в связи с запросами Законодательного Собрания Республики Карелия и Октябрьского районного суда города Мурманска : постановление Конституционного Суда Российской Федерации от 27 июня 2005 г. № 7-П // Доступ из СПС «КонсультантПлюс».

REFERENCES

1. Uголовno-processual'ny'j kodeks Rossijskoj Federacii ot 18.12.2001 № 174-FZ (red. ot 28.12.2024) (s izm. i dop., vstup. v silu s 05.02.2025) // Sbranie zakonodatel'stva RF. — 2001. — № 52 (ch. I). — St. 4921.

2. Shestalo S. S. Poryadok obzhalovaniya postanovlenij o vzbuzhdenii ugovnogo dela i ob otkaze v vzbuzhdenii ugovnogo dela // SPS «Konsul'tantPlyus». 2025.

3. Kolomeecz E. V. Obespechenie zakonnosti reshenij ob otkaze v vzbuzhdenii ugovnogo dela sredstvami prokurorskogo reagirovaniya // Vestnik Omskoj yuridicheskoy akademii. — 2018. — № 3. — S. 314—318.

4. Lunina N. N. Stadiya vzbuzhdeniya ugovny'x del: neobxodimost' sovershenstvovaniya ochevidna // Rossijskij sud'ya. — 2023. — № 11. — S. 23—28.

5. Po delu o proverke konstitucionnosti polozhenij chastej vtoroj i chetvertoj stat'i 20, chasti shestoj stat'i 144, punkta 3 chasti pervoj stat'i 145, chasti tret'ej stat'i 318, chastej pervoj i vtoroj stat'i 319 Uголовno-processual'nogo kodeksa Rossijskoj Federacii v svyazi s zaprosami Zakonodatel'nogo Sobraniya Respubliki Kareliya i Oktyabr'skogo rajonnogo suda goroda Murmansk : postanovlenie Konstitucionnogo Suda Rossijskoj Federacii ot 27 iyunya 2005 g. № 7- P // Dostup iz SPS «Konsul'tantPlyus».

СВЕДЕНИЯ ОБ АВТОРАХ

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.

Кретинин Анатолий Витальевич. Государственный инспектор безопасности дорожного движения районного экзаменационного отделения.

Отдел МВД России по Нововоронежскому городскому округу Воронежской области.

E-mail: Kretinin770@yandex.ru

Россия, 396070, Нововоронеж, ул. Мира, 1.

Akhmedov Ulvi Nizami ogli. Associate Professor of the chair of Criminal Proceedings. 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.

Cretinin Anatoly Vitalievich. State traffic safety inspector of the district examination department.

Department of the Ministry of Internal Affairs of Russia for the Novovoronezh City District of the Voronezh Region.

E-mail: Kretinin770@yandex.ru

Work address: Russia, 396070, Novovoronezh, Mira Str., 1.

Ключевые слова: уголовное судопроизводство; процессуальные решения; процессуальные нарушения или ошибки; возбуждение уголовного дела; отказ в возбуждении уголовного дела.

Key words: criminal proceedings; procedural decisions; procedural violations or errors; initiation of criminal proceedings; refusal to initiate criminal proceedings.

УДК 343.1

М. М. Буслов, кандидат юридических наук, доцент

О. С. Иванченко, кандидат юридических наук, доцент

А. В. Пугачев, кандидат педагогических наук, доцент

НЕЗАКОННЫЙ ОБОРОТ ОРУЖИЯ В РОССИИ: КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА И МЕРЫ ПРЕДУПРЕЖДЕНИЯ

ILLEGAL ARMS TRAFFICKING IN RUSSIA: CRIMINOLOGICAL CHARACTERISTICS AND PREVENTIVE MEASURES

В статье рассмотрены криминологические аспекты незаконного оборота оружия в России, включая статистические данные за три года и особенности личности осужденных. Анализируется судебная практика и выявляются факторы, способствующие совершению преступлений в сфере незаконного оборота оружия. Подчеркивается транснациональный характер подобной деятельности и ее взаимосвязь с иными формами преступности. Отмечается важность комплексного подхода к профилактике, включающей правовое регулирование, оперативно-розыскные меры и социально-экономические программы. В ходе исследования выявляются основные тенденции и предлагаются пути совершенствования уголовной политики.

The article examines the criminological aspects of illegal arms trafficking in Russia, including statistical data for three years and the personality traits of convicted individuals. It analyzes judicial practice and identifies factors that contribute to the commission of crimes in the sphere of illegal arms trafficking. It emphasizes the transnational nature of such activity and its relationship with other forms of crime. It notes the importance of a comprehensive approach to prevention, including legal regulation, operational and investigative measures, and socio-economic programs. The study identifies key trends and suggests ways to improve criminal policy.

Незаконный оборот оружия в Российской Федерации на протяжении длительного времени остается одним из наиболее опасных видов преступлений, представляющих серьезную угрозу общественной безопасности и правопорядку. В России ежегодно фиксируется значительное количество уголовных дел, связанных с хранением, перевозкой, сбытом и использованием оружия без соответствующих разрешений и лицензий. Учитывая политическую и экономическую значимость борьбы с преступностью в сфере незаконного оборота оружия, а также транснациональный характер [1] данной формы криминальной деятельности, исследование ее специфики, тенденций и факторов, способствующих ее распространению, представляется весьма актуальным.

Одной из ключевых особенностей преступлений, связанных с оборотом оружия, является их многоаспектность. С одной стороны, незаконный оборот оружия тесно связан с другими формами преступности (терроризм, экстремизм, незаконный оборот наркотиков и т. д.). С другой — эти

преступления зачастую имеют межгосударственный характер, что значительно усложняет правовое регулирование и международное сотрудничество в данной сфере. Современные технологии, включая «скрытую сеть» (darknet) и криптовалютные платежные системы, еще более расширяют возможности для анонимного приобретения, сбыта и транспортировки оружия, минуя официальные каналы контроля. Это создает новые вызовы для правоохранительных органов и ставит вопрос о необходимости совершенствования как технических, так и правовых методов противодействия.

Актуальность проблемы также обусловлена вовлечением в незаконный оборот оружия широкого круга лиц, многие из которых ранее не имели криминального опыта. На сегодняшний день оружие и его аналоги могут быть изготовлены, переоборудованы либо отремонтированы в полукустарных условиях, а также приобретены у лиц, занимающихся контрабандой или самодельным изготовлением. Преступления данного типа совер-

шаются не только организованными преступными группами, но и гражданами, не состоящими на учете в правоохранительных органах и не проявлявшими ранее интереса к противоправной деятельности. Таким образом, государство сталкивается с необходимостью сформировать эффективную систему раннего выявления и пресечения, учитывающую разные социальные группы и каналы распространения оружия [2].

Отмечается, что незаконный оборот оружия не ограничивается рамками одной страны. Транснациональные преступные сообщества используют каналы контрабанды, а также легальные «лакуны» в законодательстве разных государств как условия злоупотребления правом. Россия, имеющая обширные границы и протяженные транспортные коридоры, вынуждена уделять повышенное внимание вопросам межведомственного и международного взаимодействия в этой сфере [3]. На уровне глобальной безопасности проблема незаконного оборота оружия тесно связана с терроризмом, военными конфликтами и другими деструктивными процессами, угрожающими стабильности различных регионов мира.

Важным аспектом является и демографический профиль осужденных за преступления в сфере незаконного оборота оружия. Анализ данных Судебного департамента при Верховном Суде РФ показывает, что среди лиц, вовлеченных в подобные преступления, есть как молодые люди, так и граждане средних лет, мужчины и женщины, представители разных социальных слоев и уровней образования. Это свидетельствует о том, что преступность в данной сфере не имеет четких социальных или возрастных границ и требует широкого спектра профилактических мер.

Криминологическая характеристика незаконного оборота оружия предполагает рассмотрение совокупности признаков, отражающих специфику данного вида преступности, а именно:

1. *Объект посягательства.* Незаконный оборот оружия посягает на общественную безопасность, а в ряде случаев и на здоровье и жизнь граждан. Оружие, находящееся в нелегальном обороте, может быть использовано при совершении других тяжких преступлений (убийство, разбой, терроризм, экстремизм).

2. *Способы совершения преступления.* Наиболее распространенными способами являются незаконное изготовление, переделка травматического оружия в боевое, контрабанда через государственные границы, кражи оружия у граждан и из воинских частей, а также приобретение и сбыт через нелегальные интернет-площадки [4].

3. *Характер и степень общественной опасности.* Преступления в сфере незаконного оборота

оружия характеризуются высокой степенью общественной опасности, так как способствуют росту вооруженной преступности и осложняют раскрытие иных преступлений.

4. *Пространственно-временные характеристики.* С точки зрения географии наибольшее распространение незаконного оборота оружия отмечается в приграничных районах, крупных мегаполисах и регионах с повышенным уровнем организованной преступности. Во временном аспекте наблюдается стабильная тенденция к росту или сохранению высокого уровня данного вида преступлений в течение последних лет.

5. *Личность преступника.* Лица, совершающие незаконный оборот оружия, нередко обладают либо навыками обращения с оружием (бывшие военнослужащие, работники охранных структур), либо доступом к техническому оборудованию, необходимому для изготовления и переоборудования оружия. В ряде случаев они являются участниками организованных групп, имеющих каналы сбыта и контрабанды, установленные деловые связи в криминальной среде. Однако встречаются и одиночки, которые занимаются изготовлением или хранением оружия исключительно для личных нужд либо с целью разовой финансовой выгоды.

6. *Социальные и демографические характеристики.* Судебная практика последних лет отражает, что в незаконный оборот оружия вовлекаются как мужчины (преимущественно), так и женщины, как молодые люди, так и лица среднего и старшего возраста. Уровень образования колеблется от среднего общего до высшего, при этом немало лиц, имеющих техническую специальность и навыки работы с металлом и оборудованием.

7. *Мотивация.* Мотивы могут быть различными: получение прибыли (сбыт оружия), чувство страха или стремление к самозащите (хранение оружия), идеологические убеждения (экстремизм, террористическая деятельность), а также банальное любопытство или интерес к «запрещенному» (особенно среди молодежи).

Указанные характеристики являются важными для понимания динамики и структуры данного вида преступности. Они также позволяют корректно выстраивать профилактические программы и механизмы противодействия, учитывая специфические условия и особенности в различных регионах Российской Федерации.

Важным источником информации о реальном состоянии преступности в сфере незаконного оборота оружия служат данные Судебного департамента при Верховном Суде РФ. За 2021—2023 гг. наблюдаются следующие тенденции:

1. *Общее количество зарегистрированных преступлений.* Несмотря на некоторые колебания по годам, общее количество уголовных дел по статьям, связанным с незаконным оборотом оружия (ст. 222, 222.1, 222.2, 223, 223.1, 226, 226.1 УК РФ), остается стабильно высоким. В совокупности по указанным статьям в 2023 году было осуждено 6577 человек, в 2022 году — 6451, в 2021 году — 6503 (без учета ст. 222.2, поскольку она была введена только в июле 2021 года, в силу чего статистические сведения, касающиеся данной нормы, отсутствуют) [5].

2. *Региональные особенности.* Наибольшее число дел фиксируется в Центральном, Приволжском и Северо-Кавказском федеральных округах. После начала специальной военной операции не отстают и приграничные территории субъектов РФ, где отмечается высокий уровень контрабандного перемещения оружия из соседних государств, что отражается на структуре преступлений.

3. *Демографические характеристики осужденных:*

- пол: среди осужденных преобладают мужчины (90—95%). Однако доля женщин постепенно растет, что связано как с изменением роли женщины в криминальных группах, так и с вовлечением их в «схемы» по перевозке и хранению оружия;

- возраст: значительная часть (40—50%) приходится на возрастную группу от 25 до 40 лет. При этом прослеживается тенденция к омоложению преступников: в последние годы увеличивается доля осужденных в возрастной группе 18—25 лет;

- образование: около 60% имеют среднее общее или среднее специальное образование; высшее образование встречается у 10—15% осужденных;

- род занятий: значительная часть осужденных (до 40%) не имела постоянной работы.

4. *Виды и способы совершения преступлений.* По статистике, наиболее распространено хранение и ношение огнестрельного оружия, взрывчатых веществ и устройств без соответствующего разрешения. Кроме того, регистрируется немало случаев переделки травматического оружия в боевое, а также нелегальная продажа охотничьих ружей.

5. *Меры наказания.* Как правило, суды назначают наказания в виде условного лишения свободы, особенно в случаях, когда преступление не повлекло тяжких последствий. Для организованных групп наказания, как правило, более строгие и предусматривают реальные сроки лишения свободы. В совокупности по вышеуказанным статьям в 2023 году было назначено наказание в виде

условного лишения свободы 3480 лицам, к реальному отбыванию наказания в местах лишения свободы приговорены 1000 человек [5].

Сопоставительный анализ судебной статистики показывает, что при общем росте или стабильно высоком уровне выявленных преступлений сохраняется высокая латентность данной сферы. Нередко оружие обнаруживается лишь после совершения других преступлений (разбоев, убийств), что указывает на недостаточность профилактических мер.

Анализ личности преступника, совершившего преступление в сфере незаконного оборота оружия, позволяет выявить комплекс факторов, способствующих вовлечению в подобную деятельность.

Среди них:

1. *Социально-экономическая неустроенность.* Отсутствие стабильной работы и достаточного дохода побуждает некоторых граждан искать быстрые и относительно легкие способы заработка, одним из которых может быть нелегальная торговля оружием.

2. *Низкий уровень правовой культуры.* Недостаточное понимание правовых последствий и уровня общественной опасности при незаконном обращении с оружием приводит к тому, что часть граждан не осознает тяжести возможного наказания.

3. *Преступная субкультура.* Лица, вовлеченные в криминальные сообщества, зачастую рассматривают оружие как неотъемлемую часть «профессиональной» деятельности. В таких кругах формируется мнение об оружии как о средстве решения конфликтов и поддержания авторитета.

4. *Личные психологические особенности.* Для некоторых граждан владение оружием ассоциируется с самоутверждением, защитой, повышением статуса. Отдельные осужденные указывают на чувство страха перед реальными или мнимыми угрозами, вынуждающими их «обезопасить себя».

5. *Использование сети Интернет и «теневых» рынков.* Развитие технологической инфраструктуры, анонимные платформы, способы шифрования транзакций (криптовалюты) — все это облегчает доступ к оружию и затрудняет деятельность правоохранительных органов.

6. *Коррупция.* В некоторых случаях факт незаконного оборота оружия оказывается связан с коррупционной деятельностью должностных лиц, которые могут «закрывать глаза» на отдельные каналы поставки или хранения оружия за вознаграждение [6].

7. *Проведение Россией специальной военной операции по демилитаризации и денацификации*

Украины также выступает одним из ключевых факторов, способствующих вовлечению в подобную деятельность по различным мотивам в силу законного доступа к оружию, боеприпасам, взрывчатым веществам и взрывным устройствам [7].

Таким образом, личность преступника в сфере незаконного оборота оружия нередко характеризуется совокупностью социально-экономических и психологических факторов, а также доступом к преступной инфраструктуре (за исключением последнего пункта).

Предупреждение незаконного оборота оружия следует рассматривать как многоуровневую, многосубъектную и многоцелевую систему согласованных мер. Эти меры направлены не только на пресечение уже совершаемых преступлений, но и на устранение или нейтрализацию факторов, способствующих распространению оружия в нелегальном сегменте [8]. В связи с этим предлагаем некоторые меры по совершенствованию законодательства и правоприменительной практики:

1) ужесточить контроль за легальным оборотом оружия. Необходимо совершенствовать порядок выдачи лицензий на хранение и ношение оружия, включая более детальную проверку личности заявителя, его психического здоровья, наличия судимости и т. д.;

2) ввиду проведения СВО усилить контроль оборота оружия на приграничных территориях (усилить досмотр лиц и транспортных средств при выезде из зоны СВО, обеспечить централизованный учет оружия и т. д.);

3) синхронизировать правовые нормы с международными стандартами. Российское законодательство должно оперативно адаптироваться к изменениям в международных соглашениях, регулирующих борьбу с транснациональным оборотом оружия;

4) совершенствовать межведомственное взаимодействие: обмен информацией между пограничной службой, таможенными органами, ФСБ и полицией, необходимый для своевременного выявления контрабандных каналов; участие российских правоохранительных органов в совместных операциях с Интерполом, Европолом и правоохранительными структурами сопредельных государств [9].

5) разработать специальные нормы, регулирующие оборот основных частей оружия. Учитывая, что самодельное или восстановленное оружие зачастую собирается из отдельных деталей, необходимо усилить контроль за их производством и продажей, а именно запретить продажу составных частей (например, частей ударно-спускового механизма), конструктивно подходящих в том числе для боевого оружия, на маркет-плейсах;

6) усилить ответственность за повторное и групповое совершение преступления. Особое внимание следует уделять организованным группам, которые имеют устойчивые каналы поставки и сбыта оружия;

7) использовать потенциал общественных организаций. Налаживание контактов с негосударственными структурами (фондами, общественными объединениями), которые занимаются реабилитацией и адаптацией бывших заключенных с целью оказания социальной адаптации и психологической помощи;

8) обеспечить цифровизацию контроля законного оборота оружия (единые базы данных, электронные лицензии и т. д.). Совершенствование информационных систем, позволяющих отслеживать перемещения оружия, в том числе по маркировке и баллистическим характеристикам. Использование систем видеонаблюдения, средств автоматического обнаружения оружия, биометрических технологий при выдаче лицензий.

Исследование криминологических аспектов и проблем предупреждения незаконного оборота оружия в Российской Федерации позволяет сформулировать следующие выводы:

1. *Многофакторный характер преступности в сфере оборота оружия.* Причины и условия, способствующие совершению данных преступлений, лежат в сфере экономики (безработица, неустойчивое финансовое положение), психологии (стремление к самозащите, самоутверждению), криминальной субкультуры (уважение, «авторитет») и цифровых технологий (анонимные интернет-площадки, криптовалюты).

2. *Транснациональный характер угроз.* Нелегальный оборот оружия часто имеет международные корни, связанные с контрабандой и деятельностью организованных преступных групп. Для эффективного противодействия требуется укрепление международного сотрудничества, обмен информацией и координация правоохранительных органов разных стран [10].

3. *Значимость судебной статистики в формировании уголовной политики.* Данные Судебного департамента при Верховном Суде РФ за последние три года демонстрируют устойчивое количество осужденных за незаконный оборот оружия, рост вовлеченности молодежи, а также повышенную долю организованных форм преступной деятельности. Эти тенденции должны учитываться при разработке законопроектов и в правоприменительной практике.

4. *Роль личности преступника и профилактики рецидива.* Личность правонарушителя, мотивы и социально-демографический профиль имеют ключевое значение для выработки адрес-

ных мер профилактики. Необходимо усилить работу по социальной адаптации, реабилитации и трудоустройству лиц, освободившихся из мест лишения свободы.

5. *Комплексность предупредительной деятельности.* Предупреждение незаконного оборота оружия следует рассматривать как систему, включающую совершенствование законодательства, повышение эффективности правоохранительных органов, развитие социально-экономических программ и профилактическую работу с группами риска.

6. *Перспективные направления развития уголовной политики.* Предполагается, что эффективное противодействие данной категории преступлений возможно только при дальнейшей цифровизации контроля (единые базы данных, элек-

тронные лицензии), тесном взаимодействии между ведомствами и активном участии общества в профилактических программах.

Таким образом, совокупность рассмотренных факторов указывает на необходимость постоянного совершенствования методов борьбы с незаконным оборотом оружия в России. В условиях ускоренного научно-технического прогресса и глобализации криминальных сетей особенно важны системные, согласованные меры, направленные на нейтрализацию и устранение преступных каналов поставок, а также на формирование у граждан правосознания и ответственности за хранение и использование оружия. Только в таком случае можно рассчитывать на снижение криминогенного потенциала и укрепление общественной безопасности.

ЛИТЕРАТУРА

1. Пихов А. Х-А. Транснациональная преступность: система понятий // Вестник Московского университета МВД России. — 2017. — № 6. — С. 109—113.

2. Шалагин А. Е., Гребенкин М. Ю. Незаконный оборот оружия и его предупреждение // Вестник Казанского юридического института МВД России. — 2017. — № 2 (28). — С. 55—60.

3. Патрушев Н. П. Транснациональная преступность, взаимосвязь наиболее опасных ее видов — терроризма, наркотрафика, нелегальной миграции, незаконного оборота оружия и радиоактивных материалов, пиратства // Право и безопасность. — 2010. — № 4. — С. 20—23.

4. Злобин С. Г. Криминологическая характеристика незаконного оборота оружия в РФ // Человеческий капитал как фактор инновационного развития общества : сборник статей международной научно-практической конференции, Магнитогорск, 11 апреля 2019 года. Ч. 1. — Магнитогорск : ОМЕГА САЙНС, 2019. — С. 221—223.

5. Судебная статистика РФ. — URL: <https://stat.api-press.rf> (дата обращения: 15.03.2025).

6. Токманцева Д. Д., Байкалов В. А. К вопросу о причинах преступности, связанной с незакон-

ным оборотом оружия, и мерах по ее предупреждению // Научный компонент. — 2024. — № 4 (24). — С. 109—117.

7. Робак В. А., Закомолдин Р. В. О дополнительных мерах противодействия незаконному обороту оружия в изменяющихся условиях // Искусство правоведения. — 2024. — № 1. — С. 63—68.

8. Желудков Д. В. Криминологическая характеристика и предупреждение незаконного оборота оружия // Актуальные проблемы юриспруденции в России и за рубежом : сборник научных трудов по итогам международной научно-практической конференции, Новосибирск, 10 февраля 2015 года. Вып. II. — Новосибирск : Инновационный центр развития образования и науки, 2015. — С. 23—25.

9. Совершенствование деятельности по предупреждению незаконного оборота оружия на транспорте как фактор обеспечения национальной безопасности // Материалы Шестого международного транспортно-правового форума / под ред. А. А. Чеботаревой, В. Е. Чеботарева, Л. М. Малешиной. — М. : Юридический институт РУТ (МИИТ), 2024. — С. 359—362.

10. Бунакова Т. Н. Проблемы предупреждения преступлений в сфере незаконного оборота оружия // Криминологический журнал. — 2018. — № 3. — С. 4—7.

REFERENCES

1. Pihov A. H-A. Transnacional'naya prestupnost': sistema ponyatij // Vestnik Moskovskogo universiteta MVD Rossii. — 2017. — № 6. — S. 109—113.

2. Shalagin A. E., Grebenkin M. Yu. Nezakonnnyj oborot oruzhiya i ego preduprezhdenie //

Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii. — 2017. — № 2 (28). — S. 55—60.

3. Patrushev N. P. Transnacional'naya prestupnost', vzaimosvyaz' naibolee opasnyh ee vidov — terrorizma, narkotrafika, nelegal'noj migracii,

nezakonnogo oborota oruzhiya i radioaktivnyh materialov, piratstva // Pravo i bezopasnost'. — 2010. — № 4. — S. 20—23.

4. Zlobin S. G. Kriminologicheskaya harakteristika nezakonnogo oborota oruzhiya v RF // Che-lovecheskij kapital kak faktor innovacionnogo razvitiya obshchestva : sbornik statej mezhdunarodnoj nauchno-prakticheskoy konferencii, Magnitogorsk, 11 aprelya 2019 goda. Ch. 1. — Magnitogorsk : OMEGA SAJNS, 2019. — S. 221—223.

5. Sudebnaya statistika RF. — URL: <https://stat.api-press.rf> (data obrashcheniya: 15.03.2025).

6. Tokmanceva D. D., Bajkalov V. A. K voprosu o prichinah prestupnosti, svyazannoy s nezakonnym oborotom oruzhiya, i merah po ee preduprezhdeniyu // Nauchnyj komponent. — 2024. — № 4 (24). — S. 109—117.

7. Robak V. A., Zakomoldin R. V. O dopolnitel'nyh merah protivodejstviya nezakonnemu oborotu oruzhiya v izmenyayushchihsya usloviyah //

Iskusstvo pravovedeniya. — 2024. — № 1. — S. 63—68.

8. Zheludkov D. V. Kriminologicheskaya harakteristika i preduprezhdenie nezakonnogo oborota oruzhiya // Aktual'nye problemy yurisprudencii v Rossii i za rubezhom : sbornik nauchnyh trudov po itogam mezhdunarodnoj nauchno-prakticheskoy konferencii, Novosibirsk, 10 fevralya 2015 goda. Vyp. II. — Novosibirsk : Innovacionnyj centr razvitiya obrazovaniya i nauki, 2015. — S. 23—25.

9. Sovershenstvovanie deyatel'nosti po preduprezhdeniyu nezakonnogo oborota oruzhiya na transporte kak faktor obespecheniya nacional'noj bezopasnosti // Materialy Shestogo mezhdunarodnogo transportno-pravovogo foruma / pod red. A. A. Chebotarevoj, V. E. Chebotareva, L. M. Maleshinoj. — M. : Yuridicheskij institut RUT (MIIT), 2024. — S. 359—362.

10. Bunakova T. N. Problemy preduprezhdeniya prestuplenij v sfere nezakonnogo oborota oruzhiya // Kriminologicheskij zhurnal. — 2018. — № 3. — S. 4—7.

СВЕДЕНИЯ ОБ АВТОРАХ

Буслов Максим Михайлович. Доцент кафедры уголовно-исполнительного и уголовного права. Кандидат юридических наук, доцент.

Воронежский институт ФСИН России.

E-mail: maksimbuslov@mail.ru

Россия, 394072, Воронеж, ул. Иркутская, 1а.

Иванченко Ольга Степановна. Доцент кафедры уголовного права. Кандидат юридических наук, доцент.

Центральный филиал Российского государственного университета правосудия им. В. М. Лебедева.

E-mail: iskorka5@yandex.ru

Россия, 394006, Воронеж, ул. 20-летия Октября, 95.

Пугачев Алексей Валериевич. Заместитель начальника кафедры огневой подготовки. Кандидат педагогических наук, доцент.

Воронежский институт МВД России.

E-mail: aleks-vgfk@yandex.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Buslov Maxim Mikhailovich. Associate Professor of the chair of Criminal Executive and Criminal Law. Candidate of Legal Sciences, Associate Professor.

Voronezh Institute of the Federal Penitentiary Service of Russia.

E-mail: maksimbuslov@mail.ru

Work address: Russia, 394072, Voronezh, Irkutskaya Str., 1a.

Ivanchenko Olga Stepanovna. Associate Professor of the chair of Criminal Law. Candidate of Law, Associate Professor.

The Central branch of the Russian State University of Justice named after V. M. Lebedeva.

E-mail: iskorka5@yandex.ru

Work address: Russia, 394006, Voronezh, 20-letiya Oktyabrya Str., 95.

Pugachev Aleksey Valerievich. Deputy Head of the chair of Fire Training. Candidate of Pedagogical Sciences, Associate Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: aleks-vgifk@yandex.ru.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: незаконный оборот оружия; преступность; предупреждение; судебная статистика; личность преступника; уголовная политика.

Key words: illegal arms trafficking; crime; prevention; judicial statistics; offender profile; criminal policy.

УДК 343.85

А. И. Гайдин, кандидат юридических наук, доцент
Ю. И. Дутов, кандидат педагогических наук, доцент
Н. Ю. Дутов, кандидат юридических наук, доцент
Е. В. Касьянова

ПРОБЛЕМЫ РАССЛЕДОВАНИЯ УГОЛОВНЫХ ДЕЛ О ПРЕСТУПЛЕНИЯХ, СВЯЗАННЫХ С ОБОРОТОМ СРЕДСТВ ПЛАТЕЖЕЙ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ НЕПРАВОМЕРНОГО ОСУЩЕСТВЛЕНИЯ ПРИЕМА, ВЫДАЧИ, ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ

THE PROBLEMS OF INVESTIGATING CRIMINAL CASES OF CRIMES RELATED TO THE TURNOVER OF FUNDS OF PAYMENTS INTENDED FOR THE UNLAWFUL ACCEPTANCE, ISSUANCE, TRANSFER OF FUNDS

В статье рассматриваются проблемы расследования уголовных дел, связанных с незаконным оборотом средств платежей, включая подделку платежных карт, фальсификацию документов, использование электронных средств и технических устройств для совершения преступлений в финансовой сфере. Проанализированы теоретико-правовые основания преступлений, сформулированных статьёй 187 УК РФ, выявлены особенности криминальных схем и проблемы формирования системы доказательств. Особое внимание уделено вопросам квалификации деяний, установлению умысла, а также проблемам взаимодействия правоохранительных органов при расследовании данных преступлений. На основе анализа судебной практики и теоретических исследований предложены рекомендации по совершенствованию методики расследования подобных дел.

The article discusses the problems of investigating criminal cases related to the illicit trafficking of means of payment, including the forgery of payment cards, falsification of documents, the use of electronic means and technical devices to commit crimes in the financial sector. The theoretical and legal bases of crimes formulated by Article 187 of the Criminal Code of the Russian Federation are analyzed, the features of criminal schemes and the problems of the evidence base are revealed. Special attention is paid to the issues of qualification of acts, the complexity of establishing intent, as well as the problems of law enforcement cooperation in the investigation of these crimes. Based on the analysis of judicial practice and theoretical research, recommendations are being developed to improve the practice of investigating such cases.

Цифровизация финансовой сферы, развивающаяся особенно быстро в последнее десятилетие, оказала положительное влияние на качество финансовых услуг и скорость доступа к ним граждан, позволила государству и финансовым организациям выстроить систему контроля за осуществлением транзакций и перемещением финансовых средств, что повлекло качественное улучшение реализации фискальной политики государства. Позитивной стороной данного процесса является ужесточение условий для ведения теневого бизнеса, сокращение возможностей для сокрытия доходов и уклонения от уплаты налогов, легализации средств, полученных преступным путем.

Однако возникшие в связи с этим трудности успешно преодолеваются криминальным сообществом путем реализации новых криминальных схем, связанных с обналичиванием финансовых средств через использование электронных платежных систем при фальсификации данных субъектов транзакций, что отражается на количестве совершенных преступлений с использованием информационно-телекоммуникационных технологий.

Так, согласно официальным данным МВД России, в 2024 году зарегистрировано 765 365 преступлений, совершенных с использованием информационно-телекоммуникационных

технологий или в сфере компьютерной информации. При этом в 2023 году зарегистрировано 676 951 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Тем самым рост только за один год составил 13,1%. Для примера, в 2022 году количество таких преступлений составило всего 522 065. Рост зарегистрированных преступлений можно объяснить влиянием ряда факторов. Одним из них является ускорение темпов проникновения информационных технологий во все сферы человеческой жизни, и прежде всего в сферу финансов. Стремительное внедрение новых программных и технических решений в сферу финансовых отношений формирует благоприятную среду для совершения преступлений в отношении лиц, являющихся потребителями финансовых услуг на основе современных информационных технологий, но физически не успевающих в полной мере разобраться в тонкостях функционирования электронных финансовых инструментов.

При этом статистика преступлений, совершенных с использованием или применением фиктивных электронных платежей, в последние годы демонстрировала рост количества таких деяний. В частности, в 2022 году прирост составил 39%, в 2023 — 38%. В 2024 году произошло резкое сокращение зарегистрированных уголовных дел по таким преступлениям — на 61,8% [1]. В условиях отсутствия видимых экономических предпосылок к снижению количества таких преступлений мы склонны считать причиной сложившейся ситуации неопределенность судебной практики привлечения к ответственности по ст. 187 УК РФ, что повлекло снижение уровня наступательной активности правоохранительных органов по выявлению и расследованию данных преступлений. Сложившееся положение дел связано с Кассационным определением Восьмого кассационного суда общей юрисдикции от 17.10.2024 по делу № 77- 4159/2024, в котором суд обосновывал отмену обвинительного приговора, указав, что предъявленное обвинение не содержит описание признаков, подтверждающих назначение электронных средств и электронных носителей информации, которые сбыла осужденная, для неправомерного осуществления приема, выдачи, перевода денежных средств [2].

Изменение судебной практики фактически декриминализовало значительную долю противоправных действий по вовлечению в криминальный оборот электронных средств платежей, обеспечивающих сокрытие сведений о реальных субъектах осуществления транзакций. Это не может не оказать негативного влияния на сложившуюся

систему мер противодействия экономическим преступлениям.

Проблематика данных преступлений приобретает особую актуальность ввиду сложности их выявления и квалификации, определения методов расследования, что подтверждается как статистическими данными МВД России, так и материалами судебной практики. В этой связи целесообразно рассмотреть как сам механизм совершения данных преступлений, так и выделить проблемы, возникающие в ходе их расследования и квалификации.

Статья 187 УК РФ предусматривает уголовную ответственность за неправомерный оборот средств платежей, где под данное понятие подпадают как физические платежные карты, так и электронные носители информации, технические устройства и компьютерные программы. Законодателем был проведен четкий градационный подход: предмет преступления включает поддельные платежные средства, распоряжения о переводе денежных средств, а также документы, используемые при проведении безналичных расчетов. При этом, формулируя данную статью, законодатель использует отсылочную конструкцию нормы, не разъясняя включенные в нее понятия, что вызывает проблемы у сотрудников правоохранительных органов.

Платежные карты — это эмитированные кредитной организацией банковские карты, в том числе расчетные (дебетовые), кредитные и предоплаченные карты. В России предусмотрен оборот дебетовых, кредитных и предоплаченных карт, предусмотренных статьей 7 Федерального закона «О национальной платежной системе».

Следует учитывать, что к предмету преступления не относятся карты, эмитированные организациями, не имеющими статуса кредитных, включая те, которые предназначены для осуществления расчетов за предварительно оплаченные товары, работы или услуги (например, телефонные и проездные карты, а также карты, выпускаемые различными торгово-сервисными предприятиями) [3].

Распоряжения о переводе денежных средств — документы, обеспечивающие доступ к безналичным и электронным денежным средствам в рамках предусмотренных законом форм безналичных расчетов. Разъяснения по данному виду платежей закреплены положением Банка России от 29.06.2021 № 762-П, согласно которому к числу распоряжений о переводе денежных средств отнесены: платежные поручения, распоряжения и требования; инкассовые поручения; платежные и банковские ордера, следовательно, это документы, обеспечивающие доступ к безналичным денежным средствам и распоряжение ими в форме безналичных расчетов. В частности,

под квалификацию статьи 187 УК РФ подпадают действия лица, которое занимается обналичиванием, составляет заведомо для себя поддельное платежное поручение для того, чтобы банк осуществил перевод. Например, ФИО1, генеральный директор ООО ПКФ «Юг Прайм», изготовил поддельное платежное поручение № от ДД.ММ.ГГГГ о переводе денежных средств в размере 301 480 рублей с расчетного счета своей компании на расчетный счет ООО «Первая Логистическая». Платежное поручение содержало заведомо ложные сведения о размере и факте платежа. Используя это платежное поручение, ФИО1 обманул сотрудников ООО «Первая Логистическая», которые, полагая, что получили 100-процентную предоплату за поставку товара по договору, отгрузили в адрес ООО ПКФ «Юг Прайм» три вида пигмента общей стоимостью 301 480 рублей. Этими средствами ФИО1 распорядился по своему усмотрению [4].

Документы оплаты — иные документы на бумажных носителях или в электронном виде (кроме распоряжений о переводе денежных средств), оформляемые кредитной организацией при совершении операций по приему, выдаче или переводу денежных средств (приходный кассовый ордер, расходный кассовый ордер, денежный чек и т. п.). В частности, судебная практика считает преступлением использование в личных целях поддельного документа — расходного кассового ордера как средства для неправомерного осуществления выдачи денежных средств [5].

Не образует состава преступления неправомерный оборот документов, не дающих обладателю имущественных прав, не удостоверяющих требование, поручение или обязательство перечислить денежные средства, фиксирующие факт платежа или его начисления (например, товарные, кассовые чеки) [3], так как товарный (кассовый) чек лишь фиксирует факт оплаты товара или услуги.

Согласно статье 187 УК РФ, указанные предметы преступления должны быть поддельными. В классическом понимании подделка платежного средства подразумевает его изготовление лицом, не имеющим соответствующих полномочий, либо внесение недостоверных сведений, искажающих первоначальное содержание и не соответствующих волеизъявлению его эмитента. Таким образом, совершение подделки возможно исключительно субъектом, не уполномоченным на эмиссию данного средства платежа [6]. При этом поддельный объект должен обладать существенным сходством с подлинными платежными инструментами как по внешнему виду, так и по физическим характеристикам, поскольку значительное расхождение с оригиналом исключает

его оборотоспособность и, следовательно, основания для квалификации деяния по статье 187 УК РФ [7].

Далее законодатель перечисляет еще ряд предметов.

Электронные средства платежа — средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств (например, электронных кошельков) [8].

Проведенный анализ судебно-следственной практики позволяет определить, что в качестве электронных средств чаще всего выступают: банковская карта; электронно-цифровая подпись; одноразовые СМС-пароли, позволяющие идентифицировать клиента посредством сети Интернет и управлять удаленно расчётным счётом организации; логин и одноразовый пароль в виде СМС-сообщения; абонентский номер мобильного телефона, на который приходят СМС-сообщения; ключи электронных подписей; код подтверждения в системе дистанционного банковского обслуживания. В частности в качестве примера можно привести умышленную передачу доступа к системе дистанционного банковского обслуживания «Сбербанк Бизнес Онлайн» с целью неправомерного осуществления приема, выдачи, перевода денежных средств [9].

Отдельного рассмотрения заслуживает само содержание диспозиции ч. 1 ст. 187 УК РФ. Так, если осуществить анализ её грамматической структуры, то можно сделать вывод об отсутствии необходимости в установлении признака «поддельности» в отношении электронных средств и электронных носителей информации. В частности, использование законодателем союза «а также» указывает на присоединение однородного члена предложения, который, будучи дополнительным, отделяется от предыдущих элементов [10]. Данный вывод подтверждается результатами правоприменительной практики: когда предметом преступления становятся средства платежей, относящиеся ко второй части диспозиции, их квалификация, как правило, основывается не на факте подделки (то есть их изготовления неуполномоченным лицом или внесения в них недостоверных сведений), а на нарушении воли владельца денежных средств либо на отсутствии правовых оснований для их перевода. В связи с этим можно согласиться с позицией исследователей, отмечающих, что в данном случае происходит

подмена категории «поддельности» понятием «незаконность» [11].

Следовательно, передача полученных легально в финансовой организации соответствующих средств и носителей третьим лицам для совершения ими неподконтрольных номинальному владельцу счета операций подразумевает сбыт предмета преступления в целях неправомерного осуществления приема, выдачи, перевода денежных средств [11].

Электронный носитель информации — материальные носители, используемые для оборота информации с помощью ЭВМ [12]. К таким можно отнести различного рода внешние накопители (USB-устройства), используемые для аутентификации пользователя или подтверждения проведенных транзакций в системе онлайн-платежей [13], а также различные накопители информации — внешние накопители на жестких магнитных дисках, SSD, карты памяти и так далее. Например, клонирование в целях продажи USB-ключа банк-клиента (аппаратного токена) при наличии на то соответствующего запрета кредитной организации несет в себе основания привлечения к ответственности по статье 187 УК РФ [14]. При этом судебно-следственная практика в контексте статьи 187 УК РФ чаще всего определяет в качестве электронного носителя информации USB-токен, на котором содержатся сведения — логин и пароль для осуществления платежных действий [15].

Технические устройства — это различного рода приспособления, предназначенные для осуществления незаконных операций с денежными средствами. К техническим устройствам, попадающим под действие статьи 187 УК РФ, можно отнести: электронный терминал (POS-терминал), банкомат, платежный терминал, устройства с модулем NFC и т. д., алгоритм работы которых предполагает проведение неправомерных платежных операций. Стоит отметить, что к техническим устройствам и компьютерным программам по смыслу ст. 187 УК РФ не относятся устройства для скимминга и другое аналогичное оборудование, а равно вредоносное программное обеспечение для получения неправомерного доступа к конфиденциальной информации владельцев банковских счетов или «электронных кошельков» [3]. При этом ряд ученых к таковым относят и именно скимминговое оборудование [16], что вызывает недопонимание среди правоприменителей. Таким образом, следователь должен понимать, что в действующем законодательстве отсутствует понятие и перечень технических устройств. Вследствие этого их виды следователь вправе определять самостоятельно, исходя из грамматического толкования данного термина,

целевого назначения такого устройства. В случае возникновения сложностей с определением данной категории необходимо привлекать специалиста.

Примерами незаконного использования технических устройств могут являться: сбыт электронного терминала, в алгоритм работы которого заложена отправка поступающих от покупателя денежных средств не на счет продавца, а на сторонний расчетный счет; разработка банкомата, позволяющего осуществлять расчетные операции по заблокированным банком-эмитентом платежным картам; приобретение самодельного ридера, позволяющего дистанционно считывать банковские карты и совершать транзакции по списанию с них безналичных средств [14].

Вновь акцентируем внимание на том, что объектом преступного деяния, предусмотренного статьёй 187 Уголовного кодекса Российской Федерации, выступает исключительно программное обеспечение (ПО), предоставляющее возможность осуществления несанкционированных денежных операций в обход установленных процедур проведения платежей.

Функционал такого программного обеспечения должен включать в себя возможность выполнения незаконных операций с денежными средствами уже на этапе разработки. Примером может служить создание вредоносного программного обеспечения («червя»), предназначенного для внедрения в систему интернет-банкинга клиента, что позволяет осуществлять несанкционированное списание денежных средств со счёта организации в интересах злоумышленника.

Объективная сторона статьи 187 УК РФ выражена в совершении определенных действий.

Изготовление как элемент преступной деятельности в сфере незаконного оборота средств платежей включает создание предметов преступления либо частичную их подделку с целью последующего использования в противоправных схемах.

Основные формы данных действий включают:

клонирование банковских карт, осуществляемое посредством неправомерного доступа к конфиденциальной информации владельцев счетов;

оформление платежных карт на подставных лиц, неосведомленных о незаконном использовании их персональных данных;

фальсификацию платежных поручений, выполняемую от имени фиктивных юридических лиц с целью осуществления мнимых финансовых транзакций;

регистрацию электронных кошельков, используя данные подставных лиц, что позволяет обходить системы финансового контроля;

создание фиктивных платежных инфраструктур, таких как ненастоящие банкоматы и терминалы, не аффилированные с кредитными организациями [3].

Приобретение предполагает любую форму завладения предметом деяния, включая покупку, получение в дар или находку.

Хранение предполагает размещение объекта преступления в определённом месте или у конкретного лица, включая условия, которые обеспечивают его сохранность. Таким образом, следственные органы должны определить места и условия хранения поддельных платежных средств, а также лиц, ответственных за их сохранность. Это помогает выявить возможных соучастников и дополнительные эпизоды преступления.

Транспортировка представляет собой процесс перемещения объекта, связанного с совершением противоправного деяния, из одной локации в другую с применением транспортных средств. Необходимо установление маршрутов и способов транспортировки поддельных платежных средств от места изготовления или приобретения к месту сбыта.

Сбыт поддельных платёжных средств подразумевает передачу другим лицам поддельных платёжных карт или иных платёжных инструментов под видом настоящих (продажа, дарение и т. д.). В случае если такие поддельные платёжные карты или иные платёжные инструменты заведомо непригодны для использования, подобные действия квалифицируются как мошенничество и подлежат рассмотрению в соответствии со статьями 158.1 или 159 Уголовного кодекса Российской Федерации, согласно пункту 18 Постановления Пленума Верховного Суда РФ от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

Таким образом, при отсутствии цели сбыта действия лица, изготовившего указанные документы, будут квалифицированы по другим статьям УК РФ. Так, изготовление кредитных (расчетных) карт с целью незаконного использования самим изготовителем и, таким образом, последующего незаконного присвоения и расходования не принадлежащих ему денежных средств либо использование им этих документов будет квалифицировано либо как приготовление к мошенничеству, либо как оконченное преступление — мошенничество.

Преступление считается оконченным с того момента, как лицо изготовило хотя бы одну карту или платежный документ, независимо от того, удалось ли осуществить их сбыт или нет, то есть наступление общественно опасных последствий в данном случае не обязательно [17].

Анализ судебной практики показал, что наиболее часто суды квалифицируют деяния по ч. 1 ст. 187 УК РФ, когда лица представляют документ, удостоверяющий личность, для внесения в единый государственный реестр юридических лиц сведений о подставном лице, а затем приобретают в целях сбыта и осуществляют сбыт электронных средств и электронных носителей информации, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств [18].

Таким образом, обстоятельства, подлежащие установлению и доказыванию по делам о неправомерном обороте средств платежей, включают в себя ряд ключевых из них, требующих детального рассмотрения и анализа, так как их доказанность оказывает наибольшее влияние на квалификацию соответствующих преступлений, а также на обеспечение справедливого судебного разбирательства.

Отметим, что в вопросах выявления и квалификации данных преступлений особое значение приобретает механизм преступной деятельности, связанной с оборотом средств платежей, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств.

Типовая криминальная схема незаконного обналичивания средств и вывода их из-под учета может включать в себя систему действий, реализуемых чаще всего участниками преступной группы в рамках заранее разработанного плана.

Обозначим ключевые процедуры, порождающие основной объем следов преступлений:

- поиск подставных лиц для регистрации на их имена юридических лиц и индивидуальных предпринимателей за денежное вознаграждение;
- привлечение к преступной деятельности за денежное вознаграждение лиц в целях их использования при осуществлении незаконной банковской деятельности путем регистрации в качестве подставных лиц при регистрации (создании) в отношении них юридических лиц и индивидуальных предпринимателей;
- сопровождение подставных лиц в уполномоченный государственный орган для регистрации ими на свои имена юридических лиц и в качестве индивидуальных предпринимателей;
- оплата государственной пошлины при регистрации (создании) юридического лица и в качестве индивидуального предпринимателя, внесении изменений в сведения о нем, содержащихся в ЕГРЮЛ (при смене исполнительного органа);
- нотариальное заверение документов, необходимых при регистрации юридического лица и индивидуального предпринимателя, смене учредителя и исполнительного органа;

- консультирование подставных лиц о порядке и последовательности действий при сдаче в уполномоченный государственный орган документов, необходимых для регистрации (создания) юридического лица и в качестве индивидуального предпринимателя, внесения изменений в сведения о нем, содержащихся в ЕГРЮЛ;

- получение, хранение и использование в преступной деятельности поданных документов;

- изготовление и получение печатей подконтрольных юридических лиц и индивидуальных предпринимателей, используемых в обналичивании средств;

- хранение печатей и учредительных документов;

- сопровождение подставных лиц в кредитные организации для подачи заявок на открытие расчетных счетов, а также подача заявлений посредством телекоммуникационных каналов связи на открытие счетов для придания видимости осуществления финансово-хозяйственной деятельности данных юридических лиц и индивидуальных предпринимателей;

- получение доступа к программам «Банк-Клиент» и обеспечение возможности незаконных транзакций;

- получение электронных ключей, паролей и шифров, использующихся для доступа к управлению расчетными счетами подконтрольных юридических лиц и индивидуальных предпринимателей путем использования системы удаленного доступа к ним посредством сети Интернет, а также получение банковских карт, оформленных на подставных лиц, для незаконного обналичивания денежных средств путем снятия наличности в банкоматах;

- приискание среди руководителей различных коммерческих организаций заинтересованных в «обналичивании» имеющих на счетах их организаций денежных средств;

- непосредственные контакты лично и с использованием средств коммуникации с клиентами по обсуждению вопросов технологии обналичивания денежных средств с учетом направленности деятельности их организаций с целью маскировки противоправности действий, передача им информации о наименованиях подконтрольных преступникам организаций и реквизиты их расчетных счетов для перечисления подлежащих последующему обналичиванию денежных средств;

- разработка и реализация процедур обналичивания средств, которые типично включают действия по переводу средств на расчетные счета подконтрольных юридических лиц и индивидуальных предпринимателей от субъектов предпри-

нимательской деятельности (клиентов) по вымышленным основаниям бесхозяйственных отношений, их снятие в терминалах банков посредством банковских карт и в отделениях банков по чековым книжкам, возврат клиентам наличных денежных средств за минусом комиссионного вознаграждения;

- осуществление документального «прикрытия» перечислений клиентами денежных средств на подконтрольные преступной группе расчетные счета и дальнейшее их движение по этим счетам путем оформления подложных документов между организациями клиентов и подконтрольными преступникам фирмами, а также, для дополнительной маскировки, между подконтрольными организациями. Интеллектуальный подлог в документах выражается в фиктивном отражении не имеющих реального характера хозяйственных отношений (поддельные договоры, товарные накладные, счета-фактуры, акты выполненных работ (приема-передачи товара), платежные поручения и иные необходимые документы или их копии). Они передаются клиентам обналичивания и используются в отчетности подконтрольных фирм с целью создания видимости правомерности осуществляемых транзакций;

- осуществление личных встреч с клиентами для передачи им наличных денежных средств;

- ведение учета движения денежных средств, полученных преступным путем;

- подбор лиц из числа сотрудников кредитных организаций, нотариальных контор и иных лиц, способствующих подготовке необходимых документов для открытия расчетных счетов, получения электронных носителей и т. д., с целью дальнейшей передачи этими лицами средств платежей или электронных носителей.

Уголовное законодательство в настоящее время закрепляет ряд составов преступлений, которые в последнее время получили распространение и активно реализуются в криминальных схемах по обналичиванию безналичных денежных средств. Статья 172 УК РФ регулирует ответственность за незаконную банковскую деятельность без регистрации или лицензии, если это привело к крупному ущербу или извлечению дохода в крупном размере. Статья 173.1 УК РФ касается незаконного образования юридических лиц через подставных лиц, включая: создание и реорганизацию юрлиц через подставных лиц; подачу данных для внесения сведений о подставных лицах в реестр юридических лиц. Часть 1 статьи 173.2 УК РФ предусматривает ответственность за предоставление документов, удостоверяющих личность; выдачу доверенности для внесения данных о подставном лице в реестр юридических

лиц. Часть 2 статьи 173.2 УК РФ регулирует ответственность за незаконное приобретение документов, удостоверяющих личность; использование незаконно полученных персональных данных; действия по введению данных о подставных лицах в реестр юридических лиц. Все эти преступления направлены на сокрытие данных о субъектах криминальных транзакций при обналичивании денежных средств.

Механизм преступной деятельности по неправомерному обороту средств платежей представляет собой совокупность взаимосвязанных действий, направленных на извлечение незаконной материальной выгоды посредством манипуляций с финансовыми инструментами. Ключевым элементом данного механизма является предмет преступного посягательства.

Исходя из диспозиции ст. 187 УК РФ, предмет преступления включает в себя:

- 1) поддельные платёжные карты;
- 2) поддельные распоряжения о переводе денежных средств;
- 3) поддельные документы и средства оплаты (за исключением случаев, предусмотренных ст. 186 УК РФ);
- 4) электронные средства, электронные носители информации, технические устройства, компьютерные программы, предназначенные для неправомерного приёма, выдачи, перевода денежных средств.

Проведенный нами анализ судебно-следственной практики и научной литературы, исходя из предмета преступной деятельности, позволил выделить наиболее распространенные механизмы преступной деятельности по неправомерному обороту средств платежей [19].

Наиболее распространенными способами совершения преступления являются:

1) сбыт электронных средств и электронных носителей информации, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств.

Данный способ типично является составной частью экономической преступной схемы, в которой субъект за вознаграждение соглашается стать учредителем и номинальным руководителем организации. Этот субъект открывает банковские счета с дистанционным обслуживанием (ДБО), а затем передает электронные платежные средства организатору преступной схемы. Эти средства используются для доступа к системам ДБО и выполнения незаконных переводов, снятия наличных и других финансовых операций.

Однако, как было указано выше, на сегодняшний день позиция судов по квалификации выражена в необходимости доказывания сбыта под-

дельных карт и электронных средств, которые по своему функционалу позволяют проводить операции с деньгами без ведома владельца счета и в обход системы безопасности банка. Открытие банковских счетов, получение соответствующих документов и карт является законным действием. Нарушение условий договора с банком может привести к гражданским последствиям, но не к уголовной ответственности.

Например, оправдательный приговор по ч. 1 статьи 187 УК РФ был вынесен в 2025 году. Обвиняемая Л. была оправдана, потому что не знала о незаконном использовании переданных ею электронных средств и носителей информации.

По версии обвинения: Л., будучи директором ООО «Меридиан», передала за вознаграждение электронные средства платежа и носители информации, используемые для операций с денежными средствами на счетах в различных банках. Она осознавала, что эти операции будут проводиться без законных оснований и по указанию третьих лиц.

Суд первой инстанции признал Л. виновной в сбыте электронных средств и квалифицировал её действия по ч. 1 ст. 187 УК РФ.

Хотя факты передачи электронных средств были установлены, суд не учел, что статья 187 УК РФ предусматривает ответственность только за сбыт средств, изначально созданных для противоправных целей. В деле отсутствуют доказательства того, что Л. знала о последующем незаконном использовании переданных средств. Её показания указывают на то, что она действовала ради вознаграждения, а о незаконности деятельности компании узнала позже.

Таким образом, по мнению суда, действия Л. не содержат признаков преступления, предусмотренного статьей 187 УК РФ. Это стало основанием для прекращения уголовного дела и признания права Л. на реабилитацию [21].

Несмотря на кардинальное изменение судебной практики привлечения к ответственности по ст. 187 УК РФ за действия, совершаемые рассматриваемым способом, считаем преждевременным исключать соответствующую систему действий из группы типичных способов неправомерного оборота средств платежей, ввиду всё же продолжающегося периода формирования судебной практики и понимания того, что такие неправомерные действия являются составной частью криминальных схем экономических преступлений;

2) изготовление и использование поддельных платежных поручений, на основании которых с целью обналичивания осуществляется неправомерный перевод денежных средств с расчетных счетов организации на расчетные счета фиктивных юридических лиц.

Преступник, являясь руководителем организации, используя свое служебное положение, действуя из корыстных побуждений, изготавливает и использует поддельные платежные поручения, на основании которых в целях дальнейшего обналичивания осуществляет неправомерный перевод денежных средств. Документы признаются поддельными, если установлено наличие в них признаков как незаконного изменения отдельных частей подлинного документа, искажающего его действительное содержание, так и изготовления нового документа, содержащего заведомо ложные сведения [21]. Например, фиктивные платежные поручения по несуществующим поставкам [22], услугам [23];

3) изготовление поддельных дубликатов платёжных карт жертв на основе заранее полученных данных о карте при помощи специальных технических средств (в частности, скиммера, клавиатурных накладок, скрытых камер наблюдения и др.) с последующим хищением денежных средств, имеющихся на балансе счета.

За последние годы число случаев подделки банковских карт сократилось кратно. Это обусловлено тем, что системы защиты банкоматов и платежных карт в последние годы стали совершеннее, небезопасные банковские карты (с магнитной полосой без чипа) выходят из оборота, а преступники стали чаще использовать методы социальной инженерии для получения данных платежных карт и их использования для хищения средств со счетов. Ранее преступники устанавливали в банкоматах и POS-терминалах скиммеры (накладки на слоты для считывания карты), которые копируют всю информацию о карте, хранящуюся в магнитной полосе: имя держателя, номер карты, срок окончания ее действия, CVV и CVC коды. После этого создавалась копия карты, которую использовали для оплаты. Для получения доступа к PIN-коду использовались мини-видеокамеры, реже — накладные клавиатуры. Эти устройства устанавливались либо в банкоматах, либо около POS-терминалов. Информация с чипа обычным путем не может быть скопирована, поэтому преступники не подделывают такого рода платежные карты [24].

Таким образом, ряд современных криминальных схем преступной деятельности в экономической сфере представляют собой сложную в организационном аспекте совокупность криминальных действий, направленных на извлечение преступного дохода при совершении противоправных транзакций в электронных платежных системах, в том числе с использованием возможностей дистанционного банковского обслуживания. В механизме соответствующей преступной деятельности присутствуют способы, квалифицируемые

по различным составам УК РФ. В экономических криминальных схемах неправомерный оборот средств платежей, выражающийся чаще всего в сбыте электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств, выступает составной неотъемлемой частью реализации преступного замысла, обеспечивает возможность использования в криминальных целях электронных финансовых инструментов и сокрытие данных об участниках преступной деятельности.

На основании вышеизложенного можно сделать вывод о том, что одной из главных проблем при расследовании преступлений, связанных с оборотом средств платежей, является сложность формирования доказательной базы.

Следователи сталкиваются с рядом трудностей:

1. Отсутствие или фрагментарность цифровых источников доказательственной информации. В связи с тем что преступные финансовые операции совершаются в электронной среде, зачастую требуется проведение комплексных экспертиз, направленных на восстановление и анализ соответствующих транзакций. Предметом таких исследований выступают электронные носители информации и данные, зафиксированные на них. Недостатки в деятельности по их собиранию зачастую невозможно компенсировать иными источниками, что влечет неполноту доказательственной базы.

2. Проблемы квалификации деяния. В ряде случаев происходит «подмена» понятия «поддельность» на «незаконность», что затрудняет правильную правовую оценку действий подозреваемых. Например, когда речь идет об использовании поддельных платежных поручений для осуществления переводов, необходимо четко установить наличие умысла и понимание субъектом характера совершенного деяния.

3. Сплоченность и криминальный профессионализм преступных групп. Действия организованных групп зачастую маскируются под легальные финансовые операции, что приводит к трудностям в установлении полной картины преступной деятельности.

Низкая эффективность решения указанных проблем приводит к последствиям, выражающимся в снижении количества уголовных дел данной категории и росте количества оправдательных приговоров.

Таким образом, проведенный нами анализ позволяет сделать вывод, что преступления, связанные с оборотом средств платежей, представляют собой сложную и многогранную проблему,

требующую междисциплинарного подхода и постоянного совершенствования как нормативно-правовой базы, так и методик расследования. Сложности в квалификации деяния, низкое качество системы доказательств по уголовным делам, технологическая сложность преступных схем и высокая организованность преступных групп являются основными вызовами для следственных органов.

Преодоление указанных проблем нам видится в комплексе действий:

совершенствовании законодательства с учетом специфики цифровых источников доказательственной информации;

совершенствовании методов и форм кримина-

листического сопровождения процесса расследования;

повышении уровня квалификации следователей, осуществляющих производства по рассмотренной категории дел;

усилении международного сотрудничества в борьбе с транснациональными преступными схемами.

Реализация этих мер позволит не только повысить эффективность расследования уголовных дел, но и создать условия для более быстрого и справедливого судебного разбирательства, что в конечном итоге будет способствовать укреплению финансовой безопасности и стабильности в стране.

ЛИТЕРАТУРА

1. Состояние преступности в России: статистические данные // URL: <https://мвд.рф/reports> (дата обращения: 22.03.25).

2. Кассационное определение Восьмого кассационного суда общей юрисдикции от 17.10.2024 по делу № 77-4159/2024 // СПС «КонсультантПлюс».

3. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / К. А. Барышева, Ю. В. Грачева, Р. О. Долотов [и др.] ; под ред. Г. А. Есакова. 9-е изд., перераб. и доп. — М. : Проспект, 2021. — 816 с.

4. Приговор № 1-150/2023 1-19/2024 от 23 января 2024 г. по делу № 1-19/2024 // URL: <https://sudact.ru> (дата обращения: 23.03.2025).

5. Приговор № 1-43/2024 1-637/2023 от 30 января 2024 г. по делу № 1-43/2024 // URL: <https://sudact.ru> (дата обращения: 23.03.2025).

6. Соловьева Е. А. О проблемах правоприменительной практики, формируемой при применении уголовной ответственности за неправомерный оборот платежных документов // *Ex jure*. — 2020. — № 1. — С. 95—105.

7. Нудель С. Л., Печегин Д. А. Вопросы квалификации неправомерного оборота средств платежей (по признаку предмета) // *Уголовное право*. — 2020. — № 3. — С. 35.

8. О национальной платежной системе : Федеральный закон от 27.06.2011 № 161-ФЗ // СПС «КонсультантПлюс».

9. Приговор № 1-336/2023 1-34/2024 от 26 января 2024 г. по делу № 1-336/2023 // URL: <https://sudact.ru> (дата обращения: 23.03.2025).

10. Быкова Е. Г., Казаков А. А. Дискуссионные аспекты признания электронных средств и электронных носителей информации предметом преступления, предусмотренного ст. 187 УК РФ // *Российский судья*. — 2024. — № 4. — С. 13—18.

11. Чернышев Д. Б. К вопросу о предмете преступления, предусмотренного статьей 187 Уголовного кодекса Российской Федерации // *Вестник Казанского юридического института МВД России*. — 2022. — № 3 (49). — URL: <https://cyberleninka.ru/article/n> (дата обращения: 23.03.2025).

12. О введении в действие межгосударственных стандартов : приказ Росстандарта от 22.11.2013 № 1628-ст // СПС «КонсультантПлюс».

13. Уголовно-правовая охрана финансово-бюджетной сферы: научно-практическое пособие / В. Ю. Артемов, Н. А. Голованова, Е. В. Горенская [и др.] ; отв. ред. И. И. Кучеров, О. А. Зайцев, С. Л. Нудель. — М. : ИЗиСП, КОНТРАКТ, 2021 // СПС «КонсультантПлюс».

14. Домкин П. Что относится к средствам платежей? // URL: <https://www.advodom.ru/practice/advokat-sredstva-platezhej-po-state-187-ukrf.php> (дата обращения: 23.03.2025).

15. Уголовное дело № 1-567/2020 // URL: <https://sudact.ru> (дата обращения: 23.03.2025).

16. Комментарий к Уголовному кодексу Российской Федерации: в 4 т. (постатейный) / А. В. Бриллиантов, А. В. Галахова, В. А. Давыдов и др. ; отв. ред. В. М. Лебедев. — М. : Юрайт, 2017. — Т. 2 : Особенная часть. Разделы VII – VIII. — 371 с.

17. Уголовная ответственность за изготовление или сбыт поддельных кредитных или расчетных карт или иных платежных документов (разъяснение законодательства) // URL: https://epp.genproc.gov.ru/web/proc_78/activity/legaleducation/explain?item=25104372 (дата обращения: 23.03.2025).

18. Приговор № 1-27/2024 1-321/2023 от 26 января 2024 г. по делу № 1-27/2024 // URL: <https://sudact.ru> (дата обращения: 23.03.2025).

19. Карпов Н. О. Предмет неправомерного оборота средств платежей (правовой и криминалистический аспекты) // Вестник Санкт-Петербургского университета МВД России. — 2017. — № 3 (75) — С.119—122.

20. Апелляционное определение Челябинского областного суда от 18 февраля 2025 года по делу № 10-654/2025 (дата обращения: 03.04.2025).

21. Приговор № 1-384/2023 1-41/2024 от 12 февраля 2024 г. по делу № 1-384/2023 // URL: <https://sudact.ru> (дата обращения: 03.04.2025).

22. Апелляционное определение № 22-2096/2021 от 10 ноября 2021 г. // URL: <http://www.ulobsud.ru/index.php?option=3&id=90&idCard=96482> (дата обращения: 03.04.2025).

23. Приговор № 1-384/2023 1-41/2024 от 12 февраля 2024 г. по делу № 1-384/2023 // URL: <https://sudact.ru> (дата обращения: 03.04.2025).

24. Почему в России перестали подделывать банковские карты // URL: <https://pro.rbc.ru/demo/5d7f8989a79471ed24cbf76> (дата обращения: 03.04.2025).

REFERENCES

1. Sostoyanie prestupnosti v Rossii: statisticheskie dannye // URL: <https://mvd.rf/reports> (data obrashheniya: 22.03.25).

2. Kassacionnoe opredelenie Vos'mogo kassacionnogo suda obshhej yurisdikcii ot 17.10.2024 po delu № 77-4159/2024 // SPS «Konsul'tantPlyus».

3. Kommentarij k Ugolovnomu kodeksu Rossijskoj Federacii (postatejnyj) / K. A. Barysheva, Yu. V. Gracheva, R. O. Dolotov [i dr.] ; pod red. G. A. Esakova. 9-e izd., pererab. i dop. — M. : Prospekt, 2021. — 816 s.

4. Prigovor № 1-150/2023 1-19/2024 ot 23 yanvarya 2024 g. po delu № 1-19/2024 // URL: <https://sudact.ru> (data obrashheniya: 23.03.2025).

5. Prigovor № 1-43/2024 1-637/2023 ot 30 yanvarya 2024 g. po delu № 1-43/2024 // URL: <https://sudact.ru> (data obrashheniya: 23.03.2025).

6. Solov'eva E. A. O problemax pravoprimenitel'noj praktiki, formiruemoj pri primenenii ugolovnoj otvetstvennosti za nepravomernyj oborot platezhnyx dokumentov // Ex jure. — 2020. — № 1. — С. 95—105.

7. Nudel' S. L., Pechegin D. A. Voprosy kvalifikacii nepravomernogo oborota sredstv platezhej (po priznaku predmeta) // Ugolovnoe pravo. — 2020. — № 3. — С. 35.

8. O nacional'noj platezhnoj sisteme : Federal'nyj zakon ot 27.06.2011 № 161-FZ // SPS «Konsul'tantPlyus».

9. Prigovor № 1-336/2023 1-34/2024 ot 26 yanvarya 2024 g. po delu № 1-336/2023 // URL: <https://sudact.ru> (data obrashheniya: 23.03.2025).

10. Bykova E. G., Kazakov A. A. Diskussionnye aspekty priznaniya elektronnix sredstv i elektronnix nositelej informacii predmetom prestupleniya, predusmotrennogo st. 187 UK RF // Rossijskij sud'ya. — 2024. — № 4. — С. 13—18.

11. Cherny'shev D. B. K voprosu o predmete prestupleniya, predusmotrennogo stat'ej 187 Ugolovnogo kodeksa Rossijskoj Federacii // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii. —

2022. — № 3 (49). — URL: <https://cyberleninka.ru/article/n> (data obrashheniya: 23.03.2025).

12. O vvedenii v dejstvie mezhgosudarstvennyx standartov : prikaz Rosstandarta ot 22.11.2013 № 1628-st // SPS «Konsul'tantPlyus».

13. Ugolovno-pravovaya ohrana finansovobyudzhethnoj sfery: nauchno-prakticheskoe posobie / V. Yu. Artemov, N. A. Golovanova, E. V. Gorenskaya [i dr.] ; otv. red. I. I. Kuchеров, O. A. Zajcev, S. L. Nudel'. — M. : IZISP, KONTRAKT, 2021 // SPS «Konsul'tantPlyus».

14. Domkin P. Chto odnositsya k sredstvam platezhej? // URL: <https://www.advodom.ru/practice/advokat-sredstva-platezhej-po-state-187-uk-rf.php> (data obrashheniya: 23.03.2025).

15. Ugolovnoe delo № 1-567/2020 // URL: <https://sudact.ru> (data obrashheniya: 23.03.2025).

16. Kommentarij k Ugolovnomu kodeksu Rossijskoj Federacii: v 4 t. (postatejnyj) / A. V. Brilliantov, A. V. Galaxova, V. A. Davydov i dr. ; otv. red. V. M. Lebedev. — M. : Yurajt, 2017. — T. 2 : Osobennaya chast'. Razdely VII – VIII. — 371 s.

17. Ugolovnaya otvetstvennost' za izgotovlenie ili sbyt' poddelnyx kreditnyx ili raschetnyx kart ili inyx platezhnyx dokumentov (raz'yasnenie zakonodatel'stva) // URL: https://epp.genproc.gov.ru/web/proc_78/actiity/legaleducation/eplain?item=25104372 (data obrashheniya: 23.03.2025).

18. Prigovor № 1-27/2024 1-321/2023 ot 26 yanvarya 2024 g. po delu № 1-27/2024 // URL: <https://sudact.ru> (data obrashheniya: 23.03.2025).

19. Karpov N. O. Predmet nepravomernogo oborota sredstv platezhej (pravovoj i kriminalisticheskij aspekty) // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. — 2017. — № 3 (75) — С.119—122.

20. Apellyacionnoe opredelenie Chelyabinskogo oblastnogo suda ot 18 fevralya 2025 goda po delu № 10-654/2025 (data obrashheniya: 03.04.2025).

21. Prigovor № 1-384/2023 1-41/2024 ot 12 fevralya 2024 g. po delu № 1-384/2023 // URL:

<https://sudact.ru> (data obrashheniya: 03.04.2025).

22. Apellyacionnoe opredelenie № 22-2096/2021 ot 10 noyabrya 2021 g. // URL: <http://www.ulobl-sud.ru/index.php?option=3&id=90&idCard=96482> (data obrashheniya: 03.04.2025).

23. Prigovor № 1-384/2023 1-41/2024 ot 12 fev-

ralya 2024 g. po delu № 1-384/2023 // URL: <https://sudact.ru> (data obrashheniya: 03.04.2025).

24. Pochemu v Rossii perestali poddely`vat` bankovskie karty` // URL: <https://pro.rbc.ru/demo/5dd7f8989a79471ed24cbf76> (data obrashheniya: 03.04.2025).

СВЕДЕНИЯ ОБ АВТОРАХ

Гайдин Александр Иванович. Начальник кафедры уголовного процесса. Кандидат юридических наук, доцент.

Воронежский институт МВД России.

E-mail: Gaidin78@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Дутов Юрий Иванович. Доцент кафедры юридических дисциплин. Кандидат педагогических наук, доцент.

Воронежский государственный аграрный университет имени императора Петра I.

E-mail: puschay@mail.ru

Россия, 394087, Воронеж, ул. Мичурина, 1.

Дутов Николай Юрьевич. Доцент кафедры уголовного процесса. Кандидат юридических наук, доцент.

Воронежский институт МВД России.

E-mail: dutov.nick@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Касьянова Евгения Васильевна. Старший преподаватель кафедры уголовного процесса.

Воронежский институт МВД России.

E-mail: kasyanova-evgeniya@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Gaidin Alexander Ivanovich. Head of the chair of Criminal Proceedings. Candidate of Law, Associate Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: Gaidin78@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Dutov Yury Ivanovich. Associate Professor of the chair of Legal Disciplines. Candidate of Pedagogical Sciences, Associate Professor.

Voronezh State Agrarian University named after Emperor Peter I.

E-mail: puschay@mail.ru

Work address: Russia, 394087, Voronezh, Michurina Str., 1.

Dutov Nikolay Yurievich. Associate Professor of the chair of Criminal Proceedings. Candidate of Law, Associate Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: dutov.nick@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Kasyanova Evgeniya Vasilyevna. Senior lecturer of the chair of Criminal Proceedings.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: kasyanova-evgeniya@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: незаконный оборот средств платежей; подделка платежных карт; фальсификация документов; преступления в финансовой сфере.

Key words: illegal turnover of means of payment; forgery of payment cards; falsification of documents; crimes in the financial sphere.

УДК 343.1

А. Г. Задоров, кандидат юридических наук, доцент

**К ВОПРОСУ О ВОЗМОЖНОСТИ УСТАНОВЛЕНИЯ
ПОСЛЕДОВАТЕЛЬНОСТИ ПЕРЕСЕКАЮЩИХСЯ ШТРИХОВ,
ВЫПОЛНЕННЫХ РАЗЛИЧНЫМИ МАТЕРИАЛАМИ ПИСЬМА,
В РАМКАХ ПРОИЗВОДСТВА ТЕХНИКО-
КРИМИНАЛИСТИЧЕСКОЙ ЭКСПЕРТИЗЫ ДОКУМЕНТОВ**

**ON THE QUESTION OF THE POSSIBILITY OF ESTABLISHING
A SEQUENCE OF INTERSECTING STROKES MADE BY VARIOUS
WRITING MATERIALS, WITHIN THE FRAMEWORK
OF PRODUCTION TECHNICAL AND FORENSIC
EXAMINATION OF DOCUMENTS**

В статье рассматриваются возможности исследования пересекающихся штрихов в различных комбинациях (вариантах), оставленных наиболее распространенными материалами письма. Проблематика, затронутая в статье, обусловлена отсутствием универсальной методики в соответствующем направлении, а также множеством красящих веществ, используемых при оформлении документов. В дополнение к этому необходимо учитывать разный временной период, прошедший между нанесением первоначального и последующего штрихов. Автором проведена экспериментальная работа с сопровождающим ее иллюстративным материалом.

The article discusses the possibilities of studying intersecting strokes in various combinations (variants) left by the most common writing materials. The problems raised in the article are due to the lack of a universal methodology in the appropriate direction, as well as a variety of coloring substances used in the preparation of documents. In addition, it is necessary to take into account the different time period that has elapsed between the application of the initial and subsequent strokes. The author conducted an experimental work with the accompanying illustrative material.

История появления и развития материалов письма уходит корнями в прошлое. Так, в древности, к примеру, люди применяли при нанесении изображений на поверхностях такие вещества, как охра, уголь, известь, некоторые виды растений и т. п. Примерами этому служат наскальные рисунки с изображениями животных, охотников, ритуальных обрядов. Кроме собственно камня в качестве основы (подложки) могли использоваться шкуры животных, береста, папирус и иные материалы, в зависимости от географической локации и временного периода. Инструментами письма, в свою очередь, служили перья птиц, иглы, кисти из меха животных. В дальнейшем, постепенно, по мере прогресса, на смену вышеперечисленным материалам пришла бумага, а в качестве красящих веществ начали использовать карандаши, пасты шариковых ручек, чернила и др.

Сегодня современный рынок насыщен различными видами, разновидностями материалов

документов: в продаже имеется бумага разных сортов; для оттисков печатей предлагается штемпельная краска множества цветов и производителей; для печати изображений на принтерах — чернила (для капельно-струйных устройств); порошки-тонеры для аппаратов, реализующих принцип получения изображений способом электрофотографии, и типографские краски, используемые в полиграфической печати. Основным материалом для рукописных записей также разнообразен — существуют помимо классических авторучек роллерные, капиллярные, гелевые и пр.

Материалы письма, как известно, представляют собой окрашенные многокомпонентные смеси и могут быть структурированы (классифицированы) по разным основаниям. Наиболее удачной нам представляется позиция авторов, которые делят их на группы в зависимости от назначения: 1) материалы для использования в пишущих приборах (пасты для шариковых ручек, канцелярские

чернила для авторучек, чернила для фломастеров, тушь, стержни для карандашей, художественные краски); 2) материалы письма, предназначенные для создания оттисков (краски, красители для лент, используемых в знакопечатающих устройствах, копировальная бумага, полиграфические краски); 3) материалы для получения изображений электрофотографическим способом (электрографические тонеры) [1].

Следует понимать, что все материалы обладают определенными физико-химическими свойствами, что, в свою очередь, формирует структуру штрихов (их морфологические признаки). Соответственно, методы, которые эксперт планирует использовать при исследовании материалов документов, в том числе и пересекающихся штрихов, также должны обладать рядом критериев. Основными из них, наряду с научностью, обоснованностью, можно выделить результативность и надежность. Так, результативность является показателем «рентабельности» использования метода. Надежность, в свою очередь, является неким критерием достоверности, точности. Степень доверия в этом случае будет тем показателем, которым можно руководствоваться, обращаясь к методу. Конечно, в дополнение к вышесказанному, все без исключения методы должны быть безопасными с точки зрения их применения.

Практика производства экспертиз по установлению последовательности выполнения пересекающихся штрихов показала, что, к огромному сожалению, единой методики исследования таких объектов технико-криминалистической экспертизы документов (далее — ТКЭД) не существует. Это объясняется, полагаем, двумя причинами: 1) чрезвычайно большим ассортиментом материалов письма (при этом также нужно отметить различное процентное соотношение составляющих в однородных (однотипных) веществах); 2) разнообразием их комбинаций в пересекающихся штрихах [2]. При этом между нанесением первоначальной и последующей записей будет также разный временной период. Иными словами, существует бесчисленное количество вариантов, при которых такие объекты могли быть образованы.

Выбор методов исследования зависит, естественно, от состава материалов письма. Несомненно, основным методом будет микроскопический. При этом картина может быть как истинной, так и недостоверной (ложной). Такая ситуация может возникнуть в отдельных случаях, описанных в специальной литературе [3], потому не будем останавливаться на данном аспекте. Далее эксперту требуется установить природу веществ. Так, если один из штрихов выполнен матери-

лами письма на водной основе, а другой — материалами с органическими растворителями, целесообразно применить влажное копирование и адсорбционно-люминесцентный анализ. Следует учесть, что вышеперечисленные методы могут частично разрушить объект, поэтому в обязательном порядке эксперту требуется письменное согласие на их применение в исследовании. Как правило, эта информация указывается в постановлении следователя о назначении экспертизы.

Стоит отметить, что научные работы, труды последних лет в области ТКЭД посвящены, в том числе, поискам новых путей решения задач по определению относительной давности штрихов за счет совершенствования традиционных методов исследования. Однако, к сожалению, как уже было отмечено выше, вопрос в данном направлении остается открытым по вышеуказанным причинам. Практическим работникам же требуется, как минимум, информация справочного характера с элементами наглядности: она будет являться залогом более объективного и успешного решения экспертной задачи по установлению последовательности пересекающихся штрихов, оставленных разными материалами письма.

Исходя из вышесказанного, автором проделана экспериментальная работа с последующей обработкой полученных данных. В качестве объектов были использованы такие материалы письма, как: полиграфическая краска, электрографический порошок (тонер), паста для шариковых ручек, чернила для перьевых ручек, штемпельная краска, специальная штемпельная краска для красконаполненных удостоверительных печатных форм. Для практической реализации проблемы подготовлены следующие комбинации материалов письма: 1) полиграфическая краска и паста шариковой ручки; 2) полиграфическая краска и штемпельная краска; 3) полиграфическая краска и чернила; 4) полиграфическая краска и краска для красконаполненных удостоверительных печатных форм; 5) паста шариковой ручки и штемпельная краска; 6) штемпельная краска и паста шариковой ручки; 7) паста шариковой ручки и краска для красконаполненных удостоверительных печатных форм; 8) краска для красконаполненных удостоверительных печатных форм и паста шариковой ручки; 8) чернила и штемпельная краска; 10) штемпельная краска и чернила; 11) чернила и краска для красконаполненных удостоверительных печатных форм; 12) краска для красконаполненных удостоверительных печатных форм и чернила; 13) тонер и паста шариковой ручки; 14) паста шариковой ручки и тонер; 15) тонер и чернила; 16) чернила и тонер; 17) тонер и штемпельная краска; 18) штемпельная краска и

тонер; 19) тонер и краска для красконаполненных удостоверительных печатных форм; 20) краска для красконаполненных удостоверительных печатных форм и тонер. Данные комбинации материалов письма, задействованные в эксперименте, выбраны по той причине, что они наиболее часто встречаются при заполнении реквизитов.

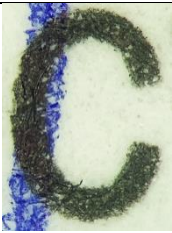
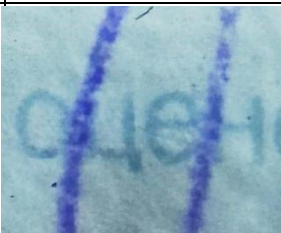
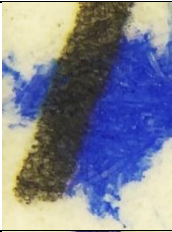
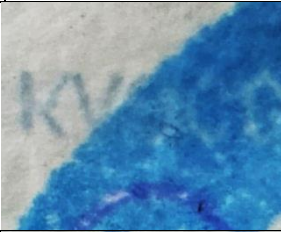
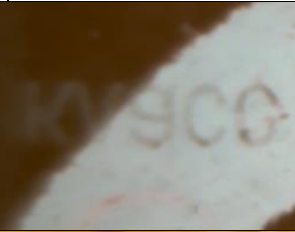
Итак, исследование пересекающихся штрихов проводилось через 1, 6 и 10 месяцев после их нанесения. Далее, собственно, осуществлялась обработка результатов. При получении экспериментальных данных применялись: 1) микроскопический метод; 2) влажное копирование (в качестве адсорбента использовалась поливинилхлоридная (ПВХ)-пленка, растворителя — диметилформамид, время контакта — 10 секунд); 3) ад-

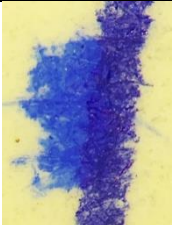
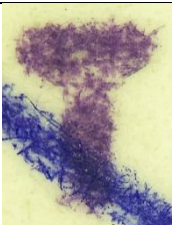
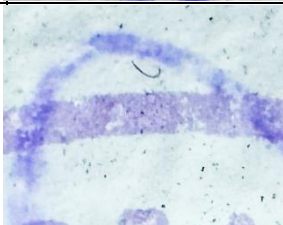
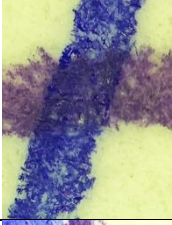
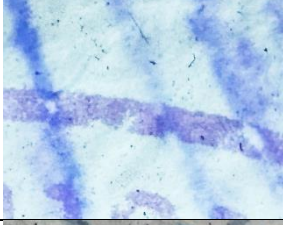
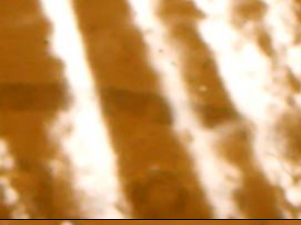
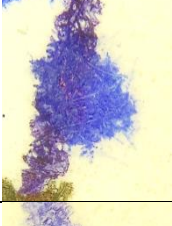
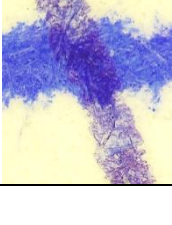
сорбционно-люминесцентный анализ (видеоспектральный компаратор «Комби Мега», длина волны — 450—610 нм). Результаты первых двух методов получены с помощью микроскопа Leica M-125 (увеличение 8—100х); вид освещения — кольцевое светодиодное, бестеневое. Снимки зафиксированы в тех же условиях, с помощью специальной насадки-фотокамеры. Формат получения снимков — jpg. Снимки в «Комби Мега» получены непосредственно с помощью данного аппарата.

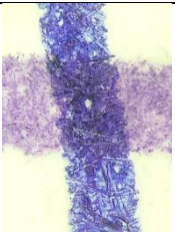
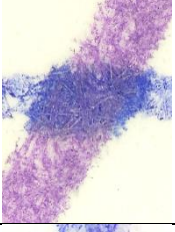
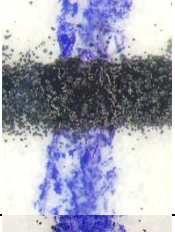
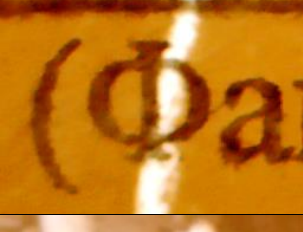
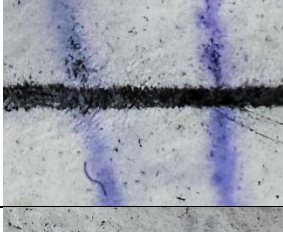
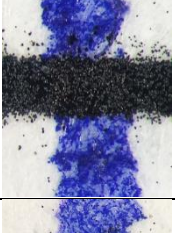
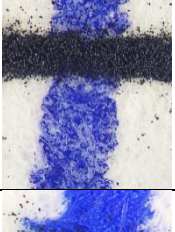
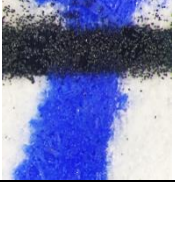
В силу большого массива экспериментального материала результаты исследования пересекающихся штрихов решено проиллюстрировать по истечении десяти месяцев после их нанесения (табл. 1).

Таблица 1

Результаты исследования пересекающихся штрихов,
полученные с помощью разных методов

Последовательность нанесения	Методы		
	микроскопический	влажного копирования	адсорбционно- люминесцентный
1. ПК + ПШР			
2. ПК + ШК			
3. ПК + чернила			
4. ПК + КНП			

Последовательность нанесения	Методы		
	микроскопический	влажного копирования	адсорбционно-люминесцентный
5. ПШР + ШК			
6. ШК + ПШР			
7. ПШР + КНП			
8. КНП + ПШР			
9. Чернила + ШК			
10. ШК + чернила			

Последовательность нанесения	Методы		
	микроскопический	влажного копирования	адсорбционно- люминесцентный
11. Чернила + КНП			
12. КНП + чернила			
13. Тонер + ПШР			
14. ПШР + тонер			
15. Тонер + чернила			
16. Чернила + тонер			
17. Тонер + ШК			

Последовательность нанесения	Методы		
	микроскопический	влажного копирования	адсорбционно-люминесцентный
18. ШК + тонер			
19. Тонер + КНП			
20. КНП + тонер			

Примечание: в таблице использованы следующие сокращения: ПК — полиграфическая краска, ПШР — паста шариковой ручки, ШК — штемпельная краска, КНП — краска для красконаполненных печатей (удостоверительных печатных форм). Первоначально нанесенным следует считать первый указанный материал письма, последующим — второй, идущий после знака «+».

Проведённая экспериментальная работа позволяет сделать определенные выводы практического характера. Так, истинные результаты при применении всех вышеуказанных методов на протяжении всего временного периода были получены в комбинациях пересечений штрихов: «ПК и ПШР», «ПК и чернила», «ПШР и тонер», «ШК и тонер». Ложный вывод наблюдается у комбинации «тонер и ШК». Выводы о невозможности решения вопроса об установлении последовательности нанесения материалов письма отмечаются у пересечения «КНП и чернила».

Истинные результаты при применении микроскопического метода отмечены у штрихов: «ШК и ПШР», «тонер и ПШР», «чернила и тонер», «КНП и тонер». Ложные выводы на протяжении всего хода эксперимента имеются в пересечениях: «ПК и ШК», «ПШР и ШК», «чернила и КНП», «тонер и КНП». Выводы в форме «Не

представляется возможным» (далее — НПВ) получены при изучении пересечения «КНП и ПШР».

При изучении пересекающихся штрихов с применением метода влажного копирования на протяжении всего времени эксперимента истинные результаты наблюдались у пересечения «КНП и ПШР». Все ложные результаты — у пересекающихся штрихов «ПШР и ШК», «ПШР и КНП», «КНП и чернила», «тонер и ПШР», «тонер и чернила», «тонер и КНП».

При изучении пересекающихся штрихов с применением адсорбционно-люминесцентного метода на протяжении трех этапов эксперимента все истинные картины наблюдались у штрихов «ШК и чернила». Все ложные результаты установлены при изучении штрихов «тонер и ПШР». Вывод в форме НПВ был дан при изучении пересечений: «чернила и КНП», «КНП и чернила», «тонер и чернила», «чернила и тонер», «тонер и КНП», «КНП и тонер».

В остальных же случаях результаты эксперимента изменялись с течением времени в разные стороны (от истинной картины до ложной). Самыми результативными оказались методы микроскопического исследования и влажного копирования, которые показали 30 и 31 (из шестидесяти) истинных результатов соответственно.

Наиболее «слабым» (неточным) методом оказался метод адсорбционно-люминесцентного анализа, с 23 положительными выводами.

Результаты эксперимента, полагаем, окажут практическую помощь экспертам-криминалистам, осуществляющим производство ТКЭД, где объектами исследования будут являться пересекающиеся штрихи. Конечно, в работе не рас-

смотрены все возможные пересечения материалов письма, так как их, как уже сказано выше, множество. Однако полученные экспериментальным путем данные позволят более уверенно ориентироваться лицам, проводящим экспертизу, в подобных ситуациях. Иллюстрации, в свою очередь, могут быть полезны с точки зрения вспомогательного справочного материала.

ЛИТЕРАТУРА

1. Техничко-криминалистическая экспертиза документов : глоссарий судебного эксперта / сост. А. В. Досова, Н. Н. Шведова, С. В. Гринченко, Ю. С. Гречкина. — Волгоград : ВА МВД России, 2023.

2. Возможности установления последовательности выполнения реквизитов докумен-

тов : методические рекомендации / И. Г. Захарова [и др.]. — М. : ЭКЦ МВД России, 2019. — 72 с.

3. Техничко-криминалистическая экспертиза документов : учебник / под ред. В. Е. Ляпичева, Н. Н. Шведовой. — Волгоград : ВА МВД России, 2013. — 268 с.

REFERENCES

1. Texniko-kriminalisticheskaya e`kspertiza dokumentov : glossarij sudebnogo e`ksperta / sost. A. V. Dosova, N. N. Shvedova, S. V. Grinchenko, Yu. S. Grechkina. — Volgograd : VA MVD Rossii, 2023.

2. Vozmozhnosti ustanovleniya posledovatel`nosti vy`polneniya rekvizitov dokumentov : metodicheskie

rekommendacii / I. G. Zaxarova [i dr.]. — M. : E`KCz MVD Rossii, 2019. — 72 s.

3. Texniko-kriminalisticheskaya e`kspertiza dokumentov : uchebnik / pod red. V. E. Lyapicheva, N. N. Shvedovoj. — Volgograd : VA MVD Rossii, 2013. — 268 s.

СВЕДЕНИЯ ОБ АВТОРЕ

Задоров Александр Геннадьевич. Доцент кафедры исследования документов учебно-научного комплекса экспертно-криминалистической деятельности. Кандидат юридических наук, доцент.

Волгоградская академия МВД России.

E-mail: zadorexpert37@mail.ru

Россия, 400075, Волгоград, ул. Историческая, 130.

Zadorov Alexander Gennadievich. Associate Professor of the chair of Document Research of the Educational and scientific complex of forensic activities. Candidate of Law, Associate Professor.

Volgograd Academy of the Ministry of Internal Affairs of Russia.

E-mail: zadorexpert37@mail.ru

Work address: Russia, 400075, Volgograd, Istoricheskaya Str., 130.

Ключевые слова: технико-криминалистическая экспертиза документов; материалы письма; методы; пересекающиеся штрихи.

Key words: technical and forensic examination of documents; writing materials; methods; intersecting strokes.

УДК 343.9

И. С. Звягин, кандидат юридических наук

ПРИМЕНЕНИЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ ДЛЯ ОБЕСПЕЧЕНИЯ КРИМИНАЛИСТИЧЕСКИХ ЗАДАЧ

THE USE OF UNMANNED AERIAL VEHICLES TO PROVIDE FORENSIC TASKS

В статье рассмотрены возможности беспилотных летательных аппаратов для решения широкого спектра криминалистических задач; проанализированы актуальные классификации беспилотных летательных аппаратов по различным основаниям; изучены проблемы, возникающие при использовании беспилотных летательных аппаратов в деятельности правоохранительных органов, и предложены рекомендации, направленные на их устранение.

The article discusses the possibilities of unmanned aerial vehicles for solving a wide range of forensic tasks. The current classifications of unmanned aerial vehicles on various grounds are analyzed. The problems arising from the use of unmanned aerial vehicles in the activities of law enforcement agencies have been studied, and recommendations aimed at their elimination have been proposed.

В настоящее время наблюдается стремительное развитие и массовое внедрение беспилотных летательных аппаратов (далее — БЛА) в различные сферы жизнедеятельности человека. Технические возможности БЛА предопределили широкий спектр их функций для выполнения различных задач. Разведка, наблюдение и рекогносцировка, осуществляемые за счет встроенных оптических приборов, являются наиболее распространенными целями применения данных устройств. Активно развивается применение беспилотников для транспортировки грузов. Во многих странах дроны осуществляют доставку еды, медикаментов и других товаров. С 2021 года в Чукотском автономном округе ими производится доставка почты в труднодоступные уголки. В ОАЭ, Китае и Японии существует практика использования БЛА в качестве городского и междугороднего такси. Беспилотники стали незаменимым инструментом в таких сферах, как логистика, строительство, сельское хозяйство, энергетика. Имеются инновационные и нестандартные примеры их применения для выполнения отдельных задач. Так, в Китае применяют дрон для тушения пожаров, способный выполнять свои функции в радиусе до 5 км от базы. А в Чили беспилотники, оснащенные технологией искусственного интеллекта, самостоятельно осуществляют сбор спелых яблок с деревьев.

Расширение функционала и задач, выполняемых БЛА, подчеркивается и активным ростом их производства. По данным различных исследований, мировой рынок дронов в 2024 году составил почти 25 млрд долларов США при среднегодовом

темпе роста в 15,8% [1]. К 2032 году аналитики оценивают масштаб производства БЛА на планете в 100 млрд долларов США [2].

Создаваемые и используемые в различных сферах беспилотные аппараты отличаются друг от друга по конструкции, типу управлению, характеристикам, предназначению и т. д.

Так, по конструкции выделяют следующие виды БЛА:

- самолетного типа;
- вертолетного типа;
- гибриды;
- аэростаты.

БЛА самолетного типа оснащены несущими крыльями, обеспечивающими подъёмную силу и полет. В основном такие устройства характеризуются большей дальностью полета, простотой обслуживания, но требуют взлетной и посадочной площадок.

БЛА вертолетного типа в зависимости от количества винтов подразделяются на однороторные (с одним большим винтом) и мультироторные (с тремя и более винтами). Однороторные устройства характеризуются, как и самолетные, высокой дальностью полета. Как правило, оснащаются двигателями внутреннего сгорания. Самыми массовыми являются мультироторные. Это связано с их дешевизной и простотой управления, возможностью зависания в любой момент и вращения вокруг оси, что позволяет расширить спектр выполняемых задач и сферы их применения. Зачастую мультироторные устройства именуют коптерами, а в зависимости от количества

винтов — трикоптерами (3 винта), квадрокоптерами (4 винта), тетракоптерами (5 винтов) и т. д.

Гибридные (смешанные) БЛА сочетают в себе конструктивные характеристики и функции самолетных и вертолетных устройств. Отличаются высокой скоростью, полезной нагрузкой, но при этом трудностями в обслуживании и дороговизной.

Конструкция аэростатов подразумевает наличие баллонов, содержащих нагретый воздух или газ. В основном они представлены непилотируемыми дирижаблями, для которых характерно длительное время полета, большие размеры и массы, невысокие скорости полета.

В зависимости от *типа управления* выделяют: дистанционные БЛА; автономные БЛА; гибридные БЛА.

Управление дистанционными устройствами осуществляется оператором посредством спутниковой связи, радиосвязи или по оптическому волокну. Автономные беспилотники запрограммированы на решение определенной задачи, оснащены микропроцессором и навигационным оборудованием. Также в последнее время активно в автономных БЛА применяются технологии ис-

кусственного интеллекта. В гибридных системах совмещены возможность ручного управления и автономная функция.

В специальной литературе распространены классификации БЛА по *летным характеристикам*, к которым относятся: взлетная масса, дальность полета, высота полета и продолжительность полета.

Так, в зависимости от взлетной массы и радиуса применения условно можно выделить:

- микро и мини БЛА с радиусом действия до 25 км и взлетной массой до 5 кг;
- легкие БЛА с радиусом действия 25-100 км и взлетной массой 5-100 кг;
- средние БЛА с радиусом действия 100-500 км и взлетной массой 100-500 кг;
- тяжелые БЛА с радиусом действия более 500 км и взлетной массой более 500 кг.

По *сфере применения* выделяют военные и гражданские БЛА. К последним относятся в том числе и летательные аппараты, используемые правоохранительными органами.

Рассмотренные классификации призваны обеспечить субъекты использования БЛА возможностью выбора среди большого спектра устройств, предназначенных для решения различных целей и задач.



Классификации беспилотных летательных аппаратов

В последние годы наблюдается активное внедрение беспилотной авиации в деятельность правоохранительных органов. Возможность выбора различных типов и видов БЛА предподре-

ляет большой потенциал их использования для обеспечения криминалистических задач по предупреждению, раскрытию и расследованию преступлений. В зависимости от решаемых задач в

сфере правоохранительной деятельности целесообразно выделить следующие виды БЛА: следственные, оперативно-розыскные и служебные.

Следственные БЛА предназначены для обеспечения производства следственных действий. Наиболее широко распространена практика применения БЛА при производстве следственных осмотров. М. В. Савельева и А. Б. Смушкин отметили эффективность их применения в ходе производства следственных осмотров при расследовании преступлений против личности; при расследовании воспрепятствования проведению собрания, митинга, демонстрации, шествия, пикетирования или участию в них; при расследовании неоднократного нарушения установленного порядка организации либо проведения собрания, митинга, демонстрации, шествия или пикетирования; при расследовании поджогов и нарушений правил пожарной безопасности; при расследовании преступлений против безопасности движения и эксплуатации транспорта; при расследовании незаконной вырубки лесных насаждений; при расследовании самовольного подключения к нефтепроводам, и газопроводам либо приведения их в негодность и др. [3. — С. 236]. Основными задачами применения беспилотников при производстве осмотров являются: поиск следов преступления, производство фотосъемки и видеозаписи хода и результатов следственного действия.

Отметим особую эффективность использования БЛА при производстве осмотров больших по площади участков местности, например лесных массивов. Обследование участка местности концентрическим, эксцентрическим или линейным способом с применением беспилотника позволит произвести осмотр с наименьшими временными и ресурсными затратами по сравнению с «наземным» обследованием. Также для обеспечения безопасности участников следственного действия целесообразно применение БЛА при производстве осмотра в труднодоступной местности и в опасных экстремальных условиях.

Стоит подчеркнуть возможность конструктивного оснащения беспилотников различными технико-криминалистическими средствами (измерительные приборы, инфракрасные камеры, газоанализаторы и т. д.), позволяющими рационализировать и повысить качество работы следователей и криминалистов при производстве осмотра места происшествия.

В последнее время наблюдается активное применение беспилотной авиации в экспертной деятельности. Использование БЛА при производстве транспортно-трасологических экспертиз способствует выявлению и исследованию следов транс-

портных средств, определению взаимного расположения объектов на месте ДТП. Имеется практика их использования для осмотра зданий и сооружений при производстве инженерно-технических, взрывотехнических и пожарно-технических экспертиз. В судебной баллистике возможно установление обстоятельств выстрела и применения огнестрельного оружия на месте происшествия.

Отметим, что существует проблема, заключающаяся в отсутствии методических указаний по тактике действий следователя и специалистов, использующих беспилотные устройства при производстве следственных действий. Алгоритм использования БЛА по осуществлению фото- и видеосъемки и оформлению иллюстративного и видеоматериалов необходим для повышения эффективности следственных действий. В противном случае, как верно отмечают О. Б. Дронова и Е. С. Храмова, ощутимых преимуществ применения беспилотников по сравнению с традиционными техническими средствами фиксации заметно не будет [4. — С. 103].

Оперативно-розыскные БЛА предназначены для обеспечения производства оперативно-розыскных и оперативно-поисковых мероприятий. Применение БЛА при производстве оперативно-розыскного мероприятия «Наблюдение» позволяет осуществлять негласное наблюдение за представляющими оперативный интерес лицами, сбор и документирование информации. При условии оснащения устройства инфракрасной камерой возможно его применение и в ночное время. Использование беспилотников при производстве таких мероприятий, как «Контролируемая поставка» и «Проверочная закупка», расширяет возможности по видеофиксации результатов и, соответственно, их доказательственного потенциала. Н. А. Моисеев и Н. Г. Новоселов отмечают большие перспективы применения БЛА в ходе оперативно-розыскного мероприятия «Отождествление личности» [5. — С. 127]. В настоящее время в разных странах активно развиваются технологии автоматической идентификации личности по внешнему облику человека. Использование такого метода распознавания требует интегрирования в беспилотник камер высокого разрешения.

Другим важным направлением использования беспилотников в оперативно-розыскной деятельности правоохранительных органов является обеспечение ими комплексных оперативно-профилактических мероприятий, направленных на выявление и пресечение преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ; незаконным оборотом оружия, боеприпасов, взрывчатых веществ и взрывных устройств; незаконным использованием биологических ресурсов и т. д.

Активно используются БЛА в мероприятиях по розыску лиц, скрывающихся от следствия. Особенно актуально применение беспилотников при розыске лиц в условиях труднодоступной местности. Технически БЛА возможно оснастить газоанализатором для обнаружения трупов.

Служебные БЛА предназначены для обеспечения охраны общественного порядка при проведении массовых мероприятий, выявления и предупреждения правонарушений. Применение беспилотников при проведении массовых мероприятий культурного, спортивного или политического характера позволяет организовать наблюдение за ходом мероприятий на открытых площадях значительных размеров. Осуществляемый с большой высоты контроль обеспечивает при необходимости оперативное выявление и фиксацию очагов конфликта.

Во многих субъектах Российской Федерации беспилотные летательные аппараты активно используются для обеспечения безопасности дорожного движения.

Их применение позволяет обеспечить выполнение таких задач, как:

- выявление и идентификация транспортных средств, водители которых допустили правонарушение;

- преследование скрывающихся с места ДТП транспортных средств;

- поиск разыскиваемых транспортных средств;
- мониторинг движения на затрудненных участках дороги и др.

В силу существующих угроз террористической направленности актуальной является и необходимость постоянного контроля за стратегическими объектами: железнодорожными и автомобильными мостами, газо- и нефтепроводами, энергетической инфраструктурой и т. д. БЛА в комплексе с традиционными методами и средствами могут способствовать эффективному решению данной задачи.

Расширению практики применения беспилотных летательных аппаратов в деятельности правоохранительных органов препятствует ряд неразрешенных проблем. Так, в условиях проведения специальной военной операции промышленные мощности в первую очередь направлены на обеспечение нужд военных ведомств, поэтому, несмотря на значительный рост производства БЛА в нашей стране, правоохранительные органы испытывают нехватку данных устройств для выполнения обозначенных задач.

Как верно отмечает А. А. Сырцев, в настоящее время актуальна и проблема подготовки квалифицированных кадров по обслуживанию беспилотной авиации [6. — С. 33]. Сегодня обучение специалистов — операторов БЛА для органов внутренних дел осуществляется в рамках повышения квалификации в Учебно-методическом центре ФКУ НПО «СТиС» МВД России. Этого недостаточно для обеспечения всех потребностей правоохранительных органов соответствующими компетентными специалистами. С учетом обозримых перспектив расширения спектра функциональных возможностей БЛА и потенциального роста потребности в операторах необходимо осуществлять подготовку специалистов в данной сфере в рамках среднего профессионального и высшего образования. Для этого требуется разработка новых специальностей и направлений подготовки для их реализации в образовательных организациях системы МВД России. По мнению Н. Г. Шурухнова, обучать навыкам применения беспилотных летательных аппаратов при производстве следственных действий необходимо не только в образовательных организациях МВД России при подготовке сотрудников следственных и экспертных подразделений, но и при обучении по юридическим специальностям во всех образовательных организациях [7. — С. 110].

Остается открытым и вопрос определения подразделения, обеспечивающего применение беспилотных летательных аппаратов в деятельности правоохранительных органов. До 2016 года беспилотники состояли на вооружении беспилотной авиации внутренних войск МВД России, а после — в подразделениях авиации Росгвардии. В конце 2023 года на базе Департамента информационных технологий, связи и защиты информации МВД России были созданы подразделения по применению и эксплуатации робототехнических комплексов и беспилотных воздушных судов. Тем не менее, исходя из потенциала беспилотной авиации по обеспечению криминалистических задач, считаем целесообразным рассмотреть возможность наделения полномочиями оператора беспилотной авиации сотрудников экспертно-криминалистических подразделений МВД России и, соответственно, вооружения данных подразделений беспилотниками. Это позволит сотрудникам следственных и оперативных подразделений активнее использовать БЛА при производстве следственных действий и оперативно-розыскных мероприятий.

ЛИТЕРАТУРА

1. UAV Drones Global Market Report 2024 // Research and Markets. — URL: <https://www.researchandmarkets.com/reports/5785548/uav-drones-global-market-report/> (дата обращения: 15.04.2025).
2. Global Unmanned Aircraft Systems Market 2024–2033 // Custom Market Insights. — URL: <https://www.custommarketinsights.com/report/unmanned-aircraft-systems-market/> (дата обращения: 15.04.2025).
3. Савельева М. В., Смушкин А. Б. Беспилотный летательный аппарат как специальное технико-криминалистическое средство и объект криминалистического расследования // Вестник Томского государственного университета. — 2020. — № 461. — С. 235–241.
4. Дронова О. Б., Храмова Е. С. Актуальные пути повышения наглядности иллюстративного материала, подготовленного с использованием

- беспилотных летательных аппаратов // Вестник Волгоградской академии МВД России. — 2021. — № 2 (57). — С. 99–107.
5. Моисеев Н. А., Новоселов Н. Г. Об использовании беспилотных летательных аппаратов в оперативно-розыскной деятельности // Вестник ДВЮИ МВД России. — 2019. — № 1 (46). — С. 125–130.
6. Сырцев А. А. Основные направления и перспективные возможности применения беспилотных летательных аппаратов подразделениями МВД России // Актуальные исследования. — 2023. — № 25 (155). — С. 31–33.
7. Шурухнов Н. Г. Беспилотные летательные аппараты — дополнительные средства повышения качества и безопасности производства осмотра места происшествия // Сибирские уголовно-процессуальные и криминалистические чтения. — 2024. — № 4. — С. 105–112.

REFERENCES

1. UAV Drones Global Market Report 2024 // Research and Markets. — URL: <https://www.researchandmarkets.com/reports/5785548/uav-drones-global-market-report/> (data obrashheniya: 15.04.2025).
2. Global Unmanned Aircraft Systems Market 2024–2033 // Custom Market Insights. — URL: <https://www.custommarketinsights.com/report/unmanned-aircraft-systems-market/> (data obrashheniya: 15.04.2025).
3. Savel'eva M. V., Smushkin A. B. Bepilotny'j letatel'ny'j apparat kak special'noe texniko-kriminalisticheskoe sredstvo i ob'ekt kriminalisticheskogo rassledovaniya // Vestnik Tomskogo gosudarstvennogo universiteta. — 2020. — № 461. — S. 235–241.
4. Dronova O. B., Xramova E. S. Aktual'ny'e puti povыsheniya naglyadnosti illyustrativnogo ma-

- teriala, podgotovlennogo s ispol'zovaniem bespilotny'x letatel'ny'x apparatov // Vestnik Volgogradskoj akademii MVD Rossii. — 2021. — № 2 (57). — S. 99–107.
5. Moiseev N. A., Novoselov N. G. Ob ispol'zovanii bespilotny'x letatel'ny'x apparatov v operativnorozы'sknoj deyatel'nosti // Vestnik DVYul MVD Rossii. — 2019. — № 1 (46). — S. 125–130.
6. Sy'rcev A. A. Osnovny'e napravleniya i perspektivny'e vozmozhnosti primeneniya bespilotny'x letatel'ny'x apparatov podrazdeleniyami MVD Rossii // Aktual'ny'e issledovaniya. — 2023. — № 25 (155). — S. 31–33.
7. Shuruxnov N. G. Bepilotny'e letatel'ny'e apparaty — dopolnitel'ny'e sredstva povыsheniya kachestva i bezopasnosti proizvodstva osmotra mesta proisshestviya // Sibirskie ugovorno-processual'ny'e i kriminalisticheskie chteniya. — 2024. — № 4. — S. 105–112.

СВЕДЕНИЯ ОБ АВТОРЕ

Звягин Иван Сергеевич. Доцент кафедры криминалистики. Кандидат юридических наук. Воронежский институт МВД России.
E-mail: patronzv@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Zvyagin Ivan Sergeevich. Associate Professor of the chair of Criminalistics. Candidate of Law. Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: patronzv@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: беспилотные летательные аппараты; тактика следственных действий; технические средства фиксации.

Key words: unmanned aerial vehicles; tactics of investigative actions; technical means of fixation.

УДК 343.98

Р. Б. Иванченко, кандидат юридических наук, доцент
А. В. Польшиков, кандидат юридических наук, доцент
О. В. Демидова, кандидат юридических наук, доцент

НОВЫЕ ПСИХОАКТИВНЫЕ ВЕЩЕСТВА: ОБЩЕМИРОВЫЕ ТЕНДЕНЦИИ И ВЫЗОВЫ ПРАВООХРАНИТЕЛЬНЫМ СИСТЕМАМ

NEW PSYCHOACTIVE SUBSTANCES: GLOBAL TRENDS AND CHALLENGES TO LAW ENFORCEMENT SYSTEMS

Статья посвящена анализу современных международных проблем, связанных с появлением и распространением новых психоактивных веществ. Рассматриваются определения новых психоактивных веществ, которые даются в международных стандартах, а также доктринальных источниках, приводится их классификация. Исследуются вопросы, связанные с масштабом появления обновленных формул психоактивных веществ на мировых рынках. Анализируется роль интернета как инструмента распространения психоактивных веществ. Авторы формулируют основные проблемы мировых правоохранительных систем, связанные с выявлением и предупреждением преступлений в сфере незаконного оборота новых психоактивных веществ, и приходят к выводу о необходимости реформирования антинаркотического законодательства, создания новых национальных и международных платформ по мониторингу такого рода веществ.

The article is devoted to the analysis of modern international problems related to the emergence and spread of new psychoactive substances. The definitions of new psychoactive substances, which are given in international standards, as well as doctrinal sources, are considered, and their classification is given. The issues related to the scale of the appearance of updated formulas of psychoactive substances on world markets are being investigated. The role of the Internet as a tool for the distribution of psychoactive substances is analyzed. The authors formulate the main problems of the world's law enforcement systems related to the detection and prevention of crimes in the field of trafficking in new psychoactive substances, and conclude that it is necessary to reform anti-drug legislation and create new national and international platforms for monitoring such substances.

Новые психоактивные вещества (НПВ) стали глобальным явлением на рынке наркотиков. Этот феномен характеризуется ежегодным появлением значительного количества новых веществ, которые не подпадают под действие международных конвенций о контроле над наркотиками, что делает их оборот законным. Несмотря на то, что эти вещества имитируют традиционные запрещенные наркотики, они могут вызывать серьезные неблагоприятные последствия для здоровья человека.

За последние несколько лет беспрецедентные темпы распространения НПВ привели к серьезным проблемам для систем общественного здравоохранения различных стран мира; число людей, которые становятся зависимыми или заболевают наркоманией, а также количество смертельных исходов постоянно растут.

С помощью интернета НПВ распространяются с такой скоростью, что ни законодательные,

ни правоохранительные органы не могут достаточно быстро реагировать по вопросам установления ответственности и противодействия обороту этих веществ.

Негативное социальное и экономическое воздействие НПВ на мировое сообщество является значительным, а проблемы, стоящие перед правоохранительными органами, судебной системой и органами государственной власти, являются беспрецедентными.

Новые психоактивные вещества не подпадают под глобальную систему контроля над наркотиками и определяются как «наркотические или психотропные средства, которые не включены в перечень в соответствии с Конвенциями ООН 1961 или 1971 годов, но которые могут представлять угрозу, аналогичную незаконным наркотикам, перечисленным в этих конвенциях» [1].

В литературе и на рынке НПВ также упоминаются как «дизайнерские наркотики», «аналоги», «легальные наркотические средства», «растительные наркотические средства», «соли для ванн», «синтетические наркотики».

Предпочтительным термином, принятым Европейским сообществом в 2005 году, является «новые психоактивные вещества» [2]. Здесь термин «новые» не обязательно означает некое новое изобретение, а определяет вещества, которые стали доступны недавно. Ярлыки «синтетические наркотики» и «легальный наркотик» часто используются для того, чтобы намеренно ввести потребителей в заблуждение, заставив их поверить, что это традиционные запрещенные синтетические наркотики (например, ЛСД или МДМА) или легальные вещества [3].

Управление ООН по наркотикам и преступности (УНП ООН) классифицирует НПВ по восьми категориям (и еще одной, дополнительной категории «Другие вещества») в зависимости от «сходства химической структуры (например, фенилэтиламины, триптамины) и/или по их основным фармакологическим эффектам (например, агонисты каннабиноидных рецепторов)» [1]. Классификация УНП ООН учитывает тот факт, что «сходство в химической структуре не всегда вызывает аналогичные фармакологические эффекты, а известный фармакологический эффект может быть вызван НПВ с иной химической структурой» [1].

Категория других веществ «охватывает вещества с плохо изученными фармакологическими эффектами и/или различной химической структурой» [1].

Во Всемирном докладе о наркотиках за 2022 год указывается на то, что в период с 2009 по 2021 год 134 страны сообщили о 1127 таких веществах в консультативный совет УНП ООН по раннему предупреждению о новых психоактивных веществах, и новые вещества продолжают обнаруживаться и добавляться в список [4].

Согласно рекомендациям УНП ООН по раннему предупреждению о НПВ, по состоянию на декабрь 2021 года в УНП ООН было зарегистрировано более 504 веществ [5].

Существует основная группа из более чем 80 НПВ, которые демонстрируют устойчивость на мировом наркорынке (с 2009 по 2015 г.), в то время как 60 НПВ исчезли с него после 2013 года [1. — С. 29]. К наиболее популярным и пользующимся спросом веществам относятся: синтетические каннабиноиды серии JWH, мефедрон и его производные, несколько аналогов амфетамина и пиперазины, а также ряд триптамиинов и аналогов 2C-B [1. — С. 30].

После быстрого роста в период с 2009 по 2018 год количество различных НПВ, обнаруживаемых на мировых рынках наркотиков, в последние

5 лет стабилизировалось на уровне около 550, то есть примерно вдвое меньше, чем когда-либо выявлялось на рынках наркотиков.

В 2020 году государства — члены УНП ООН сообщили о наличии на рынке 548 НПВ, из которых 77 были выявлены впервые [5. — С. 22]. С 2021 по 2022 год количество предлагаемых на рынке НПВ снизилось с 618 до 566 веществ, из которых 44 были идентифицированы впервые [5].

В период с 2016 по 2020 год большинство выявленных НПВ были стимуляторами (в основном катинонами и фенилэтиламины), за которыми следовали агонисты синтетических каннабиноидных рецепторов, галлюциногены (в основном триптамины и некоторые фенилэтиламины) и опиоиды (в основном аналоги фентанила).

Чтобы в полной мере оценить текущую ситуацию, важно понимать, что несмотря на большое количество НПВ, присутствующих на рынках наркотиков, общий объем оборота таких веществ относительно невелик по сравнению с рынками запрещенных наркотиков. Однако стремительные темпы распространения НПВ привели к значительному риску для общества и породили новое явление в сфере наркоторговли.

Феномен НПВ характеризуется главным образом постоянным появлением новых веществ, которые юридически не подпадают под действие международных конвенций о контроле над наркотиками. В прошлом предпринимались многочисленные попытки обойти законы о наркотиках путем производства аналогов, которые не контролировались международными конвенциями.

В настоящее время особой проблемой становится сложность, масштаб и доступность рынка НПВ по сравнению с прошлыми десятилетиями, и этот рынок очень быстро реагирует на законодательные изменения. Комиссия УНП ООН по наркотическим средствам отмечает: «НПВ, находящиеся под национальным контролем, быстро заменяются новыми неконтролируемыми веществами, а вещества, находящиеся под национальным контролем в одной стране, вновь появляются в странах с более слабой правовой базой... или в интернете...» [6. — С. 6—7].

Новые психоактивные вещества разработаны таким образом, чтобы имитировать действие традиционных запрещенных наркотиков, и могут представлять серьезную угрозу для здоровья населения. Они используются по тем же причинам, что и традиционные наркотики, или в качестве заменителя предпочитаемого наркотика, когда последний недоступен на рынке. К сожалению, в большинстве случаев пользователи не знают о составе и дозировке веществ, содержащихся в некоторых НПВ. Они также не знают о

фармакологических эффектах веществ, которые они покупают.

Полагаем, что число людей, нуждающихся в стационарном лечении в результате употребления НПВ, будет расти, и нельзя исключать кризиса в области общественного здравоохранения, вызванного НПВ.

Использование НПВ может привести к неблагоприятным последствиям для здоровья, серьезным травмам (иногда в результате дорожно-транспортных происшествий или агрессивного поведения), а также к суицидам и другим ситуациям со смертельным исходом [7].

Очевидна взаимосвязь между употреблением НПВ и ростом распространения заболеваний, включая ВИЧ и гепатит С, а также вспышками массовых отравлений. К сожалению, врачи и медицинские работники часто не осведомлены о новых тенденциях и новых веществах, появляющихся на рынке [8]. Почти ничего не известно об их вредных свойствах, долгосрочных последствиях и способах противодействия им. Л. А. Кинг и А. Т. Кикман указывают в этой связи: «то небольшое, что нам известно, мы почерпнули из отдельных работ в области токсикологии животных, смертельных отравлений у людей и клинических наблюдений за пациентами, находящимися в состоянии алкогольного опьянения» [9. — С. 403].

Ситуация осложняется еще и тем, что потребители часто не знают о содержании или дозировке вещества, которое они употребляют, и, как правило, превышают дозу. Это представляет серьезную угрозу для здоровья населения из-за синергетического эффекта, который бывает непредсказуемым, а зачастую смертельным.

Легкий доступ и растущая прибыльность увеличивающегося рынка наркотиков делают его все более привлекательным как для потребителей, так и для организованной преступности. Распространение наркотиков в эпоху интернета отличается от ранее существовавшей модели, связывавшей нарколаборатории и конечных потребителей.

Глобализация и технологии существенно влияют на распространение НПВ, объединяя важные знания о производстве таких веществ и наиболее простые пути их распространения на рынке.

В анализе Европейского центра мониторинга наркотиков и наркозависимости указывается: «Сочетание глобализации и инноваций в коммуникационных технологиях означает, что наркотические вещества разрабатываются, производятся на транснациональном уровне с огромной скоростью и открыто продаются в специализированных магазинах в малых и больших городах, так же успешно, как и через интернет» [10. — С. 9].

Основными странами происхождения НПВ считаются Китай и Индия. Производство осуществляется либо в нелегальных лабораториях, либо на законных объектах, принадлежащих компаниям, которые открыто производят вещества, не подпадающие под регулирование. Эти компании производят «новые» химические вещества или модифицируют уже существующие наркотики, а затем доставляют продукцию в различные пункты назначения либо для дальнейшей переработки, либо для непосредственной продажи. Вещества часто рекламируются как безвредные или даже легальные, создавая ложную видимость безопасности продукта. По этой причине поставщики называют их «пищевыми добавками», «химикатами для научных исследований» или «легальными добавками». Более того, в большинстве случаев необычные логотипы и цвета используются как агрессивный маркетинговый метод привлечения молодежи.

Исследование 2015 года, в котором анализировалось использование НПВ подростками и молодыми людьми, показало, что «потенциальные потребители, включая наиболее уязвимых лиц, таких как дети и пациенты психиатрических клиник, становятся мишенью агрессивных маркетинговых стратегий в интернете (привлекательные названия, красочная упаковка, бесплатные образцы для тестирования)» [11. — С. 296].

Новые психоактивные вещества выпускаются под своим собственным названием, под вымышленными названиями (например, «экстази», «героин» или «кокаин») или даже могут продаваться в виде смесей с контролируруемыми наркотиками или другими НПВ. Эти продукты продаются недорого и открыто на улицах, в магазинах, на рынках запрещенных наркотиков или через интернет. Когда вещество становится контролируемым в одной стране, поставщики могут немедленно перейти на новые неконтролируемые НПВ или просто перенести бизнес в другую страну.

В 2013 году УНП ООН признало важность интернета для распространителей НПВ, отметив, что «значительный информационный, рекламный и дистрибьюторский потенциал интернета играет главенствующую роль на рынке НПВ, поэтому глобальный сетевой маркетинг и дистрибуция, отличные от нелегальных уличных рынков, имеют в настоящее время серьезное развитие» [12. — С. 53].

Онлайн-продажи стали малорисковым инструментом распространения, который обеспечивает как пользователю, так и поставщику высокую степень гибкости и анонимности. УНП ООН отмечает в этой связи, что «потребители наркотиков могут получать информацию через онлайн-

форумы, чаты и блоги и узнавать о новых продуктах» [13].

Организованные преступные группировки (ОПГ) считают рынок НПВ весьма привлекательным как для производителей, так и для продавцов.

Масштабы распространения и число участников этих группировок будут возрастать, поскольку рынок НПВ весьма перспективен в плане доходности. Выявление таких групп, скрывающихся за рынком НПВ, является непростой задачей для правоохранительных органов, поскольку производство и незаконный оборот НПВ — это сложная система, которая охватывает страны по всему миру.

Еще в 2014 году Комиссия Организации Объединенных Наций по наркотическим средствам установила, что «интернет-сайты, участвующие в обороте НПВ, могут находиться не в тех странах, в которых производятся и/или поставляются НПВ, а различия в законодательстве затрудняют поиск общего подхода к проблеме противодействия обороту НПВ. Еще одной сложностью является продажа НПВ в «даркнете», доступ к которому возможен только с помощью программного обеспечения для анонимизации» [6. — С. 7].

Возможность получения прибыли — это основная причина, по которой ОПГ вовлечены в рынок НПВ, и, к сожалению, включение НПВ в список контролируемых веществ часто делает это вещество еще более привлекательным для организованных преступных групп: когда предложение уменьшается, а спрос остается стабильным или растет, прибыль также существенно возрастает.

Говоря об основных проблемах, стоящих перед правоохранительными органами различных государств в сфере противодействия обороту НПВ, в первую очередь необходимо выделить высокую степень неосведомленности сотрудников об этом явлении. Более того, усилия по информированию общественности, которые могли бы дать базовые знания о НПВ, ограничены или вообще отсутствуют.

В исследовании УНП ООН о тенденциях в области НПВ, проведенном в 2016 году, отмечается, что «хотя некоторые государства-члены предприняли усилия по информированию..., информационные кампании не проводились на систематической основе; это означает, что во многих странах отсутствует система информирования» [6. — С. 13].

В результате для правоохранительных органов единственным источником информации по всем аспектам НПВ, от химического состава и страны-производителя до методологии распространения и демографии конечных пользователей, становится интернет.

Основная проблема, связанная с пресечением контрабанды НПВ, заключается в выявлении мест производства, переработки и веб-сайтов, используемых для незаконного оборота. Сайты, посвященные одному конкретному НПВ, могут находиться в разных странах, что делает отслеживание поставщиков и преступных группировок, получающих прибыль от оборота НПВ, сложной задачей.

Эта задача еще более усложняется из-за несоответствий в законодательстве различных стран, а какие-либо устоявшиеся стандарты международного сотрудничества практически отсутствуют. Кроме того, поставщики часто обходят национальные законы, либо предлагая потребителям новые неконтролируемые НПВ, либо просто перенося свою деятельность в страны с менее обременительной законодательной политикой.

Выявление и изъятие НПВ в ходе полицейских операций является еще одной серьезной проблемой в борьбе с распространением этих веществ. Правоохранительные органы могут столкнуться с химическими веществами в различных формах, например, с жидкостями, таблетками, порошками или растениями, которые не могут быть признаны НПВ или прекурсорами НПВ из-за недостатка знаний об этих веществах.

Выявление и изъятие НПВ в ходе таможенных процедур является решающим шагом в борьбе с контрабандой. Согласно опросному листу, разработанному УНП ООН по проблемам противодействия обороту НПВ, большинство респондентов назвали использование воздушного транспорта в качестве самого распространенного способа перемещения НПВ, за которым следует пересылка таких веществ по почте [12]. По этой причине во Всемирной таможенной организации была создана Сеть таможенного контроля (CEN), призванная повысить эффективность контроля за трансграничными операциями, связанными с НПВ, путем сбора и обмена информацией об способах трафика таких веществ [6].

Наконец, сотрудники правоохранительных органов, сталкиваясь с крупными лабораториями по производству или переработке наркотиков или с большими партиями химических веществ, не должны забывать об элементарных правилах техники безопасности. Так во Всемирном отчете о наркотиках за 2017 год указывается, что в Канаде и США были зарегистрированы случаи госпитализации сотрудников правоохранительных органов, которые проводили изъятия фентанила и аналогов [1]. Управление по борьбе с наркотиками США опубликовало предупреждения о мерах безопасности и разработало процедурные прото-

колы, направленные на снижение риска причинения вреда сотрудникам правоохранительных органов по всему миру.

Зачастую НПВ не идентифицируются не только правоохранительными органами на местах, но и специализированные лаборатории не всегда в состоянии определить новое вещество, поступающее в продажу. Наибольшей проблемой является идентификация и количественный анализ НПВ в биологических матрицах, осуществляемые в лабораториях судебной экспертизы, поскольку аналитически трудно уследить за быстрыми темпами изменения этих веществ, главным образом из-за отсутствия справочных материалов, необходимых для разработки методов анализа [1. — С. 48]. Более того, препятствия для обнаружения и анализа возникают, когда в новом психоактивном веществе, потребляемом человеком, биологический образец которого исследуется, присутствуют смеси веществ или они содержатся в следовых количествах (например, синтетические опиоиды из-за их высокой активности).

Таким образом, сложность в выявлении НПВ в лабораторных условиях в биоматериалах, а также идентификации веществ в качестве НПВ может привести к искажению информации о масштабах их появления на рынке. Занижение количественных данных о фактах обнаружения и применения НПВ препятствует международному контролю, а также разработке мер по борьбе с незаконным оборотом наркотиков и злоупотреблением ими.

Следует заметить, что некоторые группы потребителей НПВ вызывают особое внимание со стороны правоохранительных органов. Одной из таких групп являются военнослужащие. Так, например, синтетические каннабиноиды являются наиболее популярным наркотиком среди военнослужащих США из-за того, что эти НПВ не выявляются при проверке на наркотики, ошибочно считаются безопасными, дешевы и их легко купить [13. — С. 1041]. В публикации М. Ф. Вивера, Ж. А. Хоппера и Е. В. Гундерсона отмечается: «Дизайнерские наркотики особенно популярны среди тех, кто служит в армии» [14. — С. 10].

Вторая подгруппа — это осужденные. В тюрьмах также растет потребление НПВ, поскольку эти вещества не выявляются ни в ходе

внутренних проверок на наркотики, ни с помощью специально обученных собак. Употребление НПВ в местах лишения свободы сопряжено с агрессией и применением насилия. Так, согласно Всемирному докладу о наркотиках за 2017 г. употребление осужденными синтетических каннабиноидов вызывает ряд последствий, дезорганизующих деятельность мест лишения свободы: проблемы долгов одних осужденных перед другими, массовые беспорядки, членовредительство, суициды, психические заболевания и насилие среди заключенных и в отношении персонала [1. — С. 44].

Таким образом, любое эффективное решение проблемы распространения НПВ требует комплексного подхода. Общая позиция государства является ключом к реформированию наркополитики, а инновационное законодательство — наиболее вероятным решением проблемы распространения НПВ.

В то время как существующие платформы для выявления НПВ, в том числе УНП ООН и Европейский центр мониторинга наркотиков и наркомании, должны использоваться и расширяться для эффективного обмена информацией и опытом, необходимо создание такой системы оповещения и в рамках СНГ или даже БРИКС, для того чтобы быть лидерами в решении проблемы НПВ.

Без сомнения, качественная подготовка сотрудников правоохранительных органов и медицинских работников должна рассматриваться как важнейший фактор в борьбе с распространением НПВ и его тяжелыми последствиями.

Соответствующим министерствам, которые так или иначе занимаются противодействием НПВ, потребуется финансирование, необходимое для поддержания их усилий в этой борьбе.

Если сдерживание потребления НПВ во всем мире будет малоэффективным, финансовые и человеческие потери будут расти серьезными темпами. Расходы, необходимые для борьбы с наркотизмом, неблагоприятными последствиями для здоровья населения и преступлениями, связанными с потреблением психоактивных веществ, намного превысят инвестиции, необходимые для внедрения комплексного подхода, основанного на сотрудничестве. Только межгосударственное сотрудничество поможет снизить распространение НПВ во всем мире.

ЛИТЕРАТУРА

1. World Drug Report 2017. Booklet 4 «Market Analysis of Synthetic Drugs: Amphetamine-type Stimulants, New Psychoactive Substances». —

UNODC, 2017. — URL: <https://archive.org/details/wdr-2017-4> (дата обращения: 16.02.2025).

2. Council Decision 2005/387/JHA (10 May

2005 on the Information Exchange, Risk-Assessment and Control of New Psychoactive Substances) // Official Journal of the European Union. — 2005. — L127/32: Article 3 (b) & (c). — URL: <https://eurlex.europa.eu/eli/dec/2005/387/oj> (дата обращения: 18.02.2025).

3. Sutherland R., Barrat M. New (and Emerging) Psychoactive Substances // NDARC Fact Sheet (University of New South Wales, National Drug and Alcohol Research Centre, 2016.) — URL: <https://ndarc.med.unsw.edu.au/sites/default/files/ndarc/resources/NDA073%20New%20Psychoactive%20Substances%20%28NPS%29.pdf> (дата обращения: 20.02.2025).

4. УНП ООН. Всемирный доклад о наркотиках за 2022 год (издание Организации Объединенных Наций, 2022 год). — URL: https://www.eegyn.com/World_drug_report_2022 (дата обращения: 20.02.2025).

5. УНП ООН. Всемирный доклад о наркотиках за 2024 год (издание Организации Объединенных Наций, 2024 год). — URL: <https://nps-info.org/resyrsy/publikatsii/vsemirnyj-doklad-o-narkotikah-2024-god/> (дата обращения: 20.02.2025).

6. New Psychoactive Substances: Overview of Trends, Challenges and Legal Approaches. — UNODC: Commission on Narcotic Drugs, E/CN.7/CRP.2, 2016.

7. Smith C. D., Williams M., Shaikh M. Novel Psychoactive Substances: a Novel Clinical Challenge. — BMJ Case Rep., 2013. — URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3762549/pdf/bcr-2013-00663.pdf>. (дата обращения: 16.02.2025).

8. Evans-Brown M., Sedefov R. New Psychoactive

Substances // Driving Greater Complexity into the Drug Problem. Addiction 112, no. 1 (January 2017). — URL: <https://pubmed.ncbi.nlm.nih.gov/30194542/> (дата обращения: 16.02.2025).

9. King L. A., Kickman A. T. A Brief History of «New Psychoactive Substances» // Drug Testing and Analysis. — 2011. — № 7-8 (July-August). — URL: <https://doi.org/10.1002/dta.319> (дата обращения: 16.02.2025).

10. European Monitoring Centre for Drugs and Drug Addiction and Eurojust. New Psychoactive Substances in Europe: Legislation and Prosecution — Current Challenges and Solutions. — Luxenberg : Publications Office of the European Union, 2016. — URL: http://www.emcdda.europa.eu/publications/joint-publications/eurojust/nps-legislationandprosecution_en (дата обращения: 16.02.2025).

11. Novel Psychoactive Substances and Behavioral Addictions / G. Martinotti, O. Corazza, S. Achab, Z. Demetrovics // BioMed research international. — 2015. — URL: <https://onlinelibrary.wiley.com/doi/10.1155/2014/534523> (дата обращения: 16.02.2025).

12. The Challenge of New Psychoactive Substances: Global SMART Programme Report. — UNODC, 2013. — URL: <https://www.unodc.org/unodc/en/scientists/> (дата обращения: 18.02.2025).

13. Spice, Bath Salts, and the U.S. Military: The Emergence of Synthetic Cannabinoid Receptor Agonist and Cathinones in the U.S. Armed Forces / G. Loeffler, D. Hurst, A. Penn, K. Yung // Military Medicine. — 2012. — № 9.

14. Weaver M. F., Hopper J. A., Gunderson E. W. Designer Drug 2015: Assessment and Management // Addiction Science & Clinical Practice. — 2015. — № 8 (March). — URL: <https://doi.org/10.1186/s13722-015-0024-7>

REFERENCES

1. World Drug Report 2017. Booklet 4 «Market Analysis of Synthetic Drugs: Amphetamine-type Stimulants, New Psychoactive Substances». — UNODC, 2017. — URL: <https://archive.org/details/wdr-2017-4> (data obrashcheniya: 16.02.2025).

2. Council Decision 2005/387/JHA (10 May 2005 on the Information Exchange, Risk-Assessment and Control of New Psychoactive Substances) // Official Journal of the European Union. — 2005. — L127/32: Article 3 (b) & (c). — URL: <https://eurlex.europa.eu/eli/dec/2005/387/oj> (data obrashcheniya: 18.02.2025).

3. Sutherland R., Barrat M. New (and Emerging) Psychoactive Substances // NDARC Fact Sheet (University of New South Wales, National Drug and Alcohol Research Centre, 2016.) — URL: <https://ndarc.med.unsw.edu.au/sites/default/files/>

[ndarc/resources/NDA073%20New%20Psychoactive%20Substances%20%28NPS%29.pdf](https://ndarc.med.unsw.edu.au/sites/default/files/ndarc/resources/NDA073%20New%20Psychoactive%20Substances%20%28NPS%29.pdf) (data obrashcheniya: 20.02.2025).

4. UNP OON. Vsemirnyj doklad o narkotikah za 2022 god (izdanie Organizacii Ob"edinennyh Nacij, 2022 god). — URL: https://www.eegyn.com/World_drug_report_2022 (data obrashcheniya: 20.02.2025).

5. UNP OON. Vsemirnyj doklad o narkotikah za 2024 god (izdanie Organizacii Ob"edinennyh Nacij, 2024 god). — URL: <https://nps-info.org/resyrsy/publikatsii/vsemirnyj-doklad-o-narkotikah-2024-god/> (data obrashcheniya: 20.02.2025).

6. New Psychoactive Substances: Overview of Trends, Challenges and Legal Approaches. — UNODC: Commission on Narcotic Drugs, E/CN.7/CRP.2, 2016.

7. Smith C. D., Williams M., Shaikh M. Novel Psychoactive Substances: a Novel Clinical Challenge. — BMJ Case Rep., 2013. — URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3762549/pdf/bcr-2013-00663.pdf>. (data obrashcheniya: 16.02.2025).

8. Evans-Brown M., Sedefov R. New Psychoactive Substances // Driving Greater Complexity into the Drug Problem. Addiction 112, no. 1 (January 2017). — URL: <https://pubmed.ncbi.nlm.nih.gov/30194542/> (data obrashcheniya: 16.02.2025).

9. King L. A., Kickman A. T. A Brief History of «New Psychoactive Substances» // Drug Testing and Analysis. — 2011. — № 7-8 (July-August). — URL: <https://doi.org/10.1002/dta.319> (data obrashcheniya: 16.02.2025).

10. European Monitoring Centre for Drugs and Drug Addiction and Eurojust. New Psychoactive Substances in Europe: Legislation and Prosecution – Current Challenges and Solutions. — Luxemburg : Publications Office of the European Union, 2016. — URL: [http://www.emcdda.europa.eu/publications/joint-publications/eurojust/nps-legislationand-](http://www.emcdda.europa.eu/publications/joint-publications/eurojust/nps-legislationand-prosecution_en)

[prosecution_en](http://www.emcdda.europa.eu/publications/joint-publications/eurojust/nps-legislationand-prosecution_en) (data obrashcheniya: 16.02.2025).

11. Novel Psychoactive Substances and Behavioral Addictions / G. Martinotti, O. Corazza, S. Achab, Z. Demetrovics // BioMed research international. — 2015. — URL: <https://onlinelibrary.wiley.com/doi/10.1155/2014/534523> (data obrashcheniya: 16.02.2025).

12. The Challenge of New Psychoactive Substances: Global SMART Programme Report. — UNODC, 2013. — URL: <https://www.unodc.org/unodc/en/scientists/> (data obrashcheniya: 18.02.2025).

13. Spice, Bath Salts, and the U.S. Military: The Emergence of Synthetic Cannabinoid Receptor Agonist and Cathinones in the U.S. Armed Forces / G. Loeffler, D. Hurst, A. Penn, K. Yung // Military Medicine. — 2012. — № 9.

14. Weaver M. F., Hopper J. A., Gunderson E. W. Designer Drug 2015: Assessment and Management // Addiction Science & Clinical Practice. — 2015. — № 8 (March). — URL: <https://doi.org/10.1186/s13722-015-0024-7>

СВЕДЕНИЯ ОБ АВТОРАХ

Иванченко Роман Борисович. Заведующий кафедрой уголовного права. Кандидат юридических наук, доцент.

Центральный филиал Российского государственного университета правосудия им. В. М. Лебедева.

E-mail: rivanchenko@yandex.ru

Россия, 394006, Воронеж, ул. 20-летия Октября, 95.

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.

Ivanchenko Roman Borisovich. Head of the chair of Criminal Law. Candidate of Law, Associate Professor.

The Central branch of the Russian State University of Justice named after V. M. Lebedev.

E-mail: rivanchenko@yandex.ru

Work address: Russia, 394006, Voronezh, 20-letiya Oktyabrya Str., 95.

Polshikov Alexander Vasilyevich. 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 Vasilyevna. Professor of the chair of Criminal-executive and Criminal Law. Candidate of Law, Associate Professor.

Voronezh institute of the Russian Federal Penitentiary Service.

E-mail: oks-dem.78@mail.ru

Work address: Russia, 394072, Voronezh, Irkutskaya Str., 1a.

Ключевые слова: новые психоактивные вещества; наркотики; правоохранительные органы; наркополитика; международное сотрудничество; мониторинг наркотиков.

Key words: psychoactive substances; drugs; law enforcement agencies; drug policy; international cooperation; drug monitoring.

УДК 343.575

А. А. Караваев, кандидат юридических наук, доцент
А. Г. Галустян

К ВОПРОСУ О СОВЕРШЕНСТВОВАНИИ ФОРМ И МЕТОДОВ ПРОПАГАНДЫ БЕЗОПАСНОСТИ ДОРОЖНОГО ДВИЖЕНИЯ

ON THE QUESTION OF IMPROVING FORMS AND METHODS OF ROAD SAFETY PROPAGANDA

В статье рассматриваются актуальные вопросы совершенствования пропаганды безопасности дорожного движения и профилактики аварийности в Российской Федерации. Проанализированы основные каналы и формы информационного воздействия на участников дорожного движения, освещены современные тенденции использования цифровых ресурсов и социальных сетей в целях снижения аварийности. Предложены направления повышения эффективности пропаганды за счёт дифференцированного подхода к целевым аудиториям, использования интерактивных форм обучения и продвижения концепции «нулевого травматизма» (Vision Zero). Отмечены дискуссионные моменты организации пропаганды административных правонарушений сотрудниками подразделений Госавтоинспекции. Результаты могут быть использованы органами государственной власти, образовательными учреждениями и общественными организациями при разработке программ по предупреждению дорожно-транспортных происшествий.

The article considers current issues of improving the promotion of road safety and accident prevention in the Russian Federation. The main channels and forms of information impact on road users are analyzed, modern trends in the use of digital resources and social networks in order to reduce accidents are highlighted. The directions for increasing the effectiveness of propaganda through a differentiated approach to target audiences, the use of interactive forms of training and the promotion of the concept of "zero injuries" (Vision Zero) are proposed. Controversial aspects of organizing the propaganda of administrative offenses by employees of the State Traffic Safety Inspectorate units are noted. The results can be used by government agencies, educational institutions and public organizations in developing programs to prevent road accidents.

Развитие технологий современного общества, снижение временных затрат на логистические и коммуникационные процессы, по нашему мнению, является одной из титульных заслуг автомобилизации различных социальных страт. Наличие у физического лица личного (коммерческого, социального и др. видов) транспорта уже воспринимается как объективная необходимость, а не атрибут высокой материальной обеспеченности. Однако подобные позитивные социально-экономические процессы формируют для правоохранительной системы любого демократического государственного образования серьезные «вызовы», угрозы в части, касающейся ежедневного обеспечения защиты конституционного права человека на жизнь (здоровье).

Именно в рамках дорожного движения происходят аварийные ситуации, различные происшествия, которые могут деструктивно влиять на жизнь, здоровье человека. Необходимо отметить, что участниками дорожного движения могут являться совершеннолетние и несовершеннолетние

физические лица, автомобилисты и пешеходы, контрольно-надзорные и обеспечивающие органы в лице своих должностных лиц. Зачастую исследуемые транспортные происшествия являются результатом нарушений различных установленных правил, стандартов, норм реализации дорожного движения.

Следовательно, большинство научных изысканий подобного рода обращается в сторону изучения способов общей и частной превенции дорожных деликтов. По нашему мнению, именно пропаганда безопасности дорожного движения может выступать титульным инструментарием такого метода административной деятельности полиции в рассматриваемой сфере общественных отношений, как убеждение. Необходимо отметить, что с позиции материальных затрат предупреждение является более выгодным для государственного образования, поскольку исключает необходимость реализации административных и процессуальных процедур, сопровождающих пресечение правонарушения.

Ключевым инструментом профилактики дорожно-транспортных происшествий (далее — ДТП) выступает пропаганда безопасности дорожного движения, целью которой выступает формирование у разных групп социума культуры безопасного поведения на дороге. В условиях цифровизации возникает необходимость в совершенствовании пропаганды, которая должна не информировать, а мотивировать к изменению поведения, ориентированного на снижение аварийности.

Задачи по разъяснению законодательных и иных нормативных правовых актов Российской Федерации по вопросам обеспечения безопасности дорожного движения возлагаются на подразделения Госавтоинспекции МВД России.

Приказ МВД России от 29.12.2018 № 903 [1] утвердил Наставление по организации деятельности Государственной инспекции безопасности дорожного движения Министерства внутренних дел Российской Федерации по пропаганде безопасности дорожного движения. Отметим, что в период реализации деятельности по пропаганде безопасности дорожного движения также необходимо руководствоваться следующими нормативными правовыми актами:

- Конституция Российской Федерации [2];
- Федеральный закон от 10.12.1995 № 196-ФЗ «О безопасности дорожного движения» [3];
- Федеральный закон от 29.12.2017 № 443-ФЗ «Об организации дорожного движения в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» [4];
- Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» [5];
- Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ [6];
- Постановление Правительства Российской Федерации от 23.10.1993 № 1090 «О Правилах дорожного движения» [7].

На международном уровне значительную роль играет концепция Vision Zero, впервые предложенная в Швеции (1997). Она ориентирована на полное исключение смертности и тяжёлых травм на дорогах. В рамках этой концепции пропаганда безопасности дорожного движения рассматривается как постоянный процесс воздействия на поведение участников движения, подкреплённый изменениями городской среды, совершенствованием федерального и регионального законодательства [8].

Распоряжением правительства Российской Федерации от 8 января 2018 года № 1-р [9] утверждена Стратегия безопасности дорожного движения в Российской Федерации на 2018—2024 годы. Отметим, что в ней декларируется стремление к

нулевой смертности на дорогах к 2030 году. В качестве целевого ориентира на 2024 год установлен показатель социального риска, составляющий не более четырёх погибших на 100 тысяч населения. В своём выступлении на заседании ежегодной расширенной коллегии МВД России 5 марта 2025 года Президент Российской Федерации В. В. Путин нацелил деятельность министерства на снижение смертности в ДТП к 2030 году минимум в полтора раза [10].

Исходя из поставленных главой государства задач предлагается совершенствовать пропагандистскую работу органов внутренних дел в сфере безопасности дорожного движения по следующим направлениям:

1. Переход к цифровым инструментам: активное использование социальных сетей, мобильных приложений, онлайн-курсов и тестов по ПДД.
2. Мультимедийные и интерактивные методы обучения: симуляторы вождения, виртуальная реальность, «геймификация» (использование игровых механик для обучения безопасному поведению).
3. Целевые кампании для отдельных групп: разные форматы продвижения для подростков, начинающих водителей, профессиональных водителей (например, грузового транспорта), пожилых людей.
4. Совместные проекты с автошколами, учебными заведениями и общественными организациями, направленные на формирование культуры безопасного поведения.
5. Использование методов психологического воздействия: «эмоциональные» видеоролики, истории очевидцев, примеры последствий ДТП, пропагандирующие соблюдение правил дорожного движения не через запугивание, а путем формирования ответственного отношения.

По нашему мнению, актуальными причинами дорожно-транспортных происшествий, возникающих в результате нарушения административного законодательства участниками дорожного движения, являются неуважение к другим участникам дорожного движения, несоблюдение общей культуры поведения и законности, недисциплинированность и невнимательность водителей.

Безопасность дорожного движения (далее — БДД) остается одним из приоритетных направлений государственной политики, так как ДТП, согласно статистическим данным, ежегодно уносят тысячи жизней и приводят к экономическим потерям, сопоставимым с бюджетами крупных регионов нашей страны. Анализ статистических данных МВД России позволяет заключить, что наблюдается некоторое снижение числа ДТП, однако уровень тяжести

последствий все еще остается достаточно высоким [11].

За период с 2013 по 2023 год количество погибших в результате ДТП снизилось (с более чем 27 тысяч до менее 15 тысяч). Позитивная динамика во многом связана с усилением контроля над нарушениями ПДД (например, внедрение автоматических комплексов фиксации, увеличение штрафов), а также с развитием инфраструктуры (улучшение состояния автомобильных дорог, освещение, разделительные барьеры и др.).

Из более чем десятка основных видов ДТП, рассматриваемых государственной статистической отчетностью, выделяются наиболее распространенные причины дорожных происшествий: превышение скорости, нарушение правил обгона, управление транспортом в состоянии опьянения, невнимательность водителей, нарушение правил пешеходами и некоторые другие. Многие нарушения объясняются низким уровнем знаний правил дорожного движения, недостатком ответственного поведения и слабой эффективностью используемых методов профилактики.

Подсчет экономического ущерба от ДТП обычно включает:

- прямые потери (повреждение транспорта и дорог общего пользования, расходы на медицинскую помощь пострадавшим, страховые выплаты);

- косвенные потери (снижение производительности труда, моральный ущерб, организационные расходы и др.). По данным различных исследований, в отдельные годы совокупные потери от ДТП в России могут достигать до 2—3% валового внутреннего продукта. В цифрах это может быть свыше 1—1,5 трлн рублей ежегодно (в ценах соответствующего периода). В разных источниках эта сумма варьируется, так как методики расчета могут отличаться [12].

Существенное влияние на организацию безопасности дорожного движения оказывают системные меры: совершенствование законодательства, пропаганда безопасности дорожного движения, улучшение дорожной инфраструктуры и технических средств контроля. Важен комплексный подход, сочетающий информационно-разъяснительную работу, образовательные программы и адресные мероприятия, ориентированные на разные группы населения (водители, пешеходы, дети, пожилые люди). Воспитание культуры безопасного вождения должно начинаться с раннего возраста.

В течение нескольких десятков лет методы пропаганды менялись, но, как утверждает Е. Н. Ноговицина, неизменной считается целенаправленная и регулярная деятельность по распространению информации о том, как обезопасить дорожное движение [13]. Представляется

необходимым согласиться с точкой зрения И. А. Былинина, согласно которой культура безопасности дорожного движения обязана лежать в основе профилактики среди участников данного движения и являться одним из наиболее значимых векторов в пропаганде данной безопасности [14].

В настоящее время при реализации вопроса пропаганды безопасности дорожного движения используются традиционные формы и каналы:

- печатные материалы и наружная реклама. Постеры, плакаты, листовки, баннеры на улицах, вблизи учебных заведений. Их преимущество заключается в доступности, простоте восприятия. Однако воздействие на поведенческую мотивацию целевой аудитории в условиях медиаперегруженности нередко достаточно ограничено;

- социальная реклама на телевидении, радио. Данные информационно-коммуникационные каналы сохраняют охват значительной части социума, преимущественно в старших возрастных группах. Вместе с тем отсутствует взаимодействие с аудиторией, что снижает «условную» вовлеченность;

- выступления инспекторов Госавтоинспекции в учебных заведениях. Живое общение со школьниками (студентами) помогает формировать первичные знания о правилах дорожного движения, однако требует методической подготовки и регулярного обновления форматов.

По нашему мнению, к более современным формам пропаганды безопасности дорожного движения следует отнести цифровые каналы, инструменты:

- 1) интернет-сайты, мобильные приложения. Разработка специализированных порталов (например, сайт Госавтоинспекции) и мобильных сервисов с функциями уведомлений, тестирования знаний правил дорожного движения;

- 2) социальные сети, мессенджеры, площадки. Таргетированная реклама, тематический контент в «ВКонтакте», Telegram и прочих. Вместе с тем важно учитывать специфику каждой платформы для точечного воздействия на целевую аудиторию;

- 3) игровые форматы, интерактивные тренажеры. Создание симуляторов ДТП, онлайн-игр, квизов по правилам дорожного движения. Игровой метод повышает мотивацию к обучению и степень вовлеченности.

При внедрении новых форм пропаганды наблюдается постепенное снижение аварийности и рост уровня знаний участников дорожного движения, хотя эффект может проявляться не сразу. Важное значение имеет постоянный мониторинг и анализ статистических показателей, позволяющих оперативно корректировать методику, содержание пропаганды.

К проблемным аспектам реализации пропаганды безопасности дорожного движения можно отнести:

- недостаток межведомственного взаимодействия. Разобщенность различных структур (Госавтоинспекция, образовательные организации, транспортные компании) приводит к несогласованности мероприятий;

- ограниченная финансовая база. Региональные бюджеты не всегда могут выделять достаточные средства на проведение регулярных пропагандистских кампаний, особенно с использованием современных цифровых инструментов;

- низкая мотивация участников. Часть населения воспринимает пропаганду формально или негативно, не считая вопрос безопасности дорожного движения личным приоритетом;

- ограниченность методического сопровождения. Отсутствие единых образовательных программ для сотрудников Госавтоинспекции, преподавателей школ и вузов, общественных организаций снижает эффективность кампаний.

С целью повышения уровня эффективности пропаганды безопасности дорожного движения рекомендуется использование дифференцированного подхода к целевым аудиториям, когда каждая группа (дошкольники, школьники, водители-новички, водители со стажем, пешеходы пожилого возраста и др.) требует отдельных методов (форм) воздействия.

К примеру, для детей дошкольного возраста эффективными могут быть мультфильмы и ролевые игры, а для водителей со стажем — аналитические материалы и социальная реклама с эмоционально «сложными» сюжетами. Современные цифровые форматы позволяют вовлекать широкую аудиторию в обучение правилам дорожного движения и приемам безопасного вождения. Онлайн-квесты, симуляторы ситуаций на дороге, конкурсы в социальных сетях и мобильные приложения (например, квизы на знание правил дорожного движения с накоплением баллов) повышают интерес, особенно у молодежи.

Межведомственное и межсекторное сотрудничество позволит объединять усилия Госавтоинспекции, министерств образования и здравоохранения, общественных организаций и средств массовой информации. Совместные акции, форумы, конкурсы и другие мероприятия позволят сформировать комплексный подход, уменьшить дуб-

лирование ресурсов.

Необходимо отметить, что идея «нулевого травматизма» (Vision Zero) подчеркивает ценность человеческой жизни и способствует формированию ответственного поведения на дороге.

В рамках данной концепции рекомендуется:

- внедрять системные кампании, интегрирующие изменения инфраструктуры, контроля и обучения;

- формировать у водителей, пешеходов убеждение, что трагических случаев можно избежать при соблюдении правил и взаимном уважительном поведении. Регулярная оценка, корректировка пропагандистских мероприятий позволяет гибко реагировать на меняющиеся условия. Важен анализ статистики ДТП, социологических опросов, данных из цифровых каналов (просмотры, лайки, комментарии), чтобы понимать реальную эффективность кампаний, а также корректировать их в режиме реального времени.

Совершенствование пропаганды безопасности дорожного движения в современных условиях требует комплексного подхода, сочетающего традиционные и инновационные инструменты воздействия. Значительно возрастает роль цифровых платформ, интерактивных технологий, психологии поведения и целевого маркетинга. Важным направлением становится продвижение ценностей Vision Zero, ориентированных на полное исключение человеческих травм (жертв) в ДТП. Актуализация форм и методов пропаганды безопасности дорожного движения является непрерывным (комплексным) процессом, требующим взаимодействия государства, общественных организаций, образовательных учреждений и средств массовой информации.

Считаем актуальным подчеркнуть необходимость проведения дальнейших научных исследований (экспериментов), направленных на повышение эффективности профилактических мер, а также разработку современных методик, адаптированных к условиям цифровизации общества и его техническим возможностям. Практическая реализация обозначенных в исследовании мер превентивного характера, по нашему мнению, сможет привести к снижению уровня аварийности, уменьшению тяжести последствий ДТП, формированию устойчивой культуры безопасного (ответственного) поведения на автомобильных дорогах общего пользования.

ЛИТЕРАТУРА

1. Об утверждении Наставления по организации деятельности Государственной инспекции безопасности дорожного движения Министерства внутренних дел Российской Федерации по пропаганде безопасности дорожного движения : приказ МВД России от 29 декабря 2018 г. № 903 // СПС «КонсультантПлюс».

2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «КонсультантПлюс».

3. О безопасности дорожного движения : Федеральный закон от 10.12.1995 № 196-ФЗ // СПС «КонсультантПлюс».

4. Об организации дорожного движения в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 29.12.2017 № 443-ФЗ // СПС «КонсультантПлюс».

5. О полиции : Федеральный закон от 07.02.2011 № 3-ФЗ // СПС «КонсультантПлюс».

6. Кодекс Российской Федерации об административных правонарушениях : Федеральный закон от 30.12.2001 № 195-ФЗ // СПС «КонсультантПлюс».

7. О Правилах дорожного движения : постановление Правительства РФ от 23.10.1993 № 1090 // СПС «КонсультантПлюс».

8. Ротем Дж. П. Психология безопасности дорожного движения и кампании по информированию общественности. — Лондон : Routledge, — 2019.

9. Об утверждении Стратегии безопасности дорожного движения в Российской Федерации на 2018—2024 годы : распоряжение Правительства РФ от 08.01.2018 № 1-р // СПС «КонсультантПлюс».

10. Материалы расширенной коллегии МВД России. — URL: <http://www.kremlin.ru/events/president/transcripts/76408> (дата обращения: 4.03.2025).

11. Официальная статистика ГИБДД РФ. — URL: <https://нцбдд.мвд.рф/ресурсы/аналитические-обзоры-состояния-безопасности> (дата обращения: 04.03.2025).

12. Казиахмедов Г. М., Поцелуев П. А. Социально-экономические аспекты последствий дорожно-транспортных происшествий в России // Региональная экономика: теория и практика. — 2007. — № 7. — С. 124—129.

13. Ноговицина Е. Н. Роль ГИБДД в формировании правосознания участников дорожного движения // Управление деятельностью по обеспечению безопасности дорожного движения: состояние, проблемы, пути совершенствования. — 2021. — № 1. — С. 338—342.

14. Былинин И. А. Некоторые аспекты повышения безопасности дорожного движения в современных условиях // Административное право и практика администрирования. — 2019. — № 4. — С. 6—11.

REFERENCES

1. Ob utverzhdenii Nastavleniya po organizacii deyatel'nosti Gosudarstvennoj inspekcii bezopasnosti dorozhnogo dvizheniya Ministerstva vnutrennix del Rossijskoj Federacii po propagande bezopasnosti dorozhnogo dvizheniya : prikaz MVD Rossii ot 29 dekabrya 2018 g. № 903 // SPS «Konsul'tantPlyus».

2. Konstituciya Rossijskoj Federacii (prinyata vsenarodny'm golosovaniem 12.12.1993 s izmeneniyami, odobrenny'mi v xode obshherossijskogo golosovaniya 01.07.2020) // SPS «Konsul'tantPlyus».

3. O bezopasnosti dorozhnogo dvizheniya : Federal'ny'j zakon ot 10.12.1995 № 196-FZ // SPS «Konsul'tantPlyus».

4. Ob organizacii dorozhnogo dvizheniya v Rossijskoj Federacii i o vnesenii izmenenij v otdel'ny'e zakonodatel'ny'e akty Rossijskoj Federacii : Federal'ny'j zakon ot 29.12.2017 № 443-FZ // SPS «Konsul'tantPlyus».

5. O policii : Federal'ny'j zakon ot 07.02.2011 № 3-FZ // SPS «Konsul'tantPlyus».

6. Kodeks Rossijskoj Federacii ob administrativny'x pravonarusheniyax : Federal'ny'j zakon ot 30.12.2001 № 195-FZ // SPS «Konsul'tantPlyus».

7. O Pravitel'stva RF ot 23.10.1993 № 1090 // SPS «Konsul'tantPlyus».

8. Rotem Dzh. P. Psixologiya bezopasnosti dorozhnogo dvizheniya i kampanii po informirovaniyu obshhestvennosti. — London : Routledge, — 2019.

9. Ob utverzhdenii Strategii bezopasnosti dorozhnogo dvizheniya v Rossijskoj Federacii na 2018—2024 gody : rasporyazhenie Pravitel'stva RF ot 08.01.2018 № 1-r // SPS «Konsul'tantPlyus».

10. Materialy` rasshirennoj kollegii MVD Rossii. — URL: <http://www.kremlin.ru/events/president/transcripts/76408> (data obrashheniya: 4.03.2025).

11. Oficial'naya statistika GIBDD RF. — URL: <https://nczbdd.mvd.rf/resursy`analiticheskie-obzory`-sostoyaniya-bezopasnosti> (data obrashheniya: 04.03.2025).

12. Kaziamedov G. M., Podeluev P. A. Social'noe'konomicheskie aspekty` posledstvij dorozhno-transportny`x proissheshtvij v Rossii // Regional'naya e'konomika: teoriya i praktika. — 2007. — № 7. — S. 124—129.

13. Nogovicina E. N. Rol' GIBDD v formirovanii pravosoznaniya uchastnikov dorozhnogo dvizheniya // Upravlenie deyatel'nost'yu po obespecheniyu be-

zopasnosti dorozhnogo dvizheniya: sostoyanie, problemy`, puti sovershenstvovaniya. — 2021. — № 1. — S. 338—342.

14. By`linin I. A. Nekotorye` aspekty` povы'sheniya bezopasnosti dorozhnogo dvizheniya v sovremenny`x usloviyax // Administrativnoe pravo i praktika administrirovaniya. — 2019. — № 4. — S. 6—11.

СВЕДЕНИЯ ОБ АВТОРАХ

Караваев Александр Александрович. Доцент кафедры административной деятельности органов внутренних дел. Кандидат юридических наук, доцент.

Воронежский институт МВД России.

E-mail: ferrari49@yandex.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Галустян Андраник Гайкович. Старший преподаватель кафедры безопасности дорожного движения. Краснодарский университет МВД России.

E-mail: agg958@mail.ru

Россия, 350005, Краснодар, ул. Ярославская, 128.

Karavaev Alexander Alexandrovich. Associate Professor of the chair of Administrative Activities of the Internal Affairs Directorate. Candidate of Law, Associate Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: ferrari49@yandex.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Galustyan Andranik Gaikovich. Senior lecturer of the chair of Road Safety.

Krasnodar University of the Ministry of the Interior of Russia.

E-mail: agg958@mail.ru

Work address: Russia, 350005, Krasnodar, Yaroslavskaya Str., 128.

Ключевые слова: пропаганда; безопасность дорожного движения; социальная реклама; профилактика дорожно-транспортных происшествий; административное правонарушение; пешеход; водитель.

Key words: propaganda; road safety; social advertising; prevention of road accidents; administrative offense; pedestrian; driver.

УДК 343.272

Л. В. Кокорева, кандидат юридических наук, доцент

Р. А. Кокорев, кандидат юридических наук, доцент

ПЕРСПЕКТИВЫ СОВЕРШЕНСТВОВАНИЯ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ПРОВЕДЕНИИ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

PROSPECTS FOR IMPROVING THE USE OF INFORMATION TECHNOLOGY IN CONDUCTING INVESTIGATIVE ACTIONS

Современные информационные технологии (далее — ИТ) играют ключевую роль в различных сферах жизни общества, включая правоохранительную деятельность. Их использование позволяет значительно повысить эффективность проведения следственных действий, обеспечить точность и объективность расследования уголовных дел. Однако, несмотря на очевидные преимущества, существуют проблемы, связанные с недостаточным уровнем внедрения современных ИТ-решений в практику правоохранительных органов. Статья посвящена рассмотрению перспектив совершенствования применения информационных технологий при проведении следственных действий.

Modern information technologies (hereinafter referred to as IT) play a key role in various spheres of society, including law enforcement. Their use makes it possible to significantly increase the effectiveness of investigative actions, ensure the accuracy and objectivity of the investigation of criminal cases. However, despite the obvious advantages, there are problems associated with the insufficient level of implementation of modern IT solutions in the practice of law enforcement agencies. This article is devoted to the consideration of the prospects for improving the use of information technology in conducting investigative actions.

Использование информационных технологий в ходе следственных действий способствует проведению качественного расследования уголовных дел благодаря решению нескольких задач: осуществляется быстрый доступ к информации, необходимой для расследования преступлений, что помогает оперативно выявлять ключевые факторы и обстоятельства уголовного дела; производится автоматизированная запись и документирование этапов в соответствии с законодательством; сокращается время, затрачиваемое на расследование, через дистанционное взаимодействие с интеграцией информационных технологий; реализуется обмен данными, полученными в процессе следственных действий; происходит рациональное использование бюджетных средств.

В качестве подтверждения вышеизложенного приведем пример из правоприменительной практики, когда достижения науки и техники помогли органам предварительного следствия раскрыть преступление, произошедшее более десяти лет назад. Несмотря на длительный промежуток времени с момента совершения преступления, следователям удалось установить лицо, совершившее особо тяжкое преступление.

Согласно официальной информации, опубликованной на сайте Следственного управления Следственного комитета России по ЛНР [1], в ноябре 2014 года в центре станицы Луганской прогремел взрыв в магазине строительных материалов, принадлежащем местному бизнесмену. В результате инцидента владелец магазина получил множественные ранения и от полученных травм скончался. Следователю передали рисунок, который успел нарисовать потерпевший перед смертью. На рисунке был изображен символ немецкого производителя автомобилей. В январе 2023 года мать погибшего предпринимателя обратилась в Станично-Луганский межрайонный отдел с заявлением о том, что его смерть может быть связана с действиями его бывшего знакомого. Родственники утверждали, что между мужчинами часто происходили конфликты и автомобиль немецкого концерна, принадлежащий этому знакомому, был замечен рядом с магазином в день трагического происшествия. Следователи провели детальную проверку места происшествия, применив современное криминалистическое оборудование. В результате были найдены осколки взрывного устройства, что подтвердило

версию о преднамеренном взрыве внутри строения. Тем не менее подозреваемый решительно отверг свою причастность, заявив, что осенью 2014 года происходил артиллерийский обстрел и взрыв стал следствием этого события. Следователи обратились к архивным данным космической съемки, чтобы проверить свою гипотезу. По снимкам было видно, что детонация взрывного устройства произошла внутри помещения, а не снаружи, что исключает возможность артиллерийского обстрела. Это стало важным доказательством в установлении факта убийства. Проведенные следственные действия и полученные доказательства позволили предъявить обвинение в убийстве, совершенном общеопасным способом. Уголовное дело направлено в суд.

В настоящее время в научной литературе обсуждаются идеи по расширению системы следственных действий посредством нововведений в процессуальном доказывании, основанных на познавательных методах и достижениях науки в области высоких технологий, что вызывает определенный интерес.

Перспективным направлением, соответствующим условиям цифровой трансформации, являются новые следственные действия, которые предполагают дистанционный формат производства. Некоторые исследователи предлагают инновационные изменения в перечне следственных действий, предусмотренных уголовно-процессуальным законодательством [2. — С. 67—77]. К таким направлениям относятся дистанционные и электронные действия, которые в значительной мере пересекаются между собой. Под действиями, о которых идет речь, понимаются операции с цифровыми данными, которые не зависят от используемых носителей. Важно внести в УПК РФ новые нормы, касающиеся таких процедур, как осмотр электронного объекта и мониторинг электронных отправок с возможностью их копирования.

Особое внимание стоит уделить такому следственному действию, известному и широко применяемому в зарубежной практике, как онлайн-обыск [3. — С. 117—123] (виртуальный, цифровой или электронный обыск). Данное следственное действие предполагает правомерный взлом цифрового устройства и обход средств его защиты для поиска данных, имеющих значение для уголовного дела [4]. Для этого используют специальные компьютерные вирусы, например программы Magic Latern («Волшебный фонарь»), CIPAV (Computer and Internet Protocol Address Verifier — верификатор адресов компьютеров и интернет-протоколов), State Trojan («ГосТроян»), которые устанавливаются на компьютер обвиняемого (подозреваемого) или других лиц в случаях,

предусмотренных законом. После этого программа может сохранять введенные пароли, самостоятельно включать микрофон устройства и веб-камеры для записи переговоров, получать фотографии, искать определенные файлы на жестком диске устройства и передавать их органам предварительного расследования. В свою очередь, проведение онлайн-обыска строго регулируется законом, так как это вмешательство в права граждан. Для рассматриваемого следственного действия существует ограниченный круг процессуальных оснований, например расследование только особо тяжких преступлений. Так, в 2008 году в ФРГ приняли закон, позволяющий применять «ГосТроян» при расследовании преступлений, связанных с терроризмом. В 2017 году сферу разрешенного использования расширили, включив в нее расследование особо тяжких преступлений (геноцид, военные преступления) и других категорий преступлений (легализация доходов, полученных незаконным путем, кража, хранение и сбыт наркотиков) [5]. Кроме того, для проведения онлайн-обыска необходимо получить разрешение суда.

Иными словами, онлайн-обыск включает в себя инфицирование цифрового устройства специальным вирусом с обходом его защитных систем для получения доказательств по уголовному делу. Пока он проводится только правоохранительными органами зарубежных стран, но впоследствии такой механизм можно перенять и для отечественного уголовно-процессуального закона, поскольку его достоинства состоят из: сокращения времени, требуемого для получения необходимых доказательств — в данном случае отсутствует необходимость в проведении традиционного обыска и изъятии цифрового устройства, а также в длительной компьютерной экспертизе изъятых материалов. Доказательства образуются в онлайн-режиме, аналогично контролю и записи телефонных переговоров в соответствии со ст. 186 УПК РФ; непрямого сохранения и передачи органам предварительного расследования файлов cookie и журналов соединений с облачными сервисами — это существенно упрощает процесс обнаружения необходимых доказательств среди других данных на удаленном устройстве; исключения риска утраты доказательств при изъятии компьютера у подозреваемого или обвиняемого, а также утраты доступа к удаленному хранилищу через это устройство.

Не можем не добавить несколько размышлений об искусственном интеллекте, который представляет собой процесс создания машин, способных осуществлять действия, которые человек воспринимает как проявления интеллекта [6. — С. 15;

7. — С. 190—194]. Следовательно, можно заключить, что данная система относится к сфере разработки компьютерных технологий, связанных с человеческим умом, охватывающих такие элементы, как логическое мышление, обучение и решение проблем.

В настоящее время практические сотрудники, в отличие от представителей научного сообщества, скептически относятся к предложениям о широком использовании технологий искусственного интеллекта в уголовном судопроизводстве. По результатам проведенного опроса сотрудников правоохранительных органов, в 89 % случаев респонденты высказали недоверие к массовому применению технических средств при проведении следственных действий. Анкетирование слушателей заочного отделения проводилось в феврале-марте 2025 г. на территории МОФ МосУ МВД России имени В. Я. Кикотя. Лишь незначительная часть респондентов относится положительно к внедрению технологий на базе искусственного интеллекта — ими отмечены их важность для осуществления следственных и других процессуальных действий (5%).

Полагаем, что данные технологии имеют потенциал для оценки фактических условий уголовного дела с учетом правил доказательственного отбора, могут анализировать соблюдение норм уголовно-процессуального законодательства при принятии решений, а также, возможно, предлагать варианты решений в специфических ситуациях.

Стоит отметить, что Следственный комитет России активно применяет цифровые технологии, включая искусственный интеллект и методы BigData, с целью повышения результативности своих расследований. В августе 2024 года председатель Следственного комитета России А. И. Бастрыкин на встрече, посвященной развитию информационных технологий в организации, заявил о разработке новых инструментов, которые значительно улучшат возможности анализа больших массивов информации [8].

По данным ТАСС, новейшие системы искусственного интеллекта значительно помогут следователям в быстрой обработке данных [9]. Это выведет процесс расследования преступлений на новый уровень. Тем не менее он не сможет полностью заменить человека в этой сфере. Искусственный интеллект будет служить помощником следователям, содействуя в нахождении ключевых сведений и анализе больших объемов данных [8].

Таким образом, возникает необходимость в разработке унифицированных алгоритмов для обоснования и осуществления решений в уголовном производстве, которые можно было бы встре-

ить, например, в экспертную деятельность. В зависимости от предоставленных данных и их свойств экспертная деятельность будет определять наиболее подходящий алгоритм для специалистов, занимающихся обнаружением и изъятием улик. К примеру, в ходе введения цифровых инноваций в Следственном комитете специалистами оперативно используются программы, разработанные на основе алгоритмов искусственного интеллекта для криминалистических экспертиз. По сообщению Зигмунда Ложиса, одной из этих программ удастся сформировать психический образ злоумышленника, руководствуясь определенными признаками, выявленными на начальных этапах расследования. Эта технология, построенная на нейросетях, имеет возможность с высокой степенью точности предсказывать черты человека относительно его возраста, семейного положения и даже наличия болезней. Достоверность некоторых из этих предсказаний составляет более 80% [10].

Некоторые ученые (Е. Н. Быстряков, А. Б. Смушкин, И. В. Усанов [11. — С. 29—32; 12. — С. 90—107]) уже поднимали вопрос о возможности использования так называемых цифровых следователей (киберследователей, которые являются носителями искусственного интеллекта). Исследователи высказывают предположение о внедрении роботизированных систем в целях предотвращения, пресечения преступлений, а также для анализа и документирования ситуации при чрезвычайном происшествии. Ученые обоснованно подчеркивают второстепенную функцию цифровых следователей, представляя их как носитель искусственного интеллекта, который должен научиться разумно воспринимать нормальное развитие событий во время расследования уголовных дел.

Стоит отметить, что мы не можем согласиться с идеей полной замены человека-следователя на робота, поскольку автоматизация не способна полностью заменить человека, ответственного за судьбу уголовного дела. Считаем, что не следует возлагать завышенные ожидания на достижения информационных и цифровых технологий, предполагая, что переход уголовного процесса на цифровые форматы существенно скажется на возможностях миллионов людей, которые либо скептически относятся к инновациям (что часто вполне резонно), либо не имеют доступа к современным техническим средствам.

Кроме того, стоит учитывать ошибки в подозрении и обвинении невиновных лиц, допускаемые с использованием искусственного интеллекта. Так, в 2023 году широкий общественный резонанс вызвала история с арестом Александра

Цветкова. Нейросеть приняла московского ученого за преступника, подозреваемого в убийствах четырех человек, совершенных с особой жестокостью двадцать лет назад. Прежде чем ошибка искусственного интеллекта была доказана и А. Цветкова освободили из СИЗО, человек провел в заключении десять месяцев [13].

Таким образом, совершенствование применения информационных технологий в процессе проведения следственных действий представляет собой комплексную задачу, требующую значительных усилий со стороны государства и профессионального сообщества. Интеграция передовых IT-решений в повседневную работу правоохранительных органов способствует повышению эффективности борьбы с преступностью, обеспечению справедливости и правопорядка.

При этом следует подчеркнуть, что правоприменительная практика демонстрирует в некоторых случаях игнорирование применения органами предварительного расследования современных информационных технологий.

Во-первых, наблюдается нехватка технических возможностей и недостаточное оснащение органов предварительного расследования современными устройствами и программами. Отметим, что отсутствие необходимой технической инфраструктуры для системы видео-конференц-связи существенно осложняет внедрение информационных технологий во многих территориальных подразделениях МВД России. Согласно требованиям уголовно-процессуального закона, для эффективного использования систем видео-конференц-связи необходимо наличие соответствующих технических возможностей (ч. 1 ст. 189.1 УПК РФ).

Во-вторых, использование современных средств уведомления участников процесса осуществляется не в полной мере. Несмотря на то, что уголовно-процессуальный закон допускает применение информационных технологий, таких как оповещение участников уголовного судопроизводства через SMS с их согласия, правоохранительные органы осуществляют вызов участников процесса лишь посредством телефонного звонка с последующей передачей повестки по запросу участника следственного действия.

В-третьих, наблюдается нехватка сотрудников правоохранительных органов со знаниями в сфере современных технологий и последних достижений науки, особенно в удаленных районах страны.

По мнению С. Г. Еремина и О. А. Решняк, сотрудники следственного подразделения должны регулярно повышать свои профессиональные навыки в области цифровой грамотности [14. — С. 46—50].

Исследователи небезосновательно отмечают основные факторы, способствующие улучшению качества расследования, особенно преступлений, совершаемых в сфере информационно-телекоммуникационных технологий.

1. Стремление к личностному и профессиональному развитию в условиях риска и неопределенности. Самосовершенствование выгодно сказывается на актуализации навыков и внутренней мотивации. Следователь (да и дознаватель) обязан повышать квалификацию, чтобы сохранять свою востребованность, продуктивность и эффективность.

2. Способность находить и анализировать информацию в Интернете. В большинстве случаев следователи (дознаватели) обладают этими навыками, способны работать с виртуальными данными в интернет-пространстве. Однако существует группа сотрудников, для которых работа с электронными материалами является сложной задачей. Поэтому эти навыки требуют постоянного совершенствования и обновления.

3. Организация взаимодействия в киберпространстве. Сочетание различных программ и софтов представляет собой значительную проблему для органов предварительного расследования. Сотрудники правоохранительных органов не используют полный спектр доступного функционала, что затрудняет проверку данных параллельно и поддержание коммуникации. Это отражается на сроках проведения расследований уголовных дел. Глобальные тенденции, связанные с цифровой трансформацией, оказывают влияние на работу следователей (дознавателей), и им необходимо адаптироваться к этим изменениям, чтобы обеспечить эффективность расследований. Отметим, что в августе 2024 года в некоторых подразделениях Следственного комитета России в рамках программы по импортозамещению программного обеспечения начался пилотный проект по тестированию отечественных софтов. Также ведомство планирует интегрировать свои информационные системы с государственными цифровыми сервисами, что поможет создать единую и более эффективную платформу по обмену сведениями [15].

4. Навыки в сфере управления данными. Управление данными и обеспечение их безопасности являются ключевыми компетенциями для сотрудников органов предварительного расследования. Личные сведения, которые в последнее время рассматриваются как конфиденциальная информация, часто оказываются под угрозой раскрытия или передачи третьим лицам, что совершенно недопустимо. Такая проблема возникает, когда не осознается важность защиты личной информации.

Информацию следует не только безопасно хранить, но и правильно ею управлять.

Для успешного внедрения современных технологий необходимо использовать системный подход, который включает как совершенствование законодательства в области уголовного процесса, так и четкое определение полномочий правоохранительных органов при использовании новых информационных технологий. Также важно разработать критерии и рамочные условия для применения информационных методов в ходе расследования, а кроме того, легализовать новые направления в этой области.

В заключение стоит отметить, что в деятельности органов предварительного расследования присутствует достаточно большой арсенал цифровых средств, которые позволяют решить множество задач расследования, — сокращается время проверки, осуществляется быстрая фиксация улик (в дальнейшем вещественных доказательств), снижаются риски неправомерных действий должностных лиц. Перспективы совершенствования технологий сводятся к внедрению цифрового УПК РФ, нейронных сетей, возможностей искусственного интеллекта, а также приходу новых следственных действий на смену традиционным.

ЛИТЕРАТУРА

1. В ЛНР следователи с помощью космической съемки раскрыли убийство предпринимателя, совершенное десятилетие назад. — URL: <https://lnr.sledcom.ru/news/item/1910230/> (дата обращения: 08.04.2025).

2. Зуев С. В., Зазулин А. И. Цифровой УПК: новая концепция развития права // Правопорядок: история, теория, практика. — 2024. — № 1 (40). — С. 67—77.

3. Зазулин А. И. Онлайн-обыск как самостоятельное следственное действие: предпосылки, перспективы и недостатки // Казанские уголовно-процессуальные и криминалистические чтения : материалы междунар. науч.-практ. конф. (Казань, 28 апр. 2022 г.) : в 2 ч. / [ред. кол.: Ю. Н. Кулешов (отв. ред.) и др.] ; Казан. ин-т (фил.) ВГУЮ. — Казань : ЮрЭксПрактик, 2022. — Ч. 1. — С. 117—123.

4. Уголовный процесс Германии в контексте национальных и международных тенденций по цифровизации права. Новые следственные мероприятия, разработанные в цифровую эпоху. Онлайн-обыск (§ 100b УПК). — URL: https://bstudy.net/1015767/pravo/onlayn_obysk_100b (дата обращения: 03.01.2025).

5. Зазулин А. И. Компьютерные вирусы на службе правосудия: опыт западных стран. — URL: http://www.intellec.ru/press/works/ugolovno_protseussual_nyu_kiberpank/ (дата обращения: 03.01.2025).

6. Джонс М. Т. Программирование искусственного интеллекта в приложениях / пер. с англ. А. И. Осипова. — М. : ДМК-Пресс, 2018. — 312 с.

7. Моругина Н. А., Кузьмина О. Л. Оценка допустимости распространения опыта цифровизации в уголовном судопроизводстве России // Со-

временные проблемы уголовного процесса: пути решения : сборник материалов V Международной науч.-практ. конф., Уфа, 04–05 апреля 2024 года. — Уфа : Уфимский юридический институт МВД России, 2024. — С. 190—194.

8. В СК появятся новые разработки ИИ для анализа больших данных. — URL: <https://tass.ru/obschestvo/21597175> (дата обращения: 04.04.2025).

9. Хан Т. Руководитель НИИ криминалистики СК РФ: идеальных преступлений не бывает. — URL: <https://tass.ru/interviews/12688681> (дата обращения: 03.04.2025).

10. В СКР рассказали о помощи искусственного интеллекта в поимке преступников. — URL: <https://rossaprimavera.ru/news/5cdef98d> (дата обращения: 03.04.2025).

11. Быстряков Е. Н., Усанов И. В. Киберследователь // Проблемы уголовного процесса, криминалистики и судебной экспертизы. — 2017. — № 1 (9). — С. 29—32.

12. Смушкин А. Б. Цифровая трансформация процесса расследования как объективная реальность // Вестник СПбГУ. Право. — 2023. — Т. 14. — Вып. 1. — С. 90—107.

13. Роботы вместо следователей — цифровизация подкрадывается к правоохранительным органам. — URL: <https://dzen.ru/a/ZnA4oINIOGbMcC1b> (дата обращения: 03.04.2025).

14. Еремин С. Г., Решетняк О. А. Цифровая грамотность как способ повышения качества расследования преступлений // Юрист-Правовед. — 2022. — № 2 (101). — С. 46—50.

15. В Следственном комитете обсудили применение информационных технологий. — URL: <https://rg.ru/2024/08/> (дата обращения: 04.04.2025).

REFERENCES

1. V LNR sledovateli s pomoshch'yu kosmicheskoy s"emki raskryli ubijstvo predprinimatel'ya, sovershennoe desyatiletie nazad. — URL: <https://lnr.sledcom.ru/news/item/1910230/> (data obrashcheniya: 08.04.2025).
2. Zuev S. V., Zazulin A. I. Cifrovoy UPK: novaya koncepciya razvitiya prava // Pravoporyadok: istoriya, teoriya, praktika. — 2024. — № 1 (40). — S. 67—77.
3. Zazulin A. I. Onlajn-obysk kak samostoyatel'noe sledstvennoe dejstvie: predposylki, perspektivy i nedostatki // Kazanskije ugolovno-processual'nye i kriminalisticheskie chteniya : materialy mezhdunar. nauch.-prakt. konf. (Kazan', 28 apr. 2022 g.) : v 2 ch. / [red. kol.: Yu. N. Kuleshov (otv. red.) i dr.] ; Kazan. in-t (fil.) VGUYu. — Kazan' : YurEksPraktik, 2022. — Ch. 1. — S. 117—123.
4. Ugolovnyj process Germanii v kontekste nacional'nyh i mezhdunarodnyh tendencij po cifrovizacii prava. Novye sledstvennye meropriyatiya, razrabotannye v cifrovuyu epohu. Onlajn-obysk (§ 100b UPK). — URL: https://bstudy.net/1015767/pravo/onlayn_obysk_100b (data obrashcheniya: 03.01.2025).
5. Zazulin A. I. Komp'yuternye virusy na sluzhbe pravosudiya: opyt zapadnyh stran. — URL: http://www.intelects.ru/press/works/ugolovno_protsesual_nyy_kiberpank/ (data obrashcheniya: 03.01.2025).
6. Dzhons M. T. Programmirovaniye iskusstvennogo intellekta v prilozheniyah / per. s angl. A. I. Osipova. — M. : DMK-Press, 2018. — 312 s.
7. Morugina N. A., Kuz'mina O. L. Ocenka dopustimosti rasprostraneniya opyta cifrovizacii v ugolovnom sudoproizvodstve Rossii // Sovremennye problemy ugolovnogo processa: puti resheniya : sbornik materialov V Mezhdunarodnoj nauch.-prakt. konf., Ufa, 04–05 aprelya 2024 goda. — Ufa : Ufimskij yuridicheskij institut MVD Rossii, 2024. — S. 190—194.
8. V SK poyavyatsya novye razrabotki II dlya analiza bol'shih dannyh. — URL: <https://tass.ru/obschestvo/21597175> (data obrashcheniya: 04.04.2025).
9. Han T. Rukovoditel' NII kriminalistiki SK RF: ideal'nyh prestuplenij ne byvaet. — URL: <https://tass.ru/interviews/12688681> (data obrashcheniya: 03.04.2025).
10. V SKR rasskazali o pomoshchi iskusstvennogo intellekta v poimke prestupnikov. — URL: <https://rossaprimavera.ru/news/5cdef98d> (data obrashcheniya: 03.04.2025).
11. Bystryakov E. N., Usanov I. V. Kibersledovatel' // Problemy ugolovnogo processa, kriminalistiki i sudebnoj ekspertizy. — 2017. — № 1 (9). — S. 29—32.
12. Smushkin A. B. Cifrovaya transformaciya processa rassledovaniya kak ob"ektivnaya real'nost' // Vestnik SPbGU. Pravo. — 2023. — T. 14. — Vyp. 1. — S. 90—107.
13. Roboty vmesto sledovatelej — cifrovizaciya podkradyvaetsya k pravoohranitel'nyh organam. — URL: <https://dzen.ru/a/ZnA4oINIOGbMcC1b> (data obrashcheniya: 03.04.2025).
14. Eremin S. G., Reshetnyak O. A. Cifrovaya gramotnost' kak sposob povysheniya kachestva rassledovaniya prestuplenij // Yurist-Pravoved". — 2022. — № 2 (101). — S. 46—50.
15. V Sledstvennom komitete obsudili primenenie informacionnyh tekhnologij. — URL: <https://rg.ru/2024/08/> (data obrashcheniya: 04.04.2025).

СВЕДЕНИЯ ОБ АВТОРАХ

Кокорева Любовь Владимировна. Профессор кафедры уголовного процесса. Кандидат юридических наук, доцент.

Московский областной филиал Московского университета МВД России имени В. Я. Кикотя.

E-mail: Kokoreva80@mail.ru

Россия, 143103, Московская обл., Рузский г.о., п. Старотеряево.

Кокорев Роман Александрович. Заместитель начальника кафедры криминалистики. Кандидат юридических наук, доцент.

Московский областной филиал Московского университета МВД России имени В. Я. Кикотя.

E-mail: Kokorev_roman@mail.ru

Россия, 143103, Московская обл., Рузский г.о., п. Старотеряево.

Kokoreva Lyubov Vladimirovna. Professor of the chair of Criminal Procedure. Candidate of Law, Associate Professor.

Moscow Regional Branch of the Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot.

E-mail: Kokoreva80@mail.ru

Work address: Russia, 143103, Moscow region, Ruzsky g. o., Staroteryaev.

Kokorev Roman Alexandrovich. Deputy Head of the chair of Criminalistics. Candidate of Law, Associate Professor.

Moscow Regional Branch of the Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot.

E-mail: Kokorev_roman@mail.ru

Work address: Russia, 143103, Moscow region, Ruzsky g. o., Staroteryaev.

Ключевые слова: следственные действия; информационные технологии; расследование уголовных дел; профессиональные навыки в области цифровой грамотности.

Key words: investigative actions; information technology; criminal investigation; professional skills in the field of digital literacy.

УДК 343.132

Е. П. Новикова, кандидат юридических наук, доцент
К. С. Чернышова

СВАТТИНГ КАК РАЗНОВИДНОСТЬ ТЕРРОРИЗМА: УГОЛОВНО-ПРАВОВОЙ АСПЕКТ

SWATTING AS A TYPE OF TERRORISM: THE CRIMINAL LAW ASPECT

В статье рассматривается новое негативное социальное явление, направленное на дестабилизацию общества и правоохранительных структур, дается его уголовно-правовая характеристика и вносятся предложения по криминализации этого деструктивного деяния.

The article examines a new negative social phenomenon aimed at destabilizing society and law enforcement agencies, provides its criminal and legal characteristics, and makes proposals to criminalize this destructive act.

В условиях современных реалий общества, когда происходит мощный цикл изменений в области информационно-коммуникационных технологий, возникают новые угрозы для общества, которые пока юридически не находят своего отражения и нуждаются в глубоком изучении. Так, особое внимание привлекает такое социальное деструктивное явление как сваттинг, англоязычное название которого берет свои истоки из Соединенных Штатов Америки, где существует одно из наиболее известных в мире специальных подразделений полиции с аббревиатурой SWAT, название которого раньше означало в расшифровке Special Weapons Assault Team, что в переводе на русский «штурмовая группа со специальным вооружением», а ныне — Special Weapons and Tactics — «специальное оружие и тактика» [1]. Мировой феномен сваттинга заключается в том, что из обычного хулиганства он трансформировался в настоящее преступное движение террористической направленности [2].

Сваттинг — это разновидность террористической деятельности, обозначающая ложное сообщение, содержание которого включает в себя информацию об уже совершаемом или готовящимся к совершению в ближайшее время террористическом акте или ином общественно опасном деянии, которое создает или может создать угрозу общественному правопорядку и влечет за собой тяжкие последствия. Это сообщение адресовано правоохранительным органам с целью отвлечения их внимания, а также внимания других экстренных оперативных служб от реально существующих проблем, в том числе преступного характера. Важно отметить, что данный общественно опасный акт создает значительные нагрузки для экс-

тренных оперативных служб, которые затрачивают определенные ресурсы, реагируя на такие сообщения, а также отвлекает их внимание от повседневной деятельности. Таким образом, целью сваттинга является распространение чувства паники среди населения путем воздействия на общественное сознание и создание помех в деятельности оперативных структур через нарушение функциональности социальной системы.

Также следует сказать, что сваттинг может быть осуществлен злоумышленником для розыгрыша или для отместки человеку, чтобы спецподразделения прибыли на указанный адрес псевдопреступника и задержали его до выяснения обстоятельств. Мировой феномен сваттинга заключается в том, что из обычного хулиганства он трансформировался в настоящее преступное движение террористической направленности.

Несмотря на то, что сваттинг с момента своего появления рассматривался как одна из форм «троллинга» (преследования), на сегодняшний день подобные деяния имеют ярко выраженный террористический характер.

Предшественниками данного явления являются телефонные розыгрыши и злые шутки. У сваттинга много схожего с пранк-звонками, так как именно термин «пранк» (от англ. «prank» — шутка, проделка) означает розыгрыш, мистификацию, которые совершаются в отношении других людей, тем самым поставив последних в положение жертвы. Пранк может быть реализован в различных формах — телефонные звонки, видеосообщения, сообщение в социальных сетях, мессенджерах, а также наиболее устаревшим способом — в виде бумажной рукописи, письма.

Сваттинг, имея схожие черты с пранком, в свою очередь, характеризуется отличительными особенностями:

1. Получатель сообщений о псевдотеррористическом акте. В первую очередь, при сваттинге к числу получателей ложных сообщений относятся правоохранные органы (МВД, ФСБ, Росгвардия) и экстренные службы.

2. Цели и мотивы злоумышленника. Основопологающей целью лица, занимающегося сваттингом, выступает обвинение конкретного лица в якобы готовящемся преступлении, а также дестабилизация нормальной деятельности органов государственной власти, органов местного самоуправления, экстренных служб и правоохранительных органов и их отвлечение от реально имеющейся работы с переключением внимания на устранение мнимой опасности. Злоумышленник, который занимается сваттингом, руководствуется хулиганскими мотивами, корыстью, местью, враждой или ненавистью в отношении конкретного человека или определенной общественной группы, выделяемой им по этническим, идеологическим, национальным и иным признакам.

3. Масштабность совершения. Сваттингер, совершая данное преступление в отношении определенного человека, неумышленно вовлекает в процесс обширный круг лиц, затрагивая граждан других стран, что позволяет говорить о том, что проблема выходит на международный уровень, делая проблему сваттинга транснациональной. Так, например, колоссальный круг пострадавших возник от сваттинга, осуществленного в конце 2021 — начале 2022 года посредством использования сети Интернет на территориях Российской Федерации, а также Азербайджана, Армении, Беларуси, Казахстана, Молдовы и на тот момент не признанных Донецкой и Луганской Народных Республик. Установлено, что ложные террористические угрозы распространялись преступниками в целях дестабилизации обстановки в Российской Федерации и сопредельных государствах, вымогательства денежных средств и из хулиганских побуждений. В ходе расследования выяснилось, что к организации указанной преступной деятельности причастны участники так называемых сваттинговых интернет-сообществ, а их организаторами и администраторами являлись гражданин Украины Антон Осипчук, 2003 г.р., а также его подельники [3].

Необходимо отметить, что такое явление, как сваттинг, имеет негативные последствия и для конкретного человека. Например, жертва (псевдопреступник) может столкнуться с задержанием и вытекающим из него ограничением своих прав и законных интересов сотрудниками полиции или иных спасательных служб. Кроме того, сваттинг

может иметь серьезные психологические последствия для жертвы, такие как посттравматический стрессовый синдром и тревожные расстройства [4].

Именно поэтому важным является изучение уголовно-правового содержания сваттинга, так как он представляет собой сложный и многогранный процесс, требующий всестороннего анализа в рамках уголовного законодательства, в том числе эффективных мер профилактики.

Как было отмечено ранее, сваттинг как отдельное преступление на территории Российской Федерации не имеет своего юридического закрепления, в связи с чем проблема квалификации регулярно вызывает затруднения, так как объективная сторона деяния может пересекаться с диспозициями других статей Уголовного кодекса Российской Федерации, такими как терроризм, хулиганство, заведомо ложный донос о преступлении.

По нашему мнению, сваттинг наиболее схож с преступлением, ответственность за которое предусмотрена ст. 207 УК РФ «Заведомо ложное сообщение об акте терроризма». Однако нами будет предложено выделение такого общественно опасного деяния, как сваттинг, в отдельную статью в целях недопущения в практической деятельности правоохранительных органов конкуренции норм, а следовательно, невозможности применения к лицу (сваттингеру) справедливого наказания, что является нарушением основных принципов УК РФ.

Так, разбирая состав преступления, связанного со сваттингом, необходимо рассмотреть четыре его основных элемента, а именно объект в классифицирующем виде, объективную сторону, субъект и субъективную сторону.

Объект преступления классифицируется на общий, видовой, родовой и непосредственный.

В связи с этим основным объектом преступления при сваттинге выступает совокупность благ и интересов общества и государства, на которые непосредственно посягает данное деяние, а конкретно — общественная безопасность. Таким образом, основной непосредственный объект — это общественные отношения, обеспечивающие защиту безопасности граждан и предотвращение угроз в отношении общества и государства.

В качестве факультативного (дополнительного) объекта сваттинга можно выделить общественные отношения в области охраны здоровья граждан, имущественные отношения, а также нормальную деятельность организаций и учреждений. Например, затраты сил, средств и иных ресурсов правоохранительных органов и других экстренных оперативных служб на проверку таких сообщений, а также убытки предприятий в связи с вынужденным приостановлением своей

деятельности и прочие финансовые потери, которые в совокупности наносят значительный материальный ущерб.

Рассматривая объективную сторону сваттинга, необходимо отметить, что она выражается исключительно в активных действиях в виде передачи сообщения, которое заведомо для злоумышленника (сваттингера), его передающего, ложное. Также важным является то, что такое сообщение чаще включает информацию о готовящихся мероприятиях террористического характера, которые якобы подготавливаются либо находятся в процессе совершения или уже совершены третьим лицом. Следует отметить, что передача сообщения может быть осуществлена в любой форме, с использованием различных способов анонимизации: при его передаче через сеть Интернет — социальные сети, мессенджеры, электронная почта (например, использование псевдонима или сокрытие IP-адреса путем использования VirtualPrivateNetwork (VPN), PROXY, TheOnionRouter (сеть TOR), виртуальных серверов и прочего). Либо, напротив, злоумышленник передает ложные сообщения, не скрывая своей личности, особенно если находится за рубежом.

Совершение таких действий направлено на создание чувства страха, тревоги и паники у граждан, а также отвлечение внимания правоохранительных органов и иных экстренных оперативных служб от своей непосредственной работы, зачастую в целях маскировки совершения иных преступных действий (в том числе террористического характера) на других объектах, чтобы минимизировать шанс пресечения преступления силами специальных служб и оказания помощи пострадавшим. При этом заведомо ложная информация должна носить публичный характер, то есть содержащиеся в ней сведения должны не утаиваться, а любым способом распространяться.

Следует отметить, что при передаче правонарушителем сообщений такого рода могут наступить общественно опасные последствия, к которым относятся отвлечение и затраты ресурсов, сил и средств правоохранительных органов и экстренных служб, дезорганизация нормальной деятельности предприятий, учреждений и организаций, а также причинение вреда здоровью людей, порождение у них чувства страха, безысходности, нервозности, паники и стресса, а также наиболее тяжкие последствия — гибель людей.

Изучая субъект совершения сваттинга, следует отметить, что это физическое вменяемое лицо, достигшее возраста уголовной ответственности. Наиболее целесообразно установить по отношению к данному преступлению минимальный возраст уголовной ответственности — 14 лет.

Связано это с повышенной общественной опасностью противоправного деяния, а также с тем, что данная возрастная группа наиболее часто совершает схожие преступления, будучи вовлеченной взрослыми преступниками.

Стоит отметить, если лицо совершило преступление в день своего рождения, а именно в 14-летие, то с юридической точки зрения фактическое наступление минимального возраста уголовной ответственности наступает на следующий день, то есть с нуля часов нуля минут следующих суток, согласно п. 5 Постановления Пленума Верховного Суда РФ от 1 февраля 2011 года № 1 (в редакции от 28.10.2021) «О судебной практике применения законодательства, регламентирующего особенности уголовной ответственности и наказания несовершеннолетних» [5].

Субъективная сторона сваттинга играет важную роль в дифференциации уголовной ответственности и наказания виновного лица, выборе режима лишения свободы, замене одного вида наказания на другое и так далее. Содержание субъективной стороны раскрывается через такие понятия, как «вина», «мотив» и «цель» совершения преступления.

Субъективная сторона сваттинга определяется виной в форме прямого умысла, что подразумевает осознание лицом общественно опасного характера своих действий в процессе передачи ложных сведений о готовящемся или совершающемся преступлении, в частности террористического характера. Намерение сваттингера совершить противоправные действия, связанные с передачей ложной информации, представляет собой волевой аспект умысла. Преступник полностью осознает, что совершенные им действия могут привести к общественно опасным последствиям, желая их наступления. Ключевым аспектом является то, что сваттингер, передавая ложное сообщение, должен осознавать его объективное несоответствие реальности.

Целями сваттинга являются: создание ложной угрозы совершения преступления и наступления противоправных последствий, что может привести к панике граждан, их возможной эвакуации; значительные затраты со стороны специальных оперативных служб на проверку такой информации; нарушение общественного порядка, а именно дестабилизация нормальной жизнедеятельности общества и государства; привлечение внимания; месть конкретному человеку, которого сватингер обвиняет в совершении преступления.

Рассматривая мотивы сваттинга, необходимо отметить, что ст. 207 УК РФ «Заведомо ложное сообщение об акте терроризма» предусматривает обязательный и исключительный мотив — хулиганские побуждения. Однако сваттинг предусматривает не

хулиганские побуждения, а желание мести или преследования, где сваттингерство используется как средство отмщения по отношению к конкретным лицам или организациям, подразумевающее личную неприязнь.

Таким образом, следует сказать о том, что сваттинг является мировым и критически угрожающим для общества и государства феноменом, имеет специфическую природу и может рассматриваться как разновидность террористической деятельности. Данное деяние предполагает активные действия, которые выражаются в передаче правоохранительным органам и иным экстренным оперативным

службам сообщений о преступлениях, в том числе террористической направленности. С уголовно-правовой точки зрения сваттинг имеет ярко выраженные цели и мотивы, в частности заключающиеся в желании отомстить другому лицу или конкретной организации. Данные аспекты позволяют криминализировать сваттинг как отдельное преступление в УК РФ. Учитывая большое количество технологий и способов анонимизации в сети Интернет, такое явление, как сваттинг, становится все более актуальной проблемой, которая требует особого внимания со стороны законодателя и правоохранительных органов.

ЛИТЕРАТУРА

1. SWAT — элитное подразделение американской полиции. — URL: <https://teletype.in/@viktor-poltava/BJdsL9NU4> (дата обращения: 10.02.2025).
2. Розыгрыша ради? Феномен сваттинга в России. — URL: <https://www.cismms.ru/poleznye-materialy> (дата обращения: 12.03.2025).
3. Пресечена деятельность лиц, причастных к массовым заведомо ложным сообщениям о готовящихся террористических актах. Национальный антитеррористический комитет. — URL: <http://nac.gov.ru/print/terrorizmu-net/fsb> (дата обра-

щения: 15.02.2025).

4. Что такое сваттинг и с чем его едят? — URL: https://dzen.ru/a/Zbd60RILCAnfVR_L (дата обращения : 15.02.2025).

5. О судебной практике применения законодательства, регламентирующего особенности уголовной ответственности и наказания несовершеннолетних : постановление Пленума Верховного Суда РФ от 01.02.2011 № 1 (ред. от 28.10.2021). — URL: <https://sudact.ru/law/postanovlenie-plenuma-verkhovnogo-suda-rf-ot-01022011/> (дата обращения : 16.03.2025).

REFERENCES

1. SWAT — e`litnoe podrazdelenie amerikanskoj policii. — URL: <https://teletype.in/@viktor-poltava/BJdsL9NU4> (data obrashheniya: 10.02.2025).
2. Rozy`gry`sha radi? Fenomen svattinga v Rossii. — URL: <https://www.cismms.ru/poleznye-materialy> (data obrashheniya: 12.03.2025).
3. Presechena deyatel`nost` licz, prichastny`x k massovy`m zavedomo lozhny`m soobshheniyam o gotovyashhixsya terroristicheskix aktax. Nacional`ny`j antiterroristicheskij komitet. — URL: <http://nac.gov.ru/print/terrorizmu-net/fsb> (data

obrashheniya: 15.02.2025).

4. Chto takoe svatting i s chem ego edyat? — URL: https://dzen.ru/a/Zbd60RILCAnfVR_L (data obrashheniya : 15.02.2025).

5. O sudebnoj praktike primeneniya zakonodatel`stva, reglamen-tiruyushhego osobennosti ugolovnoj otvetstvennosti i nakazaniya nesovershennoletnix : postanovlenie Plenuma Verxovnogo Suda RF ot 01.02.2011 № 1 (red. ot 28.10.2021). — URL: <https://sudact.ru/law/postanovlenie-plenuma-verkhovnogo-suda-rf-ot-01022011/> (data obrashheniya : 16.03.2025).

СВЕДЕНИЯ ОБ АВТОРАХ

Новикова Елена Павловна. Доцент кафедры уголовного права и криминологии. Кандидат юридических наук, доцент.

Воронежский институт МВД России.

Е-mail: epasyaeva@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Чернышова Ксения Сергеевна. Слушатель.

Воронежский институт МВД России.

Е-mail: ksusha.chernyshova2002@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.

Chernyshova Ksenia Sergeevna. Listener.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: ksusha.chernyshova2002@yandex.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: деструктивное явление; преследование; террористическая деятельность; уголовно-правовой анализ.

Key words: destructive phenomenon; persecution; terrorist activity; criminal law analysis.

УДК 343.9

Е. А. Пидусов, кандидат юридических наук, доцент

К ВОПРОСУ О СУЩНОСТИ КРИПТОВАЛЮТЫ

ON THE ISSUE OF THE ESSENCE OF CRYPTOCURRENCY

В статье рассматриваются некоторые теоретические и правовые аспекты, раскрывающие содержание криптовалюты.

The article discusses some theoretical and legal aspects that reveal the content of cryptocurrencies.

В современном мире все активнее используются информационно-телекоммуникационные технологии, включая сеть Интернет, для расчетов применяются специфические формы, связанные с использованием электронных средств платежа, к которым относится и цифровая валюта. Понятие цифровой валюты является общим родовым при описании виртуальных валют и регулируемых электронных денег (электронных денежных средств, в соответствии Федеральным законом от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе») [1]. Цифровая валюта предполагает цифровое выражение цифровой (электронной) денежной стоимости.

Следует учитывать, что цифровая валюта и электронные денежные средства (ЭДС) — понятия не тождественные. Если первая — это цифровое выражение электронно-цифровой валюты, то вторая — фиатной валюты (выпущенных государством и регулируемых Центробанком страны законных платежных средств, включая рубли, евро, доллары, юани и т. д.). При этом целью применения ЭДС является осуществление электронного перевода стоимости, выраженной в фиатной валюте [2].

Цифровые валюты фиатными не являются в силу того, что их выпуск носит децентрализованный характер, то есть не зависит от государства.

Цифровая валюта без своего физического выражения именуется криптовалютой (кибервалютой). Понятие «криптовалюта» на сегодня законодательно не определено и в таком виде не употребляется в нормативных правовых актах. При этом важно учитывать положения Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [3], который в ч. 3 ст. 1 содержит определение цифровой валюты как «совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или)

могут быть приняты в качестве средства платежа, не являющегося денежной единицей...». Однако между цифровой валютой и криптовалютой имеются различия. Последняя есть разновидность первой (наряду с токенами, стейблкоинами, игровыми деньгами). При этом цифровая валюта может быть централизованной или децентрализованной.

Централизованными признаются цифровые валюты, у которых имеется единый эмитент. Они эмитируются администратором, контролирующим всю систему (например, WebMoney, QIWI, PayPal, Perfect Money и многие другие).

Под централизованной цифровой валютой понимаются деньги, которые эмитируются центральными банками современных государств. Такая валюта имеет вид кода на специализированных цифровых платформах, а ее стоимость полностью привязана к национальной наличной валюте государства и им гарантируется [4].

Спецификой децентрализованных цифровых валют является отсутствие у них единого администратора и, соответственно, централизованного контроля (надзора) (Bitcoin, Ethereum, Tether, USD Coin, Litecoin, Ripple, Solana и многие другие). Данная разновидность цифровых валют и есть криптовалюта.

Криптовалюта — это любая разновидность цифровой (виртуальной) валюты, для защиты транзакций которой используется шифрование (криптография) [5].

С технологической точки зрения криптовалютой является математический код, обращаемый в системе распределенного реестра — учетной записи, подтверждающей наличие криптовалюты [6].

Отдельные исследователи предлагают свои авторские дефиниции криптовалюты. В частности, Д. М. Фарахiev понимает под криптовалютой «разновидность платежного средства, учет которого обеспечивается посредством децентрализованной платежной системы» [7].

В варианте, предлагаемом М. М. Долгиевой, криптовалюта — это электронно-цифровое имущество, созданное с помощью криптографических методов, в основе функционирования которого лежат технологии распределенного реестра [8].

Криптовалюта также истолковывается как представленная в цифровом виде стоимость, функционирующая на базе технологии распределенного реестра [9].

По мнению А. В. Иванова и И. В. Кондратьева, понятие «криптовалюта» означает разновидность цифровой валюты, создаваемой и контролируемой посредством применения криптографических методов, в отношении которой отсутствует централизованный учет, и функционирующей на основе блокчейн и технологии распределенного реестра [10].

И. А. Ишин считает, что криптовалютой является цифровая валюта, создание и контроль за которой базируются на применении криптографических методов, и характеризуемая наличием децентрализованной формы эмиссии и учета [11].

В. А. Перов предлагает авторское определение криптовалюты с позиций уголовного права, как результат процесса информатизации и взаимодействия субъектов информационной инфраструктуры, основанной на использовании математического кода и криптографических элементов. При этом он рассматривает криптовалюту в качестве одной из разновидностей цифровой валюты в форме электронного платежного средства, оборот которой происходит в информационной системе [12].

В представлении Н. С. Зиновьева криптовалюта представляет собой зашифрованное по определенному математическому алгоритму средство платежа в киберсреде, не контролируемое государством [13].

На взгляд М. А. Егоровой, криптовалюта есть децентрализованная цифровая валюта, созданная и защищенная методами криптографии [14].

А. В. Токолов считает возможным рассматривать криптовалюту как вид цифровых финансовых активов, специфическую разновидность электронного платежного средства в виде математического кода, использующего криптографические элементы — электронную цифровую подпись, оборот которой происходит в информационно-коммуникативной сети [15].

На основе анализа рассмотренных в статье и других определений криптовалюты мы приходим к заключению о том, что определение данного понятия может быть сформулировано следующим образом: «криптовалюта — это созданная программным обеспечением разновидность цифровой валюты, функционирующая на основе алгоритмов шифрования (криптографии), создание и

контроль над которой реализуются с использованием криптографических методов и в отсутствие централизованного учета».

Криптовалюта представляет собой результат развития и совершенствования информационно-телекоммуникационных технологий и информационной инфраструктуры.

Сущность криптовалюты можно понять на основе выделения и анализа ее основных признаков:

- криптовалюта является разновидностью цифровой валюты;
- ее создание и контроль над ней основываются на применении криптографических методов;
- данная система не имеет единого администратора, который бы осуществлял выпуск криптовалюты и ее учитывал на счетах пользователей.

Представляется важным обозначить криминалистически значимые признаки криптовалюты. По данному вопросу высказываются различные точки зрения, которые все же имеют больше сходства, чем отличий.

Например, интересный подход демонстрирует Л. Л. Мельник. Данный автор выделяет главный признак — нематериальную природу криптовалюты, что означает отсутствие ее материального выражения в виде купюр (монет), абсолютно цифровой характер (биткойны существуют в виде записей в электронной базе блокчейн). При этом суть признака нематериальности криптовалюты проявляется в следующем: выражается в электронно-цифровой форме; отсутствует единый эмиссионный центр; служит универсальным финансовым инструментом; использование анонимно; необратимость операций с криптовалютой [16].

С позиций криминалистики, на наш взгляд, значимыми признаками криптовалюты являются ее свойства, носящие преимущественно технический характер, в числе которых:

- анонимность транзакций держателей криптовалют, что обеспечивается благодаря тому, что транзакции проводят между адресами криптокошельков пользователей, не привязанными к конкретным личностям [17]. Такие операции напрямую с личностью человека не связаны, они записываются в общедоступный реестр (блокчейн). Все это идентификацию лиц, вовлеченных в преступную деятельность, делает затруднительной;
- легкость доступа, что означает возможность доступа к криптовалюте через сеть Интернет из любой точки мира;
- отсутствие каких-либо ограничений по сумме переводов денежных средств;
- трансграничный характер (фактическое отсутствие государственных и таможенных границ для транзакций в криптовалютах);

- необратимость (безотзывность) проведенных транзакций как невозможность возврата отправленных адресату средств, даже в случаях ошибки;

- отсутствие единого центра (банковской системы), осуществляющего выпуск (эмиссию) и обращение криптовалют, на который возлагается обязанность информирования уполномоченных государственных органов о подозрительных транзакциях.

Анализ криминалистически значимых признаков криптовалют необходим для выяснения того, является ли тот или иной цифровой знак (токен) криптовалютой, а также для получения и фиксации информации, представляющей интерес для следствия по уголовным делам, совершаемым с ее использованием.

В настоящее время самыми распространенными и известными разновидностями криптовалюты являются: Bitcoin (BTC) — на начало 2025 года в обращении более 19 миллионов BTC; Ethereum (ETH) — более 120 миллионов ETH; Tether (USDT) — более 83 млрд USDT; USD Coin (USDC) — более 25,7 млрд USDC; Ripple (XRP) — более 53 млрд XRP; Toncoin (TON) — более 3,5 млрд TON; Solana (SOL) — более 412 млрд SOL и некоторые другие [18]. На 13 января 2025 года курс криптовалют составлял: Bitcoin — 91.429,2 \$, Ethereum — 3.110,70 \$, Ripple (XRP) — 2,4123 \$, Solana — 177,325 \$ [19].

Самый высокий курс у Bitcoin. Эта криптовалюта является самой популярной, в том числе среди преступников. Bitcoin (BTC) — это функционирующий в информационной сети цифровой актив, ничем не подкрепленный (в отличие от физических монет), его стоимость формируется только лишь спросом и предложением. При этом под биткоинами понимаются расчетные единицы, представленные уникальной цепочкой цифровых и буквенных знаков [20].

Таким образом, представляется возможным сделать ряд следующих выводов:

1. Криптовалюта — это созданная программным обеспечением разновидность цифровой валюты, функционирующая на основе алгоритмов шифрования (криптографии), создание и контроль над которой реализуются с использованием криптографических методов и в отсутствие централизованного учета.

2. Криптовалюта характеризуется такими криминалистически значимыми признаками, как: анонимность транзакций; легкий доступ через сеть Интернет из любой точки мира; неограниченность переводов по сумме; транснациональность; необратимость транзакций; отсутствие единого эмиссионного центра; универсальность как финансового инструмента. Знание основных признаков криптовалюты необходимо для разработки методик расследования преступлений, связанных с ее использованием.

ЛИТЕРАТУРА

1. О национальной платежной системе : Федеральный закон от 27 июня 2011 г. № 161-ФЗ (ред. от 28.12.2022) // Собрание законодательства РФ. — 2011. — № 27. — Ст. 3872.

2. Шурухнов Н. Г., Мерецкий Н. Е., Жердев П. А. Роль криминалистических данных о механизме функционирования криптовалюты в выявлении и раскрытии преступлений // Вестник Дальневосточного юридического института МВД России. — 2019. — № 1 (46). — С. 95.

3. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 31 июля 2020 г. № 259-ФЗ (ред. от 25.10.2024) // Собрание законодательства РФ. — 2020. — № 31. — Ч. I. — Ст. 5018.

4. Цифровые валюты центральных банков: особенности эмиссии и их роль в трансформации финансовой системы на современном этапе / Е. С. Матерова, Е. В. Евсеев, Б. Л. Сафиуллин, Э. Г. Захаров // Креативная экономика. — 2023. —

- Т. 17. — № 5. — С. 1926.

5. Что такое криптовалюта и как она применяется? — URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-cryptocurrency> (дата обращения: 20.02.2025).

6. Коржова И. В. Юридические основы обращения криптоактивов : учеб. пособие для студ. высш. учеб. заведений / под ред. В. А. Северина. — М. : Юр-БАК, 2020. — С. 11.

7. Фарахiev Д. М. Деятельность органов внутренних дел в процессе раскрытия и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий (на примере криптовалютных активов) // Юридический вестник Самарского университета. — 2023. — Т. 9. — № 3. — С. 83.

8. Долгиева М. М. Операции с криптовалютами : актуальные проблемы теории и практики применения уголовного законодательства // Актуальные проблемы российского права. — 2019. — № 4 (101). — С. 137.

9. Сафарли Азиз Хафис Оглы. Цифровые валюты в системе финансовых отношений Российской Федерации : дис. ... канд. экон. наук. — М., 2023. — С. 31.

10. Иванов А. В., Кондратьев И. В. Противодействие финансированию терроризма через криптовалюты // Использование криптовалют в противоправных целях и методика противодействия : материалы международного научно-практического «круглого стола» (Москва, 25 апреля 2019 года) / под общ. ред. А. М. Багмета. — М. : Московская академия Следственного комитета России, 2019. — С. 57.

11. Ишин И. А. Особенности производства отдельных следственных действий и роль начальника органа дознания при расследовании преступлений, совершенных с использованием криптовалюты // Академическая мысль. — 2020. — № 2 (11). — С. 83.

12. Перов В. А. Квалификация преступлений, совершаемых с использованием криптовалюты : дис. ... канд. юрид. наук. — М., 2023. — С. 11.

13. Зиновьева Н. С. Возможности блокчейн-технологии в раскрытии и расследовании преступлений в интернет-пространстве // Вестник Восточно-Сибирского института МВД России. — 2018. — №3 (86). — С. 185.

14. Егорова М. А. Проблемы соотношения и правового регулирования криптовалюты, битко-

ина, цифровой и виртуальной валюты : российский и зарубежный опыт // Вестник Университета имени О. Е. Кутафина. — 2020. — № 2. — С. 55.

15. Токолов А. В. Правовое регулирование информационных отношений в сфере оборота цифровых финансовых активов : дис. ... канд. юрид. наук. — М., 2022. — С. 28.

16. Мельник Л. Л. О криминалистической характеристике криптовалюты как предмета и платежного средства совершения преступлений // Теория и практика борьбы с компьютерной преступностью : материалы заоч. междунар. науч.-практ. конф. (Минск, октябрь 2019 г.). — Минск, 2020. — С. 64.

17. Что нужно знать про анонимные криптовалюты. — URL: https://www.maff.io/media/anonymous_kriptovaluty/ (дата обращения: 20.02.2025).

18. 10 самых популярных криптовалют в 2025 году в России и мире. — URL: <https://www.kp.ru/money/investitsii/samye-populyarnye-kriptovaluty/> (дата обращения: 15.03.2025).

19. Ведущие криптовалюты. — URL: <https://ru.investing.com/> (дата обращения: 15.03.2025).

20. Колчевский И. Б., Кузнецов А. Г. Криптовалюты на территории стран Содружества : оценка вероятных криминальных рисков и угроз. — М. : ФГКУ «ВНИИ МВД России», 2018. — С. 12.

REFERENCES

1. O nacional'noj platezhnoj sisteme : Federal'nyj zakon ot 27 iyunya 2011 g. № 161-FZ (red. ot 28.12.2022) // Sobranie zakonodatel'stva RF. — 2011. — № 27. — St. 3872.

2. Shuruxnov N. G., Mereczkij N. E., Zherdev P. A. Rol' kriminalisticheskix dannyx o mexanizme funkcionirovaniya kriptovalyuty v vy'yavlenii i raskry'tii prestuplenij // Vestnik Dal'nevostochnogo yuridicheskogo instituta MVD Rossii. — 2019. — № 1 (46). — S. 95.

3. O cifrovyyx finansovyx aktivax, cifrovoy valyute i o vnesenii izmenenij v otdel'ny'e zakonodatel'ny'e akty Rossijskoj Federacii : Federal'nyj zakon ot 31 iyulya 2020 g. № 259-FZ (red. ot 25.10.2024) // Sobranie zakonodatel'stva RF. — 2020. — № 31. — Ch. I. — St. 5018.

4. Cifrovye valyuty central'nyx bankov: osobennosti e'missii i ix rol' v transformacii finansovoj sistemy na sovremennom etape / E. S. Materova, E. V. Evseev, B. L. Safiullin, E. G. Zaxarov // Kreativnaya e'konomika. — 2023. — T. 17. — № 5. — S. 1926.

5. Chto takoe kriptovalyuta i kak ona primenyaetsya? — URL: <https://www.kaspersky.ru/>

resourcecenter/definitions/what-is-cryptocurrency (data obrashheniya: 20.02.2025).

6. Korzhova I. V. Yuridicheskie osnovy obrashheniya kriptoaktivov : ucheb. posobie dlya stud. vy'ssh. ucheb. zavedenij / pod red. V. A. Severina. — M. : Yur-VAK, 2020. — S. 11.

7. Faraxiev D. M. Deyatel'nost' organov vnutrennix del v processe raskry'tiya i rassledovaniya prestuplenij, sovershaemyx s ispol'zovaniem informacionno-kommunikacionnyx texnologij (na primere kriptovalyutnyx aktivov) // Yuridicheskij vestnik Samarskogo universiteta. — 2023. — T. 9. — № 3. — S. 83.

8. Dolgieva M. M. Operacii s kriptovalyutami : aktual'ny'e problemy teorii i praktiki primeneniya ugovnogo zakonodatel'stva // Aktual'ny'e problemy rossijskogo prava. — 2019. — № 4 (101). — S. 137.

9. Safarli Aziz Xafis Ogly. Cifrovye valyuty v sisteme finansovyx otnoshenij Rossijskoj Federacii : dis. ... kand. e'kon. nauk. — M., 2023. — S. 31.

10. Ivanov A. V., Kondrat'ev I. V. Protivodejstvie finansirovaniyu terrorizma cherez kriptovalyuty // Ispol'zovanie kriptovalyut v protivopravnyx

celyax i metodika protivodejstviya : materialy` mezhdunarodnogo nauchno-prakticheskogo «kruglogo stola» (Moskva, 25 aprelya 2019 goda) / pod obshh. red. A. M. Bagmeta. — M. : Moskovskaya akademiya Sledstvennogo komiteta Rossii, 2019. — S. 57.

11. Ishin I. A. Osobennosti proizvodstva otel'ny`x sledstvenny`x dejstvij i rol' nachal'nika organa doznaniya pri rassledovanii prestuplenij, sovershenny`x s ispol'zovaniem kriptovalyuty` // Akademicheskaya my'sl'. — 2020. — № 2 (11). — S. 83.

12. Perov V. A. Kvalifikaciya prestuplenij, sovershaemy`x s ispol'zovaniem kriptovalyuty` : dis. ... kand. jurid. nauk. — M., 2023. — S. 11.

13. Zinov`eva N. S. Vozmozhnosti blokchejn-tehnologii v raskry'tii i rassledovanii prestuplenij v internet-prostranstve // Vestnik Vostochno-Sibirskogo instituta MVD Rossii. — 2018. — № 3 (86). — S. 185.

14. Egorova M. A. Problemy` sootnosheniya i pravovogo regulirovaniya kriptovalyuty`, bitkoina, cifrovoj i virtual'noj valyuty` : rossijskij i zarubezhny`j opyt // Vestnik Universiteta imeni O. E. Kutafina. — 2020. — № 2. — S. 55.

15. Tokolov A. V. Pravovoe regulirovanie informacionny`x otnoshenij v sfere oborota cifrovy`x finansovy`x aktivov : dis. ... kand. jurid. nauk. — M., 2022. — S. 28.

16. Mel'nik L. L. O kriminalisticheskoy xarakteristike kriptovalyuty` kak predmeta i platezhnogo sredstva soversheniya prestuplenij // Teoriya i praktika bor'by` s komp'yuternoj prestupnost'yu : materialy` zaoch. mezhdunar. nauch.-prakt. konf. (Minsk, oktyabr' 2019 g.). — Minsk, 2020. — S. 64.

17. Chto nuzhno znat' pro anonimny`e kriptovalyuty`. — URL: https://www.maff.io/media/anonymnye_kriptovaluty/ (data obrashheniya: 20.02.2025).

18. 10 samy`x populyarny`x kriptovalyut v 2025 godu v Rossii i mire. — URL: <https://www.kp.ru/money/investitsii/samye-populyarnye-kriptovalyuty> (data obrashheniya: 15.03.2025).

19. Vedushhie kriptovalyuty`. — URL: <https://ru.investing.com/> (data obrashheniya: 15.03.2025).

20. Kolchevskij I. B., Kuznecov A. G. Kriptovalyuty` na territorii stran Sodruzhestva : ocenka veroyatny`x kriminal'ny`x riskov i ugroz. — M. : FGKU «VNII MVD Rossii», 2018. — S. 12.

СВЕДЕНИЯ ОБ АВТОРЕ

Пидусов Евгений Александрович. Начальник кафедры криминалистики.
Кандидат юридических наук, доцент.
Воронежский институт МВД России.
E-mail: epidusov@mvd.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: epidusov@mvd.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: электронные денежные средства; цифровая валюта; криптовалюта; расследование преступлений; информационные технологии.

Key words: electronic money; digital currency; cryptocurrency; crime investigation; information technology.

УДК 343.1

М. Ю. Пучнина, кандидат юридических наук

КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ НЕСОВЕРШЕННОЛЕТНИХ В СЕТИ ИНТЕРНЕТ: ПСИХОЛОГИЧЕСКИЕ И КРИМИНОЛОГИЧЕСКИЕ АСПЕКТЫ

AN INTEGRATED APPROACH TO ENSURING THE SAFETY OF MINORS ON THE INTERNET: PSYCHOLOGICAL AND CRIMINOLOGICAL ASPECTS

В статье рассматриваются актуальные проблемы обеспечения безопасности несовершеннолетних в сети Интернет, где широко распространяются материалы, способствующие развитию деструктивного поведения. Анализируются психологические и криминологические аспекты данной проблемы, что позволяет определить основные пути профилактики и контроля негативного воздействия виртуальной среды. Обосновывается необходимость постоянного мониторинга реальной ситуации с применением современных технологий, а также совершенствования законодательства и правоприменительной практики.

The article examines current issues of ensuring the safety of minors on the Internet, where materials that promote destructive behavior are widely distributed. Psychological and criminological aspects of this problem are analyzed, which allows us to determine the main ways of preventing and controlling the negative impact of the virtual environment. The need for constant monitoring of the real situation using modern technologies, as well as improving legislation and law enforcement practice is substantiated.

Современная цифровая эпоха формирует новые формы социальной коммуникации среди подростков. Интернет предоставляет неограниченные возможности для обучения и саморазвития, однако именно в виртуальной среде нередко распространяется контент, провоцирующий агрессию, склоняющий к суицидальному поведению или способствующий иным деструктивным формам общения. Актуальность проблемы обусловлена и тем, что несовершеннолетние отличаются повышенной внушаемостью, недостатком жизненного опыта и интересом к экспериментам, что делает их особо уязвимыми перед манипулятивными методами, используемыми кураторами деструктивных групп. Недооценка угрозы родителями и педагогами во многом связана с быстрым технологическим развитием и тем, что взрослым зачастую не хватает опыта общения в цифровой среде. В результате многие негативные процессы могут проходить незамеченными до тех пор, пока ситуация не примет опасный оборот. В этих условиях вопросы профилактики, законодательного регулирования и межведомственного взаимодействия в сфере обеспечения безопасности несовершеннолетних в сети Интернет приобретают особую значимость.

Основной проблемой является отсутствие достаточных механизмов, позволяющих своевременно выявлять и блокировать деструктивные онлайн-сообщества, а также недостаточная информированность родителей и педагогов о рисках, с которыми сталкиваются подростки в виртуальной среде. Несмотря на введение Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», на достаточно большое количество вносимых в него изменений (22 раза с момента введения, 4 раза за 2024 год!), в практике остаются пробелы, связанные с недостаточной эффективностью правоприменения и отсутствием четких алгоритмов взаимодействия между правоохранительными органами, образовательными учреждениями, социальными службами и интернет-провайдерами. Кроме того, динамическое развитие сетевых технологий порождает новые формы негативного контента, что требует постоянного мониторинга и внесения соответствующих корректив в нормативно-правовую базу. Несмотря на существующие в России нормативные правовые акты, призванные ограничивать доступ к деструктивным материалам, и деятельность, осуществляемую Роскомнадзором, многие опас-

ные интернет-ресурсы продолжают функционировать, перетекая в закрытые пространства, куда доступ имеет только ограниченный круг лиц, или мигрируя между платформами, где нет должного контроля.

Правоприменительная практика также сталкивается с рядом трудностей:

- анонимность, позволяющая кураторам и создателям подобных деструктивных интернет-сообществ скрывать свою личность;

- отсутствие достаточных инструментов для межгосударственного взаимодействия при выявлении и пресечении противоправной деятельности в сети Интернет;

- низкий уровень цифровой грамотности и информационно-гигиены широких слоев населения, особенно старшего поколения (родителей, педагогов, социальных работников).

Правоохранительные органы нередко оказываются в ситуации, когда процедура блокировки, экспертизы контента или розыска анонимных администраторов групп затягивается, теряя при этом эффективность. Кроме того, сложность доказательной базы по делу о вовлечении подростков в деструктивные действия требует глубоких криминологических знаний и межведомственной координации.

Анализ научной литературы позволяет выделить несколько ключевых направлений исследования данной проблемы. В работах ряда авторов подробно рассматривается феномен интернет-зависимости у подростков, приводящий к повышенной подверженности онлайн-манипуляциям [1]. Отмечается, что важными компонентами профилактики являются информационные кампании и вовлечение самих подростков в социальные проекты, направленные на позитивное использование цифровых технологий [2]. Другие авторы анализируют кибербуллинг как еще одно проявление деструктивного взаимодействия в сети и подчеркивают, что без поддержки родителей и педагогов многие дети скрывают от взрослых факты травли, что может привести к тяжелым психологическим последствиям [3]. Ряд исследователей описывает криминологические особенности противоправных сообществ, действующих в сети Интернет, в том числе экстремистских [4] и суицидальных групп [5]. В работах подчеркивается транснациональный характер проблемы, затрудняющий поиск и наказание организаторов.

Международные организации, в частности ЮНЕСКО, указывают на необходимость системной профилактики, объединяющей технические, правовые и просветительские механизмы. Это согласуется с общемировой тенденцией к развитию «цифровой безопасности» (Digital Safety), ориентированной не только на защиту технических

устройств, но и на сохранение психологического здоровья пользователей [6].

Важно понимать, что деструктивные сообщества в сети Интернет в основном ориентированы на подростковую целевую аудиторию и используют широкий спектр методов вербовки: от публикации провокационных постов, мемов до прямых личных сообщений, содержащих призывы к самоповреждению, агрессии, осуществлению антиобщественной, экстремистской, террористической и иной преступной деятельности [7]. Сами кураторы подобных интернет-сообществ могут маскировать свою деятельность под «игры» или «квесты», формируя у подростков ложное ощущение принадлежности к «элите» и поощряя развитие психологической зависимости [8].

Деятельность деструктивных сообществ в сети Интернет основывается на уязвимости подростковой психики. Подростковый возраст характеризуется повышенной эмоциональной неустойчивостью, поиском новой идентичности, желанием самоутвердиться. Кураторам деструктивных групп легче воздействовать на тех, кто испытывает дефицит общения в семье или школе, переживает личные кризисы или страдает от депрессивных состояний. С точки зрения психологии, подростки, имеющие низкую самооценку, нередко ищут подтверждения своей значимости в любых доступных «сообществах», даже носящих деструктивный характер. Дополнительным фактором риска служит недостаток родительского контроля и внимания: родители не знают, как, с кем и в каких группах происходит общение ребенка в сети Интернет. В таких условиях подросток остается один на один с манипуляторами, искажающими его представления о реальности.

С криминологической точки зрения деструктивные сообщества в сети Интернет могут рассматриваться как сложные, многосубъектные структуры, имеющие преступный характер. Зачастую их деяния уголовно наказуемы и связаны с доведением до самоубийства, побуждением к совершению опасных действий, осуществлению экстремистской и террористической деятельности. Однако в условиях анонимности и транстерриториальности интернета привлечение участников подобных групп к ответственности сталкивается с рядом препятствий:

- деятельность кураторов таких групп находится за пределами национальных юрисдикций. Это усложняет их поиск и наказание, а также выявление истинного масштаба проблемы. Законодательство в части регулирования информационного пространства должно учитывать международную природу сети и предусматривать расши-

рение правомочий органов правопорядка при взаимодействии с иностранными государствами и глобальными цифровыми платформами [9];

- доказательство вины требует сбора цифровых следов, что доступно лишь при активном и достаточно ускоренном международном сотрудничестве;

- существуют трудности в идентификации участников и разграничении «создателей» и «приверженцев» деструктивной идеологии;

- информация с деструктивных интернет-ресурсов быстро размножается и перемещается на другие платформы или в мессенджеры с шифрованием, что создает ряд сложностей для сотрудников правоохранительных органов.

В настоящее время в России в качестве борьбы с деятельностью деструктивных групп в интернет-пространстве выбран метод блокировки противоправных ресурсов и удаления информации, причиняющей вред здоровью и (или) развитию детей. Однако быстрая смена доменных имен, использование анонимайзеров и иных технологий обхода блокировок существенно снижают эффективность таких мер. В связи с этим возникает потребность в развитии комплексных программ профилактики и в постоянном мониторинге контента, особенно на популярных среди подростков платформах.

Одним из наиболее перспективных подходов является внедрение автоматизированных систем фильтрации и анализа текстового и визуального контента. Современные алгоритмы машинного обучения позволяют обнаруживать в социальных сетях ключевые слова, образы, фразы, связанные с пропагандой насилия или суицида. Однако реализация таких систем требует значительных финансовых ресурсов и высококвалифицированных специалистов. Тем не менее попытки автоматизировать деятельность по выявлению противоправных интернет-ресурсов предпринимаются. Так, в 2022 году была создана информационная система «Антифишинг», которая предназначена для автоматического выявления фишинговых сайтов, что становится особенно актуально в условиях растущих киберугроз [10]; в 2023 году Роскомнадзор запустил систему автоматического поиска запрещенного контента «Окулус». Отмечается ее постоянное совершенствование и обучение более детальному анализу действий людей в интернет-пространстве [11].

Важно сочетать технологические инструменты с повышением информированности всех участников образовательного процесса. Не менее важен психологический аспект, включающий воспитание критического мышления и эмоциональной устойчивости у подростков [12]. Школьные

программы и родительские собрания должны содержать информационные блоки о возможных сетевых рисках, а в образовательных учреждениях необходимо регулярно проводить тренинги и семинары по цифровой безопасности. Педагогам рекомендуется проходить курсы повышения квалификации в области цифровой безопасности, чтобы распознавать симптомы вовлечения ребенка в деструктивную группу и вовремя принять меры. Родителям самостоятельно также следует уделять внимание цифровой грамотности: обсуждать с подростком его онлайн-опыт, объяснять риски и предлагать безопасные альтернативы для самоутверждения и общения [13].

Как показывает практика, максимальную эффективность обеспечивает согласованная деятельность различных ведомств и институтов: правоохранительных органов, образовательных учреждений, медицинских и социальных служб, а также самих интернет-провайдеров и общественных организаций.

При слаженном взаимодействии:

- правоохранительные структуры оперативно обмениваются информацией, выявляют и блокируют деструктивные интернет-сообщества;

- социальные службы и психологи предоставляют экстренную помощь подросткам, которые уже оказались под негативным влиянием;

- родители и педагоги получают инструменты для раннего выявления и предотвращения потенциальной угрозы.

Подводя итоги, следует отметить, что проблема деструктивных интернет-сообществ, ориентированных на несовершеннолетних, носит комплексный характер и требует масштабной работы на всех уровнях. Интернет, с одной стороны, становится площадкой для получения образования и развития, с другой — открывает перед злоумышленниками практически неограниченные возможности по установлению контактов с психологически уязвимыми подростками.

Несомненно, предпринятые в России законодательные и иные меры являются важным шагом на пути к защите детей от вредной информации, однако их реализация осложнена анонимностью сети и скоростью, с которой контент перемещается между платформами.

Только скоординированное взаимодействие всех заинтересованных субъектов способно обеспечить надежный отпор оказываемому деструктивному воздействию в виртуальной среде. Поддержка семьи, школы, государственных структур и гражданского общества даст возможность создать благоприятные условия, при которых подростки смогут в полной мере пользоваться преимуществами интернета без риска столкнуться с угрозами для своего физического

и психического здоровья. В конечном счете, комплексный подход к обеспечению безопасности несовершеннолетних в сети Интернет позволит

защитить подрастающее поколение, обеспечив им надежную поддержку в важнейший период их развития.

ЛИТЕРАТУРА

1. Смоленцева Ю. Н. Интернет-зависимость молодежи: постановка проблемы // Социальные и гуманитарные науки: теория и практика. — 2021. — № 1 (5). — С. 192—203.

2. Ильницкий А. С. Противодействие криминальной идеологии в сети Интернет : дис. ... канд. юрид. наук. — Краснодар, 2022. — 213 с.

3. Алешина А. В. Кибербуллинг среди несовершеннолетних: понятие, виды, профилактика // Уголовно-процессуальная охрана прав и законных интересов несовершеннолетних. — 2023. — № 1 (10). — С. 5—10.

4. Штефан А. В. Сущность экстремизма: социальный и криминологический аспекты // Историческая и социально-образовательная мысль. — 2021. — Т. 13, № 5. — С. 88—106.

5. Шалагин А. Е., Идиятулов А. Д. Криминологическая характеристика и предупреждение преступлений, связанных с побуждением к суициду, совершаемых с использованием информационно-телекоммуникационной сети «Интернет» // Ученые записки Казанского юридического института МВД России. — 2018. — №. 3 (6). — С. 82—87.

6. Цифровая политика: потенциал и инклюзия. — URL: <https://www.unesco.org/ru/digital-policy-capacities-inclusion> (дата обращения: 15.03.2025).

7. Орлов И. А. Язык деструктивных интернет-сообществ в юрислингвистическом аспекте // Наука XXI века: проблемы, поиски, решения : материалы XLV научно-практической конференции, посвящённой 25-летию Миасского филиала Челябинского государственного университета,

Миасс, 30 апреля 2021 года / под ред. И. И. Валола. — Челябинск : Челябинский государственный университет, 2021. — С. 292—296.

8. Пучнин А. В., Пучнина М. Ю. Механизм деятельности сторонников деструктивных интернет-сообществ и портрет их типичного участника (на примере «групп смерти» и движения «Колумбайн») // Вестник Воронежского института МВД России. — 2021. — № 3. — С. 229—234.

9. 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.

10. Минцифры: «Антифишинг» выявил 765 тыс. противоправных ресурсов. — URL: <https://senatinform.ru/news/> (дата обращения: 15.03.2025).

11. Роскомнадзор запустил систему автоматического поиска запрещенного контента «Окулус». — URL: <https://www.vedomosti.ru/technology/> (дата обращения: 15.03.2025).

12. Игнатов А. Н. Криминогенный потенциал современной информационной среды // Наука. Образование. Современность. — 2021. — № 1. — С. 61—65.

13. Голубых Н. В., Потанин К. В. Предупреждение вовлечения несовершеннолетних в деятельность деструктивных интернет-сообществ экстремистской направленности // Вестник Уральского юридического института МВД России. — 2020. — № 4. — С. 121—124.

REFERENCES

1. Smolenceva Yu. N. Internet-zavisimost` molodezhi: postanovka problemy` // Social`ny`e i gumanitarny`e nauki: teoriya i praktika. — 2021. — № 1 (5). — S. 192—203.

2. Il`niczkij A. S. Protivodejstvie kriminal`noj ideologii v seti Internet : dis. ... kand. yurid. nauk. — Krasnodar, 2022. — 213 s.

3. Aleshina A. V. Kiberbulling sredi nesovershennoletnix: ponyatie, vidy`, profilaktika // Uголовно-processual`naya oxrana prav i zakonny`x interesov nesovershennoletnix. — 2023. — № 1 (10). — S. 5—10.

4. Shtefan A. V. Sushhnost` e`kstremizma: social`ny`j i kriminologicheskij aspekty` // Istoriicheskaya i social`noobrazovatel`naya my`sl`. — 2021. — T. 13, № 5. — S. 88—106.

5. Shalagin A. E., Idiyatulov A. D. Kriminologicheskaya xarakteristika i preduprezhdenie prestuplenij, svyazanny`x s pobuzhdeniem k suicidu, sovershaemy`x s ispol`zovaniem informacionno-telekommunikacionnoj seti «Internet» // Ucheny`e zapiski Kazanskogo yuridicheskogo instituta MVD Rossii. — 2018. — №. 3 (6). — S. 82—87.

6. Cifrovaya politika: potencial i inklyuziya. — URL: <https://www.unesco.org/ru/digital-policy-capacities-inclusion> (data obrashheniya: 15.03.2025).

7. Orlov I. A. Yazyk destruktivnykh internet-soobshhestv v yurislingvisticheskom aspekte // Nauka XXI veka: problemy, poiski, resheniya : materialy XLV nauchno-prakticheskoy konferencii, posvyashhyonnoy 25-letiyu Miasskogo filiala Chelyabinskogo gosudarstvennogo universiteta, Miass, 30 aprelya 2021 goda / pod red. I. I. Valova. — Chelyabinsk : Chelyabinskij gosudarstvennyj universitet, 2021. — S. 292—296.

8. Puchnin A. V., Puchnina M. Yu. Mexanizm deyatel'nosti storonnikov destruktivnykh internet-soobshhestv i portret ix tipichnogo uchastnika (na primere "grupp smerti" i dvizheniya «Kolumbajn») // Vestnik Voronezhskogo instituta MVD Rossii. — 2021. — № 3. — S. 229—234.

9. Kolesnikov R. V. Protivodejstvie verbovochnoj deyatel'nosti e'kstremistskix i terroristich-

eskix organizacij v seti Internet v kontekste obespecheniya informacionno-psixologicheskoy bezopasnosti nesovershennoletnix // Uchenye zapiski Kazanskogo yuridicheskogo instituta MVD Rossii. — 2023. — T. 8, № 1 (15). — S. 36—41.

10. Mincifry: «Antifishing» vy'yavil 765 ty's. protivopравny'x resursov. — URL: <https://senatinform.ru/news/> (data obrashheniya: 15.03.2025).

11. Roskomnadzor zapustil sistemu avtomaticheskogo poiska zapreshhennogo kontenta «Okulus». — URL: <https://www.vedomosti.ru/technology/> (data obrashheniya: 15.03.2025).

12. Ignatov A. N. Kriminogennyj potencial sovremennoj informacionnoj sredy // Nauka. Obrazovanie. Sovremennost'. — 2021. — № 1. — S. 61—65.

13. Golubyx N. V., Potanin K. V. Preduprezhdenie вовлечения nesovershennoletnix v deyatel'nost' destruktivnykh internet-soobshhestv e'kstremistskoj napravlenosti // Vestnik Ural'skogo yuridicheskogo instituta MVD Rossii. — 2020. — № 4. — S. 121—124.

СВЕДЕНИЯ ОБ АВТОРЕ

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.

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.

Ключевые слова: безопасность несовершеннолетних; Интернет; агрессивное поведение; суицид; экстремизм; терроризм; деструктивные группы; психологические аспекты; криминологические аспекты; международное сотрудничество; педагоги; родители.

Key words: safety of minors; Internet; aggressive behavior; suicide; extremism; terrorism; destructive groups; psychological aspects; criminological aspects; international cooperation; teachers; parents.

УДК 343.85

И. Г. Савицкая, кандидат юридических наук, доцент

СИСТЕМА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ И РЕСПУБЛИКИ КАМЕРУН: СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ

THE SYSTEM OF INVESTIGATIVE ACTIONS OF THE RUSSIAN FEDERATION AND THE REPUBLIC OF CAMEROON: COMPARATIVE LEGAL ANALYSIS

Статья посвящена сравнительно-правовому анализу системы следственных действий в Российской Федерации и Республике Камерун. Автор обращает внимание на то, что ряд процессуальных действий, согласно УПК РФ, УПК Камеруна относит к следственным, а следственные действия рассматривает как процессуальные, поскольку многие из них не регламентированы законом. В конце статьи автор формулирует предложения, направленные на совершенствование системы следственных действий в уголовном процессе Республики Камерун.

The article is devoted to the comparative legal analysis of the system of investigative actions in the Russian Federation and the Republic of Cameroon. The author draws attention to the fact that according to the CPC of the Russian Federation, the CPC of Cameroon classifies a number of procedural actions as investigative, and considers investigative actions as procedural, since many of them are not regulated by law. At the end of the article, the author formulates proposals aimed at improving the system of investigative actions in the criminal process of the Republic of Cameroon.

27 июля 2005 года в Камеруне был принят Уголовно-процессуальный кодекс (далее — УПК РК) [6], который был назван африканскими правоведами во многом новаторским и революционным [1, 4], так как стал результатом сочетания норм романо-германского и англосаксонского уголовного судопроизводства.

Это связано с тем, что правовая система Камеруна, в том числе и уголовное судопроизводство, стала результатом колонизации этой страны британцами и французами, вследствие чего на протяжении длительного времени в ней сосуществовали две отдельные правовые системы: британское общее право и французское право, которые влияли и продолжают влиять в Камеруне на развитие уголовно-процессуального законодательства.

Иллюстрацией такого влияния является то, что уголовный процесс Камеруна до 2006 года регулировался во франкоязычной зоне (восемь регионов страны) Кодексом уголовного расследования 1938 года, а в англоязычной части (два региона страны) — Постановлением об уголовном судопроизводстве и рядом других документов [3. — С. 9].

Сосуществование двух уголовно-процессуальных законов порождало неравенство в правах

преследуемого лица в зависимости от части территории Камеруна (бывший Восточный Камерун, бывший Западный Камерун).

В связи с этим законодательный орган Камеруна пришел к выводу о том, что необходимо привести уголовно-процессуальное законодательство к единообразию, чтобы все камерунцы пользовались одинаковым режимом в вопросах уголовного процесса. Результатом этой деятельности стало принятие закона № 2005/007 от 27 июля 2005 г. об Уголовно-процессуальном кодексе, который остается в истории камерунского права новаторским инструментом, призванным удовлетворить определенные потребности, совместимые «с преследуемыми общественными целями». Он основан на сосуществовании двух процедур и на единственности двух процедур.

Законодательное единство в области уголовного судопроизводства было достигнуто в Камеруне путем замены Кодекса уголовного расследования и Постановления об уголовном судопроизводстве Уголовно-процессуальным кодексом Камеруна и отмены всех предыдущих положений, противоречащих ему.

Новый УПК Камеруна существенно изменил и систему следственных действий.

Следует отметить, что в Российской Федерации производство следственных действий, наряду с процессуальными действиями, согласно ч. 1 ст. 86 Уголовно-процессуального кодекса РФ (далее — УПК РФ) [7], является одним из основных способов собирания доказательств, осуществляемых в ходе уголовного судопроизводства субъектами доказывания. Согласно п. 32 ст. 5 к процессуальным действиям относятся следственные, судебные и иные действия. При этом, к следственным действиям относятся только те, которые непосредственно направлены на собирание доказательств, сопряжены с принуждением и облечены в строгую процессуальную форму [5. — С. 274].

Перечень следственных действий, проводимых в рамках уголовного судопроизводства, предусмотрен главами 24—27 УПК РФ, является исчерпывающим и не подлежит расширительному толкованию. К ним относятся: следственный осмотр (ст. ст. 176—178); освидетельствование (ст. 179); следственный эксперимент (ст. 181); обыск (ст. 182); выемка (ст. 183); личный обыск (ст. 184); наложение ареста на почтово-телеграфной отравления, их осмотр и выемка (ст. 185); контроль и запись переговоров (ст. 186); получение информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186¹); допрос (ст. 187—191); очная ставка (ст. 192); предъявление для опознания (ст. 193); проверка показаний на месте (ст. 194); производство судебной экспертизы (гл. 27).

Таким образом, можно сказать, что система следственных действий, регламентированная УПК РФ, является достаточно разнообразной, чего нельзя сказать о системе следственных действий в Республике Камерун, которая представлена гораздо скромнее.

Так, Уголовно-процессуальный кодекс Камеруна формально выделяет следующие следственные действия: следственный осмотр, допрос и очную ставку (ст. 92, ч. 1, п. «а»), обыск (ст. 93), выемку (ст. 96), содержание под стражей (ст. 118); перехват, запись или расшифровку всей корреспонденции, отправленной по телекоммуникациям, и съемку в частных местах (ст. 92.3), реквизиции (ст. 92.2).

Очевидно, что по сравнению с российской системой, состоящей из четырнадцати следственных действий, регламентированных УПК РФ, система следственных действий Камеруна наполовину меньше и насчитывает только семь. И если российский следователь может осуществлять собирание доказательств только исключительно посредством закрепленных в УПК РФ следственных действий, то камерунский следователь таким запретом не ограничен. Некоторые известные нам следственные действия широко применяются на практике камерунскими следователями и при

этом не закреплены в Уголовно-процессуальном кодексе Камеруна.

Например, такие следственные действия, как освидетельствование (ст. 179 УПК РФ) и личный обыск (ст. 184 УПК РФ) в УПК Камеруна никак не регламентируются, хотя обычно практикуются камерунскими следователями примерно на тех же основаниях и в порядке, который регламентирован УПК РФ.

Предъявление для опознания (ст. 193 УПК РФ) не регламентировано УПК Камеруна как следственное действие, однако применяется на практике с указанием результата этого процессуального действия в протоколе допроса.

Проверка показаний на месте (ст. 194 УПК РФ) согласно УПК Камеруна не является отдельным следственным действием и проводится в форме осмотра места происшествия, а его результаты отражаются в протоколе следственного осмотра.

Наложение ареста на почтово-телеграфные отправления, их осмотр и выемка (ст. 185 УПК РФ) осуществляется в качестве обычной выемки, не являясь отдельным следственным действием.

Контроль и запись переговоров (ст. 186 УПК РФ), на наш взгляд, можно сравнить с камерунским «аналогом» этого следственного действия под названием «перехват, запись или расшифровка всей корреспонденции, отправленной по телекоммуникациям, и съемка в частных местах» (ст. 92.3 УПК РК), однако камерунский вариант несколько шире — включает в себя возможность следователя в рамках уголовного дела, с санкции прокурора или следственного судьи, фотографировать интересующих лиц в частных местах без их разрешения, когда совершенное преступление или проступок наказывается лишением свободы на срок более 2 лет. Следует отметить, что контроль и запись переговоров санкционируется либо прокурором на все время следствия, либо следственным судьей, однако не предусматривает возможности производить данное следственное действие при наличии угрозы совершения насилия, вымогательства и других преступных действий в отношении потерпевшего, свидетеля или их близких родственников, родственников, близких лиц по их письменному заявлению. В отличие от названных выше, это следственное действие регламентировано УПК РК.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186¹ УПК РФ) согласно УПК Камеруна не является самостоятельным следственным действием и подпадает под так называемые «реквизиции» — то есть запросы следователя, направляемые им любому лицу (частному лицу,

учреждению, государственному органу, организации) в целях получения информации, представляющей интерес для расследования. Таким образом, без судебного решения следователь может запрашивать, истребовать и получать информацию о соединениях между абонентами и (или) абонентскими устройствами.

Такое распространенное у нас следственное действие, как следственный эксперимент (ст. 181 УПК РФ), в УПК Камеруна вовсе не упоминается.

Таким образом, многие из регламентированных УПК РФ следственных действий фактически производятся и ходе расследования уголовных дел в Республике Камерун, при этом законом не регламентированы, не относятся к следственным, процессуально никак не оформляются, их результаты лишь отражаются в общем отчете о расследовании, который следователь направляет прокурору.

Как уже говорилось выше, УПК Камеруна не регламентирует многие привычные нам следственные действия, при этом предусматривает производство следственных действий, которые УПК РФ традиционно относит к процессуальным. К ним относятся содержание под стражей (ст. 118 УПК РК) и реквизиции (ст. 92.2 УПК РК).

Содержание под стражей в полиции согласно ст. 118 УПК Камеруна является следственным действием и представляет собой аналог российской меры пресечения в виде заключения под стражу (ст. 108 УПК РФ).

Содержание данного следственного действия состоит в том, что лицо в случае производства предварительного следствия в целях установления истины содержится под стражей в отделении судебной полиции ограниченный срок под ответственность следователя, в распоряжении которого оно находится. Решение о содержании подозреваемого под стражей принимается следователем под контролем органа юстиции (прокурора или следственного судьи).

Что касается реквизиций (от лат. *requisitio* — требование, исследование) [2], то, согласно ч. 2 ст. 92 УПК РК, это следственное действие, которое, как уже уточнялось выше, состоит в направлении следователем любому лицу (частному лицу, учреждению, государственному органу, организации) запросов в целях получения информации, представляющей интерес для расследования.

Представляется, что реквизиции представляют собой аналог норм УПК РФ в части направления следователем поручений и запросов, предъявленных им в пределах его полномочий учреждениям, предприятиям, организациям, должностным лицам и гражданам и обязательных для исполнения (ч. 4 ст. 21 УПК РФ).

Посредством направления реквизиции камерунский следователь вправе:

- запросить информацию у эксперта или любого лица, которое может оказать ему помощь при производстве определенного следственного или процессуального действия;

- запросить любой необходимый ему предмет или документ;

- направить в письменной форме с немедленным вступлением в силу требование о проезде в любом транспортном средстве (общественном или частном), в том числе о проезде морским, железнодорожным, наземным или воздушным транспортом. Оригинал реквизиции должен быть направлен перевозчику.

Посредством реквизиций следователь может обратиться с запросом к любому лицу, учреждению или государственному органу, любой государственной организации для получения документов или предметов, представляющих интерес для расследования.

Однако, когда такие требования направляются адвокату, врачу, нотариусу, судебному приставу, в орган печати или аудиовизуальной связи, документы следователю могут быть переданы только с их согласия.

Подытоживая вышеизложенное, можно прийти к выводу, что российский следователь имеет больше законных средств и возможностей для собирания доказательств посредством производства регламентированных законом следственных действий, чем его камерунский коллега. Действительно, в УПК РФ насчитывается четырнадцать следственных действий, в то время как УПК РК предусматривает только семь.

При этом некоторые процессуальные действия, предусмотренные УПК РФ (например, заключение под стражу или направление следователем различных требований и запросов учреждениям, предприятиям, организациям, должностным лицам и гражданам), УПК Камеруна, на наш взгляд, ошибочно относит к следственным, а фактически выполняемые следственные действия рассматривает как процессуальные, поскольку многие из них не регламентированы законом.

Такие законодательные пробелы приводят к тому, что на практике камерунский следователь производит не закрепленные УПК РК следственные действия, фиксирует их результаты в различных документах, но не может их использовать в качестве самостоятельных доказательств по уголовному делу, поэтому выходит из законодательного тупика путем переноса результатов проведенных им «нерегламентированных» действий в протоколы «регламентированных» УПК Камеруна следственных действий.

В связи с этим представляется, что такой явный законодательный пробел в УПК Камеруна, касающийся производства следственных действий, требует устранения за счет расширения перечня следственных действий, фактически проводимых следователями Камеруна на практике, и законодательного закрепления их

в уголовно-процессуальном законе. Внесение указанных поправок способствовало бы не только более легитимному производству следственных действий в уголовном процессе Республики Камерун, но и развитию уголовно-процессуального законодательства республики в целом.

ЛИТЕРАТУРА

1. Мбумень Дзессеу Серж Фредерик. Темы африканского уголовного судопроизводства: дело Камеруна. — Saarbrücken: EUE; 2011. — 316 с.

2. Научно-образовательный портал «Большая российская энциклопедия» // URL: <https://bigenc.ru/c/rekvizitsia5c36f4?ysclid=m3n2y9jnna390545169> (дата обращения: 02.04.2025).

3. Онана Этунди Феликс. Опыт гармонизации законов в Африке. Обзор ERSUMA // Бизнес — право — Профессиональная практика. — 2012. — URL: <http://revue.ersuma.org/no-1-juin-2012/doctrine-12/LES-EXPERIENCES-D-HARMONISATION> (дата обращения 02.04.2025).

4. Тамну Джипеу Жан-Мари. Дача показаний в уголовном процессе в Камеруне : дис. DEA факультета юридических и политических наук Университета Дуалы, 2006. — URL: https://www.memoireonline.com/08/09/2453/m_Let

emoignage-dans-la-procedure-penale-au-Cameroun15.html. (дата обращения 02.04.2025).

5. Уголовно-процессуальное право (Уголовный процесс) : учебник для вузов / под ред. проф. Э. К. Кутуева ; науч. ред. и вступ. слово проф. В. П. Сальникова. — 2-е изд., перераб. и доп. — СПб. : Санкт-Петербургский ун-т МВД России ; Фонд «Университет», 2019. — 583 с.

6. Уголовно-процессуальный кодекс Республики Камерун от 27 июля 2005 г. Law № 2005. — URL: <https://www.refworld.org/legal/legislation/natlegbod/2005/fr/103538> (дата обращения: 02.04.2025).

7. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 20.03.2025) // Справочно-правовая система «КонсультантПлюс». — URL: <http://www.consultant.ru> (дата обращения: 02.04.2025).

REFERENCES

1. Mbumen` Dzesseu Serzh Frederik. Temy` afrikanskogo ugovnogogo sudoproizvodstva: delo Kameruna. — Saarbrücken: EUE; 2011. — 316 s.

2. Nauchno-obrazovatel`ny`j portal «Bol`shaya rossijskaya e`nciklopediya» // URL: <https://bigenc.ru/c/rekvizitsia5c36f4?ysclid=m3n2y9jnna390545169> (data obrashheniya: 02.04.2025).

3. Onana E`tundi Feliks. Opy`t garmonizacii zakonov v Afrike. Obzor ERSUMA // Biznes — pravo — Professional`naya praktika. — 2012. — URL: <http://revue.ersuma.org/no-1-juin-2012/doctrine-12/LES-EXPERIENCES-D-HARMONISATION> (data obrashheniya 02.04.2025).

4. Tamnu Dzhipeu Zhan-Mari. Dacha pokazanii v ugovnom processe v Kamerune : dis. DEA fakul`teta yuridicheskix i politicheskix nauk Universiteta Dualy`, 2006. — URL: [https://www.memoireonline.com/08/09/2453/m_Letemoignage-dans-](https://www.memoireonline.com/08/09/2453/m_Letemoignage-dans-la-procedure-penale-au-Cameroun15.html)

la-procedure-penale-au-Cameroun15.html. (data obrashheniya 02.04.2025).

5. Ugolovno-processual`noe pravo (Ugolovny`j process) : uchebnik dlya vuzov / pod red. prof. E` K. Kutueva ; nauch. red. i vstup. slovo prof. V. P. Sal`nikova. — 2-e izd., pererab. i dop. — SPb. : Sankt-Peterburgskij un-t MVD Rossii ; Fond «Universitet», 2019. — 583 s.

6. Ugolovno-processual`ny`j kodeks Respubliki Kamerun ot 27 iyulya 2005 g. Law № 2005. — URL: <https://www.refworld.org/legal/legislation/natlegbod/2005/fr/103538> (data obrashheniya: 02.04.2025).

7. Ugolovno-processual`ny`j kodeks Rossijskoj Federacii ot 18.12.2001 № 174-FZ (red. ot 20.03.2025) // Spravochno-pravovaya sistema «Konsul`tantPlyus». — URL: <http://www.consultant.ru> (data obrashheniya: 02.04.2025).

СВЕДЕНИЯ ОБ АВТОРЕ

Савицкая Ирина Геннадьевна. Доцент кафедры уголовного процесса. Кандидат юридических наук, доцент.

Воронежский институт МВД России.

E-mail: arisha_s@list.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Savitskaya Irina Gennadievna. Associate Professor of the chair of Criminal Proceedings. Candidate of Law, Associate Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: arisha_s@list.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: процессуальные действия; собирание доказательств; следственные действия; уголовный процесс Российской Федерации; Уголовно-процессуальный кодекс Республики Камерун.

Key words: procedural actions; collection of evidence; investigative actions; criminal procedure of the Russian Federation; criminal Procedure Code of the Republic of Cameroon.

УДК 343.164

Н. А. Трусов, кандидат юридических наук, доцент
И. А. Кравцов, кандидат юридических наук, доцент
Р. И. Лукьянов

СОВРЕМЕННЫЙ ОТЕЧЕСТВЕННЫЙ ОПЫТ ПРАВОВОЙ РЕГЛАМЕНТАЦИИ ИНСТИТУТА НАКАЗА ИЗБИРАТЕЛЕЙ: ЗНАЧЕНИЕ, ПРИЧИНЫ, ПОСЛЕДСТВИЯ

MODERN DOMESTIC EXPERIENCE OF LEGAL REGULATION OF THE INSTITUTION OF ORDERS OF VOTERS: MEANING, REASONS, CONSEQUENCES

В статье кратко изложен современный отечественный опыт правовой регламентации института наказа избирателей. Проанализированы причины пробельности и незавершенности нормативной регламентации рассматриваемого института демократии в нашей стране. Авторы приходят к выводу, что внедрение наказов избирателей в практическую деятельность депутатского корпуса способно позитивно повлиять и совершенствовать всю систему государственного управления. Институт наказов избирателей способен не только повысить качество представительной и законодательной деятельности, но и значительно интегрировать власть с народом.

The article briefly describes the modern domestic experience of legal regulation of the institution of voters' orders. The reasons for the gaps and incompleteness of the normative regulation of the considered institution of democracy in our country are analyzed. The authors come to the conclusion that the introduction of voters' orders into the practical activities of the deputy corps can positively influence and improve the entire system of public administration. The institution of voters' orders can not only improve the quality of representative and legislative activities, but also significantly integrate power with the people.

На современном этапе государственного строительства вопросы развития институтов народного представительства имеют принципиально важное значение. Данное обстоятельство обусловлено множеством факторов, среди которых и повышение общей грамотности населения, сопровождаемое интересом к деятельности властных структур, и совершенствование механизма государственного управления, детерминированного конституционной реформой 2020 года, а также собственно наличие разного рода социально значимых проблем. В качестве акта ответной реакции на постоянно трансформирующуюся социальную среду, а также «вызовы времени» органы публичной власти на перманентной основе обращаются к мнению населения с целью определения наиболее приемлемых и компромиссных решений и выработки эффективных моделей государственного администрирования. И это вполне объяснимо, ведь в демократическом правовом государстве именно общество во всем его многообразии, выражая волю «источника власти», определяет ключевые вопросы организации и функционирования государства.

Рассматривая проблематику демократии в нашей стране, и ее институтов в частности, нельзя обойти стороной институт наказов избирателей, который выступает в качестве своеобразной гарантии электорату, что его интересы, его мнение, его позиция при решении задач управления и вопросов жизнедеятельности общества и государства будут учтены выборными органами публичной власти. Однако следует констатировать, что, несмотря на значимость и реальную необходимость наличия рассматриваемого института демократии в деятельности выборных органов публичной власти всех уровней, его нормативная регламентация либо отсутствует, либо пробельна, либо противоречива, не говоря уже о его практической реализации в правовой действительности.

Отмечая важную роль рассматриваемого института в общественно-политической жизни государства, Э. В. Алимов указывает, что «игнорирование наказов — это не только неисполнение соответствующей обязанности депутатом, органами публичной власти и должностными лицами, но и проявление безразличия к законной воле избирателей, которые как раз таки и наделены правомочием осуществлять

непосредственную власть, что может выражаться как в политической ответственности соответствующих лиц, так и в применении процедуры отзыва, если таковая предусмотрена» [1. — С. 24].

Представляется, что пробельность и незавершенность нормативной регламентации рассматриваемого института демократии в нашей стране обусловлены рядом факторов, к числу которых можно отнести: 1) отсутствие единого нормативного правового акта федерального значения, регламентирующего соответствующий институт, механизм его использования и наступления соответствующих правовых последствий; 2) нежелание парламентариев ограничивать собственную автономию в представительной и законодательной деятельности кругом обязательных к рассмотрению вопросов и решением задач, исходящих от населения; 3) слабую теоретико-методологическую разработку подходов к изучению указанного явления, а также отсутствие доктринального понимания его природы; 4) различие правового оформления и практического опыта работы с данным институтом в российских регионах; 5) неоднозначный опыт функционирования института наказов избирателей в отечественной историографии. Полагаем, что приведенные факторы не описывают весь причинный комплекс и в практической реализации института наказов избирателей в нашей стране могут играть роль и иные, например, экономические, бюрократические и прочие факторы.

Несмотря на широкий перечень «сдерживающих» факторов, все же полагаем, что внедрение наказов избирателей в практическую деятельность депутатского корпуса способно позитивно повлиять и совершенствовать всю систему государственного управления.

Следует отметить, что в настоящее время исследования рассматриваемого правового феномена минимизированы не только в Российской Федерации, но и в европейских государствах. Причин несколько: во-первых, европейский опыт функционирования институтов непосредственной и представительной демократии не содержит в себе упоминания о наказах, а в большей степени сводится к совершенствованию иных форм интеграции народа в управление делами государства, а во-вторых, сложилась традиционная позиция, что наказ избирателей является атрибутом недемократического государства, поскольку ограничивает свободу парламентария, который, согласно принятой концепции свободного мандата, является представителем всей нации [2].

Тем не менее, даже несмотря на скромную теоретическую разработку указанного института, отдельные представители отечественного науч-

ного сообщества убеждены в том, что деятельность по реализации воли населения невозможна без придания ей свойства обязательности, то есть полученные от народа требования (наказы) должны быть, минимум, обязательно рассмотрены и по максимуму воплощены в жизнь.

Данная позиция не является чуждой и для отечественной юридической практики. В частности, С. А. Авакьян отмечает, что «возрождаются и приобретают новое звучание некоторые незаслуженно отодвинутые на задний план институты. В частности, в десятках субъектов Российской Федерации появились законы и положения о народных (гражданских) правотворческих инициативах, акты о наказах избирателей» [3. — С. 4].

Однако имеющаяся региональная практика никак не влияет на позицию федерального центра, который продолжает оставлять без внимания вопросы нормативной регламентации института наказов избирателей. В 2018 году была предпринята попытка возрождения данного института путем инициирования принятия Федерального закона «О наказах избирателей». Но дальше законодательной инициативы дело не пошло [4. — С. 128].

Причинный комплекс такой позиции федерального законодателя видится нам в следующих факторах: 1) имеющаяся противоречивость взглядов на правовую природу наказов избирателей в отечественном политико-правовом пространстве. Расхожая позиция многих правоведов состоит в том, что современный парламентаризм не должен содержать в себе императивных мер для выборных должностных лиц, так как это создаст угрозу их независимой деятельности в пользу всех жителей страны, а не только своих избирателей, а следовательно, приведет ко многим организационным проблемам; 2) появление института наказов избирателей усилит конкуренцию на политической арене, а значит, потенциально будет способствовать обману избирателей в период избирательной кампании.

Безусловно, риски такого рода существуют, однако такие рассуждения имеют место при отсутствии детально проработанного механизма учета наказов избирателей и правовых последствий за их игнорирование. С другой стороны, нельзя отрицать и «потенциальные» аргументы иного рода, когда внедрение рассматриваемого института демократии в правовую реальность Российской Федерации позволит снизить уровень абсентеизма.

В настоящее время институт наказов избирателей имеет правовое закрепление в 35 субъектах Российской Федерации. Анализ регионального законодательства позволяет выделить че-

тыре способа оформления рассматриваемого института: 1) специальными законами о наказах избирателей (26 регионов); 2) законами, регулирующими правовой статус депутата (6 регионов — республики Адыгея, Алтай, Коми и Тыва, Калужская и Нижегородская области); 3) регламентом парламента (республики Адыгея и Башкортостан); 4) положением о наказах избирателей, утвержденным постановлением парламента (Смоленская область) [5. — С. 99]. Таким образом, необходимо отметить разнообразие подходов региональных парламентариев к определению места и значения рассматриваемого института.

Интересным представляется состояние нормативной регламентации института наказов избирателей в Нижегородской области. В части 6 статьи 16 Закона Нижегородской области от 12 октября 2011 года «О статусе депутата Законодательного Собрания Нижегородской области» [6] предусмотрено принятие специального закона о наказах. Однако до настоящего времени такой закон так и не был принят. При этом попытки принять его были. Так в 2013 году областным Законодательным Собранием был отклонен проект закона «О наказах избирателей» [7]. Среди аргументов отклонения назывались: противоречие наказов принципам разграничения полномочий между органами власти; необоснованность отдельного выделения денежных средств; необходимость комплексного подхода, а не точечного решения проблем; а также негативный опыт других субъектов Российской Федерации [4. — С. 129].

По нашему мнению, указанные аргументы не безупречны хотя бы потому, что:

во-первых, федеральным законодательством разграничены полномочия между органами публичной власти разных уровней;

во-вторых, правовая природа наказов, подразумевает наличие осведомленности избирателей о мотивированных причинах отказа, а также накладывает обязанности на кандидата в депутаты в установленный срок уведомить избирателей о движении работы по сформулированным наказам;

в-третьих, наказ необходимо рассматривать как составное звено комплексного демократического механизма управления с множеством перманентных взаимообратных связей;

в-четвертых, опыт функционирования данного института в 35 субъектах Российской Федерации воспринимается как парламентариями, так и избирателями в целом положительно, поскольку результатом его закрепления стало установление

стабильной правовой связи между населением и органами публичной власти, направленной на совместное решение значимых общественных проблем, что, бесспорно, следует расценивать в качестве позитивного правового последствия проведенного субъектами Российской Федерации правового эксперимента по нормативной регламентации и реализации в своих регионах института наказа избирателей.

Нельзя обойти вопрос финансово-экономического обеспечения деятельности по работе с наказами избирателей. В настоящее время в Нижегородской области социально-значимые вопросы разрешаются посредством привлечения средств из фонда на поддержку территорий. В постановлении правительства Нижегородской области от 07.11.2011 № 57 [8] года указан порядок использования бюджетных ассигнований данного фонда, но, исходя из содержания указанного документа, можно констатировать несколько положений, свидетельствующих об ограниченности представленного порядка реагирования на общественные проблемы. Во-первых, в п.1 данного подзаконного акта зафиксировано положение о том, что фонд не имеет предварительного распределения по видам расходов, что в свою очередь создает неопределенность в выделении приоритетных направлений. Во-вторых, наличие широкого спектра направлений финансирования значительно занижает значимость проблем конкретных категорий населения.

Представляется, что правовое закрепление наказов избирателей позволит заблаговременно выявить круг наиболее злободневных социальных проблем и вопросов, сформулировать приоритетные направления публичной деятельности на определенный период времени, а также заранее подготовиться к ее финансовому обеспечению при формировании годового бюджета.

Таким образом, следует резюмировать, что современная демократическая система управления обществом подразумевает необходимость наличия устойчивых механизмов влияния населения на развитие государства и решение проблем общества. По нашему мнению, институт наказов избирателей способен не только повысить качество представительной и законодательной деятельности, но и значительно интегрировать власть с народом. Отечественный опыт самостоятельного правового регулирования данного института на региональном уровне, на наш взгляд, необходим к учету при нормативной регламентации соответствующего института на федеральном уровне.

ЛИТЕРАТУРА

1. Алимов Э. В. Конституционно-правовое регулирование института наказа избирателей в Российской Федерации : дис. ... канд. юр. наук. — М., 2017. — 210 с.
2. Конституционное право: университетский курс : учебник : в 2 т. / под ред. А. И. Казанника, А. Н. Костюкова. — М., 2015. — Т. 2 // СПС «КонсультантПлюс» (дата обращения: 28.03.2024).
3. Авакьян С. А. Основные тенденции современного развития конституционного права // Конституционное и муниципальное право. — 2017. — № 4. — С. 3—7.
4. Лукьянов Р. И., Трусов Н. А. Опыт правового закрепления института наказов избирателей в России и субъектах Российской Федерации // Актуальные вопросы конституционализма : сборник материалов X Международной научно-практической конференции (г. Нижний Новгород, 8 декабря 2023 года) / под. общ. ред. Н. А. Трусова. — Нижний Новгород : Ниже-

- городская академия МВД России, 2023. — С. 127—130.
5. Васюткин Н. Е. Наказ избирателей как форма реализации законодательных идей // Право и государство: теория и практика. — 2023. — № 1 (217). — С. 99—101.
6. О статусе депутата Законодательного Собрания Нижегородской области : закон Нижегородской области от 12 октября 2011 г. № 150-3 // Нижегородские новости. — 2011. — 14 окт.
7. Комитет по госвласти не поддержал законопроект НРО КПРФ «О наказах избирателей». — URL: <http://www.ntann.ru/news/item/?ID=227349> (дата обращения: 20.03.2024).
8. Об утверждении Порядка использования бюджетных ассигнований фонда на поддержку территорий : постановление правительства Нижегородской области от 7.02.2011 № 57 (с изм. на 06.05.2024) // Нижегородские Новости. — 2011. — 19 февр.

REFERENCES

1. Alimov E. V. Konstitucionno-pravovoe regulirovanie instituta nakaza izbiratelej v Rossijskoj Federacii : dis. ... kand. yur. nauk. — M., 2017. — 210 s.
2. Konstitucionnoe pravo: universitetskij kurs : uchebnik : v 2 t. / pod red. A. I. Kazannika, A. N. Kostjukova. — M., 2015. — T. 2 // SPS «Konsul'tantPlyus» (data obrashheniya: 28.03.2024).
3. Avak'yan S. A. Osnovny'e tendencii sovremennogo razvitiya konstitucionnogo prava // Konstitucionnoe i municipal'noe pravo. — 2017. — № 4. — S. 3—7.
4. Luk'yanov R. I., Trusov N. A. Opyt pravovogo zakrepleniya instituta nakazov izbiratelej v Rossii i sub`ektax Rossijskoj Federacii // Aktual'ny'e voprosy` konstitucionalizma : sbornik materialov X Mezhdunarodnoj nauchno-prakticheskoy konferencii (g. Nizhnij Novgorod, 8 dekabrya 2023 goda) / pod. obshh. red. N. A. Trusova. — Nizhnij Novgorod : Nizhegorodskaya akademiya MVD Ros-

- sii, 2023. — S. 127—130.
5. Vasyutkin N. E. Nakaz izbiratelej kak forma realizacii zakonodatel'ny'x idej // Pravo i gosudarstvo: teoriya i praktika. — 2023. — № 1 (217). — S. 99—101.
6. O statuse deputata Zakonodatel'nogo Sobraniya Nizhegorodskoj oblasti : zakon Nizhegorodskoj oblasti ot 12 oktyabrya 2011 g. № 150-Z // Nizhegorodskie novosti. — 2011. — 14 okt.
7. Komitet po gosvlasti ne podderzhal zakonoproekt NRO KPRF «O nakazax izbiratelej». — URL: <http://www.ntann.ru/news/item/?ID=227349> (data obrashheniya: 20.03.2024).
8. Ob utverzhdenii Poryadka ispol'zovaniya byudzhethny'x assignovanij fonda na podderzhku territorij : postanovlenie pravitel'stva Nizhegorodskoj oblasti ot 07.02.2011 № 57 (s izm. na 06.05.2024) // Nizhegorodskie Novosti. — 2011. — 19 fevr.

СВЕДЕНИЯ ОБ АВТОРАХ

Трусов Николай Александрович. Доцент кафедры государственно-правовых дисциплин. Кандидат юридических наук, доцент.

Приволжский филиал Университета правосудия им. В. М. Лебедева.

E-mail: nikevor@yandex.ru

Россия, 603022, Нижний Новгород, проспект Гагарина, 17а.

Кравцов Иван Александрович. Начальник кафедры уголовного права и криминологии. Кандидат юридических наук, доцент.

Воронежский институт МВД России.

E-mail: kia52@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Лукьянов Руслан Игоревич. Заместитель командира взвода факультета подготовки оперативного состава подразделений экономической безопасности и противодействия коррупции.
Нижегородская академия МВД России.
E-mail: rlukyanov@internet.ru
Россия, 603081, Нижний Новгород, ул. Анкудиновское шоссе, 3.

Trusov Nikolay Alexandrovich. Associate Professor of the chair of Public Law Disciplines. Candidate of Law, Associate Professor.
Volga Region branch of the University of Justice named after V. M. Lebedev.
E-mail: nikevor@yandex.ru
Work address: Russia, 603022, Nizhny Novgorod, Prospect Gagarina, 17a.

Kravtsov Ivan Aleksandrovich. 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: kia52@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Lukyanov Ruslan Igorevich. Deputy platoon commander of the faculty for training operational personnel of economic security and anticorruption units.
Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia.
E-mail: rlukyanov@internet.ru
Work address: Russia, 603081, Nizhny Novgorod, Ankudinovskoe Highway, 3.

Ключевые слова: демократия; наказы избирателей; статус депутата; законодательная деятельность; правовые последствия.

Key words: democracy; orders of voters; deputy status; legislative activity; legal consequences.

УДК 342

С. Н. Чмырёв, кандидат юридических наук, доцент

А. П. Бохан, кандидат юридических наук, доцент

Е. В. Тимашкова, кандидат юридических наук

МОЛОДЁЖНЫЙ ПОЛИТИЧЕСКИЙ ЭКСТРЕМИЗМ КАК СОЦИАЛЬНОЕ ЯВЛЕНИЕ

YOUTH POLITICAL EXTREMISM AS A SOCIAL PHENOMENON

В статье рассматривается феномен молодёжного политического экстремизма как социального явления в период специальной военной операции, особенности его проявления, а также характеристики молодых людей, склонных к проявлению элементов экстремального поведения. Авторы анализируют понятия радикализма, экстремизма и экстремистской деятельности.

The article examines the phenomenon of youth political extremism as a social phenomenon during the special military operation, the peculiarities of its manifestation, as well as young people prone to the manifestation of elements of extreme behavior. The authors analyze the concepts of radicalism, extremism and extremist activity.

На сегодняшний день молодёжному экстремизму посвящено много работ, но после начала в 2022 году специальной военной операции мы в средствах массовой информации узнаем о том, что молодёжь больше стала заниматься политикой и чаще стала совершать противоправные действия экстремисткой и террористической направленности. И примеров этому на сегодняшний день немало. Так, 13 и 16 апреля 2023 года на станции в поселке Воротынске в Калужской области были подожжены релейные шкафы. 20 апреля сотрудники ФСБ задержали «диверсантов» — ими оказались три 18-летних парня и 17-летняя девушка. Юные «диверсанты» получили задание на поджог от украинских спецслужб, надеясь таким образом заработать денег. Двое из задержанных были осуждены как террористы 2-м Западным окружным военным судом к 3 годам тюрьмы и 13 годам исправительной колонии строгого режима, остальные прошли как свидетели. По словам юношей, на диверсию они пошли ради наживы — за каждый поджог некий аноним перечислял им деньги в интернете.

В Хабаровске 18-летний местный житель и его 17-летняя подруга выслушали обвинительный приговор за подготовку теракта. Установлено, что, будучи несовершеннолетним, юноша вступил в экстремистское сообщество. Он общался с его руководителем с помощью мессенджера и вовлек в противоправную деятельность свою подругу. Весной-летом 2023 года юноша подготовился к совершению нескольких террористических актов. Он должен

был поджечь ряд зданий, а также вымогать деньги у обеспеченных горожан, чтобы финансировать экстремистское сообщество. В его планы входили и нападения на людей неславянской внешности и их избиение.

Троих молодых белгородцев осудили за семь эпизодов преступлений, в числе которых реабилитация нацизма, побои, незаконное изготовление оружия, призывы к экстремистской деятельности, оправдание терроризма и вовлечение в это несовершеннолетних. В августе 2022 года 21-летний житель Белгородского района писал комментарии с призывами к экстремизму и возбуждению межнациональной розни. В сентябре того же года он оставил в группе, посвящённой Второй мировой войне, сообщения, оправдывающие нацизм. В августе 2023 года молодой человек создал в сети экстремистское сообщество и привлёк своего 16-летнего брата, а также других людей. Осенью 2023 года комментарии с призывами уже начал писать подросток. В феврале и марте 2023 года третий обвиняемый публиковал сообщения с оправданием терроризма. Молодых людей осудили и приговорили к различным срокам в колонии — от трёх до 12 лет.

И такие негативные примеры, связанные с молодыми людьми, можно, к сожалению, продолжать.

В своей научной работе П. Е. Сулонов [1. — С. 177—180] указывает, что в политическом обиходе существует устойчивый синонимический ряд терминов, описывающих интересующее нас явление. В первую очередь это радикализм, экстремизм

и терроризм. Кроме того, следует учитывать неотделимость от изучаемой проблемы феноменов фанатизма, фундаментализма и терроризма. В исследованиях ученых, которые занимаются данной проблемой, вышеуказанные явления или события изучают в едином смысловом отношении.

Данное утверждение основывается на некоторых факторах, таких как система взглядов, оценок, экономические, культурные, характеристики личности, которые влияют на её поведение, мышление, эмоциональное состояние и умственную деятельность. В научных работах акценты могут расставляться по-разному, но в любом случае одно невозможно изучать без другого. Если исследовать терроризм, то его невозможно объяснить без анализа политической составляющей, таких явлений, как попытки кардинально изменить строй (радикализм) и экстремизм. Изучая работы, посвященные типологии политического радикализма, мы видим взаимосвязь с политическим экстремизмом и в данном случае можем полагать, что оппозиционный и властвующий радикализм может привести и к политическому экстремизму.

Радикализм можно рассматривать как стремление идти до конца, добиваться коренных изменений и наиболее полных результатов в любой преобразовательной деятельности, и это комплекс социально-политических идей и действий, направленных на наиболее кардинальное, решительное, глубокое (коренное) изменение существующих социальных отношений и политических институтов в жизни общества.

Мы должны иметь в виду, что главной составляющей экстремизма является его публичность. Причём никакой роли не играет тот факт, был ли этот призыв услышан или он не достиг цели. Что же касается профилактики, то специалисты по работе с молодежью не всегда имеют верное представление о том, что заключается в этом термине и насколько важен сам процесс проведения профилактической работы. Ведь она включает в себя не только и не столько снижение уровня радикализации, сколько недопущение распространения экстремистских идей. В этом разрезе интересен опыт Дагестана, где создали Совет религиозных деятелей, который занимается разработкой памяток в исследуемой нами сфере. Отдельно хочется отметить возрождение истории и культуры народов Дагестана, молодёжные жилищные программы и попытки решить вопрос безработицы среди молодежи.

Будучи политическим, феномен радикализма обусловлен целым рядом причин исторического, социального, экономического, религиозного характера. Согласно толковым словарям, в политике радикал — «приверженец... решительных

действий, взглядов; сторонник радикализма — политического течения, ориентированного на проведение демократических реформ в рамках существующего строя», бескомпромиссный носитель и выразитель идеалов, связанных с преобразованиями в социальном устройстве, стремящийся их осуществить.

По мнению А. А. Протасевича, «радикализм есть идейно-мировоззренческое обоснование пренебрежения к праву, а молодёжный экстремизм является непосредственной реализацией такого пренебрежения» [2. — С. 172]. Можно выделить несколько ключевых моментов проявления правового нигилизма в политической сфере (правовых аспектов политического экстремизма молодёжи): молодёжь убеждена в том, что государство и власть даруют человеку его права, но эти права не принадлежат человеку от рождения; законы рассматриваются как продукт государственной власти, а не как первичный по отношению к государству фактор; право рассматривается как средство для достижения политических целей, а не является самостоятельной ценностью и целью.

Политический экстремизм является продолжением политического радикализма. Поскольку радикализм есть совокупность неких ярких, необычных, выходящих за рамки допустимого идей, то логично, что для их реализации применимы аналогичные, т. е. «крайние», средства. Перед исследователями политического экстремизма с неизбежностью встает вопрос: а что считать «крайними» средствами, что подразумевается под «крайностями»? В научной литературе на этот вопрос нет ясного и четкого ответа. Мы полагаем, что современные авторы, пишущие о политическом экстремизме, подразумевают следующее положение: сущностным признаком политического экстремизма является использование насилия для достижения своих политических целей, т. е. политического насилия.

Следует сразу отделить понятие политического насилия от понятия государственно-правового властного принуждения. Действительно, если исследовать русскую лингвистическую традицию, то можно увидеть, что понятие «насилие» не тождественно ни понятию «сила», ни понятию «принуждение». Во-первых, понятие «сила» имеет отношение не только к сфере человеческих взаимоотношений, но и к природе как таковой. В понятии же «насилие» подчеркивается направленность на человека. Во-вторых, понятие «принуждение» не несет на себе печати негативной моральной оценки (производные же от понятия «насилие» — «насилует», «насильник»). В-третьих, понятие «насилие» подразумевает именно психофизическое воздействие на индивида.

Политический экстремизм как социальное явление представляет угрозу национальной безопасности государства, поскольку приводит к конфликту общественных отношений в различных сферах жизни общества (политических, национальных, религиозных и др.). Политический экстремизм может проявиться в молодежной среде вследствие воздействия таких факторов, как безработица (особенно среди молодежи), низкий уровень потребления материальных благ и услуг, проживание в регионе с низким уровнем социально-экономического развития.

Политический экстремизм может выступать или как стремление определенных социальных сил уничтожить сложившуюся систему общественно-политических отношений, или как стремление сохранить эту систему в неизменном виде. Проявления экстремизма значительно возросли за последние тридцать лет вследствие кардинальных перемен в политической, экономической и социальной жизни общества и государства. Особенно это заметно в молодежной среде.

Определение сущности политического экстремизма через политическое насилие характерно для западной политической науки и публицистики. Зарубежные ученые указывают на негативный оценочный смысл в определении политического насилия, относя последнее к «крайним», выходящим за пределы допустимого, средствам.

Как социальное явление общественной жизни, экстремизм известен с давних пор, понятие «экстремизм» появилось еще в античности. Аристотель использовал этот термин для описания состояний, характеризующихся как противоположные стабильности и сдержанности. Идеологическое обоснование необходимости и приемлемости использования экстремизма как способа достижения своих целей сложилось в XIX веке. Немецкий радикал К. Гейнцген утверждал, что даже небольшая идеологически мотивированная группа за счет экстремистских акций способна посеять хаос в любом сильном государстве ради достижения «благородных идеалов» [3. — С. 3—19].

М. Г. Диева и Э. А. Мамонтова в своей научной работе указывают, что большинство политических, националистических, религиозных и квазирелигиозных организаций разных идеологических направлений, осуществляющих свою экстремистскую деятельность в различных сферах общественной жизни и в различных регионах нашей страны, получают открытую или завуалированную материальную и информационную помощь из-за рубежа.

Зачастую информационная помощь имеет даже большее значение, чем материальная. Пропагандистская литература поставляется в печатном варианте для распространения или в электронном

для выкладывания в интернет или социальные сети. Пропагандистская видеопродукция (видеоролики, тематические фильмы, музыкальные видеоклипы и т. п.) отличается высоким качеством съемки, с привлечением не только нанятой «массовки» для постановочных сцен, но и профессиональных актеров, гримеров, костюмеров, сценаристов, режиссеров, кинооператоров, психологов и других специалистов. Задача всей этой литературы и видеопродукции — максимально привлечь внимание молодых людей к идеологическим постулатам экстремистов, расшевелить в обществе старые межконфессиональные и социальные обиды и конфликты либо спровоцировать новые и на этой волне овладеть и манипулировать сознанием значительной части молодежи.

Для вовлечения молодежи в экстремистскую деятельность штатные психологи экстремистских организаций обучают своих вербовщиков манипулятивным психотехникам неявного (скрытого) психологического воздействия на сознание вербуемого. Поиск объектов вербовки часто ведется через интернет и социальные сети (группы знакомств или группы общения по интересам, различные психологические тренинги «позитивной мотивации», бизнес-тренинги и т. п.), через просветительские и благотворительные организации, спортивные секции восточных единоборств и йоги, клубы по интересам, земляческие общины, исправительные учреждения и т. д.

В целях контроля сознания вербуемых молодых людей применяются психотехники медитации, глубокой психической и физической релаксации, «позитивного реформирования мышления», «позитивного программирования сознания», «расширения сознания» и т. п. В процессе вербовки ничего не подозревающим молодым людям постепенно и незаметно прививают систему идеологических ценностей своего спонсора — какой-либо экстремистской организации или специальных служб иностранных государств. Главным условием и особенностью процесса манипулирования сознанием молодого индивида является сохранение у него иллюзии того, что он самостоятельно принял решение стать сторонником экстремистской организации. Такой подход гарантирует в будущем верное и последовательное служение нового завербованного целям деятельности экстремистской организации или специальных служб иностранного государства, что особенно характерно для идеологических групп.

К сожалению, в цепи целого ряда криминальных происшествий о многих можно с полной уверенностью говорить, что они инспирированы спецслужбами Украины. Вербовщики нацелились на российскую молодежь, которая еще не имеет

житейского опыта и твердых принципов, а желание подзаработать есть.

По данным Генеральной прокуратуры РФ, жертвами беспардонной «игры» становятся даже ученики младших классов. Их обманом заставляют, например, устраивать утечки газа в жилых домах. Но чаще всего молодых людей вовлекают в диверсии на железных дорогах. Есть случаи, когда подростков подталкивают совершать вооруженные нападения на школы. Впервые о привлечении подростков к диверсиям заговорили летом 2022 года. Вербовщики подходят изощренно. Они говорят, что хотят не навредить, а помочь. Например, «запугать» чиновников или сотрудников военкоматов, чтобы те лучше делали свою работу. От этого, дескать, будет благо всему обществу.

Свои уговоры кураторы подкрепляют обещаниями хорошо заплатить — за повреждение рельсового шкафа у железнодорожных путей, поджог автомобиля, за данные о передвижении воен-

ной техники... Они понимают, что привлечение к уголовной ответственности за диверсии неизбежно, а подростков рассматривают как расходный материал. У молодых людей же, решивших «влегкую» подзаработать денег на поджоге, оказывается сломанной судьба.

Молодёжный политический экстремизм выступает как образ политического действия, ориентированного на достижение поставленной цели в условиях отсутствия приемлемых политических средств, которые бы могли упорядочивать, а не дестабилизировать отношения в обществе. Результатом отсутствия или дефицита таких средств является использование «крайних», насильственных мер, приносящих в жертву идее отдельного человека. Радикалистское сознание трансформируется в экстремистскую установку на насилие, веру в то, что с помощью насилия можно решить любую сложную политическую проблему, разрешить любое противоречие.

ЛИТЕРАТУРА

1. Суслонов П. Е. Методологические основания и проблемы исследования политического экстремизма // Грамота. — 2013. — № 12 (38) : в 3 ч. — Ч. 1. — С. 177—180.
2. Протасевич А. А. О противодействии экстремизму в современном мире // Всероссийский

криминологический журнал. — 2019. — Т. 13, № 1. — С. 172—176.

3. Терроризм и экстремизм как угроза национальной безопасности : учебное пособие / М. Г. Диева, Э. А. Мамонтова. — Тамбов : Издательский центр ФГБОУ ВО «ТГТУ», 2024.

REFERENCES

1. Suslonov P. E. Metodologicheskie osnovaniya i problemy issledovaniya politicheskogo e'kstremizma // Gramota. — 2013. — № 12 (38) : v 3 ch. — Ch. 1. — S. 177—180.
2. Protasevich A. A. O protivodejstvii e'kstremizmu v sovremennom mire // Vserossijskij

kriminologicheskij zhurnal. — 2019. — T. 13, № 1. — S. 172—176.

3. Terrorizm i e'kstremizm kak ugroza nacional'noj bezopasnosti : uchebnoe posobie / M. G. Dieva, E. A. Mamontova. — Tambov : Izdatel'skij centr FGBOU VO «TGTU», 2024.

СВЕДЕНИЯ ОБ АВТОРАХ

Чмырёв Сергей Николаевич. Профессор кафедры административного права и административной деятельности. Кандидат юридических наук, доцент.

Ставропольский филиал Краснодарского университета МВД России.

E-mail: Chmyrevsn@mail.ru

Россия, 355018, Ставрополь, проспект Кулакова, 43.

Бохан Андрей Петрович. Доцент кафедры уголовного права. Кандидат юридических наук, доцент. Ростовский филиал Российского государственного университета правосудия им. В. М. Лебедева.

E-mail: boxan@mail.ru

Россия, 344038, Ростов-на-Дону, проспект Ленина, 66.

Тимашкова Елена Викторовна. Старший преподаватель кафедры административной деятельности органов внутренних дел. Кандидат юридических наук.

Воронежский институт МВД России.

E-mail: timashkova.lenochka@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Chmyrev Sergey Nikolaevich. Professor of the chair of Administrative Law and Administrative Activities. Candidate of Law, Associate Professor.

Stavropol branch of the Krasnodar University of the Ministry of Internal Affairs of Russia.

E-mail: Chmyrevsn@mail.ru

Work address: Russia, 355018, Stavropol, Prospect Kulakova, 43.

Bohan Andrey Petrovich. Associate Professor of the chair of Criminal Law. Candidate of Law, Associate Professor.

Rostov branch of the Russian State University of Justice named after V. M. Lebedev.

E-mail: boxan@mail.ru

Work address: Russia, 344038, Rostov-na-Donu, Lenina Prospect, 66.

Timashkova Elena Viktorovna. Senior lecturer of the chair of Administrative Activities. Candidate of Law.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: timashkova.lenochka@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: радикализм; экстремизм; терроризм; молодёжь; политический радикализм; политический экстремизм; политическое насилие; молодёжный политический экстремизм; социальное явление.

Key words: radicalism; extremism; terrorism; youth; political radicalism; political extremism; political violence; youth political extremism; social phenomenon.

УДК 316.628.23

Л. Б. Антонова

РЕАЛИЗАЦИЯ АЛКОГОЛЬНОЙ ПРОДУКЦИИ НЕСОВЕРШЕННОЛЕТНИМ: ВОПРОСЫ ПРИВЛЕЧЕНИЯ К АДМИНИСТРАТИВНОЙ ОТВЕТСТВЕННОСТИ

SALE OF ALCOHOLIC BEVERAGES TO MINORS: ISSUES OF BRINGING TO ADMINISTRATIVE RESPONSIBILITY

В статье на основе анализа положений действующего федерального законодательства об административной ответственности за незаконную реализацию алкогольной продукции несовершеннолетним и его применения определяются недостатки правового регулирования и даются предложения по его совершенствованию.

Based on the analysis of the provisions of the current federal legislation on administrative responsibility for the illegal sale of alcoholic beverages to minors and its application, the article identifies the shortcomings of legal regulation and makes proposals for its improvement.

К числу принципов, заложенных в основу Концепции сокращения потребления алкоголя в Российской Федерации на период до 2030 года и на дальнейшую перспективу [1], отнесен принцип приоритета защиты детей от вреда последствий употребления ими алкоголя. Одной из задач Концепции определено укрепление ценностей здорового образа жизни, формирование среды для сокращения потребления алкоголя, заболеваемости, инвалидности и смертности, связанных с алкоголем.

Употребление алкоголя, спиртосодержащей продукции несовершеннолетними влечет серьезные негативные последствия, которые выражаются в причинении таким подросткам вреда, предполагающего нарушения, во-первых, процесса их нормальной социализации; во-вторых, здоровья; в-третьих, поведения, когда оно меняется на девиантные формы, включая преступное. В итоге происходит социальная деградация пьющих подростков. Глобальное влияние употребление алкоголя несовершеннолетними оказывает на состояние всего российского общества, как в настоящее время, так и в будущем, когда подростки уже достигают совершеннолетия.

Уровень пьянства, состояние заболеваемости алкоголизмом, количественные показатели реализации несовершеннолетним алкогольной продукции в значительной мере зависят от эффективности правового регулирования оборота алкогольной продукции, его реализации, а также от эффективности административно-правовых средств противодействия правонарушениям в данной

сфере. Однако в современной России его состояние отличается непоследовательностью, фрагментарностью, вследствие чего существует необходимость дальнейшего совершенствования правового регулирования ответственности за реализацию несовершеннолетним алкогольной продукции. Это позволит более эффективно осуществлять противодействие данным правонарушениям, вести борьбу с употреблением алкоголя среди подростков.

Реализация алкогольной продукции несовершеннолетним представляет собой деяние, наказуемое в соответствии с законодательством об административных правонарушениях и уголовным законодательством. Реализация алкогольной продукции несовершеннолетним предполагает розничную продажу этой продукции данной категории граждан. Административная ответственность за это установлена ч. 2.1 ст. 14.16 КоАП РФ. В случае неоднократности такого деяния предусмотрена уголовная ответственность в статье 151.1 УК РФ. В широком смысле, полагаем, реализация включает и передачу алкогольной продукции несовершеннолетнему для ее употребления, то есть вовлечение несовершеннолетнего в употребление алкогольной продукции. Ответственность за указанное деяние предусмотрена ст. 6.10 КоАП РФ. И в первом, и во втором случаях противоправными действиями причиняется вред здоровью несовершеннолетнего в результате попадания в его распоряжение алкогольной продукции и последующего употребления этой продукции.

Законодательно основные вопросы, связанные с алкоголем и ограничением его потребления населением, решаются положениями Федерального закона от 22 ноября 1995 г. № 171-ФЗ «О государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции». Что касается несовершеннолетних, то пп. 11 п. 2 ст. 16 данного закона запрещается любая продажа им алкогольной продукции, п.п. 14 п. 2 ст. 16 в общем запрещается такая продажа дистанционным способом, п. 7 ст. 16 запрещены в целом распитие алкогольной продукции в общественных местах и ограничена продажа алкоголя по времени — не допускается его розничная продажа с 23 часов вечера до 8 часов утра [2], то есть регламентируется широкий спектр отношений, связанных с реализацией алкогольной продукции населению, в том числе и несовершеннолетним.

Непосредственный запрет на реализацию алкогольной продукции несовершеннолетним обеспечивается нормами КоАП РФ путем установления административной ответственности за его нарушение. КоАП РФ регламентирует комплекс рассматриваемых отношений, закрепляя в ч. 2.1 ст. 14.16 санкции за розничную продажу им алкогольной продукции, а в ст. 6.10 — за вовлечение их в употребление такой продукции [3].

П. 3 ст. 2 Федерального закона от 28 декабря 2009 г. № 381-ФЗ «Об основах государственного регулирования торговой деятельности в Российской Федерации» [4] дает определение розничной продажи, связывая ее с исключительным последующим использованием в целях, не связанных с предпринимательской деятельностью. При этом применительно к алкоголю законом (ч. 1 ст. 16 ФЗ № 171) установлено, что в розницу крепкий алкоголь могут продавать только организации, а алкоголь небольшой крепости — также и индивидуальные предприниматели. Вина могут продавать и индивидуальные предприниматели, но только в случаях, когда они являются сельскохозяйственными производителями, а вино произведено ими. Соответственно, к ответственности могут быть привлечены только продавец — организация или индивидуальный предприниматель, осуществляющие розничную продажу алкогольной продукции, и их работник, осуществляющий по письменному либо устному трудовому договору трудовую деятельность по продаже продуктов, товаров. Главным при определении субъекта правонарушения является факт отпуска алкогольной продукции несовершеннолетнему именно в форме розничной продажи.

Но продать алкогольную продукцию несовершеннолетнему может и любое физическое лицо,

не являющееся работником предприятия или предпринимателя, осуществляющего розничную торговлю, или даже являясь им, но не в рамках своей трудовой функции. Такая реализация розничной продажей не является, но такие факты, уж точно, исключать нельзя. Как отмечает Д. В. Андреев, продажа алкогольной продукции несовершеннолетним может осуществляться, например, гражданами на придомовой территории, из транспортных средств, а также с «доставкой на дом» [5]. Этот правовой пробел должен быть устранен.

Ч. 2 ст. 14.16 КоАП РФ устанавливает ответственность за продажу продукта, являющегося алкоголем. Что касается спиртосодержащей продукции, то она может быть непищевой и пищевой (например, пищевая — плодовые сброженные материалы, плодое или виноградное сусло, в которых спирта не менее 0,5%). По установлению нового ГОСТ 59941-2021 [6] в плодоем сброженном материале доля этилового спирта должна быть от 6,0% до 15,0% (п. 4.1.3.1) и он не может поступать в розничную продажу (п. 3.1). Поэтому в торговых точках данную продукцию несовершеннолетний приобрести не может. А вот изготовленную в домашних условиях — вполне. И такой спиртосодержащий напиток не является для несовершеннолетнего лица менее привлекательным.

Целесообразно в этих случаях законодательно закрепить ответственность граждан за продажу лицам до восемнадцати лет алкогольной и иной спиртосодержащей продукции в новой части 2.3 статьи 14.16 КоАП РФ. Это позволит повысить эффективность защиты несовершеннолетних в исследуемой сфере.

Следует сказать, что законодателем достаточно детально регламентируется процедура привлечения к административной ответственности за реализацию алкогольной продукции несовершеннолетним, однако проблемы правоприменительного характера, зависящие от качества, полноты и объективности выяснения всех обстоятельств дела, все равно имеют место.

Например, в соответствии с п. 19 Постановления Пленума Верховного Суда РФ от 24 октября 2006 г. № 18 «О некоторых вопросах, возникающих у судов при применении Особенной части Кодекса Российской Федерации об административных правонарушениях» [7] при рассмотрении дела по ст. 14.16 КоАП РФ правоприменителю необходимо выяснять, имеются ли в материалах дела доказательства, подтверждающие факт реализации товаров (например, акт контрольной закупки), иначе дело подлежит прекращению в связи с отсутствием события административного проступка, что исключает дальнейшее по нему производство. Еще одно основание прекращения

производства обозначено в п. 3 ч. 1.1 ст. 29.9 КоАП РФ — если в действиях (бездействии) содержатся признаки преступления, предусмотренные статьей 151.1 УК РФ.

Приведем два примера из судебной практики, связанные с недолжной фиксацией и сбором материалов дела на стадии возбуждения дела об административном правонарушении сотрудниками органов внутренних дел.

Так, по одному из дел за № 5-460/2017 по ч. 2.1 ст. 14.16 КоАП РФ суд указал, что производство должно быть прекращено в связи с отсутствием события административного правонарушения. Основанием для этого суд счел несоответствие требованиям допустимости собранных по делу доказательств, так как они были получены с нарушением процессуальных норм. В материалах дела отсутствовали: акт закупки или иная документация, подтверждающая, что алкоголь был приобретен именно в данном магазине; протокол об изъятии данной алкогольной продукции у несовершеннолетнего; протокол осмотра магазина с указанием наименований реализуемых товаров. Суд не признал достаточными и имевшиеся в материалах дела пояснения несовершеннолетнего, поскольку последнему продавец для опознания не предъявлялся [8].

Аналогичным образом судом было прекращено и производство по делу № 5-365/65/2020 по ч. 2.1 ст. 14.16 КоАП РФ. Суд установил, что нет допустимых доказательств виновности привлекаемого к административной ответственности лица. Основой дела явился протокол об административном правонарушении, который составил инспектор по делам несовершеннолетних о том, что продавцом была реализована бутылка пива несовершеннолетней девушке. Чек, подтверждающий факт продажи пива, в материалах дела отсутствовал. Инспектор суду показал, что протокол он составил по материалам проверки, полученным от участкового уполномоченного полиции. Из пояснений участкового свидетеля установлено, что свидетель сам очевидцем продажи пива не являлся, а знал об этом со слов несовершеннолетней. При этом саму несовершеннолетнюю опросили в отсутствие ее законного представителя [9].

За совершение реализации алкоголя несовершеннолетним законодателем предусмотрен административный штраф по ч. 2.1 ст. 14.16 КоАП РФ, казалось бы, достаточно существенный. Но, так как минимальная сумма штрафа составляет тридцать тысяч рублей, его назначение возможно с учетом ч. 2.2 ст. 4.1 КоАП РФ, когда правоприменитель может назначить его в размере менее минимального предусмотренного санкцией размера. При этом следует иметь в виду, что такое сокра-

щение может быть только в исключительных случаях, с учетом обстоятельств дела. При рассмотрении дела сторона вправе ходатайствовать о подобном снижении размера штрафа, а значит, хотя продавцу и не удастся избежать ответственности, но получается существенно ее снизить.

Существенными обстоятельствами могут являться: отсутствие существенного вреда, несоразмерность санкции последствиям правонарушения, обстоятельства, связанные с имущественным положением, исключение избыточного ограничения прав указанного лица.

Представляется также целесообразным введение в КоАП РФ еще одного вида административного наказания продавцу «аннулирование лицензии». К подобному заключению мы пришли в результате нижеследующих суждений.

При осуществлении лицензионного контроля применяются такие меры, как приостановление действия и аннулирование лицензии. Данные меры предусмотрены ст. 20 Федерального закона № 171-ФЗ. Они не являются мерами административной ответственности. В результате складывается ситуация, когда к виновному применяются эти две меры одновременно.

На основании пп. 3 п. 3.2 ст. 20 Федерального закона № 171-ФЗ лицензия на производство и оборот этилового спирта, алкогольной и спиртосодержащей продукции аннулируется по решению федерального органа по контролю и надзору за нарушение требований к розничной продаже алкоголя, установленных п. 2 ст. 16 Закона, включая запрет на розничную продажу алкоголя несовершеннолетним.

Получается, что за одно и то же нарушение применяется административное наказание (согласно КоАП РФ) и мера административного принуждения (согласно закону № 171-ФЗ), которая мерой административной ответственности не является, тогда как данные меры, полагаем, имеют практически равную силу. Эти меры по своей сути представляют собой итоговые карательные санкции, применяемые за противоправную деятельность юридических лиц и значительно ограничивающие их правоспособность, поскольку утрачивается возможность осуществления лицензируемой деятельности. Некоторые исследователи (например, Б. Ю. Джамирзе [10], Р. Р. Фаисханов [11], А. Д. Бадулин [12]) считают одновременное применение рассматриваемых мер несправедливым, предлагая ввести в КоАП РФ новый вид административного наказания — «аннулирование лицензии». На наш взгляд, поддержать вышеназванное предложение вполне возможно, поскольку, на что обращается внимание в судебной практике, административное наказание и аннулирование лицензии за одно и

то же нарушение лицензионных требований противоречит принципу соразмерности юридической ответственности [13].

С учетом вышеизложенных суждений целесообразно закрепить в КоАП РФ новый вид административного наказания — «аннулирование лицензии», дополнив соответствующей статьей, и внести необходимые изменения в статьи КоАП РФ, устанавливающие ответственность за нарушения в сфере оборота алкоголя (относительно дополнения санкций). При этом предусмотреть, что это административное наказание может применяться и как основное, и как дополнительное.

Следующая проблема связана с правом продавца (лица, непосредственно отпускающего алкогольную продукцию) потребовать от покупателя предоставления документа, удостоверяющего его личность, или другого, позволяющего установить его возраст, при возникновении сомнений в его совершеннолетии. Такое право вытекает из содержания пп. 11 п. 2 ст. 16 Федерального закона № 171-ФЗ.

Приказом Минпромторга России от 31 мая 2017 г. № 1728 [17] установлен исчерпывающий перечень документов, которые продавец вправе потребовать предъявить от лица, собирающегося приобрести алкоголь. Это направлено на предотвращение нарушения норм, устанавливающих запрет на реализацию алкогольной продукции несовершеннолетним.

Важно обратить внимание на то, что законодателем четко указано, что продавец «вправе» потребовать вышеуказанный документ. Однако Е. Е. Новичкова полагает, что при возникновении сомнений у продавца относительно возраста покупателя право требовать переходит в аналогичную обязанность [14]. На наш взгляд, подобное утверждение ни на чем не основано.

Мы считаем, что будет правильным для предотвращения продажи алкогольной продукции несовершеннолетним четко указать в законе, что продавец именно «обязан» при возникновении сомнений потребовать предъявления документа, позволяющего установить возраст покупателя. С этой целью в пп. 11 п. 2 ст. 16 Федерального закона № 171-ФЗ внести соответствующие изменения (заменить слово «вправе» на слово «обязан»).

Как представляется, определенные вопросы вызывает практическая реализация положений о возникновении у продавца сомнений в совершеннолетнем возрасте покупателя. Данное понятие носит оценочный характер. Трудно доказать, возникли у продавца такие сомнения или нет, если он будет отрицать этот факт, ведь только ему может быть это известно. Продавец исключительно из

собственного восприятия оценивает возможный возраст покупателя по его внешним признакам.

В некотором возрасте сомнения в возрасте не возникают (например, относительно ребенка или пожилого человека). Однако в возрасте от 15-16 лет до 25-28 лет человек может выглядеть явно не на свои годы. В подобных ситуациях не исключаются ошибки в определении возраста. Продавец может искренне заблуждаться. В результате сложно констатировать его вину. При этом некоторые подростки могут злоупотреблять тем, что выглядят старше своих лет, и покупать алкогольные напитки для себя или для своих сверстников. В результате розничная продажа несовершеннолетним алкогольной продукции будет продолжаться.

По нашему глубокому убеждению, пп. 11 п. 2 ст. 16 Федерального закона № 171-ФЗ целесообразно изложить следующим образом: «(11) несовершеннолетним. В случае, когда у лица, непосредственно осуществляющего отпуск алкогольной продукции (продавца), должны были возникнуть сомнения в достижении покупателем совершеннолетия, исходя из его явных внешних признаков, он обязан потребовать у этого покупателя документ, позволяющий установить возраст этого покупателя. ...». Полагаем, это позволит разрешить обозначенную проблему.

Следующая проблема касается возраста, в котором лицу может быть реализована алкогольная продукция. Сейчас этот возраст составляет 18 лет. Однако многие, например Ю. А. Коробейник, считают, что для достижения целей деалкоголизации общества необходимо в числе прочего введение запрета на продажу алкоголя лицам, не достигшим 21-летнего возраста. Приводятся примеры Японии, Индонезии, Пакистана, где алкоголь запрещен лицам до 20 лет, а также некоторых штатов Индии — 25 лет [15].

Такие предложения неоднократно вносились в Государственную Думу (в частности, в 2015, 2023 годах). И каждый раз эти законопроекты отклонялись, на что есть основания.

По гражданскому законодательству Российской Федерации общая дееспособность наступает с 18 лет, когда гражданин может «своими действиями приобретать и осуществлять гражданские права, создавать для себя гражданские обязанности и исполнять их» в полном объеме» (ч. 1 ст. 21 Гражданского кодекса Российской Федерации [16]). Следовательно, о повышении возраста, до наступления которого запрещается реализовывать алкогольную продукцию несовершеннолетним, на сегодня ставить вопрос преждевременно. Для того чтобы снизить интерес подростков к алкоголю, было бы полезно установить дополнительные требования к его розничной продаже.

Так, можно закрепить требование продажи алкогольной продукции лишь в специализированных магазинах или отдельных специальных помещениях розничных магазинов, где будет осуществляться продажа данной продукции. С этой целью абзац первый п. 1 ст. 16 Федерального закона № 171-ФЗ следует дополнить словами: «в специализированных магазинах или отдельных специальных помещениях розничных магазинов для продажи алкогольной продукции». Подобное требование в отношении алкогольной продукции выглядит совершенно логично, поскольку уже длительное время запрещена демонстрация продаваемой табачной продукции, однако в тех же самых магазинах на всеобщее обозрение выставляется

вся палитра алкоголя.

Сегодня проблема реализации алкогольной продукции несовершеннолетним не теряет актуальности, несмотря на то, что за последние годы количество рассматриваемых дел по ч. 2.1 ст. 14.16 КоАП РФ все же снижается: в 2023 году было рассмотрено 11 068 дел, в то время как в 2020 году — 15 382 [18]. Серьезным шагом в противодействии алкоголизации несовершеннолетнего населения следует считать ограничение доступности алкогольной продукции и усиление административной ответственности за розничную продажу алкогольной продукции несовершеннолетним с применением предложенных нами мер и совершенствования законодательства.

ЛИТЕРАТУРА

1. Об утверждении Концепции сокращения потребления алкоголя в Российской Федерации на период до 2030 года и на дальнейшую перспективу : распоряжение Правительства РФ от 11 дек. 2023 г. № 3547-р // Собрание законодательства РФ. — 2023. — № 51. — Ст. 9435.

2. О государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции : Федеральный закон от 22 ноября 1995 г. № 171-ФЗ // Собрание законодательства РФ. — 1995. — № 48. — Ст. 455.

3. Кодекс Российской Федерации об административных правонарушениях : Федеральный закон от 30 дек. 2001 г. № 195-ФЗ // Собрание законодательства РФ. — 2002. — № 1. — Ч. 1. — Ст. 1.

4. Об основах государственного регулирования торговой деятельности в Российской Федерации : Федеральный закон от 28 дек. 2009 г. № 381-ФЗ // Собрание законодательства РФ. — 2010. — № 1. — Ст. 2.

5. Андреев Д. В. Административно-правовая защита несовершеннолетних от угроз, исходящих от продажи им алкогольной или иной спиртосодержащей продукции // Юридическая наука и правоохранительная практика. — 2020. — № 4 (54). — С. 94.

6. ГОСТ 59941-2021. Национальный стандарт Российской Федерации. Материалы плодовые сброженные. Общие технические условия : приказ Росстандарта от 15 дек. 2021 г. № 1781-ст. — М. : ФГБУ «РСТ», 2022.

7. О некоторых вопросах, возникающих у судов при применении Особенной части Кодекса Российской Федерации об административных правонарушениях : постановление Пленума Верховного Суда РФ от 24 октября 2006 г. № 18 //

Бюллетень Верховного Суда РФ. — 2006. — № 12.

8. Постановление Автозаводского районного суда Самарской области от 14 февраля 2017 г. № 5-460/2017. — URL: <https://sudpraktika.cloud/precedent/317431.html>

9. Обобщение судебной практики Судебного участка № 1 мирового судьи Переволоцкого района Оренбургской области по делам об административных правонарушениях, предусмотренных ч. 2.1 ст. 14.16 КоАП РФ за 2020, 2021 гг. и 9 мес. 2022 г. — URL: <https://perv1.kodms.ru/press>

10. Джамирзе Б. Ю. Административная ответственность юридических лиц за нарушения лицензионных правил по новому проекту КОАП РФ // Правовая политика и правовая жизнь. — 2021. — № 1. — С. 116.

11. Фаисханов Р. Р. К вопросу о регламентации аннулирования лицензии как меры административной ответственности на примере законодательства о лицензировании в области оборота оружия // Вестник Саратовской государственной юридической академии. — 2021. — № 3 (140). — С. 110—111.

12. Бадулин А. Д. Административная ответственность за нарушения порядка производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции : автореф. дис. ... канд. юрид. наук. — М., 2013.

13. Об отказе в принятии к рассмотрению жалобы гражданина Амирова Анвара Каримовича на нарушение его конституционных прав пунктом 2 статьи 119 и пунктом 1 статьи 122 Налогового кодекса Российской Федерации : определение Конституционного Суда РФ от 16 января 2009 г. № 146-О-О. — URL: <https://legalacts.ru/doc/opredeleniekonstitutsionnogo-suda-rf-ot-16012009-n/>

14. Новичкова Е. Е. Вопросы противодействия незаконному обороту алкогольной продукции // Вестник Восточно-Сибирского института МВД России. — 2016. — № 1 (76). — С. 54.

15. Коробейник Ю. А. Анализ применения судами общей юрисдикции части 2.1 статьи 14.16 КоАП РФ (розничная продажа несовершеннолетнему алкогольной продукции) // Вопросы российской юстиции. — 2021. — № 16. — С. 468.

16. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ // Собрание законодательства РФ. — 1994. — № 32. — Ст. 3301.

17. Об утверждении перечня документов, позволяющих установить возраст покупателя алкогольной продукции, которые продавец вправе по-

требовать в случае возникновения у него сомнения в достижении этим покупателем совершеннолетия, и признании утратившим силу приказа Минпромторга России от 15 апреля 2011 г. № 524 «Об утверждении Перечня документов, удостоверяющих личность и позволяющих установить возраст покупателя алкогольной продукции, которые продавец вправе потребовать в случае возникновения у него сомнения в достижении этим покупателем совершеннолетия» : приказ Минпромторга России от 31 мая 2017 г. № 1728 // Рос. газ. — 2017. — 28 июня.

18. Судебная статистика РФ. Административные правонарушения. Показатели по отдельным правонарушениям // URL: <https://stat.апи-пресс.пф/stats/adm/t/31/s/1>

REFERENCES

1. Ob utverzhdenii Konceptii sokrashcheniya potrebleniya alkogolya v Rossijskoj Federacii na period do 2030 goda i na dal'nejshuyu perspektivu : rasporyazhenie Pravitel'stva RF ot 11 dek. 2023 g. № 3547-r // Sobranie zakonodatel'stva RF. — 2023. — № 51. — St. 9435.

2. O gosudarstvennom regulirovanii proizvodstva i oborota etilovogo spirta, alkogol'noj i spirtosoderzhashchej produkcii i ob ogranichenii potrebleniya (raspitiya) alkogol'noj produkcii : Federal'nyj zakon ot 22 noyabrya 1995 g. № 171-FZ // Sobranie zakonodatel'stva RF. — 1995. — № 48. — St. 455.

3. Kodeks Rossijskoj Federacii ob administrativnyh pravonarusheniyah : Federal'nyj zakon ot 30 dek. 2001 g. № 195-FZ // Sobranie zakonodatel'stva RF. — 2002. — № 1. — Ch. 1. — St. 1.

4. Ob osnovah gosudarstvennogo regulirovaniya torgovoj deyatel'nosti v Rossijskoj Federacii : Federal'nyj zakon ot 28 dek. 2009 g. № 381-FZ // Sobranie zakonodatel'stva RF. — 2010. — № 1. — St. 2.

5. Andreev D. V. Administrativno-pravovaya zashchita nesovershennoletnih ot ugroz, iskhodyashchih ot prodazhi im alkogol'noj ili inoj spirtosoderzhashchej produkcii // Yuridicheskaya nauka i pravoohranitel'naya praktika. — 2020. — № 4 (54). — S. 94.

6. GOST 59941-2021. Nacional'nyj standart Rossijskoj Federacii. Materialy plodovye sbrozhennye. Obschie tekhnicheskie usloviya : prikaz Rosstandarta ot 15 dek. 2021 g. № 1781-st. — M. : FGBU «RST», 2022.

7. O nekotoryh voprosah, vznikayushchih u sudov pri primenenii Osobennoj chasti Kodeksa Rossijskoj Federacii ob administrativnyh pravonarusheniyah : postanovlenie Plenuma Verhovnogo Suda RF ot 24 oktyabrya 2006 g. № 18 // Byulleten' Verhovnogo Suda RF. — 2006. — № 12.

8. Postanovlenie Avtozavodskogo rajonnogo suda Samarskoj oblasti ot 14 fevralya 2017 g. № 5-460/2017. — URL: <https://sudpraktika.cloud/precedent/317431.html>

9. Obobshchenie sudebnoj praktiki Sudebnogo uchastka № 1 mirovogo sud'i Perevolockogo rajona Orenburgskoj oblasti po delam ob administrativnyh pravonarusheniyah, predusmotrennyh ch. 2.1 st. 14.16 KoAP RF za 2020, 2021 gg. i 9 mes. 2022 g. — URL: <https://perv1.kodms.ru/press>

10. Dzhamirze B. Yu. Administrativnaya otvetstvennost' yuridicheskikh lic za narusheniya licenзионных правил по новому проекту КОАП РФ // Pravovaya politika i pravovaya zhizn'. — 2021. — № 1. — S. 116.

11. Faiskhanov R. R. K voprosu o reglamentacii annulirovaniya licenzii kak mery administrativnoj otvetstvennosti na primere zakonodatel'stva o licenzirovani v oblasti oborota oruzhiya // Vestnik Saratovskoj gosudarstvennoj yuridicheskoy akademii. — 2021. — № 3 (140). — S. 110—111.

12. Badulin A. D. Administrativnaya otvetstvennost' za narusheniya poryadka proizvodstva i oborota etilovogo spirta, alkogol'noj i spirtosoderzhashchej produkcii : avtoref. dis. ... kand. yurid. nauk. — M., 2013.

13. Ob otkaze v prinyatii k rassmotreniyu zhaloby grazhdanina Amirova Anvara Karimovicha na narushenie ego konstitucionnyh prav punktom 2 stat'i 119 i punktom 1 stat'i 122 Nalogovogo kodeksa Rossijskoj Federacii : opredelenie Konstitucionnogo Suda RF ot 16 yanvarya 2009 g. № 146-O-O. — URL: <https://legalacts.ru/doc/opredeleniekonstitucionnogo-suda-rf-ot-16012009-n/>

14. Novichkova E. E. Voprosy protivodejstviya nezakonnomu obrotu alkogol'noj produkcii // Vestnik Vostochno-Sibirskogo instituta MVD Rossii. — 2016. — № 1 (76). — S. 54.

15. Korobejnik Yu. A. Analiz primeneniya sudami obshchej yurisdikcii chasti 2.1 stat'i 14.16 KoAP RF (roznichnaya prodazha nesovershennoletnemu alkogol'noj produkcii) // Voprosy rossijskoj yusticii. — 2021. — № 16. — S. 468.

16. Grazhdanskij kodeks Rossijskoj Federacii (chast' pervaya) ot 30 noyabrya 1994 g. № 51-FZ // Sobranie zakonodatel'stva RF. — 1994. — № 32. — St. 3301.

17. Ob utverzhdenii perechnya dokumentov, pozvolyayushchih ustanovit' vozrast pokupatelya alkogol'noj produkcii, kotorye prodavec vprave potrebovat' v sluchae vozniknoveniya u nego somneniya v dostizhenii etim pokupatelem sovershennoletiya, i

priznanii utrativshim silu prikaza Minpromtorga Rossii ot 15 aprelya 2011 g. № 524 «Ob utverzhdenii Perechnya dokumentov, udostoverayushchih lichnost' i pozvolyayushchih ustanovit' vozrast pokupatelya alkogol'noj produkcii, kotorye prodavec vprave potrebovat' v sluchae vozniknoveniya u nego somneniya v dostizhenii etim pokupatelem sovershennoletiya» : prikaz Minpromtorga Rossii ot 31 maya 2017 g. № 1728 // Ros. gaz. — 2017. — 28 iyunya.

18. Sudebnaya statistika RF. Administrativnye pravonarusheniya. Pokazateli po otдел'nyim pravonarusheniyam // URL: <https://stat.api-press.rf/stats/adm/t/31/s/1>

СВЕДЕНИЯ ОБ АВТОРЕ

Антонова Лариса Борисовна. Старший преподаватель кафедры административного права. Воронежский институт МВД России.
E-mail: larisa.antonova1511@rambler.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Antonova Larisa Borisovna. Senior lecturer of the chair of Administrative Law.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: larisa.antonova1511@rambler.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: несовершеннолетние; административная ответственность; реализация алкогольной продукции; совершенствование правового регулирования.

Key words: minors; administrative responsibility; sale of alcoholic beverages; improvement of legal regulation.

УДК 342.9

Г. Н. Волкодавова, адъюнкт

ПЕРСОНАЛЬНАЯ ОТВЕТСТВЕННОСТЬ РУКОВОДИТЕЛЯ ТЕРРИТОРИАЛЬНОГО ОРГАНА ВНУТРЕННИХ ДЕЛ ПРИ ПРИНЯТИИ УПРАВЛЕНЧЕСКОГО РЕШЕНИЯ

PERSONAL RESPONSIBILITY OF THE HEAD OF THE TERRITORIAL BODY OF INTERNAL AFFAIRS WHEN MAKING A MANAGERIAL DECISION

В статье рассмотрена персональная ответственность руководителя органа внутренних дел при принятии управленческого решения, проанализированы понятия управленческого решения и персональной ответственности, выявлены специфические проблемы, связанные с принятием управленческого решения и ответственностью руководителя. Предложена формулировка понятия «персональная ответственность руководителя территориального органа внутренних дел».

The article examines the personal responsibility of the head of the internal affairs body when making a managerial decision, analyzes the concepts of managerial decision and personal responsibility, and identifies specific problems related to managerial decision-making and executive responsibility. The formulation of the concept "personal responsibility of the head of the territorial body of internal affairs" is proposed.

Защита прав и интересов человека и гражданина, развитие общества, основанного на законе, в настоящее время одна из важнейших задач цивилизованного государства. Укрепление законности и правопорядка, борьба с преступностью, вышедшей на новый, цифровой, уровень, воспитание подрастающего поколения, обеспечение контроля миграционных потоков и миграционных отношений, внедрение новых форм учетов для защиты информации и т. д. в системе Министерства внутренних дел России (далее — МВД России) на сегодняшний день обращают на себя пристальное внимание. Преступность, как и любой другой вид правонарушения, обусловлена не только социально-экономическими проблемами, но и личными. Искажённое представление о правильном поведении в обществе, необразованность молодежи и допущенные проблемы в воспитании делают преступность социальным явлением.

При реализации своих полномочий МВД России учитывает формы и методы своей работы, и результат направлен на борьбу за цивилизованное отношение людей друг к другу, за активную жизненную позицию, за развитие правовой культуры и государства в целом. Правовая социализация в данном случае представлена усвоением личностью правовых норм, умением выстраивать свои потребности в соответствии с законом и при этом превращать их в образ жизни и поведения. И роль полиции в данном контексте становится более

ориентирована на оказание разного вида услуг гражданскому обществу.

В свою очередь, успехом в реализации таких полномочий можно считать эффективное государственное управление, при этом вопросам регулирования государственной службы уделяется много внимания. Государственная служба в ОВД — не исключение, профессионализм и компетентность государственных служащих являются залогом сохранения правопорядка в государстве. В данном случае правоохранительным органам, как органам государственной власти, отведена немаловажная роль, т. к. служба в органах внутренних дел (далее — ОВД) есть вид федеральной государственной службы, представляющий собой профессиональную служебную деятельность граждан Российской Федерации на должностях в органах внутренних дел Российской Федерации [1]. Если обратиться к основным принципам построения и функционирования системы государственной службы, можно выделить несколько основных, таких как законность, равный доступ граждан к гражданской службе, открытость государственной службы и ее доступность общественному контролю, объективное информирование общества о деятельности государственных служащих и т. д. [2].

Проблемой формирования и совершенствования работы с кадрами, их воспитания, образования, обучения, развития, а также повышения эффективности оперативно-служебной и служебно-

боевой деятельности занимались такие ученые, педагоги и психологи, как В. Я. Кикоть, А. М. Столяренко, Ю. Н. Стариков и др.

Служба в ОВД на должностях младшего, среднего и высшего начальствующего состава требует неукоснительного соблюдения правовых норм. В служебной деятельности сотрудник полиции ставит государственные интересы выше своих [3].

Формирование и развитие управленческого поведения руководителя актуальны в МВД России и достаточно глубоко прорабатываются в отечественной науке и практике. Социальные изменения в обществе требуют поиска новых способов управления, это необходимо для достижения профессиональных целей и задач руководителями среднего и высшего звена при реализации своих полномочий. Качество управления, т. е. способность принятия верного управленческого решения, напрямую зависит от сформированности личности руководителя. Для принятия эффективного управленческого решения в разрешении актуальных и сложных служебных задач руководитель наряду с высоким профессионализмом и знаниями в области управления обязан обладать и управленческой компетентностью, что отражено в Кодексе этики и служебного поведения сотрудников органов внутренних дел Российской Федерации.

Наше внимание привлекает тот факт, что порядок правомерной работы и ответственность за ее соответствие закону в системе МВД России возлагается на руководителя органа. Данное правило закреплено в пункте 3 Наставления по организации правовой работы, утвержденного приказом МВД России от 5 января 2007 г. № 6 [4].

Перечень полномочий руководителя органа внутренних дел достаточно велик, от планирования мероприятий по правовому обеспечению служебной деятельности; осуществления координации правовой работы в органе (подразделении); издания в пределах предоставленных полномочий правовых актов; осуществления контроля за состоянием правовой работы в органе (подразделении) до осуществления организационно-штатного, материально-технического и кадрового обеспечения правовой работы с учетом ее специфики и объемов.

Полномочия требуют не только неукоснительного исполнения, но и принятия управленческого решения в процессе организации работы. В данном случае ответственность наступает как за действие, так и бездействие должностного лица. Дисциплинарным уставом, а именно главой 3, четко прописываются обязанности руководителя по поддержанию служебной дисциплины, служебная дисциплина в органах внутренних дел в

свою очередь — это соблюдение сотрудником установленных законодательством Российской Федерации, Присягой сотрудника органов внутренних дел Российской Федерации, Уставом, контрактом, а также приказами и распоряжениями Министра внутренних дел Российской Федерации, приказами и распоряжениями прямых и непосредственных руководителей (начальников) порядка и правил выполнения служебных обязанностей и реализации предоставленных сотруднику прав [5].

Среди полномочий руководителя территориального органа внутренних дел выделим те, которые определяют его права и обязанности по поддержанию служебной дисциплины: создавать условия для соблюдения подчиненными законодательства, служебной дисциплины; отдавать приказы и распоряжения подчиненным, проверять точность и своевременность их исполнения; следовать установленному порядку и условиям прохождения службы в органах внутренних дел, уважать честь и достоинство подчиненных, не допускать ущемления их законных прав и интересов, преследования сотрудников по мотивам личного характера; принимать меры по противодействию коррупции; знать и анализировать состояние служебной дисциплины; всесторонне изучать личные и деловые качества подчиненных; создавать необходимые условия для службы, отдыха и повышения квалификации подчиненных, профессиональной служебной и физической подготовки; обеспечивать гласность и объективность в оценке служебной деятельности подчиненных; воспитывать у подчиненных чувство ответственности за выполнение служебных обязанностей; подавать личный пример дисциплинированности, образцового выполнения служебных обязанностей; принимать меры по выявлению, пресечению и профилактике нарушений служебной дисциплины сотрудниками, а также служебных причин их совершения [5]. Перечень полномочий указывает на то, что сущность принятия управленческого решения направлена на выработку комплексного подхода к достижению служебных целей с возможностью воздействия на все элементы системы правоохранительных органов, включая сотрудников подразделения территориального органа в целом, с целью организации их деятельности и согласованного выполнения поставленных перед МВД России задач.

Именно руководитель несет ответственность за все направления деятельности не только территориального отдела, подразделения, но и каждого сотрудника, и здесь ст. 9 Дисциплинарного устава четко указывает на персональную ответственность за поддержание служебной дисциплины во вверенном ему органе внутренних дел.

При выполнении своих служебных обязанностей руководитель территориального отдела органов внутренних дел ежедневно принимает не одно управленческое решение, используя при этом такие человеческие качества, как самооценка и решительность, а также ответственность, которая часто употребляется в контексте с персональной.

Под самооценкой, в свою очередь, стоит считать возможность личностью оценивать себя, свои возможности среди других людей. Самооценка, являясь центром личности, влияет на ее поведение, эффективность деятельности и ее развитие в целом [6].

Способность человека самостоятельно принимать ответственные решения и неуклонно реализовывать их в деятельности является решительностью. Основное проявление решительности всегда связано со сложными ситуациями, в которых необходимо делать выбор, принимая решение, когда совершенный поступок связан с риском и личным выбором [6]. Таким образом, ответственность — это осуществляемый в различных формах контроль над деятельностью субъекта с точки зрения выполнения им принятых норм и правил. Ответственность личности перед обществом характеризуется сознательным соблюдением моральных принципов и правовых норм, выражающих общественную необходимость, ответственность как черта личности формируется в процессе совместной деятельности в результате интериоризации социальных ценностей, норм и правил [6].

Понятия «решение» и «персональная ответственность», на наш взгляд, тесно связаны друг с другом. Процесс принятия управленческого решения сложен ввиду того, что состоит из нескольких этапов. Во-первых, это личное волеизъявление руководителя, которое направлено в сторону соблюдения служебной дисциплины, улучшения правовой работы. Во-вторых, это метод и подход к решению той или иной проблемы или ситуации при организации работы во вверенном ему органе. В-третьих, это отношение должностного лица, принимающего решение, к его возможному результату и ответственность за него.

Управленческое решение есть акт волеизъявления компетентного (уполномоченного в определенной сфере деятельности) должностного лица, адресованного объекту управления, о необходимости выполнения последним конкретных действий [7]. Само же управленческое решение всегда представлено в виде указания, приказа или распоряжения, и поэтому постановка правильной задачи начинается именно с выбора решения, а итог — обязательное его выполнение.

Анализируя государственное управление в органах внутренних дел, основой которого являются право и закрепленные законодательно отношения подчинения, базирующиеся на единоначалии и вертикали власти, можно выделить то обстоятельство, что любое принятое управленческое решение подлежит выполнению, даже если оно доведено как просьба или рекомендация. Однако решение, адресованное подчиненному, является обязательным к исполнению только в том случае, если оно отдано должностным лицом в пределах его компетенции, оформлено в установленной законом форме и не противоречит законодательству. Подход к принятию управленческого решения есть непосредственное выполнение действий, связанных с возможностью достижения цели, заложенной как в самом указании, так и в понимании его результата. Принятие решения традиционно рассматривается как определенный этап волевого акта; оно включает в себя появление психических новообразований в виде новых целей, оценок, мотивов и установок [8]. Можно определить решение с данной точки зрения как движение или путь к достижению определенной цели при помощи выстроенной стратегии с последующим положительным результатом.

Рассматривая управленческое решение через условие и меру ответственности, стоит обратить внимание на то, что подчиненный сотрудник, приводя в исполнение принятое руководителем ОВД решение, при неудовлетворительном результате ответственности не несет. Такая ответственность возложена на должностное лицо, давшее указание и принявшее соответствующее управленческое решение за его исполнение, результат и последствия.

Принятие управленческого решения напрямую связано с умением оценить оперативную обстановку и служебную дисциплину во вверенном органе внутренних дел, в рамках и под влиянием которых оно будет выполняться. Оперативная обстановка есть качественно однородная (с точки зрения достижения поставленной цели) и тем самым формально отграниченная от общей действительности система объектов, процессов, явлений, их взаимосвязей и взаимодействий, динамично изменяющаяся с течением времени под воздействием различного рода факторов [7]. В связи с этим руководитель перед принятием решения должен осознавать ответственность, которая может наступить и в любом случае наступит, если решение будет принято неверно.

Правильность принятия решения зависит от оценки оперативной обстановки, в которой необходимо принять решение, от задачи, которую необходимо выполнить в условиях сложившейся

обстановки, выбора способа устранения проблемы, который в свою очередь должен быть представлен несколькими вариантами достижения ее решения, а также вариантом выбора управленческого решения и сформировавшейся персональной ответственностью, которая должна быть уже сформулирована самим должностным лицом, принявшим управленческое решение.

Важно понимать, что руководитель территориального органа внутренних дел самостоятельно возлагает на себя ответственность за выполнение принятого им решения, тем самым закрепляя за собой персональную ответственность. Правовая основа ответственности изложена в п. 1 ст. 42 УК РФ: не является преступлением причинение вреда охраняемым уголовным законом интересам лицом, действующим во исполнение обязательных для него приказа или распоряжения. Уголовную ответственность за причинение такого вреда несет лицо, отдавшее незаконные приказ или распоряжение [9]. Согласно статье 2.4 (КоАП РФ), должностное лицо несёт административную ответственность, если совершает правонарушение в связи с неисполнением либо ненадлежащим исполнением своих служебных обязанностей [10].

Как мы видим, ответственность руководителя территориального органа внутренних дел при принятии управленческого решения определяется законодательством РФ, ведомственными нормативными актами МВД России, а также общими принципами управленческой ответственности. При рассмотрении персональной ответственности стоит учесть виды ответственности, которые могут быть применимы к сотруднику полиции, в том числе и руководителю территориального ОВД. Нарушением служебной дисциплины признается виновное действие (бездействие), выразившееся в нарушении сотрудником органов внутренних дел законодательства Российской Федерации, дисциплинарного устава органов внутренних дел Российской Федерации, должностного регламента (должностной инструкции), правил внутреннего служебного распорядка федерального органа исполнительной власти в сфере внутренних дел, его территориального органа или подразделения, либо в несоблюдении запретов и ограничений, связанных со службой в органах внутренних дел, и требований к служебному поведению, либо в неисполнении (ненадлежащем исполнении) обязательств, предусмотренных контрактом, служебных обязанностей, приказов и распоряжений прямых руководителей (начальников) и непосредственного руководителя (начальника) при выполнении основных обязанностей и реализации предоставленных прав [1].

Руководитель территориального ОВД может быть подвержен дисциплинарной ответственности за различные нарушения служебной дисциплины, которые могут проявляться в нескольких формах. Рассмотрим некоторые из них.

Во-первых, это ситуации, когда он совершает виновные действия или, напротив, бездействует, что приводит к нарушению прав и свобод граждан. Подобные действия могут угрожать жизни и здоровью людей, создавать препятствия в работе или даже останавливать деятельность федерального органа исполнительной власти в области внутренних дел, его территориального подразделения или отдельных служб. Кроме того, эти действия могут причинять значительный вред как гражданам, так и организациям, при этом не влекут за собой уголовной ответственности.

Во-вторых, это разглашение служебной информации, которая подлежит охране законом, включая государственную тайну, ставшую известной ему в процессе выполнения своих должностных обязанностей. Если такое разглашение не приводит к уголовной ответственности, то оно, тем не менее, может стать основанием для дисциплинарного взыскания.

В-третьих, умышленное уничтожение или повреждение имущества, которое находится в оперативном управлении федерального органа внутренних дел, его территориального органа или подразделения. Если такие действия наносят значительный ущерб и не влекут за собой уголовной ответственности, это также может стать поводом для привлечения к дисциплинарной ответственности.

В-четвертых, нарушение требований охраны труда и профессиональной служебной деятельности. Если данное нарушение приводит к серьезным последствиям, таким как несчастные случаи на службе, пожары, аварии или катастрофы, либо создает реальную угрозу их возникновения, это также может стать причиной дисциплинарного взыскания, при условии, что такие действия не влекут уголовной ответственности.

В-пятых, принятие необоснованных решений, которые могут привести к нарушению сохранности имущества, находящегося в оперативном управлении соответствующего органа. Если такое решение повлечет за собой ущерб, это может стать основанием для дисциплинарного взыскания.

Заметим, что руководитель территориального ОВД несет значительную ответственность за свои действия и решения, которые могут повлиять на работу всей структуры, а также на права и безопасность граждан. Перечисленные основания подчеркивают важность соблюдения служебной дисциплины и профессиональных стандартов в работе органов внутренних дел. Важно понимать,

что привлечение к дисциплинарной ответственности не только служат наказанием за нарушение, но и направлено на поддержание порядка и законности в деятельности правоохранительных органов, что в свою очередь способствует укреплению доверия общества к МВД в целом.

Нарушение служебной дисциплины влечет за собой следующие дисциплинарные взыскания: замечание; выговор; строгий выговор; предупреждение о неполном служебном соответствии; перевод на нижестоящую должность в органах внутренних дел; увольнение со службы в органах внутренних дел.

Кроме того, за нарушение действующего законодательства руководитель может быть привлечен не только к административной и уголовной, но и гражданско-правовой ответственности.

Например, административная ответственность наступает в случае нарушения КоАП РФ. Нарушение статей главы 12, части 7 статьи 14.32, частей 1 и 3 статьи 17.14, статей 19.5.7, 19.7.2, части 5 статьи 19.8, статьи 19.12, статьи 20.4 (в части нарушения требований пожарной безопасности вне места военной службы (службы) или прохождения военных сборов). Сотрудник ОВД несет ответственность на общих основаниях.

Уголовная ответственность наступает за злоупотребление должностными полномочиями (ст. 285 УК РФ), за халатность (ст. 293 УК РФ), если решение привело к тяжким последствиям, за коррупционные преступления (взяточничество, ст. 290 УК РФ) [9].

Кроме того, как было указано выше, в отношении руководителя может быть применена при причинении ущерба принятым им решением

гражданско-правовая ответственность, и ярким примером могут служить обстоятельства, прописанные в ст. 1069 ГК РФ — ответственность государства, но возможен регрессный иск к руководителю.

Критериями оценки таких решений служат: нарушение закона или приказа МВД России, ущерб для государства, граждан или сотрудников, принятие решения с превышением полномочий или без должного обоснования.

Необходимым контролем в данном случае выступает ведомственный контроль в виде проверок МВД России, Прокуратуры, Следственного комитета, судебные иски (оспаривание решений в суде), общественный контроль, который сейчас набирает свои обороты (жалобы граждан, СМИ).

Нарушение законодательства и ведомственных приказов зачастую связано именно с неумением принимать управленческое решение в силу неправильно сформированной самооценки руководителя, возможности принимать решение самостоятельно и незнания последствий.

В данном случае недостаточная профессиональная грамотность, низкая мотивация к саморазвитию и неверно подобранный стиль руководства приводят к персональной ответственности.

Исходя из вышесказанного, персональную ответственность руководителя территориального органа внутренних дел можно представить как вид личной ответственности должностного лица, на которое возложена обязанность по принятию управленческого решения, включающая в себя чувство долга, самооценку, решительность и ответственность за последствия, возникающие в результате достижения служебной цели.

ЛИТЕРАТУРА

1. О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 30 ноября 2011 г. № 342-ФЗ. — URL: <https://www.consultant.ru> (дата обращения: 11.01.2025).

2. О системе государственной службы Российской Федерации: Федеральный закон от 27 мая 2003 г. № 58-ФЗ. — URL: <https://www.consultant.ru/document/> (дата обращения: 20.02.2025).

3. 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: 15.01.2025).

4. Об утверждении Наставления по организации правовой работы в системе МВД России :

приказ МВД России от 05.01.2007 № 6 (ред. от 23.12.2021). — URL: <https://www.consultant.ru> (дата обращения: 25.02.2025).

5. О Дисциплинарном уставе органов внутренних дел Российской Федерации : указ Президента РФ от 14 октября 2012 г. № 1377. — URL: <https://www.garant.ru> (дата обращения: 25.02.2025).

6. Психологический словарь / под ред. А. В. Петровского, М. Г. Ярошевского. — М., 1990. — С. 352.

7. Новокшанов О. Н. Управление в правоохранительных органах : учебное пособие. — 2-е изд., перераб. и доп. — М. : ДГСК МВД России. — С. 72.

8. Большой энциклопедический словарь : философия, социология, религия, эзотеризм, политехнология. — М., 2002. — С. 688—689.

9. Уголовный кодекс Российской Федерации : Федеральный закон от 13 июня 1996 г. № 63-ФЗ. — URL: <https://www.consultant.ru> (дата обращения: 09.04.2025).

10. Кодекс Российской Федерации об административных правонарушениях : Федеральный закон от 30 декабря 2001 г. № 195-ФЗ. — URL: <https://www.consultant.ru> (дата обращения: 09.04.2025).

REFERENCES

1. O sluzhbe v organax vnutrennix del Rossijskoj Federacii i vnesenii izmenenij v otдел`ny'e zakonodatel'ny'e akty` Rossijskoj Federacii : Federal'nyj zakon ot 30 noyabrya 2011 g. № 342-FZ. — URL: <https://www.consultant.ru> (data obrashheniya: 11.01.2025).

2. O sisteme gosudarstvennoj sluzhby` Rossijskoj Federacii: Federal'nyj zakon ot 27 maya 2003 g. № 58-FZ. — URL: <https://www.consultant.ru/document/> (data obrashheniya: 20.02.2025).

3. Ob utverzhdenii Kodeksa e`tiki i sluzhebnogo povedeniya sotrudnikov organov vnutrennix del Rossijskoj Federacii : prikaz MVD Rossii ot 26 iyunya 2020 g. № 460. — URL: <https://sudact.ru> (data obrashheniya: 15.01.2025).

4. Ob utverzhdenii Nastavleniya po organizacii pravovoj raboty` v sisteme MVD Rossii : prikaz MVD Rossii ot 05.01.2007 № 6 (red. ot 23.12.2021). — URL: <https://www.consultant.ru> (data obrashheniya: 25.02.2025).

5. O Disciplinarnom ustave organov vnutrennix

del Rossijskoj Federacii: Ukaz Prezidenta RF ot 14 oktyabrya 2012 g. № 1377. — URL: <https://www.garant.ru> (data obrashheniya: 25.02.2025).

6. Psixologicheskij slovar` / pod red. A. V. Petrovskogo, M. G. Yaroshevskogo. — M., 1990. — S. 352.

7. Novokshanov O. N. Upravlenie v pravooxranitel'ny`x organax : uchebnoe posobie. — 2-e izd. pererab. i dop. — M. : DGSK MVD Rossii. — S. 72.

8. Bol'shoj e`nciklopedicheskij slovar` : filologiya, sociologiya, religiya, e`zoterizm, polit`konomiya. — M., 2002. — S. 688—689.

9. Ugolovnyj kodeks Rossijskoj Federacii : Federal'nyj zakon ot 13 iyunya 1996 g. № 63-FZ. — URL: <https://www.consultant.ru> (data obrashheniya: 09.04.2025).

10. Kodeks Rossijskoj Federacii ob administrativny`x pravonarusheniyax : Federal'nyj zakon ot 30 dekabrya 2001 g. № 195-FZ. — URL: <https://www.consultant.ru> (data obrashheniya: 09.04.2025).

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. Pos-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: самооценка; полномочия руководителя; управленческое решение; персональная ответственность.

Key words: self-assessment; authority of the head; managerial decision; personal responsibility.

УДК 342.92

Д. И. Полухин

М. М. Жуков, кандидат технических наук, доцент

А. Ю. Телков, кандидат физико-математических наук, доцент

ПОИСК ТЕКСТОВОЙ ИНФОРМАЦИИ НА ОБЪЕКТАХ КОМПЬЮТЕРНОЙ ПАМЯТИ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

SEARCH OF TEXT INFORMATION ON COMPUTER MEMORY OBJECTS IN THE INVESTIGATION OF CRIMES IN THE SPHERE OF INFORMATION TECHNOLOGIES

Рассмотрены основные виды поиска текстовой информации. Продемонстрированы практические возможности по использованию различных программных средств для поиска текстовой информации при выявлении и раскрытии преступлений в сфере информационных технологий.

The main types of textual information search are considered. Practical possibilities of using various software tools for textual information search in the detection and disclosure of crimes in the field of information technology are demonstrated.

Введение. Одним из способов передачи информации между людьми является текст. Именно поэтому следует отметить, что довольно значительную часть информационных ресурсов современных компьютерных систем составляют тексты. И по этой причине текстовые сообщения являются преобладающим типом в информационных системах.

Как правило, среди информационных систем, имеющих дело с текстовой информацией, наиболее распространенными являются системы текстового поиска. Их задача заключается в том, чтобы находить в хранимом на компьютере массиве данных записей, отвечающих информационным потребностям пользователей. Сам по себе поиск данных представляет собой процесс получения определенной заранее заданной информации из массивов или записей любого вида. В основе поиска лежат алгоритмы и решения, которые предназначены для нахождения в тексте необходимой информации. Операция поиска называется «запросом», а элемент описания, по которому его можно осуществить, — «поисковый элемент».

Текстовый поиск является одной из вариаций задачи поиска информации на машинных носителях. На сегодняшний день различные подразделения правоохранительных органов используют поиск и обнаружение информации для выявления и расследования преступлений. При этом чаще

всего это относится к вопросу компьютерной экспертизы [1]. Задачи текстового поиска заключаются в обнаружении конкретной информации на технических устройствах и их носителях, поиске необходимой информации по определенным признакам [2].

Актуальность данной работы обусловлена тем, что в настоящее время, когда информационные технологии занимают все более важную роль во всех сферах человеческой деятельности, обработка и поиск текстовой информации становится необходимым инструментом для работников различных профессий. Эксперты разных отраслей науки и техники, специалисты в различных областях знаний сталкиваются с необходимостью быстрого и эффективного поиска нужных им данных [3]. Поиск информации играет значительную роль и в подразделениях правоохранительных органов. Он активно используется в целях выявления, расследования и профилактики преступлений. Так, например, стоит отметить, что поиск компьютерной информации по заданным критериям является обширной экспертной задачей, которую решают сотрудники компьютерной лаборатории. Необходимо подчеркнуть, что, в частности, эксперты отвечают на вопросы, решение которых требует применения текстового поиска.

Целью данной работы является анализ возможностей поиска текстовой информации на объектах компьютерной памяти.

Разновидности методов поиска текстовой информации.

Контекстный поиск. Контекстный поиск применяется в том случае, когда возникает необходимость в точном совпадении фразы или группы слов, при этом ключевая фраза заключается в кавычки. В прямом понимании термин «контекстный поиск» подразумевает метод поиска фрагментов текстовых записей, заключающийся в сравнении их с заданной пользователем последовательностью символов. В более широком смысле контекстный поиск предусматривает применение языка регулярных выражений, который использует метасимволы, задает правила поиска (шаблон, маску) и тем самым расширяет спектр искомых вариантов текста. С его помощью можно найти документ, содержащий определенные фразы — достаточно набрать их в поисковом окне. Также важно отметить, что он удобен для реферативного поиска информации, однако данная операция достаточно медленная, и ее выполняют не все поисковые системы [4].

Контекстный поиск информации — это метод поиска, в котором поисковая система анализирует не только ключевые слова, но и контекст запроса, для того чтобы дать наиболее точный результат поиска. Такой анализ может включать в себя использование машинного обучения и искусственного интеллекта. Он может учитывать фразы, смысл запроса, характеристики пользователя, локализацию и другие факторы, что позволяет отображать результаты, наиболее релевантные пользователю. Такой подход улучшает качество результата поиска, позволяя пользователям находить более точную и интересную им информацию.

Средства контекстного поиска позволяют искать документы по содержащимся в них словам и фразам, которые могут объединяться логическими операциями. Полученные результаты ранжируются по релевантности (соответствию критерию поиска) на основе частоты встречаемости слов запроса в найденных документах и во всей коллекции в целом.

Необходимо подчеркнуть, что в контекстном поиске предусматривается представление документа как совокупности всевозможных встречающихся в его тексте слов и словосочетаний, не считая так называемых стоп-слов. Стоп-слова — это служебные слова (предлоги, союзы и т. п.), которые содержатся практически в любом документе и не являются информативными. Поиск документов с такими словами привел бы к выдаче полной коллекции документов в ответ на запрос.

Для обеспечения высокой скорости поиска по совокупности документов предварительно создается индекс, в котором для каждого слова устанавливаются ссылки на все документы, где это слово встречалось. Кроме того, в индексе содержится информация о положении слова в документе, частоте встречаемости и т. п. Все слова в текстовом индексе могут храниться в нормальной форме, что уменьшает его объем в несколько раз. Дополнительно из индекса устраняются часто встречающиеся стоп-слова, не участвующие в поиске. При этом для индексирования документа слова, выделенные из его текста с помощью подерживаемых в системе словарей и грамматического разбора, приводятся сначала к единственному числу, именительному падежу, выделяются корни слов и т. п. Документ считается релевантным, если какие-либо слова или словосочетания из запроса встречаются с точностью до грамматических форм в тексте документа. Иногда используется более жесткий критерий релевантности — вхождение в текст документа всех названных в запросе слов и словосочетаний и т. д.

В настоящий момент контекстный поиск информации активно применяется в различных подразделениях правоохранительных органов. Он используется в целях выявления, расследования и профилактики преступлений. Контекстный поиск оказывается незаменим при поиске криминалистически значимой информации. Контекстный поиск информации в подразделениях правоохранительных органов имеет большую ценность при расследовании различных преступлений. Именно поэтому важно выбирать правильные ключевые слова и критерии поиска, чтобы получить наиболее информативные результаты.

Тематический поиск. Тематический поиск текстовой информации — это метод поиска, в котором пользователь ищет информацию на определенную тему, используя ключевые слова и фразы. Данный поиск ориентирован на нахождение документов по их содержанию, и представляет собой главную поисковую процедуру по выявлению аналогов. Он позволяет найти в коллекции документов как документы по заданной теме, так и связанные с ней по смыслу. В этом методе поиска используются специальные алгоритмы, которые анализируют поисковый запрос и определяют его тематику для нахождения более точных результатов. Данная функция оказывается незаменимой, например, в случае, если пользователь затрудняется точно подобрать ключевые слова или же если он хочет сузить область поиска, уточнив тематику, по которой следует искать документы. Общая схема такого поиска заключается в формулировании некоторого запроса пользователем отно-

сительно содержания документа и отборе из множества доступных документов тех, которые удовлетворяют запросу. Область тематического поиска представляет собой все релевантные предмету поиска (т.е. имеющие наиболее близкое к нему отношение).

Такой вариант поиска уместно проводить перед началом реализации какого-либо решения, для того чтобы своевременно избежать дублирования уже известных решений, принять во внимание все их достоинства и недостатки. Он удобен, прежде всего, тем, что нет необходимости в предварительном разделении документов по различным категориям. Особенно это актуально при значительном объеме доступных документов, высокой динамике их обновления или отсутствии необходимых реквизитов.

Основная проблема такого поиска — это сложность однозначной автоматической интерпретации содержания текстов документов и формулировок информационных потребностей пользователей. Сложность интерпретации затрудняет определение соответствия рассматриваемого документа информационным потребностям пользователя.

Эти проблемы обусловлены отсутствием какой-либо регулярной структуры у текстовых документов на естественном языке. Такие информационные ресурсы принято называть неструктурированными или слабоструктурированными.

Поиск по теме обладает более высокой точностью и полнотой по сравнению с простым контекстным поиском. Так, если контекстный поиск находит все документы, содержащие заданные слова, то тематический поиск возвращает лишь те документы, в которых словам запроса соответствует одна из ключевых тем. Кроме того, он позволяет найти документы, вовсе не содержащие слов из названия заданной темы, однако имеющие к ней отношение. Данная возможность позволяет определить «смысловое окружение» темы в коллекции документов и, уточнив зарос, выбрать требуемую информацию. Например, в ответ на запрос «экспертиза» можно получить следующий список тем: «компьютерная экспертиза», «заключение эксперта», «экспертно-криминалистический центр», «эксперт» и т. д. [5].

Нечеткий поиск. Нечёткий поиск представляет из себя поиск данных, при котором выполняется сопоставление информации заданному образцу или близкому ему значению. Поиск осуществляется с учётом возможных произвольных ошибок в написании ключевого слова и/или целого запроса.

Технология нечеткого поиска позволяет расширять запрос близкими по написанию словами, содержащимися в коллекции документов, по которым ведется поиск. Оригинальный алгоритм

способен найти все лексикографически близкие слова, отличающиеся заменами, пропусками и вставками символов. Алгоритмы нечеткого поиска используются в большинстве современных поисковых систем.

Нечеткий поиск целесообразно применять при поиске слов с опечатками, а также в тех случаях, когда нужно быстро получить ответ на свой запрос, не имея полной информации о том, как именно сформулировать его для нахождения искомого материала. Задачу нечеткого поиска можно сформулировать так: «По заданному слову найти в тексте размера n все слова, совпадающие с этим словом (или начинающиеся с этого слова) с учетом n возможных различий». Например, при запросе «Картина» с учетом трех возможных ошибок, найдутся слова «Картинка», «Корзина», «Сатира», «Квартира», «Машина» и так далее.

Алгоритмы, используемые при реализации нечеткого поиска, основаны на оригинальной системе ассоциативного доступа к словам, содержащимся в текстовом индексе. В качестве единиц поиска используются цепочки букв, составляющих слово. Для ускорения поиска предварительно создается отдельный индекс, содержащий фрагменты слов со ссылками на слова, в которых эти фрагменты встретились. Так находятся слова, фрагменты которых совпадают с фрагментами слова в запросе. Задавая длину фрагментов и их количество в слове, можно регулировать полноту поиска — отбирать слова по степени близости к запросу.

Нечеткий поиск является крайне полезной функцией любой поисковой системы. Однако эффективно реализовать его намного труднее, чем выполнить простой поиск по точному совпадению.

Для того чтобы оценить сходство двух слов в тексте, применяются специальные метрики. Метрикой нечеткого поиска называют функцию расстояния между двумя словами, позволяющую оценить степень их сходства в данном контексте. В качестве метрик используют расстояния Хемминга, Левенштейна, Дамерау — Левенштейна [6].

Полнотекстовый поиск. Полнотекстовым поиском называется автоматический поиск по словам из текста документа. При таком поиске ни объем текста, ни его точность не имеют значения, ведь в данном случае поиск осуществляется по всем словам (всему содержимому документа) и во всех документах. Преимуществом является то, что нет необходимости знать, как и где хранится нужная информация. Кроме того, его главная особенность — быстрый поиск слов в очень больших объемах текстовой информации.

Этот вид поиска основан на автоматической обработке текста. При запросе на поиск тех документов, где встречается конкретное слово, автоматически происходит перебор всего массива документов

и выбор всех тех документов, где это слово встречается. В отличие от других методов полнотекстовый поиск просматривает все слова в документе, показывая при этом более подходящую и точную запрашиваемую информацию.

В общем случае данный поиск использует предварительно построенные индексы. Индексирование (или индексация), совершаемое поисковой машиной, — процесс сбора, сортировки и хранения данных с целью обеспечить быстрый и точный поиск информации.

Сам поиск делится на две больших стадии:

1. Индексация (обработка документов и раскладывание их по специальным структурам индекса, для того чтобы потом можно было быстро осуществить сам поиск),

2. Поиск (применение фильтров, булев поиск, ранжирование и т. д.).

Все слова и фразы, синонимы и прочее в каждом документе, попавшем в архив, индексируются. Получается структурированная база данных, в которой словам и словосочетаниям присвоены точные координаты — документы, в которых они присутствуют. Чтобы найти нужное слово, словосочетание, фразу или целый «кусок» текста, требуется очень мало времени, поскольку поисковая программа работает не с текстами, а именно с индексом. К тому же в самых сложных ситуациях, когда неизвестны ни номер, ни дата, ни другие атрибуты, ни точная фраза, выручает именно возможность полнотекстового поиска.

К тому же на основе полнотекстового поиска могут быть созданы различные методы формирования поисковых запросов. Простейший запрос выглядит следующим образом: найти все документы, содержащие одно слово, например ЭКСПЕРТ. Более сложным вариантом запроса является запрос на поиск всех документов, содержащих два слова, например СТАРШИЙ и ЭКСПЕРТ. Если эти два слова соединены логическим условием И, то будут отобраны только те документы, где есть одновременно оба слова. Если указаны два слова, соединенные логическим условием ИЛИ, то будут отобраны документы, где есть хотя бы одно из этих слов. Такие логические выражения могут быть еще более сложными.

При формировании сложных запросов дополнительно может использоваться признак близости слов. В запросе СТАРШИЙ И ЭКСПЕРТ может быть указано, что слова должны находиться РЯДОМ, например в пределах 2 (или 3) строк.

Полнотекстовый поиск не зависит от субъективных убеждений или ошибок специалистов и всегда по любому слову позволяет получить полный и достоверный список документов, где упоминается искомое слово, это является его основным достоинством, ведь в таком случае ничего не

будет забыто и пропущено. Иначе говоря, получить ответ возможно на любой запрос, который был подготовлен по понятному для пользователя правилу, не зависящему от субъективной позиции обработчика.

Однако, помимо всего прочего, как и у любого вида поиска, у него есть свои недостатки. В первую очередь это большое количество «шума» в полученном списке, то есть наличие файлов, где искомое слово используется не в нужном контексте и т. п. Во-вторых, при таком поиске не будут обнаружены те документы, которые содержат синонимы данного термина. Так, к примеру, задав поиск по аббревиатурам «ОАО», «ООО», невозможно автоматически распознать их расшифровку и получить те документы, где используются выражения «открытое акционерное общество» и «общество с ограниченной ответственностью». Данная проблема не в полной мере решается усложнением задаваемых поисковых выражений, но все же трудно во всех случаях добиться такой же точности и достоверности, как при заранее проделанной «ручной» обработке [7].

Поиск текстовой информации как одна из задач в компьютерной экспертизе. Поиск текстовой информации является одним из важнейших этапов компьютерной экспертизы, который позволяет выявить, собрать и проанализировать различные доказательства, связанные с цифровыми устройствами и файлами. Независимо от области знаний, в которой работает эксперт, обработка и анализ большого объема разнообразной информации являются ключевыми навыками для успешной работы [7].

Одним из основных методов поиска информации является поиск по ключевым словам. Этот подход заключается в том, что эксперт использует эти слова и словосочетания для поиска соответствующей информации. Однако этот подход имеет ряд ограничений, так как он не учитывает контекст, в котором используются ключевые слова, и может привести к получению слишком широкого или узкого набора результатов. Для успешного поиска необходимо учитывать возможность использования синонимов и различных форм одного слова, а также необходимость фильтрации результатов поиска.

Эксперты часто ищут информацию в большом объеме текстов. Они не могут ограничиваться поиском только в одном источнике, так как для получения полной картины нужно использовать данные из разных источников. При этом важным является не только количество найденных документов, но и их качество. Эксперт должен уметь выбирать и анализировать только те источники, которые действительно имеют значение для его работы.

Обычно в экспертной деятельности требуется проводить поиск текстовой информации, для которого существует множество методов и инструментов. Определение оптимального метода зависит от характера необходимой информации и особенностей работы эксперта [8].

Обзор поиска по образцу при помощи поисковой программы Total Commander. Total Commander — инструмент, предназначенный для выполнения операций с важными пользовательскими файлами и каталогами. Одной из главных его функций является обнаружение нужных фрагментов текста среди огромного количества файлов, при этом встроенная в него функция позволяет быстро просмотреть содержимое файла без его открытия. Данная возможность позволяет эксперту находить необходимые места в документе, которые связаны с определенным случаем или делом.

В данном файловом менеджере реализованы различные варианты поиска: быстрый поиск, по-

иск файлов, дубликатов файлов, пустых папок. Вдобавок в возможности Total Commander входит осуществление поиска в архивах. Файлы с расширениями ARJ, GZ, ZIP, LZH, RAR, 7Z, TAR, CAB, ACE распаковываются в оперативной памяти, в них производится поиск, после чего данные файлы удаляются. Рассмотрим несколько примеров применения программы Total Commander.

1. «Поиск файлов». Данная команда позволяет найти файлы по заданным параметрам. В опциях вкладки возможно задавать поиск файлов по их полному или сокращенному наименованию, по содержимому файлов, определять директорию и глубину вложенности каталогов.

В данном случае, задав определенные параметры, а именно указав необходимые расширения, мы получим список путей к файлам, внутри которого мы сможем найти нужные нам. Результат поиска по расширениям приведен на рисунке 1.

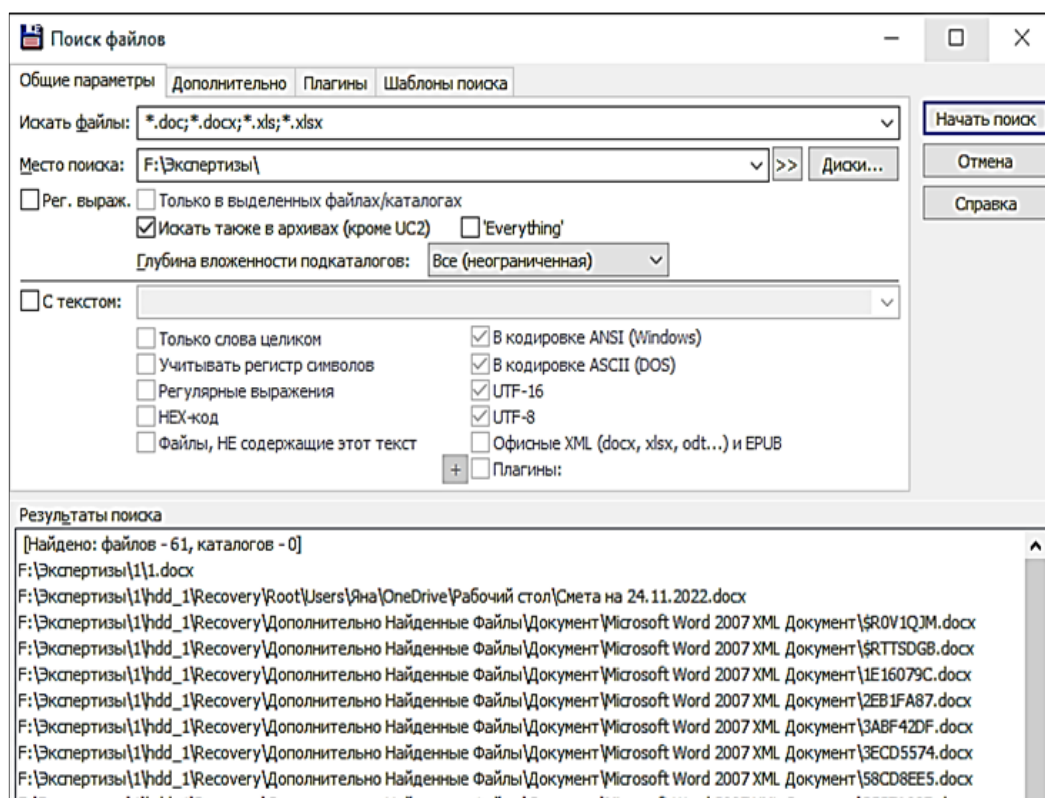


Рис. 1. Поиск файлов по расширениям

2. «Поиск по содержимому». Зная, в каком каталоге находится необходимый документ, мы можем при помощи ключевых фраз найти его. В данном случае производится поиск по ключевому

слову «ЕХХЕ» по указанному нами пути: «F:\Экспертизы\Примеры\Системные_блоки». Результат показал, что искомые файлы в данном каталоге найдены не были (см. рис. 2).

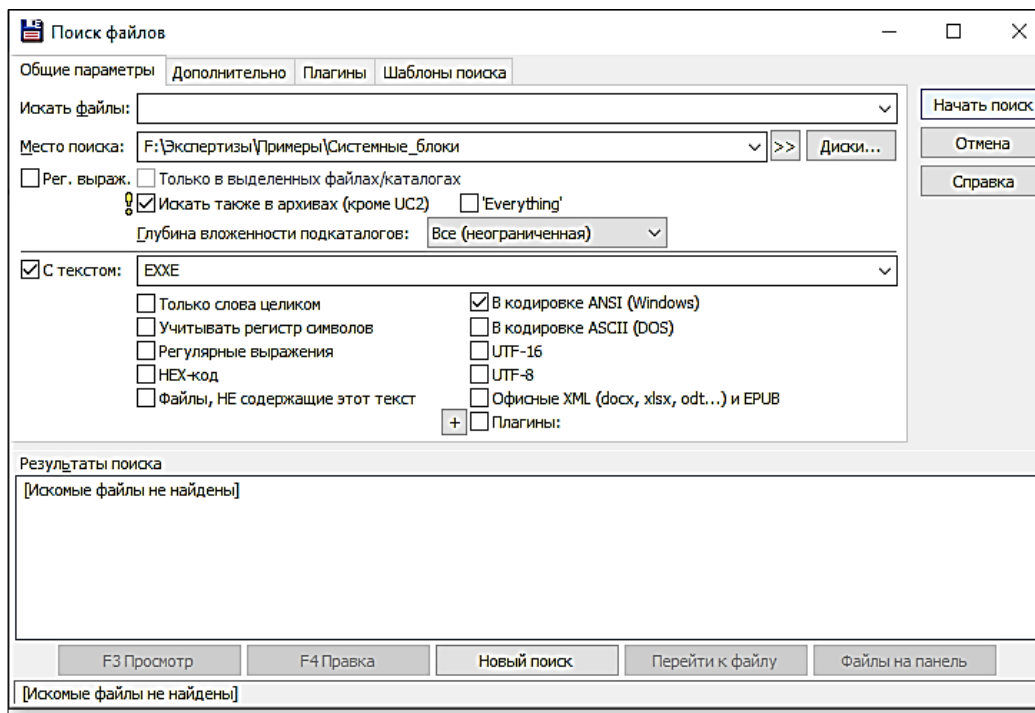


Рис. 2. Поиск по содержанию

Данная проблема возникла из-за несовпадения кодировок. При проверке таким же образом

кодировок Unicode (UTF-8, UTF-16) никакие файлы также обнаружены не были (см. рис. 3).

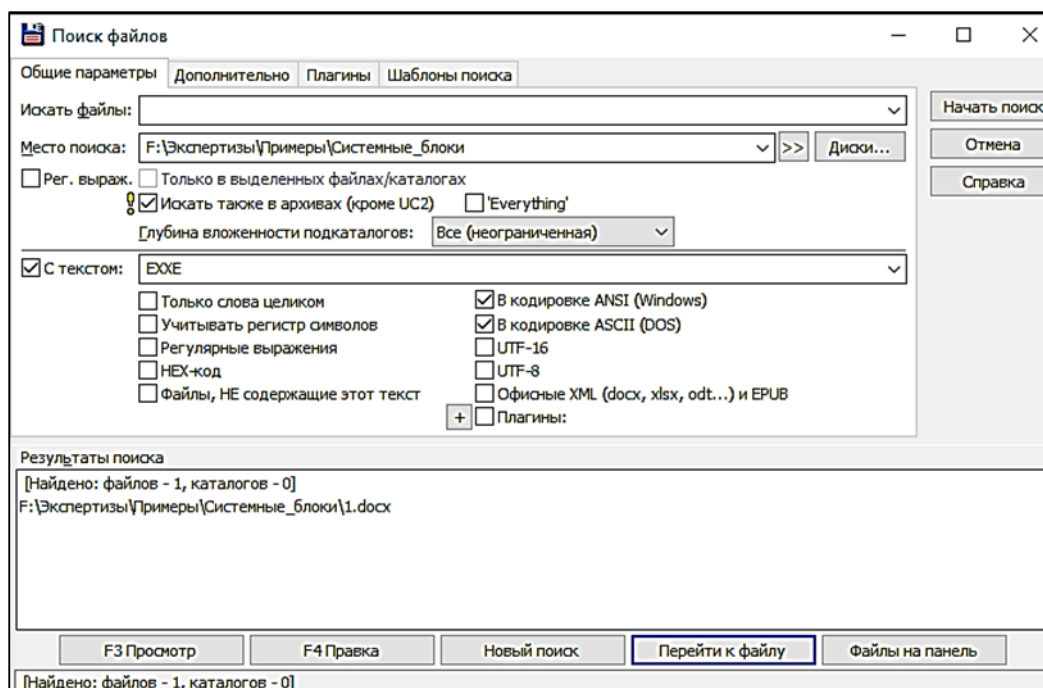


Рис. 3. Проверка других кодировок

Устраняя этот момент и отмечая необходимые кодировки, мы видим, что в результате по-

иска был найден файл, содержащий указанное нами ключевое слово «EXXE» (см. рис. 4).

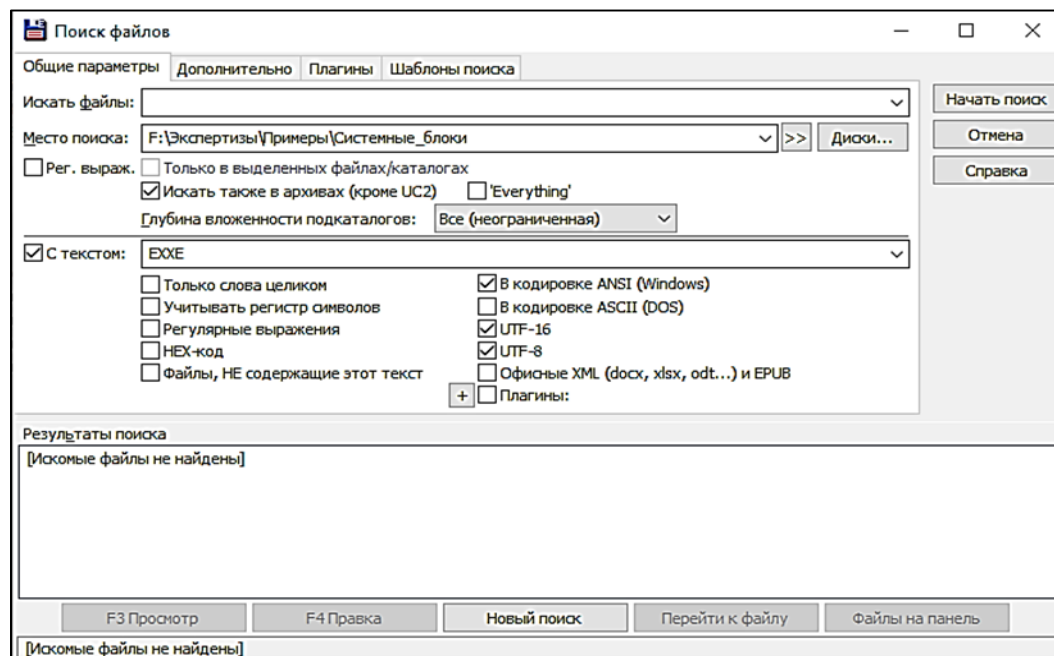


Рис. 4. Поиск файлов, содержащих ключевое слово «EXXE»

Вместе с тем необходимо отметить тот факт, что в данном случае осуществлялся и поиск в архивах, именно поэтому файл с расширением docx был найден.

Таким образом, можно выделить основные преимущества и недостатки поиска информации в программе Total Commander. Основными плюсами является то, что он позволяет осуществлять поиск в архивах и, кроме того, является минимальным доступным инструментом. Главный минус заключается в том, что в данной программе отсутствует поиск в закодированных файлах: doc, pdf, почтовых архивах, с базы данных.

Варианты поиска конкретного слова в тексте. Поиск конкретного слова в документах на экспертной практике может осуществляться несколькими способами в зависимости от того, какие инструменты доступны и насколько точно необходимо провести поиск. Перед поиском необходимо определиться с критериями, которыми руководствуются эксперты при оценке документов. Можно выделить такие критерии, как наличие ключевых слов, релевантность текста, источник информации и т. д. Такие критерии помогают эксперту быстрее находить необходимую информацию в рассматриваемых документах.

Для того чтобы найти определенное слово в документе, можно воспользоваться поиском в

тексте, который есть в большинстве текстовых редакторов, программ для просмотра pdf-файлов и других приложениях. Это является одним из самых простых способов поиска необходимой информации в файле.

Процедура поиска определённого слова в документе обычно выглядит следующим образом:

1. Открываем нужный файл, в котором хотим выполнить поиск.
2. Нажимаем клавишу «Ctrl» и клавишу «F» (в Windows) или «Cmd» и «F» (на Mac) на клавиатуре.
3. В открывшемся окне вводим ключевое слово, которое мы ищем.
4. Нажимаем кнопку «Найти» или «Find».
5. Приложение найдет первый экземпляр ключевого слова в документе. Если мы хотим найти другие экземпляры, то нажимаем на кнопку «Далее» или «Next» в поисковом окне.

Если же мы собираемся найти не только полное слово, но и его вхождения в других словах, то необходимо использовать расширенный поиск и поставить один из знаков «*»/«?» после ключевого слова. Это поможет найти все вхождения введенного ключевого слова в документе.

Если требуется провести поиск в большом количестве документов, этот метод может оказаться слишком трудоемким. В этом случае эксперты применяют специализированное программное

обеспечение, которое позволяет автоматизировать процесс поиска и выборки данных из большого количества документов [9].

Варианты поиска по ключевым словам в коллекциях документов. Немаловажную роль в проведении компьютерно-технических экспертиз при расследовании преступлений играет использование специальных аппаратных и программных средств. Особое внимание следует уделить тем, которые позволяют осуществлять поиск текстовой информации, а именно поиск по заданным ключевым словам (фразам). Такими являются программы «Архивариус 3000» и Belkasoft Evidence Center X.

«Архивариус 3000» представляет собой мощный поисковый инструмент, с помощью которого возможно найти любой файл или текст. Поиск в программе осуществляется с помощью формального запроса или по ключевым словам не только по названию или расширению файла, но и по его содержанию. Программа поддерживает поиск на десяти языках, а встроенный мастер помогает отыскать необходимый документ по заданным параметрам: размеру, расширению или дате, при этом точно указав местоположение файла.

Особенность его заключается в том, что эта программа, сканируя директории и извлекая содержимое практически любых находящихся в них файлов, содержащих текстовые данные, включая архивы и документы PDF с распознанным текстовым слоем, предварительно создает базу данных или так называемый индекс.

Belkasoft Evidence Center X — это не менее значимое программное средство, способное проводить глубокое исследование содержимого электронных устройств, файлов и процессов памяти. Оно облегчает получение, поиск, анализ, хранение и передачу цифровых улик, находящихся внутри компьютеров и мобильных устройств. С помощью специального сигнатурного поиска по базам данных программа может извлекать артефакты оперативной памяти, включая ссылки, просмотренные в инкогнито-режиме браузера, и изображения, сообщения, посланные в социальных сетях, а также ключи реестра. Это инструмент, специально разработанный для быстрого поиска и создания частичного образа важных данных. Belkasoft Evidence Center X использует подходы, которые позволяют значительно сэкономить время, находить наиболее значимые криминалистические артефакты за меньшее время, чем при использовании избыточных операций. При поиске в данном программном обеспечении предусмотрены функции быстрого поиска и фильтрации, а расширенный поиск

по регулярным выражениям позволяет проводить комплексный поиск по фразам с нечёткой структурой [10].

Заключение. В статье сформулирован и описан подход, направленный на поиск текстовой информации. Проведен анализ возможности применения специализированного ПО для поиска текстовой информации.

Поиск текстовой информации на машинных носителях имеет несколько особенностей, которые могут влиять на его эффективность и качество:

1. Формат хранения текстовой информации. Разные форматы хранения текста (например, DOC, PDF, TXT) требуют разных методов поиска. Некоторые форматы могут быть более сложными для поиска, так как они могут содержать скрытую информацию.

2. Комбинация текста и других типов файлов. Некоторые документы могут содержать не только текст, но и другие типы файлов, такие как изображения, таблицы и даже звуковые файлы. Поиск текстовой информации в таких документах может быть сложнее.

3. Объем информации. Чем больше информации находится на машинном носителе, тем сложнее и дольше будет проходить поиск. В случае поиска большого количества текстовой информации может потребоваться использование специализированного программного обеспечения.

4. Наличие ключевых слов и фраз. Если в текстовой информации нет ключевых слов, фразы или тегов, то поиск может занять больше времени. Нередко приходится проходить поиск вручную.

5. Наличие ошибок в тексте. Отсутствие точности и полноты текстовой информации может затруднить поиск. Поиск информации в текстовых данных, содержащих опечатки и другие ошибки, часто требует дополнительной обработки и анализа.

При проведении компьютерной экспертизы довольно часто требуется поиск информации по ключевым словам. Для этого используются различные методы и инструменты. Такой выбор методов и инструментов для поиска ключевых слов зависит от конкретной задачи и условий проведения экспертизы.

Таким образом, поиск текстовой информации является неотъемлемой частью выявления и раскрытия преступлений в сфере информационных технологий. Он может быть выполнен с использованием различных методов и инструментов. Выбор конкретного метода зависит от характера информации, которую необходимо найти, и особенностей работы эксперта. В целом, поиск

данных требует более высокого уровня навыков и знаний, чем при обычном поиске информации,

и является важным этапом процесса расследования преступлений.

ЛИТЕРАТУРА

1. О государственной судебно-экспертной деятельности в Российской Федерации : Федеральный закон от 31 мая 2001 г. № 73-ФЗ // СПС «КонсультантПлюс».

2. Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации : приказ МВД России от 29.06.2005 № 511 // СПС «КонсультантПлюс».

3. Об утверждении Наставления по организации экспертно-криминалистической деятельности в системе МВД России : приказ МВД России от 11 января 2009 г. № 7 // СПС «КонсультантПлюс».

4. ГОСТ Р 57429-2017. Судебная компьютерно-техническая экспертиза. Термины и определения // СПС «КонсультантПлюс».

5. Баркалов Ю. М. Подготовка экспертов по производству компьютерных судебных экспертиз : методические рекомендации. — Воронеж : Воронежский институт МВД России, 2014.

6. Баркалов Ю. М. Специальные знания, используемые при исследовании компьютерной ин-

формации: учебное пособие. — Воронеж : Воронежский институт МВД России 2017. — 45 с.

7. Типовые экспертные методики исследования вещественных доказательств. Ч. I / под ред. канд. техн. наук Ю. М. Дильдина; общая ред. канд. техн. наук В. В. Мартынова. — М. : ЭКЦ МВД России, 2010. — 568 с.

8. Типовые экспертные методики исследования вещественных доказательств. Ч. II / под ред. А. Ю. Семёнова; общая ред. канд. техн. наук В. В. Мартынова. — М. : ЭКЦ МВД России, 2012. — 800 с.

9. Полухин Д. И., Жуков М. М., Парфенов В. И. Получение криминалистически значимой информации с помощью специализированного программного обеспечения : учебно-методическое пособие. — Воронеж : Воронежский институт МВД России, 2024. — 68 с.

10. Применение специальных знаний для получения значимой информации из компьютерных систем : учебно-методическое пособие / М. М. Жуков, А. Ю. Телков, В. И. Парфенов, Д. И. Полухин. — Воронеж : Воронежский институт МВД России, 2023. — 68 с.

REFERENCES

1. O gosudarstvennoj sudebno`kspertnoj deyatel`nosti v Rossijskoj Federacii : Federal`ny`j zakon ot 31 maya 2001 g. № 73-FZ // SPS «Konsul`tantPlyus».

2. Voprosy` organizacii proizvodstva sudebny`x e`kspertiz v e`kspertno-kriminalisticheskix podrazdeleniyax organov vnutrennix del Rossijskoj Federacii : prikaz MVD Rossii ot 29.06.2005 № 511 // SPS «Konsul`tantPlyus».

3. Ob utverzhdenii Nastavleniya po organizacii e`kspertno-kriminalisticheskoy deyatel`nosti v sisteme MVD Rossii : prikaz MVD Rossii ot 11 yanvarya 2009 g. № 7 // SPS «Konsul`tantPlyus».

4. GOST R 57429-2017. Sudebnaya komp`yuterno-texnicheskaya e`kspertiza. Terminy` i opredeleniya // SPS «Konsul`tantPlyus».

5. Barkalov Yu. M. Podgotovka e`kspertov po proizvodstvu komp`yuterny`x sudebny`x e`kspertiz : metodicheskie rekomendacii. — Voronezh : Voronezhskij institut MVD Rossii, 2014.

6. Barkalov Yu. M. Special`ny`e znaniya, ispol`zuemy`e pri issledovanii komp`yuternoj informacii: uchebnoe posobie. — Voronezh : Voronezh-

skij institut MVD Rossii 2017. — 45 s.

7. Tipovy`e e`kspertny`e metodiki issledovaniya veshhestvenny`x dokazatel`stv. Ch. I / pod red. kand. texn. nauk Yu. M. Dil`dina; obshhaya red. kand. texn. nauk V. V. Marty`nova. — M. : E`KCz MVD Rossii, 2010. — 568 s.

8. Tipovy`e e`kspertny`e metodiki issledovaniya veshhestvenny`x dokazatel`stv. Ch. II / pod red. A. Yu. Semyonova; obshhaya red. kand. texn. nauk V. V. Marty`nova. — M. : E`KCz MVD Rossii, 2012.— 800 s.

9. Poluxin D. I., Zhukov M. M., Parfenov V. I. Poluchenie kriminalisticheskix znachimoj informacii s pomoshh`yu specializirovannogo programmnogo obespecheniya : uchebno-metodicheskoe posobie. — Voronezh : Voronezhskij institut MVD Rossii, 2024. — 68 s.

10. Primenenie special`ny`x znaniy dlya polucheniya znachimoj informacii iz komp`yuterny`x sistem : uchebno-metodicheskoe posobie / M. M. Zhukov, A. Yu. Telkov, V. I. Parfenov, D. I. Poluxin. — Voronezh : Voronezhskij institut MVD Rossii, 2023. — 68 s.

СВЕДЕНИЯ ОБ АВТОРАХ

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.

Жуков Михаил Михайлович. Начальник кафедры компьютерной безопасности и технической экспертизы. Кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: mzhukov25@mvd.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

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.

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.

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@mvd.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 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.

Ключевые слова: поиск информации; текстовый поиск; текстовая информация; поиск текстовой информации; поиск текста.

Key words: information search; text search; text information; text information search; text search.

УДК 004.912, 343.1

С. Г. Родин

**УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ
ЗА ФИКТИВНУЮ ПОСТАНОВКУ
НА МИГРАЦИОННЫЙ УЧЕТ (ст. 322.3 УК РФ):
ВОПРОСЫ ДИФФЕРЕНЦИАЦИИ И КВАЛИФИКАЦИИ**

**CRIMINAL LIABILITY FOR FICTITIOUS REGISTRATION
FOR MIGRATION (art. 322.3 OF THE CRIMINAL CODE
OF THE RUSSIAN FEDERATION):
ISSUES OF DIFFERENTIATION AND QUALIFICATION**

В статье проводится анализ состояния регламентации уголовной ответственности за фиктивную постановку на миграционный учет по месту пребывания иностранных граждан и лиц без гражданства в Российской Федерации. На основании оценки уголовно-правовых норм, устанавливающих ответственность в сфере нарушения миграционного законодательства, анализа судебной практики и некоторых представленных в уголовно-правовой науке точек зрения предлагаются перспективные варианты дифференциации ответственности применительно к ст. 322.3 УК РФ посредством ее дополнения квалифицирующими признаками и квалифицированными составами, а также высказывается мнение о практическом решении отдельных вопросов квалификации рассматриваемых преступлений.

The article analyzes the state of regulation of criminal liability for fictitious registration for migration purposes at the place of stay of foreign citizens and stateless persons in the Russian Federation. Based on the assessment of criminal law norms establishing liability in the sphere of violation of migration legislation, analysis of judicial practice and some points of view presented in criminal law science, promising options for differentiation of liability in relation to Art. 322.3 of the Criminal Code of the Russian Federation are proposed by supplementing it with qualifying features and qualified compositions, and an opinion is expressed on the practical solution of individual issues of qualification of the crimes under consideration.

Современная уголовная политика России в сфере нарушений миграционного законодательства, согласно последним законодательным решениям, направлена на усиление уголовно-правовой репрессии. Данное обстоятельство обусловлено ростом фактически совершенных, зарегистрированных и раскрытых преступлений, связанных с организацией незаконной миграции и фиктивной постановкой на миграционный учет. Так, в первом полугодии 2024 года прирост преступлений в сфере незаконной миграции по сравнению с 2023 годом составил 132,5%, а количество лиц, привлеченных к уголовной ответственности, в 2023 году составило 879 человек, в 2022 году этот показатель был на 30% меньше [1]. Данные обстоятельства привели к разработке и в последующем к принятию законопроекта № 729111-8 от 2 октября 2024 года, который не только предусматривал ряд уголовно-правовых меры, направленных на более эффек-

тивную борьбу с организацией незаконной миграции, но более строгую ответственность за фиктивную регистрацию и постановку на учет иностранных граждан и лиц без гражданства (ст. ст. 322.2, 322.3 УК РФ).

Федеральным законом от 9 ноября 2024 г. № 383-ФЗ [2], были увеличены верхние пределы наказаний в санкциях ст. ст. 322.2, 322.3 УК РФ:

1) период заработной платы или иного дохода осужденного при наказании в виде штрафа был увеличен с трех до *пяти* лет;

2) верхняя граница срока принудительных работ с лишением права занимать определенные должности или заниматься определенной деятельностью была повышена с трех до *пяти* лет;

3) наказание в виде лишения свободы с лишением права (или без такового) занимать определенные должности или заниматься определенной деятельностью повышено с трех до *пяти* лет.

В целом соглашаясь с необходимостью ужесточения ответственности за совершение миграционных преступлений посредством повышения верхних пределов санкций, считаем, что в действующих конструкциях указанных норм следует более глубоко использовать дифференцирующий инструментарий. Применительно к высказанной мысли необходимо отметить, что Концепция государственной миграционной политики Российской Федерации на 2019—2025 годы, утвержденная Указом Президента РФ [3], не только определяет направления совершенствования правил и административных процедур пребывания иностранных граждан и лиц без гражданства на территории России, но и предусматривает выработку адекватных соразмерных мер, в том числе уголовно-правового характера, направленных на противодействие наиболее общественно опасным нарушениям миграционного законодательства.

Следует отметить, что в юридической мысли встречается и альтернативная точка зрения относительно целесообразности установления уголовной ответственности за фиктивную постановку на миграционный учет. Например, по мнению Т. Н. Уторовой, установление уголовной ответственности за фиктивную постановку на миграционный учет является излишним, поскольку причиняемый такими деяниями вред более соответствует административным правонарушениям [4. — С. 14]. Данная позиция обосновывается тем, что предоставление ложных сведений при осуществлении миграционного учета как иностранным гражданином или лицом без гражданства, так и «принимающей стороной» влечет административную ответственность по ст. 19.27 КоАП РФ. Однако, на наш взгляд, конкуренция административно-правовых и уголовно-правовых норм в части установления ответственности за фиктивную постановку на миграционный учет носит частичный характер, поскольку, применительно к ст. 322.3 УК РФ ответственность также наступает за непредоставление помещения для проживания (пребывания) либо при отсутствии намерения у регистрируемых лиц фактически в нем проживать (пребывать).

Центральным вопросом нашего исследования выступает состояние регламентации уголовно-правового противодействия фиктивной постановке на миграционный учет применительно к ст. 322.3 УК РФ. Несмотря на ужесточение ответственности, а именно повышение верхних пределов санкции за фиктивную постановку на учет по месту пребывания иностранных граждан или лиц без гражданства, на наш взгляд, потенциал ст. 322.3. УК РФ полностью не раскрыт в действующей редакции, что с учетом реалий практической деятельности и

необходимостью более строгой реакции на нарушения миграционного законодательства говорит о необходимости расширения рассматриваемой нормы посредством выделения и дополнения ее квалифицированными составами.

Представляется целесообразным пересмотреть с позиций научно-правового анализа конструкцию статьи 322.3 УК РФ, устанавливающую уголовную ответственность за фиктивную постановку на учет по месту пребывания иностранного гражданина или лица без гражданства в Российской Федерации. Законодатель использует простую диспозицию, ограничиваясь указанием на основные характеристики деяния без конкретизации его форм и способов реализации. В то же время дополнительное разъяснение конструкции состава преступления содержится в примечании 1, что свидетельствует о стремлении законодателя сохранить обобщенный характер основной нормы, оставляя детализирующую функцию за примечанием.

Между тем анализ правоприменительной практики показывает, что реальное содержание признаков состава, предусмотренного ст. 322.3 УК РФ, отличается значительной вариативностью. Научный и практический интерес представляют как объективные, так и субъективные элементы рассматриваемого состава преступления, поскольку в ряде случаев они могут приобретать значение квалифицирующих обстоятельств. Подобная трансформация базовых признаков вотягающие обстоятельства позволит органам предварительного расследования и суду реализовать более гибкий и дифференцированный подход в процессе уголовно-правовой оценки противоправного поведения, связанного с фиктивной регистрацией иностранных граждан.

При буквальном толковании диспозиции ст. 322.3 УК РФ можно сделать однозначный вывод о том, что уголовная ответственность наступает уже за сам факт фиктивной постановки на учет одного иностранного гражданина или лица без гражданства. Однако складывающаяся в субъектах Российской Федерации судебно-следственная практика демонстрирует определенную неоднородность в подходах к применению данной нормы. Так, в отдельных регионах возбуждение уголовного дела по ст. 322.3 УК РФ ставится в зависимость от количества иностранных граждан, фиктивно поставленных на учет, и порог наступления ответственности искусственно повышается до трех, пяти и более лиц. Подобная практика противоречит как букве закона, так и его духу, создавая предпосылки для произвольного правоприменения и неоправданного расширения дискреционных полномочий правоохранительных органов.

С научной и практической точек зрения представляется обоснованной позиция, в соответствии с которой фиктивная регистрация даже одного иностранного гражданина или лица без гражданства должна рассматриваться в качестве основания для привлечения к уголовной ответственности. Этот вывод не только основан на буквальном смысле диспозиции ст. 322.3 УК РФ, но и подтверждается мнением, сформулированным в судебной практике. В частности, п. 15 Постановления Пленума Верховного Суда Российской Федерации от 9 июля 2020 г. № 18 (далее — ППВС РФ от 9 июля 2020 года № 18) указывает на то, что при наличии единого умысла на фиктивную постановку на учет двух и более иностранных граждан, содеянное рассматривается как одно преступление, квалифицируемое по ст. 322.3 УК РФ, без образования множественности преступлений [5]. Следовательно, если фиктивная регистрация нескольких лиц трактуется как единое деяние при наличии общего умысла, то фиктивная регистрация одного лица объективно должна восприниматься как самостоятельное уголовно наказуемое деяние.

Также недопустимо решение вопроса о фиктивной постановке на миграционный учет по месту пребывания одного иностранного гражданина или лица без гражданства через призму малозначительности, что считаем не соответствующим общественной опасности данного деяния и, соответственно, противоречащим букве закона и современной миграционной политике России, в связи с чем представляется целесообразным рассматривать фиктивную постановку на учет по месту пребывания двух или более иностранных граждан или лиц без гражданства при наличии единого умысла виновного не как одно преступление, а в качестве квалифицированного состава, которым необходимо дополнить ст. 322.3 УК РФ. Несмотря на то, что данная позиция вступает в противоречие с п. 15 ППВС РФ от 9 июля 2020 года № 18, она, на наш взгляд, соответствует тенденции современной миграционной политики России, которая предусматривает усиление противодействия нелегальной миграции и другим нарушениям миграционного законодательства.

Следующим дифференцирующим и квалифицирующим признаком может стать законодательное определение круга лиц, которые выступают субъектами преступления, предусмотренного ст. 322.3. УК РФ. Согласно содержанию п. 14 ППВС РФ от 9 июля 2020 года № 18, уголовной ответственности также может подлежать должностное лицо, осуществляющее регистрационные действия по постановке на учет при наличии осознания им недостоверности представленных сведений или докумен-

тов либо при наличии осознания обстоятельств, не позволяющих законно поставить на миграционный учет [5].

Поэтому считаем, что по аналогии с п. «б» ч. 2 ст. 322.1 УК РФ необходимо в качестве квалифицирующего признака ст. 322.3 УК РФ рассматривать совершение данного преступления лицом с использованием своего служебного положения. Отметим, что приведенная мысль уже высказывалась и справедливо поддерживается в отечественной уголовно-правовой науке. Например, Е. А. Лайкова, говоря о необходимости усиления уголовной ответственности лиц, обладающих специальными полномочиями по осуществлению регистрационных действий, также обращает внимание на то, что в ст. 322.3 УК РФ субъект недостаточно четко определен, а из смысла статьи вообще следует, что он специальный [6. — С. 56, 57].

Исходя из двойственности субъекта ст. 322.3 УК РФ, возникает вопрос о том, как квалифицировать ситуации, когда, например, собственник или наниматель жилого помещения с целью постановки на учет по месту пребывания иностранного гражданина или лица без гражданства предоставляет заведомо ложные сведения или документы, недостоверность которых осознается должностным лицом при осуществлении регистрационных действий по постановке на учет.

Кроме того, на практике достаточно часто встречаются случаи, когда собственник жилого помещения из корыстных побуждений по просьбе третьих лиц осуществляет фиктивную постановку на учет иностранных граждан или лиц без гражданства без их намерения фактически проживать (пребывать) там, а также без намерения принимающей стороны предоставить им жилое помещение для проживания (пребывания).

Так, например, гражданин А. был признан виновным в совершении двух преступлений, предусмотренных ст. 322.3 УК РФ. Указанные преступления А. совершил из корыстных побуждений по просьбе ранее неизвестного ему мужчины. Среди озвученных условий совершения А. фиктивной постановки на миграционный учет было материальное вознаграждение и то, что иностранные граждане фактически не будут проживать по месту регистрации. Согласившись на предложение неустановленного лица, в последующем А., выступив принимающей стороной, осуществил два факта постановки на учет иностранных граждан по месту пребывания [7].

Аналогично приведенной выше ситуации ранее судимый гражданин Б. был привлечен к уголовной ответственности по трем эпизодам фиктивной постановки на учет по месту пребывания иностранных граждан. Преступления, преду-

смотренные ст. 322.3 УК РФ, гражданин Б. совершил из корыстных побуждений, получив соответствующую информацию от неизвестного ему ранее лица [8].

Приведенные примеры свидетельствуют о том, что нередко предложения о фиктивной постановке на миграционный учет поступают от третьих лиц, однако оценка их действий остается за рамками судебно-следственной практики. Вместе с тем можно встретить судебную практику, когда в описательно-мотивировочной части приговора прямо говорится о соучастии, если принимающая сторона действует по просьбе третьих лиц.

В качестве примера можно привести обвинительный приговор Нальчикского городского суда (Кабардино-Балкарская Республика) № 1- 298/2024, которым гражданка А. была признанной виновной в совершении организации незаконного пребывания иностранного гражданина на территории Российской Федерации, совершенной группой лиц по предварительному сговору (п. «а» ч. 2 ст. 322.1 УК РФ). Этим же приговором в отношении А. было прекращено уголовное дело по ст. 322.3 УК РФ за истечением срока давности привлечения ее к уголовной ответственности. Фиктивную постановку на учет по месту пребывания иностранного гражданина А. совершила из корыстных побуждений по просьбе неустановленных лиц, которые с целью извлечения прибыли оказывали содействие иностранным гражданам в получении документов, обеспечивающих его законное пребывание на территории Российской Федерации.

В приговоре прямо указывается, что неустановленные лица осуществляли приискание соучастников, которые могли бы выступить принимающей стороной, действовали с осознанием того, что групповой способ совершения преступления повышает эффективность преступной деятельности. Суд, признав, что гражданка А. осуществила фиктивную постановку иностранного гражданина на учет по месту пребывания, действуя в составе группы лиц по предварительному сговору [9].

Исходя из действующей редакции ст. 322.3 УК РФ, применительно к рассматриваемой ситуации, в случае если бы не истекли сроки давности и гражданке А. назначалось наказание, то единственно возможной юридической оценкой ее действий с позиции института соучастия мог быть только учет положений п «в» ч. 1 ст. 63 УК РФ, т. е. в рамках обстоятельств, отягчающих наказание.

Очевидно, что приведенные выше примеры позволяют рассматривать фиктивную постановку на учет по месту пребывания иностранных граждан

и лиц без гражданства, совершенную в соучастии, как самостоятельный признак преступления, предусмотренного ст. 322.3. УК РФ, который должен образовывать более тяжкий квалифицированный состав.

Рассмотрение вопроса соучастия применительно к ст. 322.3 УК РФ предопределяет и проблематику ответственности лиц, постановка на миграционный учет которых осуществляется «принимающей стороной». Представляется, что общественная опасность действий иностранных граждан и лиц без гражданства, которых ставят на учет, не должна рассматриваться в ракурсе уголовной ответственности. Полагаем, что регистрируемые иностранные граждане и лица без гражданства в обязательном порядке должны нести административную ответственность, поскольку в первую очередь именно их потребности обуславливают совершение миграционных преступлений.

Обзор судебно-следственной практики позволяет сделать вывод о том, что наиболее часто фиктивная постановка на учет иностранных граждан или лиц без гражданства по месту пребывания осуществляется «принимающей стороной» из корыстных побуждений. Согласно проведенному нами анализу уголовных дел по Воронежской области, возбужденных органами дознания МВД России и рассмотренных мировыми судьями по ст. 322.3 УК РФ, корыстные побуждения встречаются в 84,62% случаев, иная личная заинтересованность соответственно составляет 15,38 %.

Повышенную опасность наличия у виновного корыстных побуждений при совершении преступления, предусмотренного ст. 322.3 УК РФ, относительно иных мотивов личной заинтересованности можно продемонстрировать на следующем примере. *Так, в связи с деятельным раскаянием и на основании примечания к ст. 322.3 УК РФ на стадии дознания было прекращено уголовное дело в отношении гражданина А., уроженца Республики Армения. Гражданин А., являясь собственником жилого дома, расположенного в одном из районов Воронежской области, с целью законного нахождения по месту жительства осуществил фиктивную постановку на учет по месту пребывания своих родственников, граждан Республики Армения. Принадлежащий А. дом пребывал в ветхом состоянии, отсутствовала подводка электросетей и отопление, сам он в указанном доме никогда не проживал, т. к. он был не пригоден для этих целей. При этом обвиняемый обеспечил родственников возможностью проживания по месту своего фактического жительства, какого-либо материального вознаграждения от них не получал, в ходе дознания активно способствовал установлению всех обстоятельств содеянного [10].*

Поэтому полагаем, что вполне возможна и целесообразна дифференциация уголовной ответственности за фиктивную постановку на учет по месту пребывания иностранных граждан и лиц без гражданства по такому признаку субъективной стороны, как мотив, с выделением квалифицированного состава в ст. 322.3 УК РФ, предусматривающего корыстные побуждения.

В практике применения ст. 322.3 УК РФ обращает на себя внимание возможность освобождения от уголовной ответственности, условия которой сформулированы в примечании 2. Принимаемые органами дознания и мировыми судьями уголовно-процессуальные решения свидетельствуют о том, что после возбуждения уголовного дела по ст. 322.3 УК РФ оно может быть прекращено в случае, если лицо добровольно до возбуждения уголовного дела сообщило о совершённом преступлении и активно способствовало его раскрытию. Так, в отношении гражданки Е. было прекращено уголовное дело по ст. 322.3. УК РФ в связи с тем, что она в судебном заседании полностью признала свою вину, добровольно сообщила сотрудникам полиции о совершенном преступлении, предоставила сведения о поставленных на учет лицах, что позволило установить их фактическое местонахождение, выдала домовую (поквартирную) книгу, дала полные признательные показания и представила для осмотра жилище [11].

Отметим, что одно лишь признание обвиняемым вины в совершенном деянии не является единственным и исчерпывающим обстоятельством, позволяющим прекратить уголовное преследование. Например, гражданин Л. был признан виновным в совершении преступления, предусмотренного ст. 322.3 УК РФ, за фиктивную постановку на учет по месту пребывания пяти иностранных граждан. Несмотря на признание Л. вины в полном объёме предъявленного обвинения, состояние здоровья и материальное положение, послужившие поводом совершения

преступления, уголовное дело не было прекращено, а ввиду смягчающих обстоятельств Л. было назначено наказание в виде штрафа [11].

Изложенное выше позволяет сделать ряд некоторых выводов и предложений. В первую очередь следует отметить, что тенденция развития современной миграционной политики России в части ужесточения ответственности за миграционные преступления обуславливает и саму необходимость дифференцированного подхода к регламентации таких общественно опасных деяний. Усиление борьбы с организацией незаконной миграции и соответствующее законодательное совершенствование нормы ст. 322.1 УК РФ определяет также пересмотр уголовной ответственности за фиктивную постановку на миграционный учёт.

Поставленные в статье вопросы и предложения по их решению говорят о необходимости пересмотра действующей законодательной конструкции нормы ст. 322.3 УК РФ посредством выделения в ней квалифицированных составов с целью более глубокой дифференциации уголовной ответственности и решения некоторых проблем квалификации. Развитие диспозиции ст. 322.3 УК РФ и, соответственно, усиление уголовной ответственности предлагается по следующим квалифицирующим признакам: во-первых, в зависимости от количества лиц, фиктивно поставленных на учет по месту пребывания (два и более иностранных гражданина или лица без гражданства); во-вторых, необходим учет использования служебного положения лица, осуществляющего регистрационные действия по постановке на миграционный учёт; в-третьих, следует выделить совершение рассматриваемого преступления в соучастии (с различием по формам соучастия); в-четвертых, повышенная ответственность должна быть предусмотрена при наличии корыстных побуждений.

ЛИТЕРАТУРА

1. Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» : офиц. сайт. — URL: <https://sozd.duma.gov.ru/bill/729111-8> (дата обращения : 21.01.2025).
2. О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации : Федеральный закон от 9 ноября 2006 г. № 383-ФЗ. // СПС «КонсультантПлюс», 2025 (дата обращения: 22.01.2025).

3. Концепция государственной миграционной политики Российской Федерации на 2019—2025 годы : Указ Президента РФ от 31 октября 2018 г. № 622 «О Концепции государственной миграционной политики Российской Федерации на 2019—2025 годы» (ред. от 12 мая 2023 г.) // СПС «КонсультантПлюс», 2025 (дата обращения: 22.01.2025).

4. Уторова Т. Н. Фиктивная постановка на миграционный учёт: практика применения статьи 322.3 УК РФ // Вестник института: преступление,

наказание, исправление. — 2015. — № 1 (29). — С. 10—14.

5. О судебной практике по делам о незаконном пересечении государственной границы Российской Федерации и преступлениях, связанных с незаконной миграцией : постановление Пленума Верховного Суда РФ от 09.07.2020 № 18 // СПС «КонсультантПлюс», 2025 (дата обращения: 24.01.2025).

6. Лайкова Е. А. Субъективные признаки составов преступлений, предусмотренных статьями 322.2, 322.3 Уголовного кодекса РФ // Сибирский юридический вестник. — 2017. — № 3 (78). — С. 54—59.

7. Приговор Октябрьского районного суда г. Рязани № 1-388/2023 1-62/2024 от 25 июля 2024 г. // URL: <https://sudact.ru> (дата обращения: 24.01.2025).

8. Приговор Клинского городского суда (Московская область) № 1-298/2024 // URL: <https://sudact.ru> (дата обращения: 24.01.2025).

9. Приговор Нальчикского городского суда (Кабардино-Балкарская Республика) № 1- 298/2024 // URL: <https://sudact.ru> (дата обращения: 24.01.2025).

10. Уголовное дело № 118011200026450259 от 15 мая 2018 г. // Архив ОМВД России по Рамонскому району Воронежской области.

11. Постановление о прекращении уголовного дела № 1-40/2018 от 9 октября 2018 г. // Судебный участок № 1 Мирового судьи Рамонского района Воронежской области (архив).

12. Приговор по уголовному делу № 1- 15/2019 от 29 марта 2019 г. // Судебный участок № 2 Мирового судьи Рамонского района Воронежской области (архив).

REFERENCES

1. Sistema obespecheniya zakonodatel'noj deyatel'nosti Gosudarstvennoj avtomatizirovannoj sistemy «Zakonotvorchestvo» : ofic. sajт. — URL: <https://sozd.duma.gov.ru/bill/729111-8> (data obrashcheniya : 21.01.2025).

2. O vnesenii izmenenij v Ugolovnyj kodeks Rossijskoj Federacii i stat'yu 151 Ugolovno-processual'nogo kodeksa Rossijskoj Federacii : Federal'nyj zakon ot 9 noyabrya 2006 g. № 383-FZ. // SPS «Konsul'tantPlyus», 2025 (data obrashcheniya: 22.01.2025).

3. Konceptsiya gosudarstvennoj migracionnoj politiki Rossijskoj Federacii na 2019—2025 gody : Ukaz Prezidenta RF ot 31 oktyabrya 2018 g. № 622 «O Konceptcii gosudarstvennoj migracionnoj politiki Rossijskoj Federacii na 2019—2025 gody» (red. ot 12 maya 2023 g.) // SPS «Konsul'tantPlyus», 2025 (data obrashcheniya: 22.01.2025).

4. Utorova T. N. Fiktivnaya postanovka na migracionnyj uchet: praktika primeneniya stat'i 322.3 UK RF // Vestnik instituta: prestuplenie, nakazanie, ispravlenie. — 2015. — № 1 (29). — S. 10—14.

5. O sudebnoj praktike po delam o nezakonnom peresechenii gosudarstvennoj granicy Rossijskoj Federacii i prestupleniyah, svyazannyh s nezakonnoj migraciej : postanovlenie Plenuma Verhovnogo Suda RF ot 09.07.2020 № 18 // SPS «Konsul'tantPlyus»,

2025 (data obrashcheniya: 24.01.2025).

6. Lajkova E. A. Sub"ektivnye priznaki sostavov prestuplenij, predusmotrennyh stat'yami 322.2, 322.3 Ugolovnogo kodeksa RF // Sibirskij yuridicheskij vestnik. — 2017. — № 3 (78). — S. 54—59.

7. Prigovor Oktyabr'skogo rajonnogo suda g. Ryazani № 1-388/2023 1-62/2024 ot 25 iyulya 2024 g. // URL: <https://sudact.ru> (data obrashcheniya: 24.01.2025).

8. Prigovor Klinskogo gorodskogo suda (Moskovskaya oblast') № 1-298/2024 // URL: <https://sudact.ru> (data obrashcheniya: 24.01.2025).

9. Prigovor Nal'chikskogo gorodskogo suda (Kabardino-Balkarskaya Respublika) № 1-298/2024 // URL: <https://sudact.ru> (data obrashcheniya: 24.01.2025).

10. Ugolovnoe delo № 118011200026450259 ot 15 maya 2018 g. // Arhiv OMVD Rossii po Ramonskomu rajonu Voronezhskoj oblasti.

11. Postanovlenie o prekrashchenii ugolovnogo dela № 1-40/2018 ot 9 oktyabrya 2018 g. // Sudebnyj uchastok № 1 Mirovogo sud'i Ramonskogo rajona Voronezhskoj oblasti (arhiv).

12. Prigovor po ugolovnomu delu № 1-15/2019 ot 29 marta 2019 g. // Sudebnyj uchastok № 2 Mirovogo sud'i Ramonskogo rajona Voronezhskoj oblasti (arhiv).

СВЕДЕНИЯ ОБ АВТОРЕ

Родин Станислав Геннадьевич. Преподаватель кафедры уголовного права и криминологии. Воронежский институт МВД России.
E-mail: nobilisrg@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Rodin Stanislav Gennadyevich. Lecturer of the chair of Criminal Law and Criminology.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: nobilisrsg@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: дифференциация; уголовная ответственность; наказание; квалификация; иностранные граждане; миграционное законодательство.

Key words: differentiation; criminal liability; punishment; qualification; foreign citizens; migration legislation.

УДК 343.3

П. Г. Смагин

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ МАШИНОЧИТАЕМОГО ПРАВА В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

THE USE OF MACHINE-READABLE LAW TECHNOLOGIES IN CRIMINAL PROCEEDINGS

В статье проведен анализ развития технологий машиночитаемого права на современном этапе и возможность их использования в уголовном судопроизводстве. Рассмотрены основные направления внедрения автоматизированных систем в правоприменительную деятельность, включая алгоритмизацию расследования преступлений, создание экспертных систем и использование искусственного интеллекта для анализа нормативных актов. Особое внимание уделено преимуществам и проблемам внедрения машиночитаемого права, таким как сложность интерпретации оценочных категорий и необходимость стандартизации данных. Сделан вывод о перспективах дальнейшего развития данного направления и его значимости для повышения эффективности судебного разбирательства.

The article analyzes the development of machine-readable law technologies at the present stage and the possibility of their use in criminal proceedings. The main directions of the introduction of automated systems into law enforcement activities are considered, including algorithmization of crime investigation, creation of expert systems and the use of artificial intelligence for the analysis of regulations. Special attention is paid to the advantages and problems of introducing machine-readable law, such as the complexity of interpreting evaluation categories and the need for data standardization. The conclusion is made about the prospects for further development of this area and its importance for improving the effectiveness of judicial proceedings.

Активное развитие современных информационных технологий справедливо предопределяет возможность постановки и решения ряда важных задач в сфере уголовного судопроизводства. Так, С. В. Зуев, анализируя перспективы формирования цифрового уголовно-процессуального законодательства, выделяет три ключевых направления эволюции правовой системы: цифровизацию процессов расследования, формирование цифровой (виртуальной) среды правоприменения и обеспечение машиночитаемости правовых норм [1]. В свою очередь, О. Л. Солдаткина и А. В. Малько подчеркивают, что одним из современных векторов цифровой трансформации права является алгоритмизация юридических процессов и нормотворчества, включающая в себя использование технологий искусственного интеллекта [2]. Развитие и внедрение машиночитаемого права приведет к усложнению структуры источников права, представляющей собой динамичную, многоуровневую систему правовых норм, в ряде случаев реализуемую в форме машинных алгоритмов [3].

Концепция развития технологий машиночитаемого права [4] предполагает, что технологии

машиночитаемого права в той или иной степени будут применяться во всех отраслях законодательства Российской Федерации и являются одним из эффективных способов непротиворечивого изложения правовых норм с целью повышения удобства правоприменения для государства, предпринимательского сообщества и граждан, что позволит в большей степени решить известные проблемы, о которых говорят ученые: почти нет формальных требований к юридическому языку, законодательный процесс весьма непредсказуем, нормы часто составлены непонятно и противоречиво, а контроль за их соблюдением работает избирательно [5].

В соответствии с положениями Концепции под машиночитаемым правом следует понимать основанное на онтологии права изложение определенного набора правовых норм на формальном языке (в том числе языке программирования, языке разметки), а также технологии машиночитаемого права (инструменты применения таких норм в виде необходимых информационных систем и программного обеспечения).

Под онтологией Концепция понимает описание на формальном языке множества объектов

(сфер применения машиночитаемого права, субъектов правоотношений, сделок и т. д.) в области права и связей между ними с помощью набора специальных символов и правил (операций логики, арифметики и иных отношений между словами).

К недостаткам приведенных определений можно отнести наличие тавтологии раскрытия машиночитаемого права через самого себя, а также неопределенность и сложность понимания законодателем процедур использования онтологии права в нормотворческой деятельности.

В связи с этим отдельные авторы предлагают свои интерпретации указанных понятий. Так, Н. Ф. Порываева определяет машиночитаемое право как совокупность машиночитаемых правовых норм, санкционированных государством и опосредованных в реализации техническими нормами и структурами данных. При этом под машиночитаемыми правовыми нормами понимаются «правовые положения, изложенные в виде машинных алгоритмов, реализованных на языках программирования (программного кода), понимаемые машиной с последующей машиноисполняемой реализацией» [6].

Сущность онтологии права представляет собой многогранное и динамическое явление, для которого не существует единственно верного и универсального определения. Формирование правовой онтологии является творческим процессом, обусловленным спецификой предметной области. Ключевой особенностью структуры онтологии права является ее объектно-ориентированное устройство, базирующееся на соответствующих принципах программирования. Данный подход обеспечивает представление правовых категорий в виде классов, инкапсулирующих не только их свойства, но и логику обработки соответствующих объектов.

В рамках онтологии любое понятие или сущность предметной области формализуется посредством специальной структуры, включающей субъект, предикат и объект (триплет). Совокупность триплетов образует граф понятий, где субъекты и объекты интерпретируются как вершины ориентированного графа, а предикаты определяют семантические отношения между ними. В некоторых случаях предикаты, представляя собой корреляционные связи, могут выступать в роли субъектов или объектов в других графах, что позволяет моделировать сложные логические взаимосвязи.

Каждый элемент корневого класса включает вложенные классы, которые посредством предикативных отношений и выражений устанавливают связи с аналогичными элементами других классов. Экземпляры классов могут принадлежать одновременно нескольким классам, а все классы и их экземпляры объединяются в единую

структуру при помощи отношений, выражений и скалярных констант. Такая модель позволяет формализовать правовые нормы в строгом логическом представлении.

Концепция машиночитаемого права ориентирована на трансформацию нормативных документов в форму, пригодную для автоматизированного анализа и обработки с использованием математических алгоритмов. В научной литературе машиночитаемое право рассматривается как инструментальная онтология, обеспечивающая представление нормативных правовых актов в компьютерно-программной логике. Это, в свою очередь, позволяет математическим алгоритмам извлекать, анализировать, интерпретировать и исполнять правовые нормы, а также контролировать их реализацию в автоматизированных системах правоприменения [7].

В настоящее время выделяются следующие направления развития технологий машиночитаемого права:

1. Автоматическое создание онтологии права с использованием систем искусственного интеллекта из действующих текстов нормативных правовых актов. Такой способ позволяет быстро обработать большое количество документов, выявить основные сущности, классифицировать и сгруппировать однородные правоотношения, выстроить взаимосвязи между категориями и понятиями.

2. Ручное проектирование специалистами в определенной предметной области онтологии права из текстов нормативных актов, позволяющее значительно повысить качество результата, однако требующее привлечения большого количества людей, обеспечения взаимосвязи между ними и наличия временных ресурсов.

3. Анализ правоприменительной практики для подготовки решений, основанных на праве. Основой такой системы могут выступить смарт-контракты, базирующиеся на технологии блокчейн.

Анализ опыта внедрения и использования отдельных элементов машиночитаемого права в правоприменительную деятельность позволяет выделить следующие актуальные направления:

1. Судебная система. Использование системы в рамках рассмотрения и разрешения уголовных дел в судах. Так, в Китае в рамках разработки реформы «умных судов» технологии машиночитаемого права используются для анализа фактических обстоятельств дела и проверки формальных требований законодательства при его рассмотрении и вынесении решений. В Республике Казахстан применяется система проверки проектов или принятых актов прокурора или судьи на соответствие формальным требованиям уголовного и

уголовно-процессуального законодательства Республики Казахстан. Анализ решений также позволяет собирать судебную статистику по регионам.

2. Анализ нормативных документов. В Соединенных Штатах применяется система правового анализа, направленная на выявление и устранение устаревших или избыточных регуляторных требований, содержащихся в нормативных актах. В Российской Федерации в рамках реализации федерального проекта «Цифровое государственное управление» осуществляется разработка Федеральной государственной информационной системы. Данная система, позиционируемая как «Национальная единая среда взаимодействия всех участников нормотворческого процесса при подготовке регуляторных решений», ориентирована на повышение эффективности законодательной деятельности. Она обеспечит оптимизацию процесса разработки, согласования и утверждения нормативных правовых актов, а также создаст условия для межведомственного взаимодействия государственных органов в рамках совместной работы над проектами нормативных правовых актов.

3. Составление документов. Широкое внедрение получили программы для автоматической проверки договоров на предмет их соответствия законодательству (LawGeex, Израиль), системы автоматического извлечения и систематизации информации из юридической документации (eBrevia Contract Analyzer, США), автоматические программные решения для заполнения искового заявления для обжалования штрафов (DoNotPay, США). Робот-юрист, разработанный правовым департаментом «Сбера», извлекает юридически значимую информацию из документов, проверяет корректность внесенных в нее сведений и полномочия участников сделки.

4. Создание алгоритмов правоприменения. К примеру, в Австралии действует автоматическая система, направленная на контроль соблюдения требований законодательства. Процесс правоприменения состоит из трех стадий: конвертации норм в машиночитаемый формат, контроля качества полученных норм и публикации в открытом доступе данных в виде наборов правил. Прозрачность и доступность для понимания конечным субъектом использования правовых норм сможет преобразовать формальное описание норм и адаптировать сложные языковые конструкции не только для людей без специальных юридических

знаний, но и для функционирования интеллектуальных систем [8].

5. Экспертные аналитические системы поддержки и принятия решений, позволяющие по открытым источникам информации (новостные ленты, группы в социальных сетях и т. д.) квалифицировать деяния и выработать алгоритм противодействия им [9].

Обращаясь к методологии создания указанных выше машиночитаемых систем, необходимо выделить следующие подходы:

1. Системы обработки естественного языка (большие языковые модели), которые в своей архитектуре включают создание векторного представления текста путем токенизации слов в эмбединги (преобразование буквы, части слова или слова целиком в векторное матричное представление в многомерном пространстве). Суть таких систем сводится к предсказанию (прогнозированию) последующих слов с определенной долей вероятности на основе контекста предыдущих предложений. В процессе обучения таких моделей один и тот же датасет (пакет входящих данных) проходит через математические матрицы большое количество раз, пока точность ответа не достигнет максимального показателя [10]. Процесс обучения заключается в том, что программа анализирует большие объемы данных, находит в них закономерности и может впоследствии применить их к новым задачам.

2. Графы знаний. В своей основе система опирается на онтологию, которая содержит в вершинах графов понятия и сущности, а в ребрах взаимосвязи между ними. Такая система позволяет извлекать факты из текста и создавать новые логические суждения подобно человеческому мышлению. Современные большие языковые модели по типу DeepSeek R1 и ChatGPT 4o способны эффективно работать с онтологиями, применяя к графам знаний все известные методы работы с текстом, полученные ими в ходе обучения.

3. Математические модели. Система записи правовых норм права в виде математической модели предполагает автоматическую или ручную разметку текста с целью выделения в нем интересных областей для последующей группировки и систематизации содержащихся в них данных.

Процесс создания системы машиночитаемого права можно упрощенно представить следующей схемой (рис. 1).

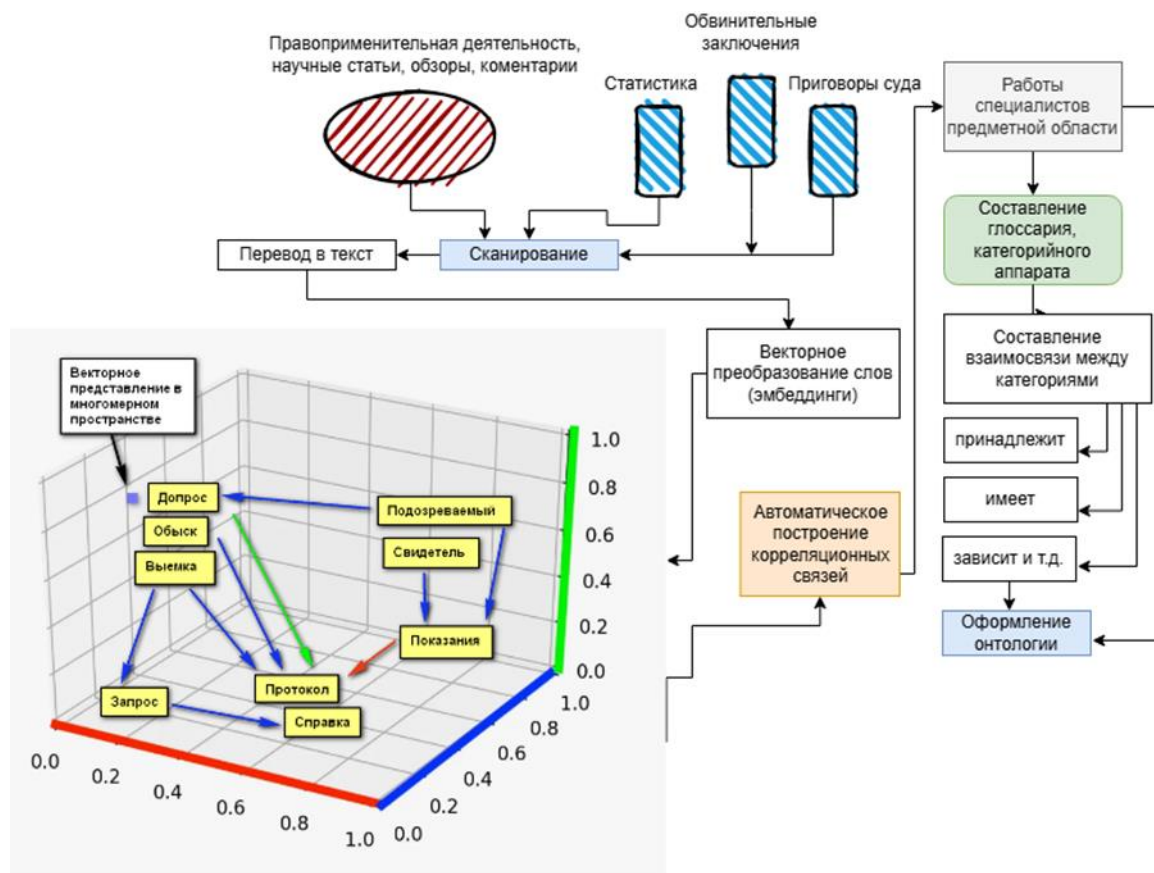


Рис. 1. Процесс создания системы машиночитаемого права

Создание онтологии машиночитаемого права состоит из нескольких этапов.

1. Сбор датасета. На данном этапе формируются категории информации по группам (статистические данные, эмпирический материал, положения нормативных правовых актов, итоговые и промежуточные решения по уголовным делам, обзоры судебной практики, комментарии, разъяснения, научные статьи и т. д.).

2. Нормализация исходных данных. Представляет собой процесс приведения собранной информации к единому, структурированному виду, удобному для последующей обработки и формализации. На данном этапе устраняется дублирование, противоречия, неоднозначность и различия в форматах представления правовых данных. К основным методам нормализации можно отнести: удаление ошибок, повторов, исправление опечаток и неточностей, фильтрацию нерелевантной информации, приведение к единому формату, преобразование текстов нормативных актов в машиночитаемый формат (например, XML, JSON), разрешение неоднозначностей, приведение синонимов к единому виду, добавление метаданных (даты, источники, типы документов), определение ключевых

понятий, выявление шаблонов и стандартных структур в законодательстве.

3. Формализация знаний. На данном этапе проводится структурирование и категоризация норм права, понятий и их взаимосвязей. Создаются концептуальные схемы, определяются ключевые термины и их атрибуты, а также устанавливаются связи между ними. Формализованные данные подготавливаются для интеграции в онтологическую модель.

4. Разработка онтологической модели. На основе собранных и нормализованных данных разрабатывается структура онтологии. Определяются классы, свойства, отношения и ограничения. Используются онтологические языки (например, OWL) и стандарты представления знаний. На данном этапе создается логическая модель, обеспечивающая машиночитаемость правовых данных.

5. Верификация и валидация онтологии. Проверяется логическая согласованность разработанной модели, тестируется её применимость к различным юридическим сценариям. Проводится сопоставление с реальными правовыми ситуациями, анализируются ошибки и возможные

пробелы в онтологии. При необходимости вносятся корректировки.

6. Интеграция и использование. Разработанная онтология интегрируется в юридические си-

стемы, системы принятия решений, базы знаний и экспертные системы.

Пример упрощенной онтологии изображен на рисунке 2.



Рис. 2. Упрощенная онтология права

При рассмотрении вопроса о применении технологий машиночитаемого права в уголовном судопроизводстве на этапе предварительного расследования следует подчеркнуть, что в отличие от норм материального права уголовно-процессуальное законодательство ориентировано прежде всего на формирование четкого алгоритма действий для субъектов расследования. Этот алгоритм создается на основе обобщенного правоприменительного опыта и опирается на законодательные нормы.

К задачам использования машиночитаемого права при производстве расследования необходимо отнести:

1. Толкование правовых норм в их взаимосвязи с подзаконными нормативными актами и смежными отраслями законодательства.

2. Анализ, обобщение, классификацию выработанной правоприменительной практики для повышения качества расследования преступлений.

3. Формальный анализ и проверку на предмет соответствия требованиям законодательства процессуальных документов, выносимых и составляемых в ходе уголовного судопроизводства.

4. Использование экспертных систем поддержки и принятия решений, начиная с момента

квалификации деяния и планирования расследования, заканчивая процессом вынесения итогового решения по уголовному делу.

5. Выявление противоречий и логических нарушений в уже составленных процессуальных документах.

6. Обработку текста процессуальных документов для формирования новых документов (к примеру, обвинительного заключения, включающего краткое изложение доказательств, собранных по уголовному делу).

7. Создание интеллектуальных справочников в предметной области для принятия обоснованных решений (справочники по виду, форме, массе наркотических средств и их прекурсорах, предварительному определению степени тяжести вреда здоровью по полученным телесным повреждениям).

8. Формирование четкого алгоритма и методики расследования конкретного вида преступления в зависимости от сложившейся следственной ситуации.

К проблемам создания рассматриваемых нами систем машиночитаемого права на современном этапе можно отнести:

1. Оценочные категории. УПК РФ содержит не совсем понятные для математической программы категории «руководствоваться законом и совестью», «честь и достоинство личности», «малозначительность преступления» и т. д. Полагаем, что данный недостаток может быть устранен только путем ручного анализа и корректирования созданной автоматически онтологии права. Отдельные авторы справедливо дополняют эту категорию нормами-принципами и

предлагают «полуавтоматический режим» анализа с привлечением человека для вынесения решений по данным категориям [11].

2. Неоднородность правоприменительной практики квалификации преступных деяний, интерпретации и толкования правовых норм различными органами предварительного расследования, прокуратурой и судами, существенные отличия в оценке доказательств и назначении наказаний.

3. Отсутствие «правильно» размеченного датасета, полученного из эмпирического материала (статистика, материалы уголовных дел, представления прокурора, частные определения суда, приговоры и иные судебные решения, обвинительные заключения и обвинительные акты, постановления о прекращении уголовных дел).

Таким образом, современное развитие технологий машиночитаемого права открывает новые перспективы для совершенствования уголовного судопроизводства. Данная концепция предполагает создание онтологически структурированной правовой среды, в которой нормативные акты становятся доступными для анализа и обработки с применением искусственного интеллекта и автоматизированных систем. Внедрение технологий машинного анализа права позволяет минимизировать юридическую неопределенность, повысить качество правоприменительной практики и автоматизировать ключевые этапы уголовного процесса. В то же время выявленные нами сложности не являются критичными для создания такого рода систем и при должном подходе могут быть нивелированы при дальнейшей разработке системы.

ЛИТЕРАТУРА

1. Зуев С. В., Зазулин А. И. Цифровой УПК: новая концепция развития права // Правопорядок: история, теория, практика. — 2024. — № 1(40). — С. 67—77.

2. Малько А. В., Солдаткина О. Л. Приоритеты российской правовой политики и изменения права в условиях цифровизации // Журнал российского права. — 2019. — № 9. — С. 8.

3. Липчанская М. А., Привалов С. А. Развитие технологий машиночитаемого права: теоретические проблемы и перспективы // Журнал российского права. — 2022. — № 10. — С. 85—96.

4. Концепция развития технологий машиночитаемого права (утв. Правительственной комиссией по цифровому развитию, использованию информационных технологий для улучшения качества

жизни и условий ведения предпринимательской деятельности, протокол от 15.09.2021 № 31) // СПС «КонсультантПлюс», 2025.

5. Машиночитаемое право: правовой вызов современности / Р. Янковский, А. Вашкевич, А. Иванов [и др.] // Закон. — 2021. — № 10. — С. 20—26.

6. Порываева Н. Ф. Алгоритмизация права : дис. ... канд. юрид. наук. — М., 2022. — 108 с.

7. Понкин И. В. Концепт машиночитаемого и машиноисполняемого права: актуальность, назначение, место в PerTexe, содержание, онтология и перспективы // International Journal of Open Information Technologies. — 2020. — Т. 8, № 9. — С. 29—67.

8. Сазонова М. М. Машиночитаемое право: возможно ли его применение в ближайшем будущем? // СПС «Гарант», 2025.

9. Веревкин В. А., Бутов В. В. Применение модели машинного обучения при анализе текста как функции информационно-аналитической работы при возникновении кризисной ситуации // Вестник Воронежского института МВД России. — 2024. — № 3. — С. 98—105.

10. Ын А., Су К. Теоретический минимум по Big Data. Все, что нужно знать о больших данных. — СПб., 2019. — С. 21—39.

11. Перевозкин А. А. Теоретико-правовая характеристика машиночитаемого права // Актуальные проблемы российского права. — 2024. — № 8. — С. 22—37.

REFERENCES

1. Zuev S. V. Cifrovoy UPK: novaya koncepciya razvitiya prava / S. V. Zuev, A. I. Zazulin // Pravoporyadok: istoriya, teoriya, praktika. — 2024. — № 1(40). — С. 67—77.

2. Mal'ko A. V., Soldatkina O. L. Prioritety` rossijskoj pravovoj politiki i izmeneniya prava v usloviyax cifrovizacii // Zhurnal rossijskogo prava. — 2019. — № 9. — С. 8.

3. Lipchanskaya M. A., Privalov S. A. Razvitie texnologij mashinochitaemogo prava: teoreticheskie problemy` i perspektivy` // Zhurnal rossijskogo prava. — 2022. — № 10. — С. 85—96.

4. Koncepciya razvitiya texnologij mashinochitaemogo prava (utv. Pravitel'svennoj komissiej po cifrovomu razvitiyu, ispol'zovaniyu informacionny`x texnologij dlya uluchsheniya kachestva zhizni i uslovij vedeniya predprinimatel'skoj deyatel'nosti, protokol ot 15.09.2021 № 31) // SPS «Konsul'tantPlyus», 2025.

5. Mashinochitaemoe pravo: pravovoj vy`zov sovremennosti / R. Yankovskij, A. Vashkevich, A. Ivanov [i dr.] // Zakon. — 2021. — № 10. — С. 20—26.

6. Pory'vaeva N. F. Algoritmizaciya prava : dis.

... kand. jurid. nauk. — М., 2022. — 108 s.

7. Ponkin I. V. Koncept mashinochitaemogo i mashinoispolnyaemogo prava: aktual'nost', naznachenie, mesto v RegTexe, sodержание, ontologiya i perspektivy` // International Journal of Open Information Technologies. — 2020. — Т. 8, № 9. — С. 29—67.

8. Sazonova M. M. Mashinochitaemoe pravo: vozmozhno li ego primenenie v blizhajshem budushem? // SPS «Garant», 2025.

9. Verevkin V. A., Butov V. V. Primenenie modeli mashinnogo obucheniya pri analize teksta kak funkcii informacionno-analiticheskoy raboty` pri vznikenovonii krizisnoj situacii // Vestnik Voronezhskogo instituta MVD Rossii. — 2024. — № 3. — С. 98—105.

10. Y`n A., Su K. Teoreticheskij minimum po Big Data. Vse, chto nu-zhno znat' o bol'shix dannyx. — SPb., 2019. — С. 21—39.

11. Perevozkin A. A. Teoretiko-pravovaya xarakteristika mashinochitaemogo prava // Aktual'ny'e problemy` rossijskogo prava. — 2024. — № 8. — С. 22—37.

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: машиночитаемое право; онтология права; информационные технологии; интеллектуальные системы; нейронные сети; модели машинного обучения; анализ текста.

Key words: machine-readable law; ontology of law; information technology; intelligent systems; neural networks; machine learning models; text analysis.

УДК 343.121

А. А. Титов

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ КРИПТОПРЕСТУПНОСТИ С ИСПОЛЬЗОВАНИЕМ КРИМИНАЛИСТИЧЕСКОГО АНАЛИЗА ДАННЫХ БЛОКЧЕЙНА

METHODS OF COUNTERING CRYPTOCRIME USING FORENSIC ANALYSIS BLOCKCHAIN DATA

В статье рассматриваются актуальные вопросы противодействия преступлениям, связанным с криптовалютами, в контексте их криминалистического и оперативно-тактического анализа. Автор подчеркивает, что криптовалютная среда, обладая такими свойствами, как децентрализация, неизменность транзакций, прозрачность блокчейна и псевдоанонимность, формирует новый тип цифровых следов, требующих специализированных методов исследования.

The article examines current issues of counteracting crimes related to cryptocurrencies in the context of their forensic and operational-tactical analysis. The author emphasizes that the cryptocurrency environment, with such properties as decentralization, immutability of transactions, transparency of the blockchain and pseudo-anonymity, forms a new type of digital traces that require specialized research methods.

Деятельность, состоящая в раскрытии и расследовании преступлений, неразрывно сопровождается поиском и последующим использованием криминалистически значимой информации. Это обусловлено тем, что информация представляет собой фундаментальную категорию, определяющую процессы познания, принятия решений и коммуникации.

Информация определяется как абстрактное понятие, представляющее собой структурированные данные, несущие потенциальную смысловую нагрузку. Происходя от латинского «informare», означающего «придавать форму», информация требует материального носителя для своего проявления и передачи [1]. Однако её фундаментальная ценность заключается не в физической форме представления, а в организованной структуре данных, позволяющей извлекать знания и делать умозаключения.

Содержание информации, являясь её семантической составляющей, отражает смысл, передаваемый сообщением [2]. В контексте следственной работы содержание информации играет определяющую роль в формировании картины преступления, установлении мотивов и идентификации лиц, причастных к совершению противоправных действий. Интерпретация следов, показаний свидетелей, результатов оперативно-розыскных мероприятий и судебных экспертиз — всё это сводится к извлечению содержания информации, скрытого за символами, знаками и сигналами.

При этом эффективность извлечения информации напрямую зависит от компетенции следователя, его способности учитывать контекст, понимать специализированные термины и логически связывать разрозненные данные.

В этой связи нельзя не отметить справедливость суждения профессора А. С. Подшибякина о том, что криминалистика должна осваивать специфические закономерности возникновения следов преступления посредством внедрения в том числе технологических новшеств и достижений науки, а также расширения междисциплинарных связей с другими областями знаний [3].

Научные методы определения ценности информации, такие как статистический анализ, моделирование и экспертные оценки, могут быть использованы для принятия обоснованных решений о приоритетности различных направлений расследования и выборе оптимальных стратегий. Например, оценка вероятности успеха различных версий, основанная на статистических данных о раскрываемости аналогичных преступлений и экспертных оценках криминалистов, позволяет следователю более эффективно распределять ресурсы. В данном контексте профессор Н. П. Яблочков уместно упоминает о том, что следователю важно извлекать из среды не столько исчерпывающе полную информацию, сколько значимую в соответствующем контексте [4].

Как представляется, это оказывает существенное влияние на глобальные экономические

процессы, а также на экономическую ситуацию в Российской Федерации, что привлекает пристальное внимание не только участников легитимного финансового сектора, но и представителей криминального мира, стремящихся использовать новые возможности в противоправных целях.

Указанное требует проведения углубленного изучения рисков и разработки эффективных мер по противодействию злоупотреблениям, направленных на поддержание стабильности и безопасности финансовой системы в целом и обеспечение прав и законных интересов граждан в частности. В связи с этим приоритетное значение приобретает углубленное исследование технологических основ, лежащих в основе цифровых финансовых активов, в частности криптовалют.

Современная криптовалютная среда, обладая уникальным криминалистическим потенциалом, формирует принципиально новый тип структурированных данных, позволяющих реконструировать механизмы преступной деятельности. Это обусловлено её ключевыми свойствами: децентрализацией, неизменностью транзакций, прозрачностью блокчейна и псевдоанонимностью участников. Примечательно, что указанные характеристики создают устойчивые цифровые следы, которые при корректной интерпретации становятся основой для установления причинно-следственных связей, идентификации субъектов и доказывания их причастности к противоправным деяниям. Более того, ценность криминалистически значимой информации в данном контексте определяется её способностью минимизировать неопределённость в процессе расследования, однако её эффективное использование требует существенной адаптации традиционных методов к специфике криптотехнологий [5].

В этой связи следует подчеркнуть, что актуальность, точность, полнота и эргономичность данных выступают ключевыми критериями их криминалистической значимости, а их анализ должен опираться на принципы критического мышления, междисциплинарный подход и интеграцию современных инструментов, таких как графовая аналитика и алгоритмы машинного обучения. В частности, технология блокчейн, являясь фундаментом криптовалютной инфраструктуры, формирует новый тип слеодообразования, что, в свою очередь, требует разработки специализированной криминалистической методики. Несмотря на устойчивость и публичность данных в распределённом реестре, их интерпретация осложняется рядом факторов, среди которых особое место занимают псевдоанонимность, использование миксеров и приватных монет, а также трансграничный характер транзакций. Следовательно, это

обуславливает необходимость создания стандартизированных протоколов работы с цифровыми следами, включая их фиксацию, верификацию и интеграцию в доказательственную базу.

При этом цифровые следы, формируемые в блокчейн-среде, обладают уникальными характеристиками, обусловленными технологическими особенностями распределённых реестров. Их ключевые свойства — неизменяемость, прозрачность и структурированность — делают их ценным источником криминалистически значимой информации. Каждая транзакция, включая метаданные (временные метки, хеши, комиссии), создаёт устойчивый «цифровой отпечаток», позволяющий реконструировать цепочки перемещения активов. Однако следует учитывать, что псевдоанонимность участников и использование инструментов маскировки следов (миксеры, приватные криптовалюты) усложняют прямую идентификацию субъектов, что, в свою очередь, требует применения специализированных методов анализа. В данном контексте особую значимость приобретают такие подходы, как графовый анализ транзакций для выявления связей между кошельками, кластеризация адресов на основе шаблонов активности, а также корреляция данных из внешних источников [6].

Важно отметить, что разделение криптопреступлений на две категории — посягательства на криптовалюты и их использование в противоправных целях — определяет дифференциацию тактических приемов расследования. Так, в первом случае приоритетным является ретроспективный анализ транзакций в публичных реестрах блокчейна с целью установления цепочек перемещения активов, тогда как во втором акцент переносится на выявление инфраструктурных элементов, что требует применения превентивных оперативно-тактических моделей. Международный опыт свидетельствует о том, что симуляция элементов крипто-валютной инфраструктуры позволяет с высокой точностью документировать деятельность организованных преступных групп, однако результативность подобных операций напрямую зависит от технологической достоверности и учета субкультурных особенностей криминальной среды [7].

Не менее существенным фактором повышения эффективности раскрытия и расследования преступлений, совершаемых в отношении и с использованием криптовалют, является углубленный анализ и систематизация закономерностей между следами, оставленными в сети блокчейн, и данными, генерируемыми и распространяемыми на различных электронных социальных ресурсах. Комплексный подход к анализу цифровых следов,

в свою очередь, позволяет не только выявить прямые связи между участниками преступной деятельности, но и установить латентные, косвенные взаимосвязи, раскрывающие полную картину преступления и способствующие установлению всех причастных лиц.

Особого внимания заслуживают тактические особенности проведения допроса жертв криптопреступлений, которые обусловлены необходимостью детализации каналов коммуникации со злоумышленниками, включая мессенджеры, социальные сети и специализированные инвестиционные платформы. При этом ключевое значение приобретает фиксация технических параметров транзакций, таких как типы криптовалют, адреса кошельков и данные криптобирж. Кроме того, установление методов манипуляции, включая обещания высокой доходности и психологическое давление, требует применения психологических подходов к анализу поведения жертв, а приобщение скриншотов переписок и выписок транзакций может существенно усилить значение опроса в поисковых мероприятиях [8].

С развитием цифровых технологий и ростом популярности криптовалют вопросы их регулирования приобретают всё большее значение для обеспечения безопасности как на международном, так и на национальном уровнях. В связи с этим криминалистическое обеспечение раскрытия и расследования преступлений, связанных с криптовалютами, развивается в различных направлениях.

В соответствии с позицией, обозначенной В. А. Ализаде и А. Г. Волеводзом, одним из приоритетных направлений стало формирование надлежащей регуляторной модели финансовых отношений, возникающих между пользователями криптовалют, и разработка комплекса соответствующих мер, направленных на противодействие противоправным действиям в этой сфере [9].

Ввиду отсутствия унифицированных нормативных рамок, регулирующих обращение криптовалют в различных юрисдикциях, международные правоохранительные организации стали активно разрабатывать систему методов контроля за этой деятельностью.

В контексте противодействия криптопреступлениям одним из определяющих элементов регуляторной стратегии, формирующим основу для накопления криминалистически значимой информации, стала политика ФАТФ, направленная на всестороннюю интеграцию сферы виртуальных активов в существующую систему противодействия отмыванию доходов, полученных преступным путем, финансированию терроризма и распространения оружия массового уничтожения

(ПОД/ФТ/ФРОМУ) [10]. Данный подход предполагает не только адаптацию действующих стандартов и рекомендаций к специфическим особенностям криптовалют, но и разработку правил, направленных на эффективное регулирование данного сегмента финансовой системы [11].

В регуляторной стратегии ФАТФ центральное место занимает так называемое «Правило путешествий». Это правило, применявшееся в отношении традиционных финансовых институтов, в настоящее время распространяется на поставщиков услуг виртуальных активов (далее — ПУВА), обязывая их собирать и передавать информацию об отправителях и получателях криптовалютных транзакций. Соответственно, указанные сведения должны аккумулироваться благодаря обязательной аутентификации личности абонентов путем сбора их полных имен, адресов проживания и реквизитов счетов отправителя и получателя (правило «Знай своего клиента», с англ. — «know your customer», далее — KYC) [12].

Как справедливо отмечается в работе индийского криминалиста Д. Халдера, «в контексте формирования эффективной глобальной системы противодействия преступлениям в секторе виртуальных активов внедрение „Правил путешествий“ является обязательным условием». Эффективное применение этого регуляторного инструмента способствует минимизации рисков, связанных с финансовыми злоупотреблениями, повышает уровень доверия к операциям с виртуальными активами и легитимизирует их функционирование в парадигме общественного и регуляторного признания» [13].

В результате создаются благоприятные условия для повышения эффективности работы оперативных и следственных органов за счёт отслеживания транзакций и идентификации субъектов, вовлечённых в незаконные операции. При этом о значимости указанных правил упоминается в работе профессора М. Наззари. По мнению автора, «решающее значение приобретает обеспечение строгого соблюдения конфиденциальности данных, передаваемых в рамках реализации „Правил путешествия“» [14].

Стремительное увеличение количества криптовалют и их использование в различных преступных схемах обусловило необходимость разработки новых подходов к системе противодействия транснациональной организованной преступности. Рекомендации ФАТФ, направленные на регулирование этой сферы, стали важным этапом в формировании правовой базы, направленной на противодействие отмыванию денег, финансированию терроризма и распространению оружия массового уничтожения.

По уместному замечанию Д. А. Кулева, «государствам предписано срочно принять законодательные и практические шаги, направленные на предотвращение злоупотребления виртуальными активами, включая оценку и понимание связанных с ними рисков, что также нашло отражение в принятой ФАТФ в 2019 г. пояснительной записке к 15-й рекомендации» [15]. Причем реализация этих рекомендаций в национальном законодательстве позволила укрепить систему финансового мониторинга и повысить прозрачность операций с криптовалютами.

В одной из своих работ П. А. Литвишко обоснованно утверждает, что положения руководства ФАТФ, касающиеся лицензирования и регистрации ПУВА, рассматриваются как ориентир при определении правил установления и осуществления более широкой территориальной и экстерриториальной уголовной юрисдикции [16]. Опираясь на такой ориентир, государства могут использовать принципы, изложенные в руководстве ФАТФ, для расширения своей юрисдикции в делах, связанных с криптопреступлениями, даже если деяние совершено за пределами их территории. Подобный подход способствует уголовному преследованию лиц, причастных к преступной деятельности, и привлечению их к ответственности, в том числе в случаях нахождения за рубежом. Стандарты ФАТФ оказывают значительное влияние на развитие международного сотрудничества в обозначенной сфере.

Указанный аспект приобретает первостепенное значение в контексте цифрового обмена информацией между национальными подразделениями финансовых разведок, вошедших в состав Группы Эгмонт (с англ. — Egmont Group of Financial Intelligence Units), которая была сформирована в целях оптимизации работы каналов взаимодействия оперативного отслеживания подозрительных финансовых операций [17]. С помощью созданной защищенной сети (Egmont Secure Web, ESW) между участниками Группы Эгмонт могут отправляться запросы в круглосуточном режиме для срочного исполнения. В условиях осуществления молниеносных транзакций между криптобиржами, находящимися в различных юрисдикциях и зачастую характеризующихся различным уровнем регуляторного контроля, сведения, полученные по каналам ESW, становятся важнейшим источником криминалистически значимой информации.

В условиях сложившейся политической обстановки участие ПФР Российской Федерации в Группе Эгмонт было приостановлено. Однако сотрудничество в по обмену информацией с отдельными странами в рамках действующих договоров о взаимном сотрудничестве продолжается.

Современные подходы к регулированию криптовалютной индустрии в различных странах напрямую влияют на возможности правоохранительных органов по сбору криминалистически значимой информации, необходимой для эффективного раскрытия и расследования преступлений, связанных с цифровыми активами.

В юрисдикциях, характеризующихся установлением тотального запрета на использование криптовалют, как это наблюдается, в частности, в Алжире, Бангладеш, Боливии, Египте, Иране и Непале, процесс получения криминалистически значимой информации сопряжен с возникновением существенных правовых и технологических трудностей. Данное обстоятельство обусловлено прежде всего перемещением преступной активности в теневой сегмент криптоэкономики, что, в свою очередь, приводит к ограничению доступа к первичным данным, генерируемым криптографическими биржами. Фактически это исключает возможность легитимного получения информации о транзакциях и лицах, представляющих оперативный интерес, из источников, функционирующих в рамках правового поля.

В обозначенных условиях эффективность мероприятий оперативно-розыскного характера оказывается в прямой зависимости от разработки и внедрения инновационных методов и инструментов, нацеленных на преодоление механизмов анонимизации и выявление преступных схем, которые, как показывает иностранная практика, все чаще выстраиваются трансграничными организованными преступными сообществами (синдикатами) на территории сразу нескольких государств. Особую актуальность приобретают методы активного получения информации, такие как внедрение агентов в криминальные сообщества, использование «кибер-приманок» и перехват трафика в Даркнете.

В заключение следует подчеркнуть, что эффективное противодействие криптопреступности требует интеграции инновационных оперативно-тактических моделей, основанных на создании контролируемых цифровых платформ, имитирующих функционал криминальной инфраструктуры. Ключевым условием успеха выступает синтез блокчейн-аналитики с традиционными оперативными методами, позволяющими реконструировать сетевые взаимодействия преступных групп и устанавливать их иерархию. Таким образом, дальнейшее развитие криминалистической методологии в данной сфере должно быть направлено на совершенствование междисциплинарных подходов, обеспечивающих комплексное исследование цифровых следов в условиях технологической эволюции преступной деятельности.

ЛИТЕРАТУРА

1. Чернавский Д. С. Синергетика и информация. Динамическая теория информации. — М.: УРСС. ЛЕНАНД. 2017. — 304 с.
2. Ладов В. А. О понятии информации в контексте современных исследований по проблемам семантики и искусственного интеллекта // Вестник Томского государственного университета. Философия. Социология. Политология. — 2013. — № 4 (24). — С. 26—32.
3. Подшибякин А. С. Современная криминалистика и ее развитие // Криминалистика и судебно-экспертная деятельность в условиях современности : материалы международной научно-практической конференции : в 2 т., Краснодарский университет МВД России, 26 апреля 2013 г. / Том I. — Краснодарский университет МВД России, 2013. — Т. 1. — С. 3—15.
4. Яблоков Н. П. К вопросу о криминалистическом мышлении // Правовые проблемы укрепления российской государственности. — Томск, 2012. — С. 156—159.
5. Использование информации, содержащейся на электронных носителях, в уголовно-процессуальном доказывании : учебное пособие / А. А. Балашова, В. Ф. Васюков, Ю. В. Гаврилин [и др.] ; под ред. Ю. В. Гаврилина и А. В. Победикина. — Москва : Академия управления Министерства внутренних дел Российской Федерации, 2021. — 140 с.
6. Стельмах В. Ю., Ефремова О. М., Васюков В. Ф. Производство следственных действий, направленных на получение и использование компьютерной информации. — М. : Проспект, 2021. — 480 с.
7. Васюков В. Ф. Расследование дел о сбыте наркотиков с использованием мессенджеров и криптовалюты // Уголовный процесс. — 2019. — № 9 (177). — С. 44—49.
8. Бессонов А. А. Проблемные вопросы установления признаков организованной группы по преступлениям, совершенным с использованием информационно-телекоммуникационных технологий // Журнал российского права. — 2024. — Т. 28, № 1. — С. 108—119.
9. Ализаде В. А., Волеводз А. Г. Неприменение ст. 174.1 Уголовного кодекса РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты, как следствие непонимания сущности легализации (отмывания) нового вида преступных активов // Наркоконтроль. — 2018. — № 1. — С. 5—13.
10. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. FATF. — Paris, France, 2025. — URL: www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatfrecommendations.html (дата обращения: 05.04.2025).
11. Levi M., Soudijn M. Understanding the laundering of organized crime money // Crime and Justice. — 2020. — Vol. 49. — P. 579—631.
12. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF. — Paris, France, 2021. — URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html> (дата обращения: 14.03.2025).
13. Halder D. Legal Challenges to Cryptocurrency and its Guardian-Less Victims in India: A Critical Victimological Analysis // International Annals of Criminology. — 2022. — Vol. 60, No. 1. — P. 79—98.
14. Nazzari M. From payday to payoff: Exploring the money laundering strategies of cybercriminals // Trends in Organized Crime. — 2023. — P. 95—112.
15. Кунев Д. А. Международно-правовые стандарты противодействия криминальному обороту криптовалют и иных виртуальных активов // Вестник Университета прокуратуры Российской Федерации. — 2022. — № 1 (87). — С. 146—151.
16. Литвишко П. А. Юрисдикционные и международно-правовые аспекты обеспечительных и конфискационных мер в отношении виртуальных активов // Законность. — 2021. — № 3. — С. 10—11.
17. Principles for information exchange between financial intelligence units approved by the heads of fuis july 2013 // Egmont Group. — URL: https://egmontgroup.org/wp-content/uploads/2022/07/2.-Principles-Information-Exchange-With-Glossary_April2023.pdf (дата обращения: 14.03.2025).

REFERENCES

1. Chernavskij D. S. Sinergetika i informaciya. Dinamicheskaya teoriya informacii. — M.: URSS. LENAND. 2017. — 304 s.
2. Ladov V. A. O ponyatii informacii v kontekste sovremennyh issledovanij po problemam semantiki i iskusstvennogo intellekta // Vestnik Tomskogo gosudarstvennogo universiteta. Filosi-fiya. Sociologiya. Politologiya. — 2013. — № 4 (24). — S. 26—32.
3. Podshibyakin A. S. Sovremennaya kriminalistika i ee razvitie // Kriminalistika i sudebno-ekspertnaya deyatel'nost' v usloviyah sovremen-

nosti : materialy mezhdunarodnoj nauchno-prakticheskoy konferencii : v 2 t., Krasnodarskij universitet MVD Rossii, 26 aprelya 2013 g. / Tom I. — Krasnodarskij universitet MVD Rossii, 2013. — T. 1. — S. 3—15.

4. Yablokov N. P. K voprosu o kriminalisticheskom myshlenii // Pravovye problemy ukrepleniya rossijskoj gosudarstvennosti. — Tomsk, 2012. — S. 156—159.

5. Ispol'zovanie informacii, sodержashchejsya na elektronnyh nositelyah, v ugovolno-processual'nom dokazyvanii : uchebnoe posobie / A. A. Balashova, V. F. Vasyukov, Yu. V. Gavrilin [i dr.] ; pod red. Yu. V. Gavrilina i A. V. Pobedkina. — Moskva : Akademiya upravleniya Ministerstva vnutrennih del Rossijskoj Federacii, 2021. — 140 s.

6. Stel'mah V. Yu., Efremova O. M., Vasyukov V. F. Proizvodstvo sledstvennyh dejstvij, napravlennyh na poluchenie i ispol'zovanie komp'yuternoj informacii. — M. : Prospekt, 2021. — 480 s.

7. Vasyukov V. F. Rassledovanie del o sbyte narkotikov s ispol'zovaniem messendzherov i kriptovalyuty // Ugolovnyj process. — 2019. — № 9 (177). — S. 44—49.

8. Bessonov A. A. Problemnye voprosy ustanovleniya priznakov organizovannoj gruppy po prestupleniyam, sovershennym s ispol'zovaniem informacionno-telekommunikacionnyh tekhnologij // Zhurnal rossijskogo prava. — 2024. — T. 28, № 1. — S. 108—119.

9. Alizade V. A., Volevodz A. G. Neprimenenie st. 174.1 Ugolovnogo kodeksa RF po delam o narkoprestupleniyah, sovershennyh s ispol'zovaniem kriptovalyuty, kak sledstvie neponimaniya sushchnosti legalizacii (otmyvaniya) novogo vida prestupnyh aktivov // Narkokontrol'. — 2018. — № 1. — S. 5—13.

10. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. FATF. — Paris, France, 2025. — URL: www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatfrecommendations.html (data obrashcheniya: 05.04.2025).

11. Levi M., Soudijn M. Understanding the laundering of organized crime money // Crime and Justice. — 2020. — Vol. 49. — P. 579—631.

12. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF. — Paris, France, 2021. — URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html> (data obrashcheniya: 14.03.2025).

13. Halder D. Legal Challenges to Cryptocurrency and its Guardian-Less Victims in India: A Critical Victimological Analysis // International Annals of Criminology. — 2022. — Vol. 60, No. 1. — P. 79—98.

14. Nazzari M. From payday to payoff: Exploring the money laundering strategies of cybercriminals // Trends in Organized Crime. — 2023. — P. 95—112.

15. Kunev D. A. Mezhdunarodno-pravovye standarty protivodejstviya kriminal'nomu oborotu kriptovalyut i inyh virtual'nyh aktivov // Vestnik Universiteta prokuratury Rossijskoj Federacii. — 2022. — № 1 (87). — S. 146—151.

16. Litvishko P. A. Yurisdikcionnye i mezhdunarodno-pravovye aspekty obespechitel'nyh i konfiskacionnyh mer v otnoshenii virtual'nyh aktivov // Zakonnost'. — 2021. — № 3. — S. 10—11.

17. Principles for information exchange between financial intelligence units approved by the heads of fuis july 2013 // Egmont Group. — URL: https://egmontgroup.org/wp-content/uploads/2022/07/2.-Principles-Information-Exchange-With-Glossary_April2023.pdf (data obrashcheniya: 14.03.2025).

СВЕДЕНИЯ ОБ АВТОРЕ

Титов Андрей Александрович. Начальник отдела управления по расследованию организованной преступной деятельности.

Следственный департамент МВД России.

E-mail: titov-aa@yandex.ru

Россия, 101000, Москва, ул. Мясницкая, 3.

Titov Andrey Aleksandrovich. Head of the Department of the Department for the Investigation of Organized Crime.

Investigative Department of the Ministry of Internal Affairs of Russia.

E-mail: titov-aa@yandex.ru

Russia, 101000, Moscow, Myasnitskaya Str., 3.

Ключевые слова: криптовалюты; блокчейн; криминалистика; оперативно-розыскная деятельность; ФАТФ; цифровые следы; деанонимизация; трансграничные преступления.

Key words: cryptocurrencies; blockchain; forensics; operational investigative activities; FATF; digital traces; deanonymization; cross-border crimes.

УДК 343

ИНФОРМАЦИЯ ДЛЯ АВТОРОВ

И. И. Иванов, П. П. Петров, С. С. Сидоров

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 авторах¹.

Аннотация на английском языке².

1. Статья представляется в одном экземпляре, заверенном подписью автора (-ов) с обратной стороны первой страницы, отпечатанном на одной стороне листов формата А4 (210 x 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:

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.

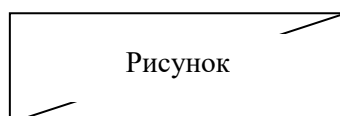


Рис. 1. Название рисунка

Отступ от рисунка до текста сверху и снизу должен быть равен 10 мм. Подписочная 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 анτισоциальных 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. Tolkovyy 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.) // Sbranie zakonodatelstva Rossiyskoy Federatsii. — 2011. — № 7. — St. 900.
5. Zhelonkin S. S. Nedeystvitelnost antisotsialnyih sdelok, narushayuschiy osnovyi pravoporyadka i нравstvennosti : 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, S. S. Sidorov

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.

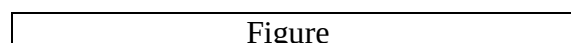


Fig.1 Figure caption

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 indentation. 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.**

REFERENCES 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. : Vysshaya shkola, 1993. — 125 s. (*editor is required*).
3. Sidorov S. S., Antonov A. A. Problemy 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 obshchey fiziki : ucheb. posobie dlya studentov vtuzov. — 2-e izd., pererab. — T. 1. Mekhanika / pod obshch. 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____