

ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

**НАУЧНЫЙ БЮЛЛЕТЕНЬ
ВОРОНЕЖСКОГО ИНСТИТУТА МВД РОССИИ**

Сборник

Выпуск 4

**Воронеж
2025**

Редакционная коллегия:

Председатель: С. В. Родин, кандидат технических наук, доцент;

Заместитель председателя: Р. В. Бузин, кандидат экономических наук;

Ответственный секретарь: Н. В. Крючкова.

Члены редакционной коллегии:

Н. В. Гвоздева, кандидат филологических наук;

С. Б. Ахлюстин, кандидат технических наук;

А. И. Ляпин, кандидат педагогических наук, доцент;

Н. В. Полякова, кандидат юридических наук, доцент;

Т. В. Мещерякова, доктор технических наук, профессор;

М. М. Жуков, кандидат технических наук, доцент;

С. В. Железный, кандидат технических наук, доцент;

С. А. Гречаный, кандидат технических наук, доцент;

А. В. Пучнин, кандидат юридических наук, доцент;

И. В. Сычев, кандидат физико-математических наук, доцент;

Е. А. Буданова, кандидат юридических наук, доцент;

О. В. Пьянков, доктор технических наук, профессор;

О. С. Авсентьев, доктор технических наук, доцент;

К. К. Панько, доктор юридических наук, доцент;

И. А. Сабирова, доктор педагогических наук, доцент;

П. П. Фомин, кандидат юридических наук, доцент.

Научный бюллетень Воронежского института МВД России : сборник. Вып. 4. [Электронный ресурс]. – Электр. дан. и прогр. – Воронеж : Воронежский институт МВД России, 2025. – 2 электр. опт. диск (CD-ROM) : 12 см. – Систем. требования: процессор Intel с частотой не менее 1,3 ГГц ; ОЗУ 512 Мб ; операц. система семейства Windows ; CD-ROM дисковод.

Сборник содержит материалы Всероссийского семинара «Использование перспективных технологий в создании технических устройств и подготовке специалистов для органов внутренних дел» (22 октября 2025 года), Всероссийского семинара «Организационно-техническое обеспечение безопасности охраняемых территорий и объектов органов внутренних дел» (28 октября 2025 года), Всероссийского круглого стола «Проблемы адаптации сотрудников подразделений по делам несовершеннолетних на первоначальном этапе профессиональной деятельности и пути их решения» (29 октября 2025 года).

Издание представляет интерес для профессорско-преподавательского состава, адъюнктов, курсантов и слушателей образовательных организаций МВД России и сотрудников правоохранительных органов.

СОДЕРЖАНИЕ
ВСЕРОССИЙСКИЙ СЕМИНАР
ИСПОЛЬЗОВАНИЕ ПЕРСПЕКТИВНЫХ ТЕХНОЛОГИЙ
В СОЗДАНИИ ТЕХНИЧЕСКИХ УСТРОЙСТВ И ПОДГОТОВКЕ
СПЕЦИАЛИСТОВ ДЛЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

С. Н. Анисимов, В. Р. Голубева

Применение искусственного интеллекта в создании инновационных технических средств в деятельности органов внутренних дел 6

И. В. Гилев

Применение SDR-приемника для локализации источника радиоизлучения: методы, алгоритмы и практическая эффективность 9

А. А. Жирнов

Оптимизационные модели в управлении проектами противодействия криминальным угрозам 13

И. А. Кубасов, Ю. В. Барашкин

О направлении развития информационных систем подразделений МВД России в сфере миграции 19

В. В. Лопухов, Э. Р. Зарипова

Проблемные вопросы преподавания математических дисциплин в подразделениях МВД России 24

Е. В. Матяшова

Проблемы адаптации и внедрения передовых технологий в повседневную практику органов внутренних дел 31

В. П. Удалов

Вопросы оценки параметров сигналов радиолокационных систем 35

П. В. Шаляпин

Разработка алгоритма оценки уровня ИТ-компетентности сотрудников МВД России 39

ВСЕРОССИЙСКИЙ СЕМИНАР
ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ
БЕЗОПАСНОСТИ ОХРАНЯЕМЫХ ТЕРРИТОРИЙ И ОБЪЕКТОВ
ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Е. М. Абросимова

Обзор современных систем видеонаблюдения с возможностью аналитики данных 43

Е. С. Бондаренко

Особенности антитеррористической защищенности и противодействия диверсиям с использованием беспилотных летательных аппаратов на объектах правоохранительных органов 46

С. А. Гречаный

Особенности защиты объекта охраны при возникновении чрезвычайной ситуации 51

П. М. Дуплякин

Повышение надежности систем безопасности при эксплуатации 59

Н. В. Зубова, В. Г. Волкова, Н. А. Садчикова

Особенности безопасного хранения гражданского оружия 64

И. С. Ивануха, Д. Ю. Калков

Специфика обеспечения безопасности зданий и сооружений органов внутренних дел 72

Д. Ю. Калков, М. А. Гудков, И. С. Ивануха

Организационно-технические мероприятия по повышению защищенности объектов органов внутренних дел, в частности от угроз беспилотных летательных аппаратов 80

П. В. Комраков, М. А. Гудков, А. А. Гапеев, Д. Ю. Калков

Прогнозирование времени выброса нефти и нефтепродуктов из резервуара при пожаре 88

А. А. Михайлов

Перспективы развития средств поражения беспилотных воздушных судов 97

А. В. Сидоров

Совершенствование защищенности объектов охраны в условиях противодействия беспилотным воздушным судам 105

О. В. Толстых	
Правовые аспекты использования беспилотных воздушных судов в охране объектов	113
А. В. Чаплыгин, А. В. Гребенкин, А. И. Янгиров	
Электромагнитная совместимость. Насущная потребность или вынужденная мера	117
А. И. Янгиров, Е. А. Рогозин	
О разработке метода количественной оценки защищенности открытых операционных систем АРМ Российской Федерации	125

ВСЕРОССИЙСКИЙ КРУГЛЫЙ СТОЛ
ПРОБЛЕМЫ АДАПТАЦИИ СОТРУДНИКОВ
ПОДРАЗДЕЛЕНИЙ ПО ДЕЛАМ НЕСОВЕРШЕННОЛЕТНИХ
НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ
ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ
И ПУТИ ИХ РЕШЕНИЯ

Д. В. Вечерникова	
К вопросу о некомплекте штатной численности подразделений по делам несовершеннолетних органов внутренних дел и минимизацией увольнений в первые годы службы	131
И. С. Губарев	
Профессиональная адаптация специалистов, впервые прибывших на службу в системе правоохранительных органов	135
А. З. Динисламова	
Некоторые вопросы реализации правовых и социальных гарантий как фактор повышения привлекательности службы для молодого специалиста подразделения по делам несовершеннолетних	139
М. М. Курашова	
Индивидуальные адаптационные маршруты выпускников МВД России: правовые возможности и ограничения	144
О. С. Павленко	
Об адаптации и некоторых адаптационных барьерах молодых специалистов подразделений по делам несовершеннолетних, окончивших образовательные организации системы МВД России	150

ВСЕРОССИЙСКИЙ СЕМИНАР
ИСПОЛЬЗОВАНИЕ ПЕРСПЕКТИВНЫХ ТЕХНОЛОГИЙ
В СОЗДАНИИ ТЕХНИЧЕСКИХ УСТРОЙСТВ И ПОДГОТОВКЕ
СПЕЦИАЛИСТОВ ДЛЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

С. Н. Анисимов, В. Р. Голубева

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА
В СОЗДАНИИ ИННОВАЦИОННЫХ ТЕХНИЧЕСКИХ СРЕДСТВ
В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

APPLICATION OF ARTIFICIAL INTELLIGENCE
IN CREATING INNOVATIVE TECHNICAL MEANS
IN THE ACTIVITIES OF INTERNAL AFFAIRS BODIES

В статье рассматриваются вопросы применения искусственного интеллекта в деятельности органов внутренних дел.

The article discusses the application of artificial intelligence in the activities of internal affairs agencies.

В последние годы искусственный интеллект (ИИ) занял важное место среди технологий, определяющих развитие различных сфер общественной жизни. Растущая зависимость общества от информационных ресурсов привела к тому, что преступная деятельность все более активно переходит в информационное пространство. Преступники используют достижения в области ИИ для совершения противоправных действий [1].

Доля преступлений, совершенных с использованием ИИ в сети Интернет, неуклонно растет. Если в 2018 году она составляла около 9%, то к 2023 году увеличилась до почти 35%. Большинство таких преступлений (примерно 70%) связаны с хищением имущества.

Исследования по противодействию преступлениям с использованием ИИ в системе МВД России находятся на начальной стадии развития. Период с 2020 по 2024 год можно охарактеризовать как этап первоначального освоения концепции ИИ и его потенциальных возможностей в борьбе с преступностью.

Рассматривая мировой опыт, мы наблюдаем такую информацию, что во многих странах искусственный интеллект играет не малую роль и служит помощником в сфере органов внутренних дел [2], так, в США используется система PredPol, которая умеет прогнозировать возможные преступления в конкретных районах с помощью исторических данных. В Китае используется специальные камеры, которые при массовых беспорядках сканируют лицо преступника с помощью системы распознавания лиц и передают эту

информацию сотрудникам, а также камеры служат для наблюдения определенных мест и, если происходит что-то подозрительное передают сигнал специалистам для того, чтобы заблаговременно останавливать незаконные действия. В Индии имеется база с искусственным интеллектом, которая анализирует данные о преступлениях, чем помогает полиции использовать определенные тактики для снижения преступлений и осуществляет контроль этих местностей. В Казахстане внедряется система видеонаблюдения с функциями распознавания лиц и автоматизированной обработки данных для улучшения скорости реагирования. К этому можно отнести проект «Сергек», который с помощью системы видеонаблюдения, следит за дорожным движением и, если произошло нарушение, фиксирует номера автомобилей и передает информацию сотрудникам, еще используется как помощник для расследования преступлений. В крупных городах производит мониторинг местности для предотвращения краж или же других преступлений, а также прогнозирует «очаги» преступности с помощью исторических данных и дает рекомендации по размещению дополнительного патруля.

Во многих странах искусственный интеллект помогает предотвратить террористические акты и другие правонарушения на аэропортах, вокзалах, торговых центрах и других мест массового скопления людей [3]. Так, например система «Безопасный город» широко используется в Китае, проводя анализ можно заметить, что ИИ с помощью своих функций моментально находит людей, которые считаются пропавшими или в розыске. За несколько месяцев эта система показала положительный результат, где сократила уровень преступности на 15%. Также эта система используется, как и многие другие для мониторинга территорий, подачи сигнала о возможном преступлении или правонарушении.

ЛИТЕРАТУРА

1. Анисимов С. Л. К вопросу о понятии «преступления в сфере высоких технологий» / С. Л. Анисимов, К. А. Ситников // Евразийский юридический журнал. – 2024. – № 2(189). – С. 421–424.
2. Попов А. В. Перспективы применения нейросетевых технологий в деятельности органов внутренних дел / А. В. Попов, С. Л. Анисимов // Актуальные проблемы кибербезопасности в сети Интернет : Сборник научных трудов Всероссийской конференции, Москва, 23 апреля 2020 года. – Москва : Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2020. – С. 111–113.
3. Голубева В. Р. Как искусственный интеллект применяется с промышленными беспилотниками / В. Р. Голубева // Актуальные вопросы эксплуатации систем охранного мониторинга и защищенных телекоммуникационных систем : Материалы Всероссийской научно-практической конференции адъюнктов, курсантов и слушателей, Воронеж, 10 июня 2025 года. – Воронеж : Воронежский институт МВД РФ, 2025. – С. 164–166.

СВЕДЕНИЯ ОБ АВТОРАХ

Анисимов Сергей Леонидович.
Доцент кафедры физики и радиоэлектроники.
Кандидат технических наук, доцент.
Воронежский институт МВД России.
E-mail: anisimov12@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Голубева Валерия Романовна.
Курсант.
Воронежский институт МВД России.
E-mail: Valgolybevaval15@gmail.com
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Anisimov Sergey Leonidovich.
Associate Professor of the Department of Physics and Radioelectronics.
Candidate of Technical Sciences, Associate Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: anisimov12@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Golubeva Valeria Romanovna.
Cadet.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: Valgolybevaval15@gmail.com
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: искусственный интеллект; преступления; правонарушения; распознавание лиц; мониторинг; предотвращение; видеонаблюдение.

Keywords: artificial intelligence; crimes; offenses; facial recognition; monitoring; prevention; video surveillance.

УДК 004.8

**ПРИМЕНЕНИЕ SDR-ПРИЕМНИКА
ДЛЯ ЛОКАЛИЗАЦИИ ИСТОЧНИКА РАДИОИЗЛУЧЕНИЯ:
МЕТОДЫ, АЛГОРИТМЫ И ПРАКТИЧЕСКАЯ ЭФФЕКТИВНОСТЬ**

**APPLICATION OF SDR RECEIVER
FOR LOCALIZATION OF RADIO EMISSION SOURCE:
METHODS, ALGORITHMS AND PRACTICAL EFFICIENCY**

В статье рассматриваются современные методы локализации источников радиоизлучения с использованием программно-определяемых радиоприемников (SDR). Анализируются три ключевых метода: пеленгация по амплитуде, разность времени прихода (TDoA) и разность частоты прихода (FDoA). Приводятся математические модели и расчеты точности для каждого метода. Показано, что комбинирование нескольких SDR-приемников в единую измерительную сеть позволяет достичь точности локализации, сопоставимой со специализированными системами, при значительном снижении стоимости аппаратного обеспечения.

This article examines modern methods for localizing radio sources using software-defined radio receivers (SDRs). Three key methods are analyzed: amplitude direction finding, time difference of arrival (TDoA), and frequency difference of arrival (FDoA). Mathematical models and accuracy calculations for each method are presented. It is shown that combining multiple SDR receivers into a single measurement network enables localization accuracy comparable to that of dedicated systems, while significantly reducing hardware costs.

Задача оперативного обнаружения и точного определения местоположения источников радиоизлучения (ИРИ) является критически важной для решения широкого круга задач: от радиоэлектронной борьбы (РЭБ) и радиоразведки до мониторинга использования спектра и поиска нелегальных передатчиков. Традиционные пеленгаторы и системы локализации, построенные на специализированной аппаратной базе, отличаются высокой стоимостью и малой гибкостью.

Технология программно-определяемого радио (SDR) совершила переворот в этом направлении, перенесла сложность обработки сигналов в программную среду. Это позволяет на базе недорогих аппаратных компонентов (RTL-SDR, HackRF, USRP) создавать высокоэффективные и адаптируемые под конкретную задачу системы локализации [2-4].

Цель данной работы – провести системный анализ методов локализации ИРИ, реализуемых с помощью SDR-приемников, дать сравнительную оценку их точности на основе математического аппарата и определить области их практического применения.

1. Метод амплитудной пеленгации [1]

Данный метод основан на использовании направленной антенны или антенной решетки. Пеленг (направление на источник) определяется путем поиска максимума амплитуды принимаемого сигнала при сканировании диаграммы направленности антенны в пространстве.

Математическая модель амплитудной пеленгации. Для вращающейся направленной антенны с диаграммой направленности (ДН), описываемой функцией $F(\theta)$, мощность принимаемого сигнала изменяется как:

$$P(\theta) = P_0 * F(\theta - \theta_0), \quad (1)$$

где P_0 – мощность сигнала, θ_0 – истинный азимут на ИРИ.

Точность метода определяется шириной ДН. Для параболической антенны ширина ДН на уровне половинной мощности приближенно равна:

$$\theta_{\text{HPBW}} \approx 70 * \lambda / D \text{ (градусов)},$$

где λ – длина волны, D – диаметр антенны.

Типичная среднеквадратическая ошибка пеленгации составляет примерно 12° .

2. Метод разности времени прихода (Time Difference of Arrival - TDoA) Метод TDoA основан на измерении разности времени прихода одного и того же сигнала на три и более разнесенных в пространстве приемных станции. Каждая измеренная разность времен определяет линию положения (гиперболу), а точка пересечения нескольких гипербол соответствует местоположению ИРИ.

Математическая модель: разность расстояний между ИРИ и двумя приемниками i и j определяется как:

$$\Delta d_{ij} = c * \Delta t_{ij} = |R_i - R_t| - |R_j - R_t|, \quad (2)$$

где c – скорость света, Δt_{ij} – измеренная разность времени прихода,

R_t – координаты ИРИ, R_i, R_j – координаты приемников.

Геометрический фактор, влияющий на точность TDoA, называется Geometric Dilution of Precision (GDOP). Погрешность определения местоположения σ_{xy} связана с погрешностью измерения времени σ_t . Современные SDR-приемники, синхронизированные от одного GPS-источника, позволяют достичь $\sigma_t \approx 10\text{-}50$ нс, что при $\text{GDOP}=2$ дает $\sigma_{xy} \approx 6\text{-}30$ м. При реализации одним из основных требований является жесткая синхронизация по времени и частоте всех приемников в сети, что достигается использованием GPS-модулей (например, GPSDO).

3. Метод разности частоты прихода (Frequency Difference of Arrival - FDoA). Метод FDoA, также известный как дифференциальная доплеровская пеленгация, используется для локации движущихся ИРИ или при движении приемников. Он основан на измерении разности доплеровских смещений частоты сигнала, принимаемого двумя разнесенными приемниками.

Математическая модель метода содержит разности доплеровских смещений и вычисляется как:

$$\Delta f_D = (f_0 / c) \cdot [(v_i \cdot u_i) - (v_j \cdot u_j)], \quad (3)$$

где f_0 – несущая частота ИРИ, v_i, v_j – векторы скорости приемников,

u_i, u_j – единичные векторы направления от приемников на ИРИ.

Погрешность FDoA сильно зависит от точности знания собственного местоположения и скорости приемных платформ. Для спутниковых систем или БПЛА с высокоточными GPS/INS системами погрешность локации может составлять сотни метров. Для реализации с использованием SDR требуются высокостабильные опорные генераторы для точного измерения.

Проведенный анализ демонстрирует, что SDR-технологии открывают широкие возможности для создания эффективных систем локализации источников радиоизлучения.

1. Амплитудные методы на базе SDR и антенных решеток являются наиболее простыми в реализации и оптимальны для задач грубой оценки направления, где не требуется высокая точность.

2. Метод TDoA является наиболее перспективным для точного позиционирования как стационарных, так и подвижных объектов. Создание сетей синхронизированных SDR-приемников позволяет строить системы мониторинга с точностью, достаточной для решения большинства практических задач.

3. Метод FDoA служит мощным дополнением к TDoA в системах с подвижными носителями (БПЛА, спутники), позволяя уточнять местоположение движущихся целей.

Ключевым преимуществом SDR-подхода является его гибкость: одна и та же аппаратная платформа может быть программно переконфигурирована для реализации различных методов локализации в зависимости от поставленной задачи и доступных ресурсов.

Перспективным направлением дальнейших исследований является разработка гибридных алгоритмов, комбинирующих TDoA, FDoA и амплитудные измерения в единый цикл обработки, а также применение методов машинного обучения для фильтрации помех и повышения точности в условиях многолучевого распространения радиоволн.

ЛИТЕРАТУРА

1. Локализация источников радиоизлучения подвижным приемником на основе измерений времени прихода периодических сигналов / И. Б. Крыжко [и др.] // Системы управления, связи и безопасности. – 2025. – № 2. – С. 87–104. – DOI: 10.24412/2410-9916-2025-2-087-104.

2. Гилев И. В. Программа автоматизации определения местоположения мобильного источника радиоизлучения с использованием приемника программно-определяемого радио / И. В. Гилев, С. В. Канавин // Вестник Воронежского института МВД России. – 2025. – № 3. – С. 148–158. – EDN JVSBGH.

3. Гилев И. В. Перспективы применения технологии программно-определяемого радио в системах радиосвязи специального назначения / И. В. Гилев // Научный бюллетень Воронежского института МВД России. – 2024. – № 3. – С. 85–88. – EDN LWXEKG.

4. Гилев И. В. Алгоритм противодействия источнику мешающего радиоизлучения при определении его местоположения комплексом радиомониторинга и радиоконтроля / И. В. Гилев, А. А. Терентьев, А. С. Лукьянов // Вестник Воронежского института МВД России. – 2022. – № 3. – С. 160–170. – EDN BENQQQ.

СВЕДЕНИЯ ОБ АВТОРЕ

Гилев Игорь Владимирович.

Старший преподаватель кафедры инфокоммуникационных систем и технологий.

Кандидат технических наук.

Воронежский институт МВД России.

E-mail: gileviv@bk.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Gilev Igor Vladimirovich.

Lecturer of the Department of Infocommunication Systems and Technologies.

Candidate of Technical Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: gileviv@bk.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: SDR; локализация; пеленгация; TDoA; FDoA; источник радиоизлучения; радиоконтроль.

Keywords: SDR; localization; direction finding; TDoA; FDoA; radio source; radio monitoring.

УДК 004.891.3

ОПТИМИЗАЦИОННЫЕ МОДЕЛИ В УПРАВЛЕНИИ ПРОЕКТАМИ ПРОТИВОДЕЙСТВИЯ КРИМИНАЛЬНЫМ УГРОЗАМ

MATHEMATICAL MODELS IN PROJECT MANAGEMENT FOR COUNTERING CRIMINAL THREATS

В статье проведен обзор разработанных моделей управления проектами противодействия криминальным угрозам. Рассмотрены возможности их применения в деятельности подразделений уголовного розыска, особенности моделей и предполагаемые направления их совершенствования и дополнения другими моделями. Отмечена важность разработки специальной информационно-аналитической системы, позволяющей упростить и автоматизировать использование данных моделей на практике.

The article provides a review of various project management frameworks developed to address criminal threats. It discusses the potential application of these frameworks in the work of law enforcement agencies, as well as their characteristics and areas for enhancement. The significance of establishing a specialized information and analysis system was highlighted in order to facilitate and streamline the use of these frameworks in real-life situations.

Одним из направлений повышения эффективности организационных систем является внедрение и применение методологии проектного управления.

Вопросы приложения методов и моделей управления проектами в деятельности правоохранительных органов ранее неоднократно рассматривались И. В. Горошко [1], В. Д. Кондратьевым [2] и другими.

Мы полагаем, что проектный подход может быть применен и для повышения эффективности деятельности подразделений уголовного розыска (далее – подразделений УР). В этих целях нами были разработаны методы и модели управления проектами противодействия криминальным угрозам (далее – проектами ПКУ), объединенные в «Методологию управления проектами в сфере противодействия криминальным угрозам».

При разработке моделей управления проектами ПКУ использовались методы исследования операций, календарно-сетевое планирование и другие.

Полное описание параметров моделей в контексте решения определенных задач управления в проектах ПКУ, формальная постановка данных задач и примеры с результатами их решения приведены в публикациях им посвященных.

Цель данной статьи – общий обзор разработанных моделей, возможностей их применения, особенностей и предполагаемых направлений совершенствования.

Модель оптимального распределения возобновляемых ресурсов в управлении проектом противодействия криминальным угрозам [3]. Разработана для применения в проектах ПКУ, направленных на раскрытие определенного преступления, где между работами проекта (оперативно-разыскными мероприятиями и другими законодательно предусмотренными действиями) заданы отношения предшествования, а при выполнении проекта имеются ограничения в ресурсах возобновляемого типа.

Под основным видом возобновляемых ресурсов в данной модели, понимаются трудовые ресурсы – члены команды проекта, сотрудники подразделения УР (далее – исполнители проекта), которых, при условии соблюдения режимов труда и отдыха, можно назначать на выполнение последовательности работ проекта.

При заданных параметрах: количестве исполнителей проекта; отношениях предшествования между работами; функции продолжительности работ от количества назначенных на ее выполнение исполнителей и ее аргументов – модель позволяет найти такое распределение исполнителей по работам проекта ПКУ, с учетом их переназначения на новые работы после выполнения ранее назначенных, которое минимизирует минимальную оценочную продолжительность последовательности работ проекта.

Для определения временных параметров работ проекта применяется этап «прямого прохода» метода критического пути [4].

Особенностью модели является механизм, позволяющий распределять ограниченное количество возобновляемых ресурсов на последовательность работ многократно, по мере их доступности.

Отметим, модель позволяет распределять по работам не конкретных исполнителей с заданным набором компетенций, а лишь их общее количество для каждой работы проекта, которое минимизирует продолжительность последовательности работ проекта.

Мы полагаем, что дальнейшее развитие модели должно идти по пути добавления возможности учета специализации исполнителей при их распределении на работы проекта.

Кроме того, для повышения адекватности модели, требуется разработка более совершенных механизмов расчета в общей продолжительности проекта, продолжительности работ, со временем реализации, не зависящим от количества распределенных на ее выполнение исполнителей (например, различного рода экспертизы).

Модель разработки расписания проекта противодействия криминальным угрозам профилактического типа [5]. Разработана для составления расписания проектов ПКУ профилактического типа. Где работы проекта, в основном – типовые профилактические мероприятия, реализуемые в рамках оперативно-разыскной профилактики. В проекте ПКУ данного типа работы не связаны отношениями предшествования.

Задача, решаемая моделью, является модификацией задачи построения расписания выполнения работ проекта с ограничением на ресурсы (англ. resource constrained project scheduling problem) [6].

При заданных параметрах: продолжительности проекта, характеристик типовых работ проекта (требуемого для их выполнения количества ресурсов, продолжительности работ, ожидаемого эффекта от реализации работы определенного типа и других), ограниченных ресурсов возобновляемого типа (например, трудовых ресурсов) и невозобновляемого типа (например, финансовых ресурсов, для обеспечения оперативно-розыскной деятельности), сезонных коэффициентов криминальных угроз – модель позволяет определить такое оптимальное количество типовых работ проекта ПКУ, и такие даты их начала, которые бы максимизировали ожидаемый эффект (воздействия на определенные криминальные угрозы) от реализации всего проекта ПКУ.

Полученные в результате решения задачи даты начала типовых работ позволяют построить расписание проекта ПКУ данного типа и построить график загрузки возобновляемых ресурсов проекта ПКУ данного типа.

Для повышения адекватности модели в ней предусмотрены:

– Механизм линейного снижения ожидаемого эффекта от реализации типовой работы проекта при ее многократной реализации. Требуемый для учета возможного снижения эффекта от реализации определенных профилактических мероприятий при их регулярном повторении и неизменном содержании.

– Механизм согласования периодов начала работ с сезонными факторами определенных криминальных угроз, если известны факты об их сезонности. Для расчета сезонности предлагается использовать метод классической декомпозиции временного ряда, рассмотренный в [7].

Размерность модели накладывает некоторые ограничения на продолжительность составляемого расписания и количество возможных типов работ проекта. В дальнейшем возможна разработка специальных эвристических методов и алгоритмов, позволяющих упростить решение задачи и получить некоторое компромиссное решение. Например, путем сегментирования задачи разработки расписания проекта на задачи меньшей размерности, их решения, и сборки в единое расписание.

Модель стационарного размещения групп задержания в управлении проектом по пресечению серии преступлений [8]. Разработана для повышения эффективности организации стационарных засад, для задержания преступников, в предполагаемых местах совершения последующих преступлений, как отдельной работы в проекте ПКУ, направленном на пресечение серии преступлений.

В основе задачи, решаемой моделью, лежит задача о размещении заданного количества объектов в заданном множестве географических точек, с минимизацией стоимости их размещения, с учетом ряда ограничений (англ. facility location problem) [9].

При заданных параметрах: конечном множестве мест для стационарного размещения групп задержания; количестве групп задержания; конечном множестве предполагаемых мест совершения преступлений; матрице попарных расстояний между предполагаемыми местами совершения преступлений; коэффициентов притяжения, характеризующих вероятность совершения преступлений в определенных местах – модель позволяет определить такое оптимальное размещение групп задержания в конечном множестве исходных точек предполагаемых мест совершения преступлений, которое минимизирует расстояние от каждой группы задержания до всех точек входящих в их зону контроля.

Отметим, что для применения модели на практике, помимо программной среды реализации модели, позволяющей решать задачи оптимизации, потребуется использование инструментария географических информационных систем (далее – ГИС), с загруженными данными о географическом расположении точек (мест размещения групп задержания и предполагаемых мест совершения последующих преступлений), и связующей их дорожной сети.

Применение ГИС обеспечивает, как автоматизацию расчета кратчайших расстояний между точками по графу дорожной сети, так и визуализацию результатов решения задачи на карте местности.

Мы полагаем, что данная модель может найти широкое применение и в других оперативных задачах подразделений УР и смежных подразделений органов внутренних дел (например, при распределении специальных сил и средств при организации задержания разыскиваемого преступника в одном из возможных мест его появления).

В то же время важно отметить, что задача, решаемая в модели, является в некотором смысле второстепенной.

Намного более важной и востребованной задачей на практике, и вместе с тем предполагающей и более сложную формализацию и модель, представляется задача об оптимальной динамической расстановке сил и средств при задержании преступника, разработке которой могут быть посвящены последующие исследования.

Естественным ограничением рассмотренных моделей является некоторая неопределенность в условиях реализации проектов ПКУ – работы проекта по раскрытию преступления могут быть существенно скорректированы уже на начальном этапе, а запланированные профилактические мероприятия могут не оказать ожидаемого воздействия на криминальные угрозы. В связи с этим на практике, при разработке управляющих воздействий потребуется инструмент, позволяющий быстро решать задачи по предложенным моделям, с учетом актуальной информации о состоянии подразделения УР (например, о количестве доступных к назначению исполнителей) и изменениях в условиях реализации проектов ПКУ.

Ряд параметров рассмотренных моделей задаются экспертными методами – это необходимо для самой возможности применения математического аппарата. Вместе с тем получить многократно повторяемое, одинаковое экспертное решение, относительно величины некоторых из параметров, в большинстве случаев невозможно.

Мы полагаем, что при целенаправленном и системном накоплении и анализе статистической информации об основных аспектах функционирования подразделения УР, как организационной системы – параметры, задаваемые экспертными методами, в дальнейшем можно будет определять по статистическим показателям. Это позволит получить более адекватные результаты решения задач при использовании моделей.

Таким образом, для автоматизации решения задач, накопления и анализа статистической информации, требуется разработка специальной информационно-аналитической системы поддержки принятия решений, некоторые функциональные требования к которой рассматривались нами ранее в [10].

Применение проектного подхода в деятельности подразделений УР, предполагает разработку адаптированных к их деятельности методов и моделей управления проектами. В данной статье нами был проведен обзор трех моделей управления проектами ПКУ. Для рассмотренных моделей намечены возможные направления их совершенствования и дополнения другими моделями, в рамках последующих исследований.

Не менее важным, по сравнению с совершенствованием имеющихся и разработкой новых моделей управления проектами ПКУ является вопрос создания информационно-аналитической системы поддержки принятия решений при управлении проектами ПКУ, позволяющей автоматизировать и упростить процессы принятия решений при управлении проектами ПКУ с использованием предложенных моделей.

ЛИТЕРАТУРА

1. Горошко И. В. Цифровая трансформация и управление проектами / И. В. Горошко. – Москва : Университет прокуратуры Российской Федерации, 2021. – С. 23–32.
2. Кондратьев В. Д. Проектное управление при реализации Стратегии безопасности дорожного движения / В. Д. Кондратьев, А. В. Щепкин // Вестник Московского автомобильно-дорожного государственного технического университета (МАДИ). – 2019. – № 4 (59). – С. 112–119.
3. Жирнов А. А. Модель оптимального распределения возобновляемых ресурсов в управлении проектом противодействия криминальным угрозам и методика ее программной реализации / Жирнов А. А. [и др.] // Моделирование, оптимизация и информационные технологии. – 2024. – Т. 12. – № 1 (44). – С. 3.
4. Krishnamoorthy M. Critical Path Method: A Review : Department of Industrial Engineering, University of Michigan, 1968. – 66 с.

5. Жирнов А. А. Модель разработки расписания проекта противодействия криминальным угрозам профилактического типа // Моделирование, оптимизация и информационные технологии. – 2023. – Т. 11. – № 4 (43).

6. Abdolshah M. A review of resource-constrained project scheduling problems (RCPSP) approaches and solutions //International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies. – 2014. – Т. 5. – №. 4. – С. 253–286.

7. Жирнов А. А. Подход к определению сезонности преступлений в проектах противодействия криминальным угрозам / А. А. Жирнов // Современные наукоемкие технологии. – 2022. – № 7. – С. 38–44.

8. Жирнов А. А. Модель стационарного размещения групп задержания в управлении проектом по пресечению серии преступлений / А. А. Жирнов // Вестник Воронежского института МВД России. – 2023. – № 2. – С. 145–158.

9. Drezner Z., Hamacher H. W. Facility Location: Applications and Theory. — Springer Science & Business Media, 2004. – 482 с.

10. Жирнов А. А. Об инструменте управления проектами противодействия криминальным угрозам // Информатизация и информационная безопасность правоохранительных органов : сборник трудов Международной научно-практической конференции. – Москва : Академия управления Министерства внутренних дел Российской Федерации, 2024. – С. 87–93.

СВЕДЕНИЯ ОБ АВТОРЕ

Жирнов Андрей Александрович.
Адъюнкт кафедры информационных технологий.
Академия управления МВД России.
E-mail: AUMSKW@yandex.ru
Россия, 125171, г. Москва, ул. Зои и Александра Космодемьянских, 8.

Zhirnov Andrey Aleksandrovich.
Postgraduate student.
Academy of Management of the Ministry of Internal Affairs of Russia
E-mail: AUMSKW@yandex.ru
Russia, 125171, Moscow, Zoya and Alexander Kosmodemyanskikh str., 8.

Ключевые слова: проект противодействия криминальным угрозам; модель распределения ресурсов; следственно-оперативная группа; проектный подход; расписание проекта.

Keywords: the project of countering criminal threats; the model of distribution; the investigative and operational group; the project approach; project schedule.

УДК 519.977.5: 005.95

**И. А. Кубасов,
Ю. В. Барашкин**

**О НАПРАВЛЕНИИ РАЗВИТИЯ ИНФОРМАЦИОННЫХ СИСТЕМ
ПОДРАЗДЕЛЕНИЙ МВД РОССИИ В СФЕРЕ МИГРАЦИИ**

**ON THE DIRECTION OF DEVELOPMENT OF INFORMATION SYSTEMS
OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA
IN THE FIELD OF MIGRATION**

В статье предлагается переход от разрозненных информационных ресурсов в сфере миграции к их интеграции на основе формирования интеллектуальной архитектуры сбора и анализа миграционных данных. Такой концептуальный подход подразумевает формирование единого контура сбора и нормализации сведений, пакетную биометрическую проверку иностранных граждан и аналитический модуль на базе искусственного интеллекта, позволяющий осуществлять прогноз миграционных потоков и выявлять аномалии. В отличие от существующих решений, информационная система подразделений МВД России в сфере миграции строится на принципах межведомственной интеграции, предиктивной аналитики и обязательного участия человека в принятии окончательных управленческих решений.

The article proposes a transition from fragmented information resources in the field of migration to their integration through the creation of an intelligent architecture for the collection and analysis of migration data. This conceptual approach involves the formation of a unified framework for data collection and normalization, batch biometric verification of foreign citizens, and an AI-based analytical module capable of forecasting migration flows and detecting anomalies. Unlike existing solutions, the information system of the Ministry of Internal Affairs of Russia in the field of migration is built on the principles of interagency integration, predictive analytics, and mandatory human involvement in final managerial decision-making.

Масштаб и скорость миграций людей в современном мире достигли беспрецедентных уровней. На перемещения людей влияют войны, экономические кризисы и климатические изменения. Эти динамичные процессы создают новые вызовы для правоохранительных органов, в том числе и в России, по обеспечению безопасности и соблюдению законных прав мигрантов. Однако, несмотря на успешно осуществляемую цифровую трансформацию МВД России, информационные системы подразделений МВД России в сфере миграции (далее – ИС), пока ограничены по архитектуре и функциональности. Методы учёта постоянно меняются, данные о потоках мигрантов собираются неполно, а часть отчётных форм исключена из

аналитического оборота [1]. При растущем объеме информации особенно остро проявляются проблемы низкой производительности, фрагментарности и слабой интеграции ведомственных ресурсов.

ИС нередко перегружены: при пиковых нагрузках снижается скорость обработки запросов и задерживается обмен данными между регионами, что замедляет принятие решений. Информационные ресурсы в сфере миграции МВД России и других ведомств действуют разрозненно, без единого информационного контура и унифицированных форматов. В результате сотрудники вынуждены вручную сверять сведения из разных источников, повышая риск ошибок и снижая оперативность.

Особо остро стоит проблема отсутствия пакетного поиска по биометрическим признакам. Для проверки группы лиц сотрудник вынужден выполнять десятки отдельных запросов к разным информационным системам, поскольку не существует централизованного шлюза запросов, способного обработать консолидированный запрос и выдать сводный результат. Такое технологическое раздробление ведёт к временным потерям, дублированию данных и искажению аналитической картины.

Встроенные аналитические модули ИС ограничены базовыми функциями учёта и отчётности. Они не поддерживают многомерный анализ, прогнозирование или пакетную биометрическую верификацию, из-за чего даже большие массивы данных остаются пассивными и слабо используемыми. Ситуацию усугубляют устаревшая инфраструктура, неравномерное качество вводимых данных, риски утечки информации и дефицит специалистов, владеющих технологиями искусственного интеллекта (далее – ИИ) и кибербезопасности. Всё это затрудняет переход от простого учёта к интеллектуальному управлению миграционными процессами.

Одним из самых перспективных направлений здесь являются интеллектуальные модули анализа миграционных данных – комплексные программно-аппаратные решения на базе технологий ИИ. Миграция и технологии ИИ ещё недавно казались далекими друг от друга сферами, но в настоящее время их сближение идёт полным ходом. Во многих странах мира уже тестируются и внедряются системы с использованием ИИ для управления миграционными процессами. Эти решения сулят повышение эффективности работы служб и более обоснованное принятие решений [2].

Предлагаемый подход к созданию интеллектуальной интегрированной системы анализа миграционных данных, направлен на устранение ключевых ограничений ИС. Цель – обеспечить переход от разрозненных реестров к единому интеллектуальному контуру, где данные не просто накапливаются, а анализируются, сопоставляются и используются для управленческих решений.

Система охватывает полный цикл обработки информации: от сбора данных из разнородных источников – ИС, биометрических хранилищ, телеметрии, видеопотоков и статистики – до выдачи аналитических рекомендаций лицу, принимающему решение. Все сведения поступают в

режиме, близком к реальному времени, проходят автоматическую проверку, нормализацию и очистку. В результате формируется согласованная модель миграционной обстановки, которая доступна в едином информационном пространстве.

Ключевая особенность такого подхода – централизованный шлюз запросов, или единая точка доступа. Это позволяет формировать консолидированные запросы и получать сводные ответы из всех подключённых систем, что устраняет необходимость множества разрозненных обращений, снижает риск ошибок и значительно сокращает время обработки запросов.

Особое место занимает биометрический контур с поддержкой пакетных операций. В едином процессе система выполняет сверку по нескольким биометрическим модальностям – лицу и дактилоскопии. Результаты автоматически объединяются, дубли устраняются, а расхождения выделяются для проверки. Такая автоматизация ускоряет проверку, повышает точность идентификации и снижает нагрузку на операторов.

В аналитическом модуле системы заложены два направления работы.

Первое – прогнозирование миграционных потоков с помощью методов машинного обучения. На основе статистики, экономических индикаторов и событийных факторов формируются вероятностные сценарии развития обстановки, что позволяет более рационально распределить ресурсы.

Второе – ситуационная безопасность: алгоритмы анализа аномалий выявляют нетипичные паттерны, связанные с рисками – от всплесков поддельных документов до подозрительных маршрутов перемещений. Такой подход превращает систему из регистратора событий в активный инструмент предупреждения угроз.

Результаты анализа преобразуются в управленческие сигналы и визуализируются в модуле поддержки решений. Руководители видят на дашбордах динамику потоков, карту рисков и прогнозы по регионам. Система формирует рекомендации – где усилить контроль, куда направить ресурсы, какие проверки приоритетны, – сопровождая их пояснениями и ссылками на исходные данные. При этом человек остаётся главным участником процесса: ИИ лишь помогает быстрее и точнее оценивать ситуацию.

Архитектура предлагаемого подхода основана на принципах масштабируемости, отказоустойчивости и безопасности. В ней предусмотрены распределённые вычисления, поточная обработка данных, федеративный слой запросов с аутентификацией, сервис пакетной биометрической сверки и модуль объяснимой аналитики, фиксирующий причинно-следственные связи в выводах. Все операции шифруются, доступ разграничивается по ролям, а действия пользователей протоколируются для аудита.

Представленный концептуальный подход к созданию интеллектуальной системы анализа миграционных данных подтверждает то, что развитие информационной инфраструктуры МВД России невозможно ограничивать

только цифровизацией существующих процедур. Главный вывод проведенного исследования состоит в необходимости смены парадигмы: от накопления и передачи информации к её осмыслению, прогнозированию и управляемому применению. Технология искусственного интеллекта здесь выступает не как самоцель, а как инструмент рационализации управленческих процессов и укрепления аналитической культуры в деятельности органов внутренних дел.

С точки зрения теории управления, данное направление развития ИС раскрывает переход от регламентного администрирования к модели адаптивного управления, где решения принимаются на основе динамического анализа и вероятностных прогнозов. Этот сдвиг требует иной подготовки кадров, иных компетенций и нового понимания управленческой ответственности. Поэтому предложенная архитектура – это не только технологическая схема, но и управленческая концепция, задающая новое качество информационного обеспечения в правоохранительной деятельности.

Перспективы дальнейшего развития связаны с опытной интеграцией ИС в информационную инфраструктуру МВД России, формированием стандартов доверия к алгоритмам, а также внедрением образовательных модулей по работе с интеллектуальными системами для сотрудников органов внутренних дел. Реализация этих направлений позволит не просто модернизировать ИС, но и создать в МВД России новую культуру аналитического управления, где решения будут приниматься быстрее, точнее и справедливее.

ЛИТЕРАТУРА

1. Войтова О. Г. Применение элементов искусственного интеллекта как один из путей развития информационных систем МВД России / О. Г. Войтова, Д. А. Тарасов // Вестник Воронежского института МВД России. – 2020. – № 2. – С. 319–322. – EDN VPODWA.

2. Кубасов И. А. Искусственный интеллект, как драйвер цифровой трансформации МВД России / И. А. Кубасов // Криминологический журнал. – 2023. – № 2. – С. 211–215. – DOI 10.24412/2687-0185-2023-2-211-215. – EDN KGTWXXN.

3. Кубасов И. А. Роль современных информационных технологий в научно-технической деятельности органов внутренних дел Российской Федерации / И. А. Кубасов // Информатизация и информационная безопасность правоохранительных органов: сборник трудов Международной научно-практической конференции, Москва, 05 июня 2025 года. – Москва : Академия управления МВД России, 2025. – С. 181–186.

4. Кубасов И. А. Роль современных цифровых технологий в предупреждении преступлений / И. А. Кубасов // Уголовная политика России на современном этапе: состояние, тенденции, перспективы :

Сборник научных трудов по материалам международной научно-практической конференции, посвященной 90-летию со дня рождения профессора Г. А. Аванесова. В 2-х частях, Москва, 27 сентября 2024 года. – Москва : Академия управления МВД России, 2024. – С. 73–79. – EDN DHTZNC.

СВЕДЕНИЯ ОБ АВТОРАХ

Кубасов Игорь Анатольевич.

Профессор кафедры информационных технологий.

Доктор технических наук, доцент.

Академия управления МВД России.

E-mail: igorak@list.ru

Россия, 125993, г. Москва, ул. Зои и Александра Космодемьянских, 8.

Барашкин Юрий Владимирович.

Начальник отдела организации миграционного контроля управления по вопросам миграции главного управления МВД России по городу Москве.

Главное управление МВД России по городу Москве.

E-mail: revizoroff@mail.ru

Россия, 27994, г. Москва, ул. Петровка, 38.

Kubasov Igor Anatolyevich.

Professor of the department of information technologies.

Doctor of Technical Sciences, Associate Professor.

Academy of management of the Ministry of internal affairs of the Russian Federation.

E-mail: igorak@list.ru

Russia, 125993, Moscow, Zoya and Alexander Kosmodemyanskikh str., 8.

Barashkin Yuriy Vladimirovich.

Head of the Department for the Organization of Migration Control of the Migration Affairs Directorate of the Main Directorate of the Ministry of Internal Affairs of Russia for the City of Moscow.

Main Directorate of the Ministry of Internal Affairs of Russia for the City of Moscow.

E-mail: revizoroff@mail.ru

Russia, 27994, Moscow, Petrovka St., 38.

Ключевые слова: интеллектуальные системы анализа данных; миграционная безопасность; машинное обучение; аналитическая поддержка решений; информационная система.

Keywords: intelligent data analysis systems; migration security; machine learning; analytical decision support; information system.

УДК 004.6

В. В. Лопухов, Э. Р. Зарипова

**ПРОБЛЕМНЫЕ ВОПРОСЫ ПРЕПОДАВАНИЯ
МАТЕМАТИЧЕСКИХ ДИСЦИПЛИН
В ПОДРАЗДЕЛЕНИЯХ МВД РОССИИ**

**FEATURES OF TEACHING MATHEMATICAL DISCIPLINES
IN EDUCATIONAL INSTITUTIONS OF THE MINISTRY
OF INTERNAL AFFAIRS OF RUSSIA**

Статья посвящена проблемным вопросам, возникающим в процессе преподавания технических, особенно математических дисциплин в учебных заведениях МВД России. Проведен анализ уровней подготовки курсантов, предложены методики преподавания, позволяющие повысить эффективность учебного процесса.

The article is devoted to the problematic issues arising in the process of teaching technical, especially mathematical disciplines in educational institutions of the Ministry of Internal Affairs of Russia. It analyzes the cadets' training levels and proposes teaching methods to improve the efficiency of the educational process.

При переходе из милиции в полицию Федеральное законодательство внесло существенные изменения в требования к образованию сотрудников полиции. В число квалификационных требований включено высшее юридическое образование [1, 2].

Ранее для офицерской должности было достаточно иметь среднее специальное образование или любое высшее образование. Такой подход повышал вероятность набора на службу большего количества человек. Например, могла быть выбрана траектория – педагогический институт, куда легко было поступить, далее – работа в милиции с более высоким статусом и заработной платой по сравнению с работой педагога.

Такой подход к комплектованию личного состава милиции обусловлен хронической нехваткой сотрудников, особенно в таких востребованных подразделениях, как уголовный розыск, участковые уполномоченные, патрульно-постовая служба и вневедомственная охрана.

Нехватка квалифицированных кадров вынуждала руководителей принимать на службу людей с разным образовательным бэкграундом, полагаясь на их адаптацию и профессиональное развитие в процессе службы.

Несмотря на то что образование сотрудников не всегда соответствовало специфике работы, служба в милиции традиционно считалась престижной и почетной. Многие сотрудники, начав службу с недостаточным теоретическим багажом, заполняли пробелы в знаниях на практике, приобретая бесценный

опыт и становясь высококвалифицированными специалистами, преданными своей профессии и стране [3].

Этот опыт, накопленный за годы работы, во многом компенсировал недостаток специализированного образования в начале карьеры. Однако такая система подготовки имела и свои недостатки: неравномерный уровень подготовки сотрудников, потенциальные трудности в адаптации к новым условиям и задачам, а также не всегда эффективное использование потенциала сотрудников. У такой системы комплектования были и свои плюсы. Возможно было принимать на службу граждан необходимых специальностей – математиков, инженеров, программистов и др.

Требование обязательного юридического образования для сотрудников полиции закрыло дорогу высококвалифицированным узким специалистам. Поэтому обучение на технических факультетах некоторых учебных заведений МВД России способно разрешить данную проблему, поскольку на них курсанты получают необходимую математическую и инженерную подготовку вместе с юридической. Важно найти баланс между строгими требованиями к образованию и обеспечением достаточного количества квалифицированных кадров для службы в полиции, учитывая специфику работы и высокую ответственность, которая лежит на плечах сотрудников правоохранительных органов.

Повышение уровня образования, несомненно, шаг в правильном направлении, но необходимо обеспечить плавный переход и создать условия для профессионального развития сотрудников, которые уже работают в полиции и не имеют высшего юридического образования, но обладают ценным практическим опытом и преданностью службе [4].

Это комплексная задача, требующая системного подхода и долгосрочной стратегии. В конечном итоге, цель всех этих изменений – обеспечение безопасности граждан и эффективное функционирование системы правоохранительных органов России.

Основной проблемой обучения курсантов математическим дисциплинам, которых нет в гражданских технических вузах, является широкая предметная направленность учебных программ – от гуманитарной юридической до прикладной математической и физической.

Разделение на «гуманитариев» и «технарей» здесь не работает, курсанты должны быть и теми и другими.

Анализ успеваемости курсантов на протяжении всего периода обучения выявляет четкое расслоение на три основные группы, начиная уже с первого курса, которое проявляется в уровне понимания материала, глубине знаний, а также в подходах к обучению и, как следствие, в профессиональных перспективах выпускников. Рассмотрим каждую категорию подробнее.

Первая группа – это элита, небольшое количество курсантов, составляющее от одного до четырех человек в учебной группе. Их отличает исключительно высокий уровень подготовки, значительно превосходящий

средний. Причиной такого преимущества является не столько эффективная работа преподавательского состава, сколько самостоятельная, глубокая и заинтересованная работа с учебным материалом. Эти курсанты, зачастую будучи увлеченными радиолюбителями, демонстрируют поразительную способность не только усваивать знания, но и применять их на практике, создавая и внедряя собственные электронные устройства. Они самостоятельно проектируют, собирают, программируют и настраивают сложные электронные схемы, проявляя при этом ярко выраженное творческое и инженерное мышление. Их успеваемость неизменно высока на протяжении всего обучения, они активно участвуют в университетской жизни, представляя собой гордость учебного заведения.

Однако необходимо подчеркнуть, что заслуга университета в их успехах относительно невелика. Университет предоставляет им среду и ресурсы для развития, направляет их потенциал в нужное русло, но сами знания они приобретают в значительной степени самостоятельно, благодаря внутренней мотивации и увлеченности [5].

После окончания университета эти выпускники, как правило, получают высокую оценку от руководителей практических подразделений, и их успехи служат отличной рекламой для университета. Их быстрая адаптация и высокая производительность подтверждают эффективность их индивидуального подхода к обучению, хотя и подчеркивают определенные недостатки в стандартной системе образования.

Вторая группа представляет собой подавляющее большинство – 80-90% курсантов. Это наиболее многочисленная и, к сожалению, проблемная категория. Обучающиеся, обычно, успешно справляются с заданиями легкой и средней сложности, учатся на удовлетворительные оценки, не вникая особенно в образовательный процесс, не интересуясь новшествами. К зачету кратковременно запоминается алгоритм решения задачи, без понимания сути, знания не перерастают в практику и не могут быть применены в дальнейшем. Отсутствует желание освоения нового, лишь желание в спокойном режиме доработать до пенсии, при этом пользуясь всеми льготами и социальными гарантиями сотрудника органа внутренних дел.

После распределения в практические подразделения такие курсанты либо меняют свое отношение к службе, приобретают необходимые знания и благополучно вливаются в коллектив, либо становятся кадровым балластом, от которого руководители стремятся избавиться.

На обучение и воспитание этой группы курсантов, формирование у них правильной жизненной позиции должны быть направлены основные усилия профессорско-преподавательского состава. В их возрасте это еще возможно сделать – заинтересовать, объяснять математические предметы в доступной форме, с примерами применения изучаемых тем в последующей практической деятельности.

Последняя группа обучающихся – это отстающие по учебе курсанты, обычно по многим дисциплинам. Часто причиной является недостаточное школьное образование. Такие курсанты требуют индивидуальной работы с преподавателями, им нужна дополнительная мотивация. Правильная работа с такими курсантами может продвинуть их во вторую группу.

Необходимо отметить важность воспитательной работы в образовательных учреждениях МВД России. Это обусловлено повышенным риском коррупции в профессии полицейского, а также тем, что криминальная направленность выпускника может иметь гораздо более серьезные последствия, чем недостаток знаний.

В то время как в гражданском образовательном учреждении имеется четкая направленность, например, «Информационная безопасность телекоммуникационных систем» или «Стоматология», технические направления в вузах МВД России должны готовить универсальных специалистов, обладающих знаниями как в области юриспруденции, так и в инженерном деле. Это усложняет задачу, учитывая, что большинство людей склонны к одному из двух типов мышления – «гуманитарному» или «техническому», в то время как универсальные способности встречаются реже.

Преподаватели образовательных учреждений МВД России могут применять методические приемы для освоения технических и математических дисциплин.

1. Связь изучаемого материала и практики.

Изучая производную функции, преподаватель может рассказать о построении нейросетей и вычислении градиента функции, который показывает, насколько нейронная сеть уверена в правильности существующего веса. Решение задач. Для изучения часто используются полиномиальные входные переменные. Изучение матриц, теории вероятностей и математической статистики, машинного обучения необходимо сопровождать практическими заданиями. Специфика профессии полицейского подразумевает готовность встретиться с различными областями, выстраивать логические цепочки, обобщать информацию, вычислять различные параметры. Знания математики и физики должны быть у вас под рукой. Вы можете столкнуться с электрическим током, при защите информации необходимо понимание физических процессов.

2. Наглядность преподаваемого материала.

Необходимо представлять учебный материал в максимально понятной и наглядной форме. Обязательно демонстрировать на занятиях по электротехнике и радиоэлектронике всю последовательность действия на специальных стендах с электро- и радиоэлементами и измерительными приборами.

3. Периодическое повторение изученного.

У обучающихся должна единообразно формироваться последовательность изучаемых тем, поэтому важно показывать связь

пройденного материала и вновь изучаемого, подчеркивать сходства и различия.

4. Внеаудиторное обучение.

Усвоение материала значительно улучшается при использовании игровых форм обучения. Доцентом кафедры естественнонаучных дисциплин Московского университета МВД им. В. Я. Кикотя на факультете подготовки специалистов в области информационной безопасности образован интеллектуальный клуб, куда приглашаются специалисты, способные обучать тонкостям анализа данных, программированию, практике. Обучающиеся с интересом участвуют в викторинах, олимпиадах, конференциях.

Участие в клубе положительно сказывается на успеваемости курсантов.

Положительным опытом следует считать организацию на кафедре естественнонаучных дисциплин кружка по прикладной математике и радиоэлектронике, где курсанты решают интересные задачи по теории вероятностей, статистической радиотехнике, радиотехническим цепям и сигналам, радиолокации. Своими руками собирают электронные схемы, работают с паяльными принадлежностями, ремонтируют неисправные стенды. Все участники данного кружка значительно повысили успеваемость по указанным выше предметам.

5. Организация образовательных экскурсий в практические подразделения.

В 2025 году осуществлено посещение отдела МВД России по Бескудниковскому району города Москвы. Практики пообщались с курсантами, рассказали о своих буднях и возможностях роста для молодых кадров. Курсантам экскурсия понравилась и оказалась познавательной. Всегда вызывают положительные эмоции посещение тематических музеев, например, Музея уголовного розыска ГУ МВД России по г. Москве.

6. Формирование преподавательского состава кафедры.

Все регалии преподавателей для курсантов важны. Интересно работать и с профессорами, доцентами, а также и с преподавателями из практических подразделений, которые имеют опыт раскрытия преступлений [6]. Каждый преподаватель делится своими наработками с обучающимися.

Технические специальности образовательных учреждений МВД России конкурируют с техническими гражданскими вузами. В Московском университете МВД России им. В. Я. Кикотя для привлечения абитуриентов на факультет подготовки специалистов в области информационной безопасности уже два года проводилась олимпиада «Университет цифровой полиции», где преподаватели кафедры напрямую принимают участие как в составлении заданий, так и в индивидуальной части презентации проектов абитуриентов.

Для преподавателей важным остается заинтересованность как абитуриентов, курсантов в образовательном процессе, так и выпускников в их будущей службе.

ЛИТЕРАТУРА

1. Эриашвили Н. Д. Профессиональная этика российского полицейского / Н. Д. Эриашвили // Вестник Московского университета МВД России. – 2012. – № 1. – С. 48–52.
2. О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 30.11.2011 № 342-ФЗ // СПС «КонсультантПлюс».
3. Лопухов В. В. Об организации работы подразделений ОРИ ГУ МВД России по г. Москве по борьбе с дистанционными хищениями денежных средств с банковских карт граждан. Актуальные вопросы теории и практики ОРД: Сборник научных трудов всероссийской научно-практической конференции, Москва, 30 ноября 2018 года / Под редакцией В. В. Абрамочкина. – Москва : Московский университет МВД России имени В. Я. Кикотя, 2019. – С. 56–62. – EDN SGBPGO.
4. Грачева О. С. Методические особенности непрерывного образования сотрудников ОВД в вузах МВД РФ / О. С. Грачева, С. А. Майорова // Вопросы российского и международного права. – 2017. – Т. 7. – № 11А. – С. 93–101.
5. Богуславский В. В. Мотивация учебной деятельности курсантов / В. В. Богуславский, М. В. Гирская // Мир образования – образование в мире. – 2014. – № 3(55). – С. 217–221.
6. Белошицкий А. В., Мещеряков Д. В. Информационно-коммуникационная компетентность преподавателя военного вуза // Педагогическое образование: вызовы XXI века : Материалы VII Международной научно-практической конференции, посвященной памяти академика В. А. Сластёнина / А. В. Белошицкий, Д. В. Мещеряков ; под общей редакцией Н. И. Вьюновой. – Воронеж : Воронежский государственный университет, 2016. – С. 177–179.

СВЕДЕНИЯ ОБ АВТОРАХ

Лопухов Владимир Викторович.

Старший преподаватель кафедры естественнонаучных дисциплин учебно-научного комплекса информационных технологий.

Московский университет МВД России имени В. Я. Кикотя.

E-mail: vlad1963-63@mail.ru

Россия, 125239, г. Москва, ул. Коптевская, 63.

Зарипова Эльвира Ринатовна.

Доцент кафедры естественнонаучных дисциплин учебно-научного комплекса информационных технологий.

Кандидат физико-математических наук.

Московский университет МВД России имени В. Я. Кикотя.

E-mail: ezarip@gmail.com

Россия, 125239, г. Москва, ул. Коптевская, 63.

Lopukhov Vladimir Viktorovich.

Senior Lecturer of the Department of Natural Science Disciplines of the Information Technology Training and Research Complex.

V. Y. Kikoty Moscow University of the Ministry of Internal Affairs of Russia.

E-mail: vlad1963-63@mail.ru

Russia, 125239, Moscow, Koptevskaya str., 63.

Zaripova Elvira Rinatovna.

Associate professor of the Natural Science Department.

Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikoty.

Candidate of Physical and Mathematical Sciences.

E-mail: ezarip@gmail.com

Russia, 125239, Moscow, Koptevskaya str., 63.

Ключевые слова: преподавание; мотивация; курсант; естественнонаучные; математические дисциплины; технические дисциплины.

Keywords: teaching; motivation; cadet; natural science disciplines; technical disciplines

УДК 378

**ПРОБЛЕМЫ АДАПТАЦИИ И ВНЕДРЕНИЯ
ПЕРЕДОВЫХ ТЕХНОЛОГИЙ В ПОВСЕДНЕВНУЮ ПРАКТИКУ
ОРГАНОВ ВНУТРЕННИХ ДЕЛ**

**PROBLEMS OF ADAPTATION AND IMPLEMENTATION
OF ADVANCED TECHNOLOGIES IN THE DAILY PRACTICE
OF INTERNAL AFFAIRS BODIES**

Данная статья посвящена некоторым проблемам адаптации и внедрения передовых технологий, в частности – беспилотных воздушных судов в повседневную деятельность органов внутренних дел. Рассматриваются ключевые трудности организационного и технического характера, которые препятствуют эффективному решению проблем ОВД. Предлагаются практические рекомендации по оптимизации процессов адаптации, направленные на повышение эффективности работы правоохранительных органов в условиях цифровой трансформации общества

This article focuses on the challenges of adapting and implementing advanced technologies, particularly unmanned aerial vehicles, in the daily operations of law enforcement agencies. It explores the key organizational and technical obstacles that hinder the effective resolution of law enforcement issues. The article provides practical recommendations for optimizing adaptation processes to enhance the efficiency of law enforcement agencies in the context of digital transformation

Для того, чтобы эффективно решать современные проблемы, органам внутренних дел необходимо шагать в ногу со временем и применять в своей деятельности достижения научно-технического прогресса. Законодательно такое право закреплено в пункте 1 статье 11 ФЗ «О полиции». Полиция в своей деятельности использует достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру [1]. К достижениям техники нашего времени можно отнести беспилотные воздушные суда (далее – БВС). Основным регулятором в области воздушного движения является Воздушный кодекс РФ. В основном законе, регулирующем движения в воздушном пространстве нашей страны, указано определение БВС. Беспилотное воздушное судно – воздушное судно, управляемое, контролируемое в полете пилотом, находящимся вне борта такого воздушного судна (внешний пилот) [2].

Беспилотные воздушные суда нашли широкую область применения в органах внутренних дел.

С их помощью можно решать следующие задачи:

1. Поиск пропавших лиц, нарушителей.

2. Видеофиксация правонарушений.
3. Производство следственных действий (идентификация личности по внешним признакам).
4. Мониторинг мест с наибольшей криминогенной обстановкой.
5. Профилактика правонарушений при проведении массовых мероприятий.

Конечно, сферы применения этим списком не ограничиваются. Развитие преступных схем, применяющих беспилотные воздушные суда, развивает и систему их пресечения и предотвращения. Однако применение современных технологий обременяется проблемами их внедрения и адаптации.

Для выполнения задач, связанных с использованием БВС, необходимо уметь управлять такими средствами, как следствие, нужна грамотно проработанная программа обучения личного состава, содержащая не только теоретические, но и практические аспекты. Имея такую программу обучения в ведомственных организациях, можно значительно улучшить качество работы таких подразделений. К данной категории проблем можно отнести и вопрос о расчете сил и средств для конкретного подразделения исходя из его численности, а также выполняемых задач.

Перед применением БВС сотруднику необходимо знать некоторые особенности правового характера. Статья 16 Воздушного кодекса Российской Федерации регламентирует разрешительный и уведомительный характер использования воздушного пространства. Подробный порядок использования указан в Федеральных правилах использования воздушного пространства, которые утверждены постановлением Правительства Российской Федерации от 11 марта 2010 г. № 138. Также эти правила закрепляют положение о том, что осуществление полетов БВС производится на судах, прошедших государственную регистрацию и имеющих страхование от причинения ущерба жизни, здоровью и имуществу третьих лиц [3].

Преступления и правонарушения совершаются круглосуточно. Своевременное реагирование на вызовы – основа успешного раскрытия инцидентов. В связи с этим встает вопрос необходимости организации полетов БВС в нерабочее время. Доступ к системе подачи планов полетов в Единую систему организации воздушного движения осуществляется для сотрудников ОВД через Единую систему информационно-аналитического обеспечения деятельности МВД России (ИСОД). Такая система функционирует в подразделениях на стационарных рабочих компьютерах сотрудников. Для решения вопроса оперативного доступа к такой системе можно предложить вариант предоставления сотруднику для работы вне здания подразделения компьютера с сим-картой с доступом в сеть ИСОД.

В данный момент учёт беспилотных гражданских воздушных судов осуществляет Федеральное агентство воздушного транспорта. Для быстрого доступа к информации сотрудникам необходимо организовать доступ в систему учёта гражданских БВС. Для сотрудников Госавтоинспекции и

патрульно-постовой службы такие сведения могут потребоваться для проверки правомерного проноса/провоза и использования БВС, а также возможность проверки правомерного использования воздушного пространства гражданскими лицами.

Поскольку беспилотные суда используются с применением видеофиксации, актуальным остается проблема защищенности каналов передачи данных с беспилотного летательного аппарата на принимающее устройство. Уязвимости в таких каналах могут привести к потере конфиденциальной информации в условиях активного развития киберпреступности. Большой проблемой использования БВС остается их дорогая стоимость [4–6].

ЛИТЕРАТУРА

1. О полиции : Федеральный закон от 07 февр. 2011 г. № 3-ФЗ // СЗ РФ. – 2011. – № 7. – Ст. 900.

2. Воздушный кодекс Российской Федерации : Федеральный закон от 19 марта 1997 г. № 60-ФЗ // СЗ РФ. – 1997. – № 12. – Ст. 1383.

3. Об утверждении федеральных правил использования воздушного пространства Российской Федерации : постановление Правительства РФ от 11 марта 2010 г. № 138 (ред. от 31 июля 2025 г.).

4. Попов А. В. Перспективы применения нейросетевых технологий в деятельности органов внутренних дел / А. В. Попов, С. Л. Анисимов // Актуальные проблемы кибербезопасности в сети Интернет : Сборник научных трудов Всероссийской конференции, Москва, 23 апреля 2020 года. – Москва : Московский университет Министерства внутренних дел Российской Федерации им. В. Я. Кикотя, 2020. – С. 111–113.

5. Талипова Э. И. Инновации в беспилотных системах: перспективы и новые подходы в создании высокотехнологичных комплексов / Э. И. Талипова // Актуальные вопросы эксплуатации систем охранного мониторинга и защищенных телекоммуникационных систем : Материалы Всероссийской научно-практической конференции адъюнктов, курсантов и слушателей, Воронеж, 10 июня 2025 года. – Воронеж : Воронежский институт МВД РФ, 2025. – С. 203–204.

6. Моделирование оценки эффективности функционирования систем безопасности объектов органов внутренних дел / Р. А. Жилин, А. В. Мельников, С. Б. Ахлюстин, В. В. Горлов. – Воронеж : Воронежский институт МВД России, 2023. – 104 с. – ISBN 978-5-88591-970-8.

СВЕДЕНИЯ ОБ АВТОРЕ

Матяшова Елена Владимировна.
Преподаватель кафедры физики и радиоэлектроники.
Воронежский институт МВД России.
E-mail: rudchik_lena@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Matyashova Elena Vladimirovna.
Lecturer at the Department of Physics and Radioelectronics.
Voronezh Institute of the Ministry of Internal Affairs of the Russian
Federation.
E-mail: rudchik_lena@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: беспилотное воздушное судно; внедрение передовых технологий; проблемы адаптации.

Keywords: unmanned aerial vehicle; introduction of advanced technologies; adaptation issues.

УДК 351.741

ВОПРОСЫ ОЦЕНКИ ПАРАМЕТРОВ СИГНАЛОВ РАДИОЛОКАЦИОННЫХ СИСТЕМ

ISSUES OF ESTIMATING THE PARAMETERS OF RADAR SYSTEM SIGNALS

В статье рассматривается вопрос оценки параметров сигналов с помощью суммарно-разностного дискриминатора, применяемого в различных радиолокационных системах.

The article discusses the issue of estimating signal parameters using a sum-difference discriminator used in various radar systems.

В радиолокационных системах (РЛС) оценивают параметры сигналов, связанные с дальностью, угловыми координатами (азимут) и скоростью движения целей, а также с помехоустойчивостью. Эти вопросы важны, так как работа РЛС происходит в условиях помех, и необходимо знать, как помехи влияют на точность оценивания параметров отражённых сигналов от целей. Оценка параметров радиолокационного сигнала является одной из важных задач, решаемых радиотехническими системами. Эта задача является актуальной в системах радиоэлектронной разведки, локации и навигации [1].

На оценку параметров сигналов радиолокационной системы влияют различные факторы [2]. К числу распространенных проблем, возникающих в этом процессе, можно отнести следующие.

Шумовые помехи: радиолокационные сигналы часто работают в условиях повышенного шума, что всегда приводит к искажению принимаемого сигнала. Шум может возникать из различных источников, включая тепловой шум, влияние других систем, что затрудняет оценку параметров.

Многолучевое распространение: во многих радиолокационных системах сигналы по мере распространения могут отражаться от различных поверхностей, прежде чем достичь приемника. Такое многолучевое распространение может привести к возникновению конструктивных и деструктивных помех, что затрудняет точную оценку таких параметров, как дальность и направление прихода сигнала.

Эффект Доплера: движение приемного устройства радара или цели может вызвать сдвиги в частоте принимаемого сигнала. При точной оценке необходимо учитывать эти сдвиги, что может привести к дополнительной сложности алгоритмов оценки параметров.

Искажение сигнала: радиолокационные сигналы могут подвергаться искажениям в радиоканале из-за различных факторов, включая атмосферные

условия, что приводит к флуктуациям амплитуды, фазы или частоты, что затрудняет оценку параметров.

Снижение мощности сигнала: по мере распространения радиолокационного сигнала его мощность уменьшается с расстоянием. Это снижение мощности может повлиять на рост влияния шумов и помех, что может усложнить оценку параметров.

Ограничения по выборке: недостаточная частота дискретизации может привести к эффектам сглаживания, которые могут скрыть истинные характеристики сигнала и затруднить оценку параметров.

Сложность алгоритма оценки: выбор и реализация алгоритмов для оценки параметров (например, метод наименьших квадратов, метод максимального правдоподобия и т.д.) может привести к усложнению вычислений, особенно в отношении сходимости и времени вычисления.

Динамика цели: динамика объекта (например, ускорение, маневрирование) может усложнить отслеживание и оценку, требуя надежных алгоритмов, способных обрабатывать быстрые изменения в движении.

Неоднозначности: при оценке таких параметров, как дальность и скорость, могут возникать неоднозначности параметра из-за периодического характера сигналов радара, особенно в импульсно-доплеровских системах.

Воздействие окружающей среды: такие факторы, как ветер, осадки, температура и атмосферные условия, могут влиять на распространение сигнала и, следовательно, на оценку параметров.

Ошибки калибровки: несовершенства компонентов радиолокационной системы (например, антенн, приемников) могут приводить к систематическим ошибкам в оценке параметров.

Для решения этих проблем необходима разработка усовершенствованных методов обработки сигналов, надежных алгоритмов и калибровки радиолокационной системы для повышения точности и надежности оценки параметров [3].

Радиолокаторы используют доплеровскую частоту для получения целевой радиальной скорости, а также для различения движущихся и неподвижных целей или объектов, таких как препятствия. Эффект Доплера описывает смещение центральной частоты падающей волны сигнала из-за движения цели относительно источника излучения. В зависимости от направления движения цели этот сдвиг частоты может быть положительным или отрицательным. Оценка несущей частоты (доплеровский сдвиг) в радиолокационных системах имеет решающее значение для таких применений, как отслеживание целей, измерение скорости и дальности.

Суммарно-разностный дискриминатор – это устройство, используемое для оценки доплеровских сдвигов в сигналах, принимаемых радиолокационными системами. Однако расчет точности дискриминатора представляет собой не решенную до конца задачу. Это связано с тем, что в

дискриминаторе используются некоторые нелинейные преобразования, изменяющие исходную гауссовскую статистику смеси сигнала и шума [2].

В то же время использование дискриминатора позволяет, например, решать задачу индикации движущихся целей. Другим примером является радар с синтезированной апертурой (SAR). В системах SAR суммарно-разностный дискриминатор может помочь усовершенствовать алгоритмы компенсации движения, улучшая качество изображения и обнаружение цели.

Радар с непрерывной частотной модуляцией (FMCW). В системах FMCW разница в частоте передаваемого и принимаемого сигнала используется для измерения расстояния и относительной скорости цели с использованием суммарно-разностной обработки.

Доплеровский радар, используемый в метеорологии и авиации, радар использует эти методы для оценки скорости и направления ветра на основе доплеровских сдвигов частиц осадков.

Таким образом, суммарно-разностный дискриминатор является мощным инструментом для оценки доплеровского сдвига в радиолокационных системах, позволяющим получать достоверные данные о скорости и движении цели [1]. Техническое решение достаточно просто реализуется на практике. Выбором структуры дискриминатора можно добиться широкого рабочего диапазона, быстродействия, устойчивости системы.

ЛИТЕРАТУРА

1. Оценивание дальности и скорости в радиолокационных системах / Под ред. А. И. Канащенкова и В. И. Меркулова. – Москва : Радиотехника, 2004. – Ч.1. – 312 с.

2. Машарова О. А. О законе распределения сигналов рассогласования некоторых типов дискриминаторов / О. А. Машарова, Ю. С. Радченко // Физические основы приборостроения. – 2017. – Т. 6, № 2 (24). – С. 90–97.

3. Радченко Ю. С. Синтез и анализ субоптимального обнаружителя радиосигналов с неравномерной фазой / Ю. С. Радченко, Т. М. Овчинникова, В. П. Удалов // Вестник Воронежского института МВД России. – 2023. – № 4. – С. 167–175.

СВЕДЕНИЯ ОБ АВТОРЕ

Удалов Валерий Петрович.

Доцент кафедры физики и радиоэлектроники.

Кандидат физико-математических наук, доцент.

Воронежский институт МВД России.

E-mail: uvalery@yandex.ru,

Россия, 394065, Воронеж, проспект Патриотов, 53.

Udalov Valery Petrovich.
Assistant Professor of the Physics and Radioelectronics Department.
Candidate of Physical and Mathematical Sciences, Assistant Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: uvalery@yandex.ru,
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: оценка несущей частоты сигнала; суммарно-разностный дискриминатор.

Keywords: estimation of the carrier frequency of the signal; total-difference discriminator.

УДК 621.391

**РАЗРАБОТКА АЛГОРИТМА ОЦЕНКИ
УРОВНЯ ИТ-КОМПЕТЕНТНОСТИ СОТРУДНИКОВ МВД РОССИИ**

**DEVELOPMENT OF AN ALGORITHM FOR ASSESSING
THE LEVEL OF IT COMPETENCE OF EMPLOYEES
OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA**

Представлен алгоритм оценки уровня информационно-технологической компетентности сотрудников органов внутренних дел. Методология включает процедуру кластеризации персонала на основе объективных показателей служебной активности с последующим применением специализированных измерительных инструментов для каждого кластера. Для обеспечения метрологической корректности измерений реализовано преобразование результатов тестирования в интервальную шкалу с использованием модели Раша. Верификация алгоритма выполнена на репрезентативной выборке сотрудников МВД России ($n = 260$). Установлена статистическая значимость различий между кластерами ($p < 0,001$). Доказана адекватность измерительной модели (инфит-статистики 0,8-1,2). Разработанный алгоритм позволяет формировать объективные основания для принятия кадровых решений в условиях цифровой трансформации правоохранительной деятельности.

The article presents an algorithm for assessing the level of information technology competence of employees of the internal affairs bodies. The methodology includes a procedure for clustering personnel based on objective indicators of service activity with subsequent application of specialized measurement tools for each cluster. To ensure metrological correctness of measurements, the results of testing are converted into an interval scale using the Rasch model. Verification of the algorithm was performed on a representative sample of employees of the Ministry of Internal Affairs of Russia ($n = 260$). Statistical significance of differences between clusters was established ($p < 0.001$). The adequacy of the measurement model was proved (infit statistics 0.8-1.2). The developed algorithm allows to form objective grounds for making personnel decisions in the conditions of digital transformation of law enforcement activities.

Интенсификация процессов цифровизации правоохранительной деятельности обуславливает повышение требований к уровню информационно-технологической подготовки личного состава органов внутренних дел. Неоднородность исходного уровня ИТ-компетентности сотрудников детерминирует необходимость разработки дифференцированных подходов к оценке соответствующих компетенций [1].

Существующие системы оценки характеризуются отсутствием адаптивности к индивидуальным особенностям испытуемых и использованием порядковых шкал, что ограничивает возможности корректного статистического анализа [2]. Преодоление указанных методологических ограничений требует применения современных методов анализа данных, включая машинное обучение для сегментации контингента и вероятностные модели для метрологически корректного измерения латентных переменных.

Разработанный алгоритм включает три последовательных этапа реализации.

Этап 1. Кластеризация персонала.

Для сегментации сотрудников по уровню ИТ-компетентности применяется модифицированный алгоритм К-средних с оптимизацией количества кластеров методом силуэта [3]. Входными параметрами выступают объективные показатели служебной активности:

- x_1 – частота использования информационных систем (обращений/день)
- x_2 – индекс разнообразия используемых инструментов (0-10)
- x_3 – объем обрабатываемых данных (ГБ/месяц)
- x_4 – показатель эффективности работы (задачи/час)

Этап 2. Разработка измерительных инструментов.

Для каждого кластера разрабатываются специализированные оценочные процедуры:

Кластер 1 (экспертный уровень):

- Формат: кейсовые задачи с политомической оценкой.
- Критерии: полнота решения, инновационность подхода, практическая применимость.
- Пример: «Разработайте алгоритм анализа массива оперативных данных объемом 1 Гб».

Кластер 2 (продвинутый уровень):

- Формат: тестовые задания дихотомического типа.
- Содержание: работа с CRM-системами, электронный документооборот, специализированное ПО.
- Пример: «Определите функцию для объединения данных из двух таблиц по ключевому полю».

Кластер 3 (базовый уровень):

- Формат: практические задания с бинарной оценкой.
- Содержание: базовые операции в ОС, работа с офисными приложениями.
- Пример: «Создайте документ установленного образца и сохраните в указанной директории».

Этап 3. Метрологическое преобразование результатов.

Для преобразования первичных результатов в интервальную шкалу применяется модель Раша [4]. Для дихотомических данных (1):

$$P(X_{ni} = 1 | \theta_n, \delta_i) = \frac{e^{(\theta_n - \delta_i)}}{1 + e^{(\theta_n - \delta_i)}} \quad (1)$$

где $P(X_{ni} = 1)$ – вероятность правильного ответа, θ_n – уровень компетентности сотрудника, δ_i – параметр сложности задания.

Для политомических данных используется модель частичного кредита (2):

$$P(X_{ni} = k | \theta_n, \delta_i, \tau_{ik}) = \frac{e^{\sum_{j=0}^k (\theta_n - \delta_i + \tau_{ij})}}{\sum_{m=0}^K e^{\sum_{j=0}^m (\theta_n - \delta_i + \tau_{ij})}} \quad (2)$$

где τ_{ik} – пороговый параметр k-ой категории задания.

Апробация алгоритма выполнена на репрезентативной выборке сотрудников МВД России (n=260). Верификация результатов включала:

1. Статистический анализ кластеров.

Однофакторный дисперсионный анализ подтвердил значимость различий между кластерами по всем входным параметрам ($p < 0,001$). Распределение сотрудников: кластер 1 – 22%, кластер 2 – 48%, кластер 3 – 30%.

2. Валидизация измерительной модели.

Калибровка параметров заданий в модели Раша показала хорошее соответствие эмпирических данных теоретической модели (инфит-статистики в диапазоне 0,8-1,2). Надежность измерения составила 0,87.

3. Построение единой шкалы компетентности.

Реализовано преобразование результатов в интервальную шкалу с метрической инвариантностью относительно кластерной принадлежности респондентов.

Разработанный алгоритм позволяет:

- обеспечить объективность оценки ИТ-компетентности сотрудников;
- реализовать дифференцированный подход к тестированию различных групп персонала;
- получать метрологически корректные измерения в интервальной шкале;
- формировать статистически обоснованные рекомендации по развитию персонала.

Перспективы исследования связаны с разработкой динамических моделей отслеживания изменения уровня компетентности во времени и интеграцией алгоритма в систему управления персоналом МВД России.

ЛИТЕРАТУРА

1. Шаляпин П. В. Разработка алгоритма кластеризации на основе методов машинного обучения и статистической валидации / П. В. Шаляпин, Л. В. Россихина // Информационные технологии в УИС. – 2025. – № 2. – С. 29–46.
2. Дубина И. Н. Математические основы эмпирических социально-экономических исследований : учебное пособие / И. Н. Дубина. – Барнаул : Изд-во Алтайского университета, 2006. – 263 с.
3. Pedregosa F. et al. Scikit-learn : Machine Learning in Python // Journal of Machine Learning Research. – 2011. – Vol. 12. – P. 2825–2830.
4. Bond T.G., Fox C.M. Applying the Rasch Model : Fundamental Measurement in the Human Sciences. – 3rd ed. – Routledge, 2015. – 340 p.

СВЕДЕНИЯ ОБ АВТОРЕ

Шаляпин Павел Владимирович.
Адъюнкт кафедры Информационных технологий.
Академия Управления МВД России.
E-mail: pavelshalaypin@mail.ru
Россия, 125993, г. Москва, ул. Зои и Александра Космодемьянских, 8.

Shalyapin Pavel Vladimirovich.
Adjunct of the Department of Information Technologies.
Academy of Management of the Ministry of Internal Affairs of Russia.
E-mail: pavelshalaypin@mail.ru
Russia, 125993, Moscow, 8, Zoi and Aleksandra Kosmodemyanskikh str., 8.

Ключевые слова: ИТ-компетентность; модель Раша; кластерный анализ; оценка персонала; алгоритм оценки; измерение компетенций.

Keywords: IT competence; Rasch model; cluster analysis; personnel assessment; assessment algorithm; competence measurement.

УДК 004.8:351.74

ВСЕРОССИЙСКИЙ СЕМИНАР
ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ
БЕЗОПАСНОСТИ ОХРАНЯЕМЫХ ТЕРРИТОРИЙ И ОБЪЕКТОВ
ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Е. М. Абросимова

ОБЗОР СОВРЕМЕННЫХ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ
С ВОЗМОЖНОСТЬЮ АНАЛИТИКИ ДАННЫХ

OVERVIEW OF MODERN VIDEO SURVEILLANCE SYSTEMS
WITH DATA ANALYTICS CAPABILITIES

В данной статье проанализированы текущее состояние, ключевые решения и особенности применения видеоаналитики в Российской Федерации.

This article analyzes the current state, key solutions, and features of the application of video analytics in the Russian Federation.

В Российской Федерации системы видеонаблюдения с аналитическими функциями активно внедряются в рамках национальных проектов «Умный город», «Безопасный город» и цифровой трансформации отраслей.

Функционирование систем регламентируется следующими документами:

- Федеральный закон № 152-ФЗ «О персональных данных» (требования к обработке биометрии);
- Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные»;
- Требования МВД России к системам видеонаблюдения для объектов транспортной инфраструктуры;
- Региональные нормативные акты (например, требования к системам «Безопасный город» в субъектах РФ).

Архитектурные особенности российских решений представлены ниже.

Типичная структура систем видеонаблюдения на российском рынке включает:

1. **Отечественные IP-камеры** (Beward, «БайтЭрг», «Випакс») с разрешением от 1 Мп до 8 Мп, поддержкой Wide Dynamic Range (WDR) и ИК-подсветки.

2. **Серверное оборудование** на базе процессоров «Эльбрус» или импортных платформ с российской сборкой.

3. **Платформы видеоменеджмента** российского производства (например, «Интеллект», «Видеоинтеллект», AxxonSoft).

4. **Локальные хранилища** с учётом требований по хранению данных на территории Российской Федерации.

5. **Каналы связи** с приоритетом на отечественные телекоммуникационные сети.

Рассмотрим ключевые российские платформы видеоаналитики:

1. «Интеллект» (ITV Group):

– функции: распознавание лиц, номеров, детектирование событий, подсчёт людей;

– интеграция с системами контроля доступа;

– сертификация ФСТЭК и ФСБ для объектов критической инфраструктуры.

2. Axhoxsoft (входит в группу «код безопасности»):

– модульная архитектура с поддержкой видеоалгоритмов;

– виды аналитики: трекинг объектов, обнаружение аномалий, тепловые карты;

– совместимость с камерами более 150 производителей.

3. «видеоинтеллект» («центр речевых технологий»):

– специализированные модули для транспортной безопасности;

– распознавание лиц с учётом масок и иных препятствий;

– поддержка мультисенсорной аналитики (видео + аудио).

4. «синезис»:

– облачные и локальные решения для ритейла и промышленности;

– анализ очередей, подсчёт посетителей, поведенческая аналитика;

– интеграция с cgm и bi-системами.

Технологические ограничения:

1. **Импортозамещение:** зависимость от зарубежных процессоров и сенсоров.

2. **Вычислительные мощности:** нехватка отечественных для обработки видеопотоков.

3. **Конфиденциальность:** строгие требования к хранению биометрических данных.

4. **Климатические условия:** необходимость адаптации камер к экстремальным температурам.

5. **Интеграция:** совместимость с legacy-системами на объектах.

Перспективные направления развития в РФ:

1. **Национальные AI-платформы:** создание единых решений на базе отечественных нейросетей.

2. **Квантовая криптография:** защита видеопотоков для объектов госсектора.

3. **5G-сети:** передача данных с низкой задержкой для edge-аналитики.

4. **Цифровые двойники городов:** интеграция видеонаблюдения

с 3D-моделями городских пространств.

5. Блокчейн для верификации: защита целостности видеоархивов.

Российский рынок видеоаналитики демонстрирует устойчивый рост благодаря государственной поддержке и спросу со стороны ключевых отраслей. Основными трендами являются: усиление требований к импортозамещению, расширение применения в задачах безопасности, интеграция с «умной» городской инфраструктурой.

ЛИТЕРАТУРА

1. О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ.

2. ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные».

3. Стратегия развития отрасли информационных технологий в РФ на 2024–2030 гг.

4. Отчёты Ассоциации разработчиков систем видеоаналитики (АРСВ) за 2023–2024 гг.

5. Материалы конференций «Цифровая индустрия промышленной России» (ЦИПР-2024).

6. Технические спецификации производителей: ITV Group, АххонSoft, «Центр речевых технологий».

СВЕДЕНИЯ ОБ АВТОРЕ

Абросимова Евгения Михайловна.

Преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга.

Кандидат технических наук.

Воронежский институт МВД России.

E-mail: chip_ik@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Abrosimova Evgeniya Mikhailovna.

Lecturer in electronic systems and complexes of security monitoring.

Candidate of technical Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: chip_ik@mail.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: видеонаблюдение; аналитика данных; видеointеллект; Умный город; Безопасный город.

Keywords: video surveillance; data analytics; video intelligence; Smart City; Safe City.

УДК 004.056

**ОСОБЕННОСТИ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ
И ПРОТИВОДЕЙСТВИЯ ДИВЕРСИЯМ С ИСПОЛЬЗОВАНИЕМ
БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ
НА ОБЪЕКТАХ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ**

**FEATURES OF ANTI-TERRORIST SECURITY AND
COUNTERACTION TO SABOTAGE USING UNMANNED AERIAL
VEHICLES AT LAW ENFORCEMENT AGENCIES**

В данной статье рассматриваются антитеррористическая защищенность и противодействия диверсиям с использованием беспилотных летательных аппаратов на объектах правоохранительных органов.

This article discusses anti-terrorism security and countering sabotage using unmanned aerial vehicles at law enforcement agencies.

Современная угроза безопасности приобрела новые, технологичные очертания. Беспилотные летательные аппараты (БПЛА), изначально создававшиеся для военных и гражданских нужд, стали мощным инструментом в руках злоумышленников и террористов. Объекты правоохранительных органов – потенциально представляют собой приоритетные цели для проведения разведки, диверсий и даже прямых атак с использованием дронов. Это обуславливает необходимость разработки и внедрения комплексных систем противодействия, адаптированных к новым вызовам.

Угроза безопасности беспилотных летательных аппаратов классифицируется:

1. Ведение разведки и наблюдения:

– картографирование и фотограмметрия (создание подробных 3D-моделей объектов, определение периметра, мест размещения постов охраны, камер видеонаблюдения, подъездных путей);

– мониторинг режимных зон (наблюдение за внутренними дворами, местами разгрузки, окнами кабинетов с целью сбора конфиденциальной информации);

– контроль за оперативной обстановкой (фиксация перемещений сотрудников и автотранспорта для планирования других противоправных действий).

2. Проведение диверсионных актов:

– доставка и сброс взрывных устройств (небольшой груз, сброшенный на имущество, может нанести значительный ущерб и привести к человеческим жертвам);

- поджоги (использование зажигательных смесей для уничтожения имущества, провоцирование пожаров);
- доставка химических, радиоактивных, биологических и иных средств поражения.

3. Нарушение работы инфраструктуры:

- создание помех (сброс металлизированной сетки или использование дронов-глушителей для нарушения работы линий связи, систем передачи данных и видеонаблюдения);
- провокации и психологическое воздействие (целенаправленные полеты для демонстрации уязвимости объекта, провоцирования паники, отвлечения внимания охраны для проведения атаки с земли).

Защита объектов правоохранительных органов от беспилотных летательных аппаратов должна быть многоуровневой и интегрированной в общую систему антитеррористической защищенности.

Первый и критически важный этап – это обнаружение беспилотных летательных аппаратов. Нельзя нейтрализовать то, что не видишь. Для обнаружения БПЛА используются следующие технические средства обнаружения:

- радиочастотный мониторинг (пеленгация и анализ сигналов управления дроном и передачи видеоданных, позволяет обнаружить аппарат до его визуального появления и определить местоположение оператора);
- радарные системы (эффективны для обнаружения БПЛА по отражаемому радиосигналу, особенно на подлете к объекту);
- акустические датчики: (распознают уникальный звуковой профиль двигателей мультикоптеров).

Также допускается применение камер с высоким разрешением и тепловизоров для визуального подтверждения, идентификации и сопровождения цели, в том числе в ночное время.

После обнаружения система должна определить, является ли объект вражеским дроном, птицей или, например, разрешенным к полету аппаратом. Это делается с помощью анализа данных с камер и радиочастотной сигнатуры.

После принятия решения о враждебности цели применяются средства противодействия:

- радиоэлектронное подавление (самый распространенный и безопасный в городских условиях метод, когда глушилка создает мощные помехи на каналах управления и радиосвязи, заставляя дрон либо вернуться к оператору, либо совершить аварийную посадку);
- радиоэлектронный захват (более сложный метод, при котором система перехватывает управление дроном, обманывая его GPS-сигнал и команды, и принудительно сажает в безопасном месте);

– непосредственный физический контакт (применение снайперского огня, сетей (выстреливаемых из специальных ружей или с помощью дронов-перехватчиков) или лазерных систем);

– высокоэнергетические лазеры и СВЧ-оружие (перспективные технологии, которые физически выводят электронику дрона из строя).

Особенности и проблемы при организации защиты объектов правоохранительных органов:

– правовое поле (применение средств нейтрализации в городской среде строго регламентировано, падение дрона может привести к жертвам и разрушениям, поэтому необходимы четкие регламенты и правила применения силы);

– интеграция с существующими системами безопасности (система противодроновой обороны не должна работать изолированно, ее необходимо интегрировать с системами видеонаблюдения, контроля доступа и оповещения, создавая единый информационный контур);

– защита от роев дронов (современная угроза предполагает атаку группой (роем) координирующихся дронов, что значительно усложняет задачу перехвата, системы должны быть способны обнаруживать и нейтрализовывать множественные цели);

– автономные дроны (угроза от БПЛА, запрограммированных на полет по заданному маршруту без активного радиоканала управления, против которых РЧ-подавление неэффективно, против них наиболее действенны радары и кинетические методы);

– обучение и подготовка сотрудников (сотрудники должны уметь не только пользоваться техникой, но и распознавать угрозу, действовать по утвержденным алгоритмам и не поддаваться панике).

Защита объектов правоохранительных органов от угроз с использованием БПЛА перестала быть теоретической задачей и стала насущной необходимостью. Успех в этом противоборстве зависит от комплексного подхода, сочетающего передовые технологии обнаружения и нейтрализации, адаптированную правовую базу, грамотное планирование защитных мер и постоянное обучение сотрудников. Создание эффективного «Антидронowego щита» – это не только вопрос технологического превосходства, но и вопрос сохранения суверенитета и безопасности критически важной государственной инфраструктуры.

ЛИТЕРАТУРА

1. Об особенностях защиты от актов незаконного вмешательства с использованием беспилотных аппаратов объектов транспортной инфраструктуры и (или) групп объектов транспортной инфраструктуры, вокруг которых устанавливаются зоны безопасности : постановление Правительства Российской Федерации от 30 апреля 2025 г. № 588.

2. Об утверждении Порядка принятия решения о пресечении нахождения беспилотных воздушных судов в воздушном пространстве в целях отражения нападения на объекты, охраняемые военизированными и сторожевыми подразделениями федерального государственного унитарного предприятия «Охрана» Федеральной службы войск национальной гвардии Российской Федерации, работников военизированных и сторожевых подразделений федерального государственного унитарного предприятия «Охрана» Федеральной службы войск национальной гвардии Российской Федерации или лиц, находящихся на этих объектах, а также Перечня должностных лиц федерального государственного унитарного предприятия «Охрана» Федеральной службы войск национальной гвардии Российской Федерации, уполномоченных на принятие такого решения : приказ Росгвардии от 17 марта 2023 г. № 66.

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.

4. Об утверждении Федеральных авиационных правил «Порядок организации и обеспечения функционирования линий управления беспилотными авиационными системами и контроля беспилотных авиационных систем для беспилотных авиационных систем в составе с беспилотными гражданскими воздушными судами : приказ Министерства транспорта Российской Федерации от 24 апреля 2025 г. № 142.

5. Жилин Р. А. Численный метод кластеризации однородных альтернатив, характеризующих качество антитеррористической защищенности объектов органов внутренних дел, на основе суммы различий взвешенных признаков / Р. А. Жилин, А. В. Мельников, Г. В. Перминов // Моделирование, оптимизация и информационные технологии. – 2020. – Т. 8, № 4 (31). – DOI 10.26102/2310-6018/2020.31.4.015.

6. Мельников А. В. Моделирование функциональной взаимосвязи результатов экспертизы опасности отдельных видов нарушителей для оценки рисков безопасности охраняемых объектов / А. В. Мельников, Р. А. Жилин, И. А. Старенков // Вестник Воронежского института ФСИИ России. – 2019. – № 3. – С. 88–92.

СВЕДЕНИЯ ОБ АВТОРЕ

Бондаренко Евгений Сергеевич.

Преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга.

Воронежский институт МВД России.

E-mail: Bondarenko-92-92@mail.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Bondarenko Evgeny Sergeevich.

Lecturer at the Department of Radio Engineering Systems and Security Monitoring complexes.

Voronezh Institute of the Ministry of internal Affairs of Russia.

E-mail: Bondarenko-92-92@mail.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: угроза безопасности; обнаружение; беспилотные летательные аппараты; правоохранительные органы; интеграция; БПЛА.

Keywords: security threat; detection; unmanned aerial vehicles; law enforcement; integration; UAVS.

УДК 340.1

**ОСОБЕННОСТИ ЗАЩИТЫ ОБЪЕКТА ОХРАНЫ
ПРИ ВОЗНИКНОВЕНИИ ЧРЕЗВЫЧАЙНОЙ СИТУАЦИИ**

**FEATURES OF PROTECTION OF THE PROTECTED FACILITY
IN CASE OF EMERGENCY**

В статье рассматриваются меры защиты объектов охраны, основанные на интегративном анализе действующей нормативно-правовой базы и практических кейсов реагирования на чрезвычайные ситуации.

The article discusses measures to protect security facilities based on an integrative analysis of the current regulatory framework and practical cases of emergency response.

В условиях нарастающей частоты и комплексного характера современных чрезвычайных ситуаций, охватывающих как природные катастрофы, так и техногенные аварии, критически важным становится совершенствование систем защиты объектов охраны. Эффективная защита таких объектов является неотъемлемым элементом обеспечения устойчивого развития инфраструктуры и поддержания стабильности общества. Это обусловлено необходимостью минимизации ущерба и сохранения функциональности ключевых систем в условиях постоянно меняющихся и динамичных сценариев рисков.

Несмотря на наличие разработанных нормативных документов и общих подходов к безопасности, сохраняется системная проблема их недостаточной адаптации к специфике локальных чрезвычайных ситуаций. Особенно остро это проявляется при возникновении комбинированных угроз, таких как пожары, сопровождающиеся наводнениями, что приводит к значительным операционным задержкам. В результате возникают существенные ресурсные потери и повышаются риски для сотрудников и работников, что подчеркивает необходимость более гибких и специфичных решений.

Целью настоящего рассмотрения вопроса является разработка оптимизированных мер защиты объектов охраны, которые будут основаны на интегративном анализе действующей нормативно-правовой базы и практических кейсов реагирования на чрезвычайные ситуации. Такой подход позволит обеспечить адаптацию защитных механизмов к многофакторным сценариям угроз, повышая эффективность превентивных и оперативных действий. Конечный результат направлен на усиление устойчивости критически важных объектов в условиях постоянно меняющейся среды рисков.

Для достижения поставленной цели в тезисе будут решены следующие задачи: проанализированы нормативные правовые акты, регулирующие защиту объектов охраны в чрезвычайных ситуациях, с выявлением ключевых требований и существующих пробелов. Далее будет проведена оценка эффективности применяемых мер защиты на реальных примерах чрезвычайных ситуаций (ЧС). На основе полученных данных будут разработаны адаптированные меры реагирования, учитывающие специфику различных типов угроз, а также проведен сравнительный анализ потенциального влияния предложенных решений на повышение устойчивости объектов охраны.

В законодательной базе Российской Федерации установлены фундаментальные регламенты, регулирующие вопросы безопасности объектов, подверженных угрозе в случае возникновения чрезвычайных ситуаций. Ведущими нормами в указанной области выступают Федеральный закон № 68 «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» [1] вместе с Федеральным законом № 69 «О пожарной безопасности», которые закладывают организационно-правовые механизмы защиты, а также очерчивают ответственность и полномочия государственных и иных структур, призванных осуществлять профилактику и оперативное реагирование при наступлении ЧС. Содержательные положения этих законов обеспечивают нормативную платформу для последующего создания отраслевых стандартов и регламентирующих актов подзаконного характера. Федеральный закон № 68, в частности, определяет архитектуру и функционирование комплексной государственной системы, предназначенной для предупреждения и оперативной ликвидации чрезвычайных ситуаций, а также устанавливает критерии для разработки специализированных планов мероприятий, направленных на профилактику и устранение последствий ЧС непосредственно на стратегически значимых объектах охраны. ФЗ № 69 определяет правовые основы обеспечения пожарной безопасности, включая обязательность соблюдения правил противопожарного режима [2]. Оба закона предусматривают ответственность за нарушение установленных норм и правил в сфере защиты от ЧС. Взаимодействие указанных федеральных законов создает комплексную систему правового регулирования безопасности объектов охраны. «Целью Типовой инструкции является упорядочение деятельности по обеспечению антитеррористической безопасности объектов» [3]. Это свидетельствует о системном подходе к формированию нормативной базы, учитывающем различные уровни регулирования.

Подзаконные акты и отраслевые стандарты конкретизируют требования федерального законодательства применительно к различным категориям охраняемых объектов. «Вопросы антитеррористической защиты объектов, решение которых требует учета специфики конкретных

сфер деятельности, изложены далее по тексту издания» [4]. В числе ключевых аспектов данных нормативных актов выделяется учет специфики эксплуатации различных комплексов, энергетических сооружений, транспортных узлов и иных значимых структур. В частности, регламентируются особые стандарты для архитектуры защиты, методы предотвращения экстремальных происшествий, а также алгоритмы реагирования в случае их наступления.

Среди рисков, характерных для защищаемых объектов во время чрезвычайных происшествий, осуществляется классификация по трем основным направлениям: природного, техногенного и антропогенного генезиса. К первой группе относят угрозы, возникающие вследствие проявления сил природы – будь то землетрясения, водные катастрофы или мощные ураганы. Ко второй категории приписывают инциденты, происходящие в результате отказов на производственных предприятиях, транспортных аварий или прекращения функционирования жизненно важных инженерных систем. В отличие от них, третий тип опасностей определяется различными действиями человеческого фактора – как преднамеренно, так и по неосторожности, включая террористические замыслы либо подрывные мероприятия. Для каждой выделенной категории разрабатываются индивидуальные механизмы защиты и специализированные методы обеспечения устойчивости защищаемых объектов. Природные явления характеризуются сезонностью и региональной привязкой, что позволяет прогнозировать их возникновение с определенной точностью. Техногенные катастрофы часто возникают из-за износа оборудования или нарушений технологических процессов. Антропогенные факторы отличаются непредсказуемостью и целенаправленным характером воздействия, что существенно осложняет меры противодействия.

Риски для объектов охраны дифференцируются по масштабу воздействия и вероятности реализации. Масштаб воздействия определяется величиной потенциального ущерба: от локальных инцидентов до катастроф федерального уровня. Вероятность реализации оценивается на основе статистических данных и экспертных оценок, учитывающих частоту возникновения аналогичных событий в прошлом. Комплексный анализ этих критериев позволяет ранжировать угрозы по степени приоритетности при разработке защитных мер. Поражающие факторы различных чрезвычайных ситуаций оказывают специфическое влияние на уязвимость объектов охраны.

В силу особенностей природы, чрезвычайные ситуации природного происхождения инициируются физическим разрушением, чему могут сопутствовать вторичные эффекты – от возгораний до химических загрязнений. В противоположность, техногенные происшествия, как правило, характеризуются выбросами токсических компонентов и

энергозатратными процессами, что создает дополнительную нагрузку на защитные механизмы. Угрозы, генерируемые человеческой деятельностью, зачастую проявляются в виде комплексного воздействия деструктивных факторов, ориентированных на нарушение стабильности систем обеспечения безопасности.

Детальный анализ аварий на охраняемых объектах представляет возможность структурировать инциденты на основании специфики их возникновения: среди них особое место занимают как техногенные происшествия, так и стихийные бедствия, а также незаконные противоправные воздействия. Каждый из этих типовых сценариев диктует применение уникальных методов защиты, адаптированных под характер угрозы. В контексте анализа развития событий выявляется, что реальные траектории течения ЧС зачастую оказываются непредсказуемо отличными от теоретически установленных алгоритмов реагирования, что определяет приоритет внедрения адаптивных стратегий. Точное определение специфики индивидуальных сценариев развития ЧС становится краеугольным камнем для формирования эффективных мер предупреждения и организации своевременного реагирования, что требует всестороннего учета множества переменных. Поэтому проектирование защитных систем должно основываться на интеграции факторов первичного и вторичного характера, а также сочетать междисциплинарный подход, обеспечивающий высокую степень адаптивности инженеринговых решений.

Прежде всего, систематизированное исследование недостатков, проявляющихся в деятельности охранных подразделений и функционировании инфраструктуры безопасности в условиях чрезвычайных ситуаций, обозначает целый спектр существенных затруднений. На практике отмечается, что на ранних этапах возникновения инцидентов часто фиксируется недостаточная оперативность ответных мер, что способствует усугублению неблагоприятных последствий. Анализ демонстрирует, что несвоевременная и не вполне точная передача информации между персоналом, а также между охраняемыми объектами и внешними экстренными службами значительно осложняет согласование действий и скоординированное реагирование. Осуществление взаимодействия между разными эшелонами системы защиты и иными организациями по-прежнему остается уязвимым местом: фрагментарная подготовка персонала к взаимодействию с существующими угрозами приводит к снижению совокупной эффективности реагирования.

Кроме того, отсутствует динамичная адаптация стандартных мер под множественные и одновременно проявляющиеся угрозы, что свойственно комбинированным чрезвычайным ситуациям, обладающим многослойной структурой развития. Данный факт акцентирует потребность в целенаправленном и непрерывном усовершенствовании обучающих

программ и обновлении техническо-организационных мероприятий. Значимыми остаются также пробелы в регулировании корпоративных инструкций в соответствии с изменяющейся природой чрезвычайных обстоятельств и ускорением технологических трансформаций в сфере угроз. Комплексный анализ разночтений между запланированными действиями и фактическим ходом развития внештатных ситуаций на объектах позволяет выделить ряд обобщённых рекомендаций, направленных на повышение качества противодействия угрозам. Необходимость рутинного пересмотра и соответствующей доработки мер реагирования, что обеспечивается регулярными практическими учениями, свидетельствует о важности гибкой организационной структуры, способной подстраиваться под динамику окружающих условий. Чётко прослеживается тенденция, согласно которой эмпирически подтверждённая способность быстро адаптировать стратегию безопасности к новому спектру возможных сценариев инцидентов становится определяющей характеристикой надёжной системы защиты.

Методологическая основа конструирования эффективных мер реагирования строится на интеграции нормативно-правовых предписаний и результатах анализа ситуаций, зафиксированных в реальном времени на объектах охраны. Такой синтетический подход позволяет формировать многоуровневые алгоритмы реагирования, учитывая не только формальные требования регулирующих органов, но и конкретные прецеденты, отражающие реальное взаимодействие факторов в условиях риска. Изучение успешного опыта предотвращения и локализации ЧС через детальное исследование международных и отраслевых практик выступает в качестве катализатора разработки усовершенствованных процедур.

Приоритетной задачей при пересмотре процедур предупреждения и нейтрализации последствий чрезвычайных ситуаций является сокращение периода между возникновением угрозы и моментом запуска действующих защитных механизмов, что позволяет минимизировать масштабы негативных последствий и повысить уровень устойчивости объекта к возникшим критическим процессам.

Оперативность действий критически важна для предотвращения эскалации чрезвычайной ситуации и снижения потенциального ущерба. «Как правило, положительный эффект от быстрого реагирования с целью предотвращения чрезвычайных ситуаций в большинстве случаев зависит от умения руководства быстро анализировать (обрабатывать) и преобразовывать полученный информационный ресурс для выработки планов, директив, проектов и распоряжений» [4].

Обязательным условием эффективности мер является обеспечение оперативной гибкости и вариативности действий сотрудников и работников. Процедуры реагирования должны быть гибко спроектированы

таким образом, чтобы приспособливаться к динамическим изменениям в условиях чрезвычайных происшествий, а не оставаться неизменными или строго закреплёнными. Подобная пластичность в протоколах обеспечивает сотрудникам и работникам пространство для принятия рациональных и адекватных решений в ситуациях, выходящих за пределы типовых сценариев, что способствует повышению общего уровня защищённости и устойчивости защищаемого объекта перед разнообразными угрозами.

Конструирование действенных мер безопасности невозможно без учета необходимости варьирования моделей реагирования в зависимости от спектра угроз. Особенности чрезвычайных ситуаций природного характера, отличающиеся значительным элементом неожиданности и непредсказуемости, противопоставляются специфике техногенных инцидентов, где основной акцент часто смещён в сторону человеческих просчётов или ошибок. В перечень антропогенных опасностей входят как проявления социальной нестабильности, так и действия террористического свойства [5]. Тщательный анализ и интеграция этих фундаментальных различий позволяет выстраивать адаптивные, адресные схемы реагирования для каждого отдельного типа рискованной ситуации.

Сложность обеспечения безопасности объектов в условиях природных катастроф определяется масштабом проявляемых деструктивных факторов и их стихийной природой. Масштабные повреждения, вызванные ураганами, паводками либо сейсмическими потрясениями, парализуют работу объектов инфраструктуры на больших площадях, что приводит к необходимости стратегического планирования наперёд и формирования автономных систем жизнеобеспечения. Немаловажно при организации мероприятий по эвакуации учитывать вероятность дезорганизации транспортных коммуникаций вследствие разрушений.

В случае возникновения аварийного события техногенного характера первостепенное значение приобретает оперативная нейтрализация очага опасности: например, устранение распространяющегося радиоактивного загрязнения, отравляющих выбросов, а также локализация пожарных очагов требует немедленного реагирования. Специализированные команды должны быть подготовлены к выполнению процедур по отделению зоны поражения, сведению к минимуму экспозиции персонала, а наличие соответствующих средств индивидуальной и коллективной защиты становится критическим фактором успешного реагирования. В условиях возникновения гибридных кризисных ситуаций, сопряжённых с одновременным проявлением чрезвычайных явлений разнообразной природы, становится необходимым интегрированный подход. К примеру, сейсмическая активность способна инициировать аварии на промышленных предприятиях, что приводит к наложению угроз различного рода. Такие сценарии требуют наличия выверенных

мероприятий, предусматривающих согласованные меры по проведению эвакуации, локальных операций по подавлению вторичных воздействий, а также четкой согласованности между задействованными оперативными структурами для рационального распределения средств и организационного взаимодействия в экстремальных условиях.

Возрастающее влияние климатических колебаний и антропогенных угроз на безопасность указывает на неотложность пересмотра существующих подходов, причем обозначенная проблема приобретает особое значение в условиях постоянного роста рисков современности. Рассмотрение действующих законодательных положений выявило многочисленные неурегулированные аспекты – прежде всего, при анализе сценариев одновременного проявления разнотипных угроз, как, например, сочетание противопожарных и гидрологических катастроф. Такой дисбаланс свидетельствует о потребности в трансформации механизмов государственного регулирования, что должно обеспечить оперативность и адекватность ответных действий субъектов при внезапных изменениях обстановки.

ЛИТЕРАТУРА

1. О пожарной безопасности : Федеральный закон от 21 декабря 1994 г. № 69-ФЗ // СПС «КонсультантПлюс».
2. О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера : Федеральный закон от 21 декабря 1994 г. № 68-ФЗ // СПС «КонсультантПлюс».
3. Малютин О. С. Современные информационные технологии в деятельности РСЧС / О. С. Малютин // Сибирский пожарно-спасательный вестник. – 2016. – № 3. – С. 18–22.
4. Пучков В. А. Правовые и институциональные основы предупреждения и ликвидации последствий чрезвычайных ситуаций / В. А. Пучков, Т. Я. Хабриева, В. С. Артамонов. – Москва : Юриспруденция, 2016. – 528 с.
5. Жилин Р. А. Численный метод кластеризации однородных альтернатив, характеризующих качество антитеррористической защищенности объектов органов внутренних дел, на основе суммы различий взвешенных признаков / Р. А. Жилин, А. В. Мельников, Г. В. Перминов // Моделирование, оптимизация и информационные технологии. – 2020. – Т. 8, № 4 (31). – DOI 10.26102/2310-6018/2020.31.4.015.

СВЕДЕНИЯ ОБ АВТОРЕ

Гречаный Сергей Анатольевич.

Начальник кафедры радиотехнических систем и комплексов охранного мониторинга.

Кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: grechan7777@mail.ru.

Россия, 394065, Воронеж, проспект Патриотов, 53.

Grechanyi Sergej Anatol'evich.

Chief of department of radio engineering systems and complexes of security monitoring.

Candidate of Technical Sciences, Associate Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: grechan7777@mail.ru.

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: защита объектов охраны; пожарная безопасность; чрезвычайная ситуация.

Keywords: protection of security facilities; fire safety; and emergency situations.

УДК 342

ПОВЫШЕНИЕ НАДЕЖНОСТИ СИСТЕМ БЕЗОПАСНОСТИ ПРИ ЭКСПЛУАТАЦИИ

IMPROVING THE RELIABILITY OF SAFETY SYSTEMS DURING OPERATION

В статье рассматриваются вопросы повышения надежности систем безопасности в процессе их эксплуатации. Предложены методы, позволяющие повысить надежность систем безопасности.

The article addresses the issues of increasing the reliability of security systems during their operation. Methods are proposed that allow for an increase in the reliability of security systems.

В современном мире системы безопасности являются критически важным элементом защиты любого охраняемого объекта. Однако проектирование и установка даже самой совершенной системы являются лишь первым шагом. Реальная эффективность любой системы безопасности определяется тем, насколько надежно она функционирует на протяжении всего жизненного цикла, то есть в процессе эксплуатации. Повышение надежности является не разовой задачей, а является непрерывным процессом, основанным на комплексном подходе.

Надежность системы безопасности в период эксплуатации складывается из нескольких ключевых методов.

К методам, позволяющим повысить надежности систем безопасности во время эксплуатации, относятся:

- 1) проектирование и установка;
- 2) резервирование компонентов и систем;
- 3) мониторинг отказов;
- 4) анализ отказов;
- 5) техническое обслуживание;
- 6) управление качеством и стандартизация;
- 7) обновление программного обеспечения;
- 8) обучение персонала;
- 9) внешние воздействия и окружающая среда;
- 10) искусственный интеллект и машинное обучение.

Рассмотрим их подробнее:

1. Проектирование и установка.

Проектирование и монтаж систем безопасности должны осуществляться специалистами высокой квалификации. Ошибки проектирования, неправильная разводка кабелей, могут негативно сказаться на работоспособности оборудования. Грамотное планирование

размещения оборудования и соблюдение стандартов монтажа обеспечивают стабильную работу системы на протяжении длительного периода.

Основные этапы правильного проектирования:

- анализ требований заказчика;
- разработка проектной документации;
- выбор оптимального расположения оборудования;
- контроль выполнения работ.

2. Резервирование компонентов и систем.

Резервирование подразумевает наличие дублирующих элементов или подсистем, которые обеспечивают бесперебойную работу основных узлов в случае отказа одного из них.

Существует несколько видов резервирования:

- активное резервирование: дублирующие элементы работают одновременно с основными, обеспечивая непрерывность работы;
- пассивное резервирование: запасные элементы активируются автоматически после выхода из строя основного компонента;
- горячее резервирование: активные запасные элементы находятся в режиме ожидания и мгновенно вступают в действие при необходимости.

3. Мониторинг отказов.

Эффективный мониторинг и диагностика позволяют выявлять неисправности на ранней стадии, предупреждая возможные сбои и повреждения.

Основные направления этого подхода включают:

- автоматическое выявление отклонений параметров работы оборудования от нормы;
- периодическую проверку исправности всех компонентов;
- сбор статистической информации о функционировании системы.

4. Анализ отказов.

Повышение надежности систем безопасности при эксплуатации невозможно без глубокого анализа отказов. Различные методы анализа надежности, применяемые в современной инженерной практике – это методы, позволяющие оценить системы безопасности и принять обоснованные решения относительно мероприятий по повышению их надежности.

Одним из самых распространенных методов анализа надежности является анализ видов и последствий отказов. Данный метод представляет собой качественный инструмент, позволяющий детально изучить возможные причины и последствия отказов в системах.

Преимущество метода:

- позволяет идентифицировать слабые звенья в структуре системы;

- помогает установить взаимосвязь между отдельными элементами и системой в целом;

- способствует разработке профилактических мер для предотвращения отказов.

У данного метода есть и определенные ограничения:

- ориентирован преимущественно на выявление известных типов отказов и не всегда способен предсказывать редкие события;

- реализация требует значительных временных ресурсов и квалифицированных специалистов [2].

Анализ видов, последствий и критичности отказов – это более углубленный вариант предыдущего метода. Помимо выявления видов отказов и их последствий, этот метод включает оценку критичности каждого типа отказа, позволяя ранжировать их по уровню значимости.

Особенности данного метода:

- расчет интегральных показателей критичности отказов;

- предназначен для детального анализа сложных систем, где требуется оценка влияния отказов на безопасность и готовность;

- используется в качестве основы для принятия управленческих решений по повышению надежности [3].

5. Техническое обслуживание.

Правильно организованное техническое обслуживание способствует поддержанию высокого уровня надежности и долговечности оборудования.

Ключевые моменты:

- разработка планов профилактического обслуживания на основе статистики отказов;

- использование специализированных инструментов и методик для выявления скрытых дефектов;

- организация регулярного обучения обслуживающего персонала современным методикам диагностики и устранения неисправностей.

6. Управление качеством и стандартизация.

Управление качеством включает разработку и реализацию процедур, направленных на поддержание высоких стандартов качества продукции и услуг. Для повышения надежности систем безопасности необходимо соблюдение международных стандартов и прохождение обязательной сертификации. Регулирующие органы регулярно вводят новые правила и рекомендации.

Важнейшие аспекты данного подхода:

- разработка эксплуатационной документации и строгое ее соблюдение;

- создание внутренних стандартов и нормативов, соответствующих международным стандартам ISO;

- регулярный внутренний аудит.

7. Обновление программного обеспечения.

Программное обеспечение, используемое в системах безопасности, должно быть надежным и совместимым с оборудованием. Несовместимые программы могут вызывать конфликты и сбои в работе системы. Рекомендуется использовать лицензионное программное обеспечение проверенных разработчиков, регулярно обновлять версии и устанавливать обновления безопасности

8. Обучение персонала.

Человеческий фактор играет значительную роль в обеспечении надежности систем безопасности. Неправильная настройка оборудования, отсутствие навыков обслуживания и ремонта могут привести к серьезным последствиям. Необходимо регулярно проводить обучение и аттестацию сотрудников, отвечающих за эксплуатацию систем безопасности. Высокий уровень профессионализма операторов обеспечивает быстрое выявление неисправностей и оперативное устранение проблем

9. Внешние воздействия и окружающая среда.

Внешние факторы, такие как климатические условия, электромагнитные помехи, механические повреждения, могут существенно влиять на работоспособность систем безопасности. При выборе оборудования важно учитывать специфику условий эксплуатации и предусмотреть меры защиты от неблагоприятных воздействий. Установка защитных кожухов, экранирование кабельных линий, заземление оборудования помогут минимизировать негативное воздействие внешних факторов.

10. Искусственный интеллект и машинное обучение.

Играют значительную роль в повышении надежности систем безопасности. Алгоритмы способны анализировать огромные массивы данных, выявляя закономерности и предупреждая о потенциальных проблемах до их возникновения. В системах видеонаблюдения искусственный интеллект используется для автоматического обнаружения подозрительных объектов или поведения, что сокращает необходимость вмешательства человека и увеличивает точность идентификации угроз. Машинное обучение применяется для оптимизации рабочих процессов и предотвращения сбоев. Предсказательная аналитика позволяет заранее выявить неисправности оборудования, минимизировать простой и увеличить продолжительность жизненного цикла активов. Исследование искусственного интеллекта и машинного обучения способно уменьшить частоту отказов оборудования.

Надежность систем безопасности обеспечивается комплексным подходом, учитывающим множество факторов. Среди них ключевую роль играют профессионализм персонала, правильное проектирование и установка, надежное программное обеспечение и защита от внешних воздействий. Современными трендами становятся применение искусственного интеллекта и машинного обучения, концепция нулевого

доверия, расширение использования интернета вещей и повышенное внимание к вопросам кибербезопасности. Все эти направления направлены на повышение эффективности и надежности систем безопасности, минимизацию рисков и повышаю надежность защиты. Недостаточно просто купить и установить оборудование. Необходимо создать полноценную эксплуатационную культуру, при которой все участники процесса от руководителя до оператора понимают свою роль в поддержании высокого уровня защищенности объекта. Для достижения максимальной надежности рекомендуется сочетать перечисленные методы.

ЛИТЕРАТУРА

1. Дуплякин П. М. Основы надежности радиоэлектронных средств : учебно-методическое пособие / П. М. Дуплякин, Е. С. Бондаренко, А. В. Сидоров. – Воронеж : Воронежский институт МВД России, 2025. – 103 с.
2. ГОСТ Р 51901.12–2007 (МЭК 60812:2006) Менеджмент риска. Метод анализа видов и последствий отказов.
3. ГОСТ 27.310–95. Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения.

СВЕДЕНИЯ ОБ АВТОРЕ

Дуплякин Петр Михайлович.

Преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга.

Воронежский институт МВД России.

E-mail: 00008540@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Duplyakin Pyotr Mikhailovich.

Lecturer at the Department of Radio Engineering Systems and Security Monitoring complexes.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: 00008540@mail.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: надежность; системы безопасности; эксплуатация системы безопасности.

Keywords: reliability; security systems; operation of the security system.

УДК 621.3.019.3

Н. В. Зубова, В. Г. Волкова, Н. А. Садчикова

ОСОБЕННОСТИ БЕЗОПАСНОГО ХРАНЕНИЯ ГРАЖДАНСКОГО ОРУЖИЯ

SPECIFICS OF SAFE STORAGE OF CIVILIAN WEAPONS

В статье рассматривается проблема обеспечения безопасного хранения гражданского оружия: анализируется нормативно-правовая база и выделяются проблемы, образовавшиеся после исключения сейфового оборудования из перечня обязательной сертификации. На основании проведенных исследований предлагаются технические требования к конструкционным параметрам, запирающим устройствам, а также установке средств хранения оружия. Рассматриваются места оптимального размещения и дополнительные средства обеспечения безопасности средств хранения оружия.

The article examines the problem of ensuring the safe storage of civilian weapons: the regulatory framework is analyzed and the problems that have arisen after the exclusion of safe equipment from the list of mandatory certification are identified. Based on the conducted research, technical requirements for design parameters, locking devices, as well as the installation of weapons storage facilities are proposed. Optimal locations and additional means of ensuring the safety of weapons storage facilities are considered.

Одной из основных функций войск национальной гвардии Российской Федерации является осуществление мероприятий по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере оборота оружия [1].

Федеральный закон от 13.12.1996 № 150-ФЗ «Об оружии» классифицирует оружие на три основных вида в зависимости от целей его применения и субъекта использования: гражданское, служебное, а также боевое стрелковое и холодное. Статья 3 данного Федерального закона закрепляет определение гражданского оружия как предназначенного для использования гражданами Российской Федерации в целях самообороны, для занятий спортом и охоты, а также в культурных и образовательных целях.

В соответствии с российским законодательством [2, 3] обязанность владельца оружия обеспечить его безопасное хранение. Действующие нормативные документы предоставляют владельцам оружия право самостоятельного выбора способа его хранения. Законодательство признает равно допустимыми такие варианты, как сейф, металлический шкаф или деревянный ящик, обитый железом, при условии, что выбранный способ гарантирует сохранность оружия, безопасность его хранения и

полностью исключает доступ посторонних лиц. При этом право выбора конкретных характеристик и оснащения средства хранения остается за владельцем оружия.

До 2020 года качество и криминальная устойчивость сейфов для оружия подтверждались обязательной сертификацией. Ситуация изменилась с принятием Постановления Правительства Российской Федерации № 116 от 10.02.2020 г. [4], которым сейфы и запирающие устройства были исключены из перечня продукции, требующей обязательного подтверждения соответствия. Данные обстоятельства создают предпосылки к тому, что недобросовестные производители могут реализовывать продукцию, не соответствующую требованиям криминальной устойчивости, что впоследствии способно привести к хищению гражданского оружия и тяжким последствиям.

В 2020 году ФКУ «НИЦ «Охрана» Росгвардии были проведены научные исследования [5] с целью выработки оптимальных технических характеристик к средствам хранения оружия и рекомендаций по обеспечению хранения оружия. Так, в соответствии с проведенными исследованиями выделены минимально необходимые требования к конструкционным параметрам, запирающим устройствам и установке средств хранения оружия.

Требования к конструкционным параметрам средства хранения оружия:

- материал – сталь;
- толщина стенок – не менее 2 мм;
- задняя и нижняя стенки должны иметь конструкционные отверстия для установки крепежных элементов;
- обязательное наличие запираемого на замок трейзера для раздельного хранения оружия и боеприпасов;
- на трейзерах, установленных снаружи средства хранения оружия, обязательное наличие запирающего устройства.

Требования к запирающим устройства средства хранения оружия:

- для средств хранения гражданского оружия длина дверцы которого превышает 0,5 м – не менее двух запирающих устройств;
- класс запирающих устройств должен быть не ниже 3 по ГОСТ 5089-2011 «Замки, защелки, механизмы цилиндрические. Технические условия» [6], либо не ниже U3 по ГОСТ Р 52582-2006 «Замки для защитных конструкций. Технические требования и методы испытаний на устойчивость к криминальному отмыканию и взлому» [7].

Требования к установке средства хранения оружия:

- беспрепятственный доступ к крепежным элементам должен быть исключён, а само средство хранения должно быть надёжно зафиксировано на капитальной конструкции (стене, полу) без зазоров.

Данные требования рекомендованы гражданам при выборе средств хранения оружия, а также производителям для отражения в технической документации на средства хранения оружия.

В общем виде внутренние конструкционные особенности средства хранения оружия представлено на рисунке 1.



Рис. 1. Внутренние конструкционные особенности

Выбор средств хранения оружия определяется, прежде всего, его габаритными параметрами. Внутренний объем и конфигурация сейфа или шкафа должны соответствовать не только количеству и размерам хранимых единиц оружия, но и предусматривать размещение сопутствующего инвентаря. Исходя из этого, важным фактором при расчете высоты средства хранения является наличие «трейзера» – внутреннего модуля (лотка), предназначенного для хранения дополнительных принадлежностей для оружия, который размещается над основным отделением.

Внутреннее пространство средства хранения оружия может быть оснащено элементами: съемными ложементами (простыми пластиковыми/деревянными, зажимными стальными или роликовыми), полками с регулируемой высотой, вертикальными перегородками и гребёнками для

шомполов и ключей. Дно, как правило, имеет мягкое ложе из войлока, дерева или пластика с углублениями для прикладов. Подобная конструкция позволяет гибко настраивать внутреннюю организацию хранения под индивидуальные потребности.

Кроме того, важной составляющей безопасного хранения является правильное размещение средства хранения оружия. Средства хранения оружия рекомендуется устанавливать в местах с ограниченным доступом для посторонних лиц: скрытых нишах, кладовых, иных вспомогательных помещениях, а также в специализированных элементах мебели (рис. 2).



Рис. 2. Размещение сейфа в скрытом от посторонних глаз месте

Эффективным признаётся расположение, затрудняющее физический доступ злоумышленника и проведение им манипуляций по вскрытию (например, в тесных гардеробных, где возможен доступ только к лицевой части сейфа).

Аналогичные принципы применимы и к транспортировке оружия в автомобиле. Средство хранения оружия должно размещаться в скрытых отсеках (под сиденьями, в технологических нишах, центральной консоли) и быть надёжно закреплено (рис. 3). Это не только противодействует хищению, но и повышает безопасность пассажиров при движении транспортного средства.



Рис. 3. Размещение средства хранения оружия в автомобиле

Для повышения уровня безопасности средства хранения оружия могут быть дополнительно оснащены техническими средствами охраны и системами контроля доступа. Это позволяет не только физически защитить оружие, но и отследить попытки доступа к нему, фиксируя время и лицо, совершившее несанкционированные действия. Такие меры особенно актуальны для коллекционного оружия или при хранении в местах с повышенными рисками.

Современный рынок предлагает многофункциональные средства хранения оружия, которые объединяют различные технологии для повышения защищенности содержимого и контроля доступа. Ключевыми особенностями таких моделей являются системы идентификации владельца и возможность скрытого монтажа.

Например, к подобным системам могут быть отнесены средства хранения оружия с биометрической и электронной идентификацией RFID (рис. 4).



Сейф с биометрической идентификацией



Сейф с RFID-меткой

Рис. 4. Средства хранения, дополнительно оснащенные техническими средствами

Альтернативным решением для хранения и контроля доступа к оружию являются сейфы-тайники. Особенностью таких сейфов является конструкция, предназначенная для скрытого монтажа за предметами интерьера или бытовой техникой. Данные модели обычно оснащаются двухуровневой системой безопасности (механической и электромеханической) и предоставляют выбор способа доступа: по коду, отпечатку пальца или с помощью дистанционного пульта. Для фиксации сейф крепится к стене или полу. Подобные средства хранения оружия изготавливают в виде картин, телевизоров и зеркал, с возможностью индивидуального подбора габаритных характеристик и исполнения (рис. 5).



Рис. 5. Варианты исполнения сейфов-тайников

Представленные в настоящем исследовании принципы и решения направлены на повышение уровня личной и общественной безопасности и могут быть применены владельцами оружия для организации его безопасного и корректного хранения. Материалы статьи могут служить практическим руководством для выбора надежного сейфа и организации безопасной системы хранения в соответствии с индивидуальными потребностями и требованиями законодательства.

ЛИТЕРАТУРА

1. О Федеральной службе войск национальной гвардии Российской Федерации : положение о Федеральной службе войск национальной гвардии Российской Федерации, утвержденное Указом Президента Российской Федерации от 30.09.2016 г. № 510 // СПС «КонсультантПлюс».
2. Об оружии : Федеральный закон Российской Федерации от 13.12.1996 г. № 150-ФЗ // СПС «КонсультантПлюс».
3. О мерах по регулированию оборота гражданского и служебного оружия и патронов к нему на территории Российской Федерации : постановление Правительства Российской Федерации от 21.07.1998 г. № 814 // СПС «КонсультантПлюс».
4. О внесении изменения в постановление Правительства Российской Федерации от 1 декабря 2009 г. № 982 : постановление Правительства Российской Федерации от 10.02.2020 г. № 116 // СПС «КонсультантПлюс».
5. Технические средства контроля доступа к оружию. Запирающие устройства, устанавливаемые в местах хранения оружия. Рекомендации по выбору и применению. Информационно-аналитический обзор. – Москва : НИЦ «Охрана» Росгвардии, 2020 – 36 с.
6. ГОСТ 5089-2011. Замки, защелки, механизмы цилиндрические. Технические условия. – Москва : Стандартинформ, 2013. – 39 с.
7. ГОСТ Р 52582-2006. Замки для защитных конструкций. Технические требования и методы испытаний на устойчивость к криминальному отмыканию и взлому. – Москва : Стандартинформ, 2008. – 9 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Зубова Наталья Вячеславовна.

Старший научный сотрудник отделения лабораторных исследований и испытаний.

Научно-исследовательский центр «Охрана» Федеральной службы войск национальной гвардии Российской Федерации.

E-mail: zubava.nv@yandex.ru

Россия, 111539, г. Москва, ул. Реутовская, 12Б.

Волкова Виктория Геннадьевна.

Старший научный сотрудник отделения лабораторных исследований и испытаний.

Научно-исследовательский центр «Охрана» Федеральной службы войск национальной гвардии Российской Федерации.

E-mail: Vikgennn91@mail.ru

Россия, 111539, г. Москва, ул. Реутовская, 12Б.

Садчикова Наталия Александровна.

Следователь специализированного отдела по расследованию преступлений общеуголовной направленности – «дистанционного хищения».

Следственное управление УВД по ЮВАО ГУ МВД России по г. Москве.

E-mail: nsadchikova6@mail.ru

Zubova Natalia Vyacheslavovna.

Senior Researcher of the Laboratory Research and Testing Department.

Research Center «Protection» of the Federal Service of the National Guard Troops of the Russian Federation.

E-mail: zubava.nv@yandex.ru

Russia, 111539, Moscow, Reutovskaya Street, 12B.

Volkova Victoria Gennadievna.

Senior Researcher of the Laboratory Research and Testing Department.

Research Center «Protection» of the Federal Service of the National Guard Troops of the Russian Federation.

E-mail: Vikgenm91@mail.ru

Russia, 111539, Moscow, 12B Reutovskaya Street.

Sadchikova Natalia Aleksandrovna.

Investigator of the Specialized Department for Investigating General Criminal Crimes – «Remote Theft».

Investigative Department of the Department of Internal Affairs for the South-Eastern Administrative District of the Ministry of Internal Affairs of Russia in Moscow.

E-mail: nsadchikova6@mail.ru

Ключевые слова: гражданское оружие; безопасное хранение; запирающие механизмы; трейзер; противодействие хищению.

Keywords: civilian weapons; safe storage; locking mechanisms; trailer; anti-theft.

УДК 683.34

СПЕЦИФИКА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗДАНИЙ И СООРУЖЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

SPECIFIC FEATURES OF ENSURING THE SAFETY OF BUILDINGS AND STRUCTURES OF INTERNAL AFFAIRS AGENCIES

Статья посвящена актуальным вопросам обеспечения безопасности зданий и сооружений органов внутренних дел в условиях растущих технологических угроз, особенно со стороны беспилотных летательных аппаратов. Подчеркивается, что традиционные системы охраны требуют модернизации в связи с появлением новых рисков – от несанкционированного видеонаблюдения до доставки опасных грузов дронами. Особое внимание уделено комплексному подходу к защите, включающему организационные, технические, инженерные и информационные меры.

The article is devoted to the current issues of ensuring the security of buildings and structures of internal affairs bodies in the context of growing technological threats, especially from unmanned aerial vehicles. It is emphasized that traditional security systems require modernization due to the emergence of new risks, from unauthorized video surveillance to the delivery of dangerous goods by drones. Special attention is paid to a comprehensive approach to protection, which includes organizational, technical, engineering, and information measures.

В эпоху стремительных технологических преобразований вопросы обеспечения безопасности зданий и сооружений органов внутренних дел приобретают особую значимость. Современные угрозы становятся всё более разнообразными, что требует постоянного совершенствования систем защиты критически важных объектов.

Особую озабоченность вызывает появление новых рисков, связанных с использованием беспилотных летательных аппаратов (далее – БПЛА) в противоправных целях. Распространение БПЛА создаёт дополнительные вызовы для системы безопасности, заставляя специалистов по защите объектов пересматривать существующие нормативы и разрабатывать новые подходы к противодействию этим угрозам.

Актуальность защиты зданий ОВД обусловлена несколькими важными факторами. Прежде всего, это растущее число случаев неправомерного использования беспилотных аппаратов вблизи охраняемых объектов. Существующие нормативные документы не всегда учитывают современные реалии, что требует их существенной доработки и актуализации. Кроме того,

критически важно совершенствовать защитные меры для обеспечения надёжности важнейших объектов инфраструктуры.

Особенности обеспечения защиты объектов ОВД. Специфика объектов ОВД определяет особый подход к их защите. На территории подразделений хранятся конфиденциальные материалы оперативно-розыскной деятельности, служебное оружие, архивные документы и другие ресурсы, от сохранности которых зависит эффективность работы всей правоохранительной системы. В зависимости от категории потенциальной угрозы, которая может варьироваться от I до IV, определяется необходимый уровень защиты каждого объекта.

Строгие требования к проектированию и строительству зданий ОВД формируют основу их безопасности. Все сооружения должны соответствовать уровню ответственности КС-2 согласно ГОСТ 27751.

Пожарная безопасность является неотъемлемым компонентом общей системы защиты. Здания должны соответствовать строгим требованиям, включающим определённую степень огнестойкости и класс конструктивной пожарной опасности. Эти комплексные меры создают многоуровневую систему защиты, способную противостоять современным угрозам.

Современные технологии защиты объектов ОВД представляют собой многоуровневую систему, включающую различные компоненты. На входе в здания могут быть установлены передовые системы контроля и управления доступом, оснащённые турникетами и шлюзами с различными типами доступа. Видеонаблюдение осуществляется с помощью современных IP-камер, способных не только вести постоянную съёмку, но и распознавать лица и номерные знаки транспортных средств.

Пропускной режим на объектах ОВД организован с учётом всех требований безопасности. Строгий контроль осуществляется как для сотрудников, так и для посетителей, что позволяет предотвратить несанкционированный доступ на территорию. Физическая охрана обеспечивается круглосуточным дежурством и регулярным патрулированием территории.

Особое внимание уделяется подготовке персонала. Регулярно проводятся учения по действиям в чрезвычайных ситуациях, сотрудники проходят инструктажи по работе с техническими средствами безопасности. Важным элементом системы безопасности является тесное взаимодействие с другими службами: оперативная связь с дежурной частью ОВД и МЧС.

В современных условиях особое значение приобретает интеграция различных систем безопасности в единый центр управления. Современные технологии позволяют объединить все элементы защиты в единую сеть, управляемую с центрального пульта. Активно внедряются системы на основе искусственного интеллекта, способные анализировать данные и прогнозировать потенциальные угрозы.

Такой комплексный подход к обеспечению безопасности позволяет создать надёжную защиту объектов ОВД от различных угроз, обеспечивая при этом эффективное функционирование всех подразделений.

В соответствии с приказом МВД России от 31 декабря 2014 года № 1152, обеспечение безопасности зданий и сооружений органов внутренних дел строится на комплексной системе защитных мер, охватывающей различные аспекты охраны объектов.

Основой всей системы безопасности является организационный блок мероприятий. На каждом объекте вводится строгий пропускной режим, который позволяет контролировать перемещение людей и транспорта. Для каждого объекта разрабатывается индивидуальный паспорт безопасности, учитывающий его особенности и потенциальные риски.

Технические средства защиты составляют важную часть системы безопасности. Объекты оснащаются современными системами видеонаблюдения, включая периметр территории. Устанавливается тревожная сигнализация, позволяющая мгновенно передавать сигнал об опасности. Инженерные заграждения, такие как противотаранные устройства и контрольно-пропускные пункты, создают физический барьер для несанкционированного доступа. Средства досмотра обеспечивают дополнительную защиту.

Особое внимание уделяется инженерным решениям в области безопасности. Основное ограждение объектов должно иметь высоту не менее 2,5 метров, а в районах с глубоким снежным покровом этот показатель увеличивается до 3 метров. Создается специальная запретная зона, оборудованная охранным освещением и системами видеонаблюдения. Контрольно-пропускные пункты оснащаются современными средствами контроля доступа и защиты от стрелкового оружия.

Специальные меры защиты применяются к особо важным объектам. Места хранения оружия оснащаются усиленными дверями и дополнительными системами сигнализации. Особое внимание уделяется безопасности при перевозке специальных грузов. Строгий контроль осуществляется за допуском персонала на территорию объекта.

Эффективность всей системы безопасности поддерживается через систематический контроль за её функционированием. Проводятся регулярные проверки состояния защищённости объектов, собирается и анализируется отчётность, что позволяет своевременно выявлять и устранять возможные уязвимости в системе безопасности.

В современных условиях безопасность зданий и сооружений органов внутренних дел подвергается множеству разнообразных угроз, требующих комплексного подхода к их предотвращению. Каждая из этих угроз представляет серьёзную опасность и может привести к дестабилизации работы правоохранительных органов.

Физическая безопасность объектов находится под постоянной угрозой несанкционированного проникновения. Информационная безопасность становится всё более актуальной в эпоху цифровизации. Особую опасность представляют диверсионные и террористические акты. Инженерно-технические угрозы связаны с возможностью повреждения систем жизнеобеспечения зданий. Природные и техногенные угрозы. Социально-политические угрозы проявляются в виде протестных акций, нападений на здания ОВД, деятельности экстремистских и террористических организаций. Внутренние угрозы связаны с возможным злоупотреблением служебным положением сотрудниками или несанкционированными действиями лиц, имеющих доступ к объекту.

Защищённость периметра остаётся критически важным аспектом безопасности. Слабые места в ограждениях, системах контроля доступа и охранной сигнализации, а также сбои в работе систем видеонаблюдения могут стать уязвимыми точками для злоумышленников.

Противодействие беспилотным летательным аппаратам. Беспилотные летательные аппараты создают новые вызовы для системы безопасности. Они могут использоваться для видеофиксации служебных помещений, а также для доставки взрывоопасных и других опасных материалов на территорию объекта.

В современном мире БПЛА стали неотъемлемой частью как повседневной жизни, так и оперативной деятельности правоохранительных органов. Однако их использование порождает целый ряд проблем и угроз, требующих особого внимания.

Потенциальная опасность БПЛА особенно актуальна в местах массового скопления людей. Беспилотные воздушные суда могут нанести серьёзный ущерб зданиям, причинить травмы посетителям и создать угрозу для воздушных судов. При этом важно отметить, что сама технология БПЛА имеет значительный потенциал для использования в оперативной и охранной деятельности ОВД.

В ответ на растущие угрозы, связанные с использованием БПЛА, правоохранительные органы принимают соответствующие меры. Согласно приказу МВД России от 16 ноября 2023 года № 865, установлен чёткий порядок принятия решений о пресечении функционирования беспилотных воздушных судов. Это особенно важно в местах проведения публичных мероприятий, следственных действий и т.д.

Основная цель применения БПЛА органами внутренних дел заключается в предотвращении правонарушений, защите государственного и частного имущества, а также обеспечении общественной безопасности. При этом необходимо учитывать технические характеристики, которые могут представлять угрозу для объектов ОВД.

Современные БПЛА обладают впечатляющими техническими возможностями. Их скорость и манёвренность позволяют развивать скорость до 140 километров в час с возможностью разгона до 100 километров в час

всего за две секунды. Высокая манёвренность затрудняет их обнаружение и нейтрализацию.

Дальность полёта современных дронов может достигать значительных показателей. Использование усилителей сигнала позволяет увеличить дальность и надёжность связи между дроном и пультом управления, делая их устойчивыми к некоторым системам подавления.

Системы навигации современных БПЛА оснащены передовыми технологиями. Принцип псевдослучайной перестройки рабочей частоты затрудняет их обнаружение и подавление. Автономные системы навигации позволяют аппаратам выполнять задачи без постоянной связи с оператором.

Особую озабоченность вызывают возможности полезной нагрузки БПЛА. Некоторые модели способны нести взрывчатые вещества или другие опасные грузы. Существуют также дроны, оснащённые контактными взрывательными устройствами, и возможность их использования в роевых атаках создаёт дополнительные угрозы.

Таким образом, БПЛА представляют собой двойственный феномен – с одной стороны, являясь мощным инструментом для правоохранительных органов, с другой – источником потенциальных угроз, требующих постоянного внимания и разработки эффективных мер противодействия.

По своим возможностям БПЛА подразделяются на несколько категорий. Автономные дроны способны работать без постоянной связи с оператором, самостоятельно корректируя маршрут движения. Особую опасность представляют аппараты с технологией псевдослучайной перестройки рабочей частоты, которые могут работать на нестандартных каналах управления, что существенно усложняет их подавление.

Важным фактором является устойчивость к внешним воздействиям. Современные дроны разрабатываются с учётом возможности противодействия попыткам подавления сигнала или другим методам нейтрализации, что существенно повышает их эффективность.

Конструктивные особенности БПЛА играют ключевую роль в их возможностях. Компактные модели трудно обнаруживаются как визуально, так и с помощью технических средств. Различные типы конструкций – вертолётные, самолётные и мультикоптеры – обеспечивают уникальные преимущества в манёвренности и грузоподъёмности.

Автоматизация процессов выводит возможности БПЛА на новый уровень. Полностью автоматизированные системы способны выполнять задачи без участия человека, что значительно ускоряет их реакцию и затрудняет противодействие.

Высокая скорость полёта современных дронов позволяет им быстро преодолевать защитные зоны и барьеры, оставляя минимальное время для их обнаружения и противодействия. Это делает традиционные методы защиты менее эффективными против современных беспилотных систем.

Таким образом, развитие технологий БПЛА создаёт новые вызовы для систем безопасности, требуя постоянного совершенствования методов защиты и противодействия беспилотным летательным аппаратам.

Для противодействия этим угрозам разрабатывается комплексный подход, включающий как технические, так и организационные меры. Оценка обстановки является первым этапом защиты. Специалисты анализируют вероятные направления полёта БПЛА и определяют возможные районы их запуска.

Инженерное оборудование объектов играет ключевую роль в создании физической защиты. На подступах к объектам устанавливаются специальные заграждения, используются габионы насыпного типа и другие фортификационные сооружения. Особое внимание уделяется маскировке объектов с учётом естественных защитных свойств местности.

Система оповещения и взаимодействие с экстренными службами обеспечивают быструю реакцию на угрозы. Назначаются ответственные лица за получение информации об угрозах и оповещение персонала. Устанавливается тесное взаимодействие с Единой дежурно-диспетчерской службой и другими экстренными службами. Разрабатывается система аудиооповещения для оперативного информирования сотрудников.

Планирование и инструктаж являются неотъемлемой частью системы защиты. Корректируются планы охраны с учётом новых угроз, разрабатываются детальные инструкции по действиям при обнаружении БПЛА. Составляются графики дежурств и планируются регулярные тренировки персонала.

Такой многоуровневый подход к защите позволяет существенно снизить риски проникновения БПЛА на охраняемую территорию и минимизировать возможные последствия их атак на здания и сооружения органов внутренних дел.

Технические средства противодействия включают комплекс различных систем. Средства радиоэлектронной борьбы устанавливаются в оптимальных точках объекта. Используются противодроновые ружья и другие специализированные устройства для подавления БПЛА.

Системы обнаружения работают в комплексе, обеспечивая надёжное выявление беспилотных аппаратов. Радиолокационные станции, оптические и акустические средства позволяют своевременно обнаруживать угрозы. Специальные устройства перехватывают и анализируют радиосигналы, что помогает в идентификации БПЛА.

Физические методы защиты включают установку специальных сетей и применение других контактных способов противодействия. Эти меры создают дополнительный барьер для несанкционированного проникновения БПЛА на охраняемую территорию.

Перспективным направлением развития системы безопасности становится интеграция различных систем защиты в единый комплекс. Активно внедряются технологии искусственного интеллекта для обнаружения и классификации угроз, совершенствуются средства радиоэлектронной борьбы. Создаётся многоуровневая система защиты, что позволяет обеспечить более надёжную безопасность объектов.

Особое внимание следует уделить нескольким ключевым аспектам. Прежде всего, это своевременное обновление технического оснащения и повышение квалификации персонала. Важным направлением становится развитие сотрудничества с научными и производственными организациями, что позволяет внедрять передовые разработки в практику защиты.

Не менее важным остаётся отслеживание новых угроз и разработка эффективных способов их нейтрализации. Успешная реализация всех предложенных мер позволит создать действительно эффективную систему защиты объектов ОВД от угроз, связанных с применением БПЛА, обеспечив надёжную безопасность как сотрудников, так и материальных ценностей.

Важно понимать, что обеспечение безопасности – это непрерывный процесс, требующий постоянного внимания и адаптации к новым вызовам. Только комплексный подход, сочетающий технические, организационные и правовые меры, может обеспечить эффективную защиту объектов ОВД в современных условиях.

ЛИТЕРАТУРА

1. 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. – URL: <https://www.mvd.rf>.

2. Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования (утв. приказом Министерства регионального развития РФ от 5 июля 2011 г. № 320) : Свод правил СП 132.13330.2011. – URL: <http://www.pravo.gov.ru>

3. Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств : приказ от 31 декабря 2014 г. № 1152. – URL: <http://www.pravo.gov.ru>

4. ГОСТ 27751-2014. Надежность строительных конструкций и оснований. Основные положения. – URL: <http://www.pravo.gov.ru>

5. Мельников А. В. Моделирование функциональной взаимосвязи результатов экспертизы опасности отдельных видов нарушителей для оценки рисков безопасности охраняемых объектов / А. В. Мельников, Р. А. Жилин, И. А. Старенков // Вестник Воронежского института ФСИИ России. – 2019. – № 3. – С. 88–92.

6. Моделирование оценки эффективности функционирования систем безопасности объектов органов внутренних дел / Р. А. Жилин, А. В. Мельников, С. Б. Ахлюстин, В. В. Горлов. – Воронеж : Воронежский институт МВД России, 2023. – 104 с. – ISBN 978-5-88591-970-8.

СВЕДЕНИЯ ОБ АВТОРАХ

Ивануха Иван Сергеевич.

Старший преподаватель кафедры информационно-аналитического и документационного обеспечения деятельности ОВД.

Тюменского института повышения квалификации сотрудников МВД России.

E-mail: scorpion-6588@mail.ru

Россия, 625049, г. Тюмень, ул. Амурская, 75.

Калков Дмитрий Юрьевич.

Доцент кафедры радиотехнических систем и комплексов охранного мониторинга.

Кандидат технических наук.

Воронежский институт МВД России.

E-mail: DmitreyRUS@mail.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Ivanukha Ivan Sergeevich,

Lecturer of the Department of Information and Analytical Support and Documentation of the Activities of the Internal Affairs Bodies.

Tyumen Institute of Advanced Training of Employees of the Ministry of Internal Affairs of Russia.

E-mail: scorpion-6588@mail.ru

Russia, 625049, Tyumen, Amurskaya str., 75.

Kalkov Dmitry Yurievich.

Associate Professor of the Department of Radio Engineering Systems and Security Monitoring Complexes.

Candidate of Technical Sciences.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: DmitreyRUS@mail.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: безопасность объектов; преступные посягательства; инженерно-технические мероприятия; антитеррористическая защищенность; беспилотный летательный аппарат.

Keywords: security of objects; criminal attacks; engineering activities; anti-terrorism security; unmanned aerial vehicle.

УДК 351.74

Д. Ю. Калков, М. А. Гудков, И. С. Ивануха

**ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ
ПО ПОВЫШЕНИЮ ЗАЩИЩЁННОСТИ ОБЪЕКТОВ
ОРГАНОВ ВНУТРЕННИХ ДЕЛ, В ЧАСТНОСТИ ОТ УГРОЗ
БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ**

**ORGANIZATIONAL AND TECHNICAL MEASURES TO INCREASE
THE SECURITY OF INTERNAL AFFAIRS BODIES, IN PARTICULAR
AGAINST THREATS FROM UNMANNED AERIAL VEHICLES**

Статья анализирует угрозы, связанные с использованием беспилотных летательных аппаратов, особенно в контексте безопасности объектов органов внутренних дел, и рассматривает комплекс мер противодействия — от правового регулирования (включая приказы МВД России и постановления правительства) до организационных и технических решений (системы обнаружения, подавления сигналов, алгоритмы реагирования). Актуальность работы обусловлена стремительным развитием технологий БПЛА и необходимостью создания многоуровневой системы защиты, сочетающей соблюдение законодательства, чёткие процедуры реагирования и внедрение современных технических средств.

The article analyzes the threats associated with the use of unmanned aerial vehicles, especially in the context of the security of internal affairs bodies, and examines a range of countermeasures, from legal regulation (including orders issued by the Ministry of Internal Affairs of Russia and government resolutions) to organizational and technical solutions (detection systems, signal suppression, and response algorithms). The relevance of this work is driven by the rapid development of UAV technologies and the need to create a multi-layered security system that combines compliance with legislation, clear response procedures, and the implementation of modern technical solutions.

Современное общество сталкивается с множеством вызовов, связанных с развитием технологий, и одним из наиболее актуальных является использование беспилотных летательных аппаратов (БПЛА). Эти устройства, изначально разработанные для военных и научных целей, сегодня находят широкое применение в гражданской сфере, включая доставку товаров, мониторинг окружающей среды и даже участие в различных мероприятиях. Однако с ростом популярности БПЛА возникает и ряд угроз, особенно в контексте безопасности объектов органов внутренних дел. Актуальность настоящей работы определяется необходимостью разработки и внедрения комплексных организационно-технических мер, направленных на повышение уровня защищённости

объектов от потенциальных угроз, связанных с использованием беспилотных летательных аппаратов (БПЛА).

Осознание тенденций развития беспилотных технологий и особенностей их применения в различных сферах деятельности позволяет более чётко оценить современные риски и вызовы. С момента появления первых экспериментальных дронов до их сегодняшнего массового распространения произошли глубокие технологические изменения, которые кардинально повлияли как на функциональные возможности БПЛА, так и на способы их потенциального использования в противоправных целях.

Особое значение в рассмотрении данной проблемы имеют правовые аспекты. Действующие законодательные инициативы и нормативные акты, в частности приказ МВД России от 16 ноября 2023 года № 865, устанавливающий порядок пресечения функционирования беспилотных воздушных судов, формируют правовую основу для противодействия угрозам. Анализ этих документов позволяет выявить существующие пробелы в правовом регулировании и выработать обоснованные рекомендации по их устранению.

Анализ угроз от беспилотных летательных аппаратов. Беспилотные летательные аппараты (БПЛА) демонстрируют широкий спектр угроз, касающихся обеспечения безопасности объектов органов внутренних дел. В первую очередь, БПЛА могут использоваться в шпионаже, позволяя злоумышленникам осуществлять наблюдения за охраняемыми объектами, что увеличивает риски утечки конфиденциальной информации. Так, инциденты с использованием БПЛА для съёмки мест, где осуществляется полицейская деятельность, подтверждают наличие угрозы высоких рейтингов в свете растущей распространённости этой технологии [3].

Кроме того, существует реальная возможность использования БПЛА для террористических атак, включая доставку взрывных устройств на охраняемые территории. Например, известны случаи использования дронов для доставки взрывных снарядов на массовых мероприятиях, что вызывает особенно высокую степень беспокойности органов безопасности [8]. БПЛА становятся инструментом для реализации различных криминальных сценариев, некоторые из которых уже имели место в мире [1].

В рамках активных воздействий на БПЛА, законодательство России предоставляет конкретные меры реагирования и право на применение силы против таких аппаратов. Сотрудники органов внутренних дел могут подавлять сигнал дистанционного управления и повреждать или уничтожать дрон, если это необходимо для защиты жизни граждан и обеспечения общественного порядка. Однако такие действия требуют четкого следования установленным процедурам. При обнаружении БПЛА

возле охраняемых объектов обязательно уведомляется руководство, разрабатываются меры по организации безопасной зоны и осуществляется мониторинг ситуации [3].

Для более эффективной борьбы с угрозами от БПЛА важно развивать системы высокотехнологичного наблюдения, которые могут включать отражение или нейтрализацию действий беспилотников. Использование специализированных систем радиолокации для выявления БПЛА на ранних этапах их приближения может значительно снизить риск потенциальных инцидентов. При этом важно, чтобы стратегии противодействия базировались на актуальных данных и были интегрированы в общую систему безопасности.

Положение о проведении специальных мероприятий в случае угрозы от БПЛА также регламентируется различными регуляциями и внутренними инструкциями, что подчеркивает важность комплексного подхода к этой проблеме [1]. Широкая осведомленность и подготовленность сотрудников органов внутренних дел в вопросах работы с беспилотными летательными аппаратами являются необходимым условием для снижения рисков, связанных с их потенциально криминальным использованием.

Исторический контекст использования БПЛА. Развитие беспилотных летательных аппаратов стало важной частью оперативной деятельности правоохранительных органов, что обусловлено их возможностями в сфере мониторинга, документирования и анализа. Правовой статус использования БПЛА в этом контексте определен Федеративным законом № 3-ФЗ «О полиции», который не только разрешает, но и обязывает использование научных достижений и технологий в служебной деятельности [8]. Это явление становится всё более актуальным в силу необходимости повышения эффективности и безопасности полицейских операций.

Появление камер и персональных дронов, которые способны отдаляться от оператора на многие километры, подняло ряд вопросов об этической стороне работы с «домашними» БПЛА. Стало известно о большом количестве злоупотреблений, когда владельцы дронов снимали происходящее в частных домах, офисах коммерческих и правительственных организаций.

Дроны падали на головы зрителям на спортивных стадионах, создавали угрозу пассажирским самолетам и промышленным объектам. В итоге во многих странах законодатели стали спешно принимать новые законы, регулирующие продажи и эксплуатацию дронов. В каждой стране свои особенности законодательства, но в большинстве случаев владельцам дронов запрещается снимать людей без явного их согласия, БПЛА нельзя использовать рядом с аэропортами, вокзалами, объектами военного и промышленного значения. В большинстве случаев дрон не может взлететь

на высоту более 150 метров, производители устанавливают ограничения как на расстояния, преодолеваемые дроном, так и на максимальную скорость.

Коптеры применяют и в медицине, например, для быстрой доставки необходимых медикаментов. Компания UPS объявила о запуске службы доставки медикаментов и образцов анализов при помощи дронов. Доставку грузов при помощи дронов опробовала компания DHL еще в 2013 году, сейчас эта практика постепенно получает все более широкое распространение.

Не отстает от DHL и Amazon – в том же 2013 году компания анонсировала сервис Prime Air (он работает в ограниченном количестве регионов), который позиционируется как самый быстрый способ доставки покупок. С его помощью покупки доставляются в течение получаса, это в четыре раза быстрее самого быстрого наземного сервиса Amazon Prime Now.

В России тестировали сервис доставки грузов коптерами Коптер-Экспресс. 21 июня 2014 года «Додо Пицца» в рекламных целях начала доставлять пиццу дронами, причем доставили всего шесть коробок. После этого чиновники решили оштрафовать создателя компании, поставляющей дроны на 50 тысяч рублей. Но хотя штраф потом отменили, доставка грузов дронами в РФ особого распространения не получила. Некоторые компании, включая Uber и Lyft, разрабатывают аэротакси.

Правовые аспекты применения БПЛА. Использование беспилотных летательных аппаратов (БПЛА) в России подчинено строгому законодательному регулированию. Согласно Постановлению Правительства РФ от 11 марта 2010 года № 138, установлены основные параметры эксплуатации БПЛА, включая их классификацию и требования к регистрации. Классификация воздушного пространства разделяет его на классы А, С и G, каждый из которых предъявляет особые требования к использованию. Полеты БПЛА, вес которых не превышает 30 кг, могут осуществляться при соблюдении условий визуального контакта и запрета на выполнение полетов в опасных или запрещённых зонах.

БПЛА делятся на три категории, в зависимости от максимальной взлетной массы: до 150 г, от 150 г до 30 кг, и свыше 30 кг. Для аппаратов массой до 150 г регистрация не требуется, тогда как более тяжёлые экземпляры подлежат государственной регистрации и учету в Федеральном агентстве воздушного транспорта [4]. Владельцы обязаны обеспечить их идентификацию путем нанесения соответствующих знаков.

Важным аспектом является получение разрешений на полеты, которое зависит от класса воздушного пространства. Например, для осуществления полётов над населёнными пунктами требуется не только разрешение от авиационных органов, но и согласование с местными властями, что влечёт необходимость подготовки дополнительного пакета документов. Кроме того, действуют специальные требования, в том числе

обязательное наличие сертификата оператора БПЛА – это условие необходимо как для выполнения авиационных работ, так и для обеспечения безопасности воздушного движения.

За нарушение правил эксплуатации беспилотных летательных аппаратов предусмотрена административная ответственность, включающая наложение штрафов за несоблюдение установленных норм. Это подчёркивает важность чёткого понимания и соблюдения всех требований всеми пользователями дронов.

Учитывая стремительный рост популярности БПЛА в различных сферах, от коммерции до частного использования, знание действующих правовых норм становится обязательным условием для всех владельцев и операторов таких устройств. Это не только помогает избежать возможных правонарушений, но и в значительной мере содействует безопасному и эффективному использованию беспилотников в соответствии с Законодательством Российской Федерации.

Организационные мероприятия по защите объектов. Система защиты объектов органов внутренних дел от угроз со стороны беспилотных летательных аппаратов (БПЛА) требует комплексного подхода и четкой организации действий в случае их обнаружения. Важным этапом является формирование единого порядка действий, который должен охватывать все возможные сценарии. На основании приказа МВД России от 16 ноября 2023 года № 865, необходимо разработать алгоритм реагирования, который будет включать в себя:

1. Выявление угрозы. Первым шагом должно стать оперативное обнаружение БПЛА. Для этого целесообразно интегрировать радарные и оптические системы наблюдения, способные фиксировать полеты беспилотников в различных условиях видимости.

2. Оценка ситуации и принятие решения. После определения угрозы ключевым моментом является оценка возможных рисков. На основании указанных в приказе данных об опасности, следует определить, какие меры необходимо принять для пресечения функционирования БПЛА.

3. Реагирование на угрозу. Установленный порядок действий предусматривает этапы реагирования, начиная с оповещения соответствующих служб и заканчивая исполнением решений о пресечении БПЛА.

4. Обучение и подготовка кадров. Ключевым аспектом в реализации вышеописанных мероприятий является подготовка сотрудников. Важно, чтобы все лица, задействованные в процессе, проходили специальное обучение по противодействию угрозам, исходящим от БПЛА.

5. Установление ответственности. Приказ четко регламентирует список должностных лиц, уполномоченных принимать решения о начале и проведении операций против БПЛА.

В условиях постоянного развития технологий беспилотной авиации и изменения способов применения БПЛА становится критически важным

регулярно анализировать методы противодействия им. Это необходимо не только для повышения уровня защищённости объектов органов внутренних дел, но и для своевременной адаптации к новым, ещё не возникшим угрозам. Такая динамика подчёркивает необходимость постоянного обновления методических подходов и нормативных документов, включая актуализацию действующих приказов.

Анализ текущей ситуации показывает, что эффективная защита возможна только при сочетании организационных и технических мер. В следующем разделе рассматривается, как технические средства могут взаимодополнять организационные мероприятия, формируя более надёжную и устойчивую систему безопасности.

Противодействие БПЛА. Современные угрозы, исходящие от беспилотных летательных аппаратов, требуют разработки и внедрения эффективных технических решений. Разнообразные типы дронов – от квадрокоптеров до аппаратов с фиксированным крылом – могут использоваться в противоправных целях, что обуславливает необходимость применения комплекса мер: радиолокационного обнаружения, подавления управляющих сигналов и физического перехвата.

Радиолокационные системы служат для обнаружения БПЛА и способны выявлять, идентифицировать и отслеживать их на значительных расстояниях. Это позволяет заранее оценить потенциальную угрозу и оперативно принять меры реагирования. Таким образом, радиолокация выступает первым и ключевым этапом в цепочке защиты. Перспективным направлением развития является интеграция радиолокационных данных с другими системами наблюдения и средствами противодействия для создания единой автоматизированной платформы.

Системы подавления сигналов играют важную роль в нейтрализации дронов. Они блокируют радиочастоты, используемые для управления БПЛА, что приводит к потере связи между оператором и аппаратом. В результате дрон может быть вынужден совершить посадку или автоматически вернуться в точку взлёта, что позволяет предотвратить его проникновение на охраняемую территорию. Этот подход способен эффективно предотвращать незаконные действия, связанные с передачей информации и транспортировкой запрещённых грузов [7].

Технологические решения в области борьбы с дронами включают усовершенствованные механизмы перехвата. Отсутствие физического воздействия на БПЛА минимизирует риск коллатерального ущерба и гарантирует безопасность окружающих. С помощью специального оборудования, разрабатываемого на основе передовых научных исследований, достигается высокая точность перехвата. Комплексы, оснащённые такими средствами, могут включать как стационарные, так и мобильные варианты.

Существуют и более сложные системы интеграции радиолокационных и подавляющих технологий, что позволяет создавать

многоуровневые оборонительные структуры. Например, объединение дронодетекторов с системой активного подавления увеличивает шанс успешного противодействия при одновременном нападении нескольких беспилотников. Использование автоматизированных средств управления обеспечивает быструю реакцию на возникающие угрозы.

Важно отметить, что разрабатываемые решения должны учитывать законодательные нюансы, касающиеся эксплуатации воздушного пространства. Компании, занимающиеся производством технических средств защиты, активно работают над тем, чтобы их продукция соответствовала всем нормам и правилам, обеспечивая легитимность их применения в реальных условиях [5].

Таким образом, технологические решения по противодействию угрозам, поступающим от беспилотников, являются важной частью системы безопасности современных объектов. Разработка и дальнейшее совершенствование этих решений позволят сохранить безопасность граждан и предотвратить возможные кризисы в условиях увеличивающегося использования дронов в каждом аспекте жизни.

ЛИТЕРАТУРА

1. Коник А. А. Анализ возможности противодействия функционированию БПЛА сотрудниками органов внутренних дел на современном этапе / А. А. Коник, К. К. Крупенникова // Вестник Белгородского юридического института МВД России. – 2024. – № 3. – С. 30–35. – URL: <https://cyberleninka.ru>.

2. Вечерникова Д. В. Актуальные вопросы, связанные с применением беспилотных воздушных судов в правоохранительной деятельности / Д. В. Вечерникова, А. А. Марина // Вестник Краснодарского университета МВД России. – 2022. – № 2 (56). – С. 67–72. – URL: <https://cyberleninka.ru>

3. Алгоритм действий сотрудников ОВД при обнаружении БВС. <https://05.мвд.пф/news/item/52471489/>

4. БПЛА: правила и ограничения. Разъяснения от... – Ространснадзор. – URL: <https://rostransnadzor.gov.ru/news>.

5. Виды и способы защиты от БПЛА. – URL: <https://luxsol sport.ru/blog/kakaya-byvaet-zashchita-ot-bpla>.

6. Глава 1. Беспилотные летательные аппараты (БПЛА) как... – URL: <https://ui.tsu.ru/wp-content/uploads>.

7. Защита от дронов и квадрокоптеров, защита от БПЛА, системы... – URL: <https://www.ao-avtomatika.ru/media>

8. Использование беспилотных летательных аппаратов... – URL: <https://tr-page.yandex.ru/translate>

СВЕДЕНИЯ ОБ АВТОРАХ

Калков Дмитрий Юрьевич.
Доцент кафедры радиотехнических систем и комплексов охранного мониторинга.

Кандидат технических наук.
Воронежский институт МВД России.
E-mail: dmitreyrus@mail.ru.
Россия, 394065, Воронеж, проспект Патриотов, 53.

Гудков Максим Андреевич.
Доцент кафедры процессов горения и экологической безопасности.
Кандидат технических наук, доцент.
Академия Государственной противопожарной службы МЧС России.
E-mail: M.Gudkov@academygps.ru.
Россия, 129366, Москва, ул. Бориса Галушкина, 4.

Ивануха Иван Сергеевич.
Преподаватель кафедры информационно-аналитического и документационного обеспечения деятельности ОВД.
Тюменский институт повышения квалификации сотрудников МВД России.
E-mail: scorpion-6588@mail.ru
Россия, 625049, г. Тюмень, ул. Амурская, 75.

Kalkov Dmitry Yurievich.
Associate Professor of the Department of radio engineering systems and security monitoring complexes.
Candidate of Technical Sciences.
Voronezh Institute of the Ministry of the Interior of Russia.
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Gudkov Maxim Andreevich.
Docent of the Department of Combustion processes and Environmental Safety.
Candidate of Technical Sciences, docent.
State Fire Academy of EMERCOM of Russia.
Moscow, 129366, Russia, Borisa Galushkina str., 4.

Ivanukha Ivan Sergeevich,
Lecturer of the Department of Information and Analytical Support and Documentation of the Activities of the Internal Affairs Bodies.
Tyumen Institute of Advanced Training of Employees of the Ministry of Internal Affairs of Russia.
E-mail: scorpion-6588@mail.ru
Russia, 625049, Tyumen, Amurskaya str., 75.

Ключевые слова: беспилотные летательные аппараты; правовое регулирование; ограничения; защита объектов; обнаружение; подавление.

Keywords: unmanned aerial vehicles; legal regulation; restrictions; object protection; detection; and suppression.

УДК 623.746.4-519

**П. В. Комраков, М. А. Гудков
А. А. Гапеев, Д. Ю. Калков**

ПРОГНОЗИРОВАНИЕ ВРЕМЕНИ ВЫБРОСА НЕФТИ И НЕФТЕПРОДУКТОВ ИЗ РЕЗЕРВУАРА ПРИ ПОЖАРЕ

PREDICTING THE TIME OF OIL AND OIL PRODUCTS EMITTED FROM A RESERVOIR DURING A FIRE

В статье рассмотрены существующие методические подходы к расчету времени выброса нефти и нефтепродуктов при пожаре в резервуарах. Актуальность исследования обусловлена участившимися случаями воздействия на резервуары с нефтепродуктами современных средств поражения, в частности беспилотных летательных аппаратов (БПЛА). Проанализированы две методики расчета времени от начала пожара до наступления выброса, показаны их ограничения и факторы, не учитываемые при расчетах. Предложен новый подход к оценке времени выброса с использованием систем компьютерного зрения на базе тепловизионных камер для мониторинга изменения тепловых полей в процессе горения нефтепродуктов.

The article discusses existing methodological approaches to calculating the ejection time of oil and petroleum products during fire in tanks. The relevance of the study is due to the increasing cases of impact on tanks with petroleum products by modern weapons, particularly unmanned aerial vehicles (UAVs). Two methods for calculating the time from the fire start to the ejection are analyzed, their limitations and factors not taken into account are shown. A new approach to assessing ejection time using computer vision systems based on thermal imaging cameras for monitoring changes in thermal fields during combustion of petroleum products is proposed.

В настоящее время вопросы вскипания и выброса нефти и нефтепродуктов в резервуарах вследствие воздействия на них современных средств поражения, в частности беспилотных летательных аппаратов (БПЛА), стоят достаточно остро. По данным различных источников, в 2024 году российские нефтеперерабатывающие заводы и нефтебазы подвергались атакам БПЛА не менее 81 раза, что привело к многочисленным пожарам и значительным материальным потерям [1, 2]. Данный факт требует комплексного подхода от заинтересованных служб и ведомств, заключающегося во всестороннем изучении особенностей вышеизложенных процессов и выработке рекомендаций по совершенствованию методики тушения. Горение нефти и нефтепродуктов в резервуарах может сопровождаться вскипанием и выбросами, которые представляют значительную опасность для личного состава пожарных подразделений,

техники, соседних резервуаров и объектов инфраструктуры [3]. Вскипание горючей жидкости происходит из-за наличия в ней взвешенной воды, которая при прогреве горячей жидкости выше 100°C испаряется, вызывая вспенивание нефти или нефтепродукта [4]. Согласно современным представлениям, вскипание и выброс нефти или мазута наступают в том случае, когда образовавшийся прогретый (гомותרмический) слой жидкости с температурой свыше 50°C достигает слоя подтоварной воды на дне резервуара [5]. При этом вода перегревается, значительная часть ее переходит в пар, который и выбрасывает горящую жидкость из резервуара, создавая угрозу не только соседним резервуарам, но и отдельным установкам, сооружениям, пожарной технике и людям [6]. Целью настоящей работы является анализ существующих методических подходов к расчету времени выброса нефти и нефтепродуктов при пожаре в резервуарах, выявление их ограничений и разработка предложений по применению современных технологий компьютерного зрения для прогнозирования выброса в условиях воздействия современных средств поражения.

В настоящее время известны два методических подхода, позволяющих рассчитать время от начала пожара до наступления выброса (τ_b) [7, 8]:

$$\tau_b = \frac{H-h}{v_{\text{л}} + v_{\text{ГТС}} + v_{\text{отк}}} \quad (1)$$

где: H – начальная высота слоя нефти в резервуаре, м;

h – толщина слоя воды на дне резервуара, м;

$v_{\text{л}}$ – линейная скорость выгорания жидкости, м/час;

$v_{\text{ГТС}}$ – линейная скорость роста гомותרмического слоя, м/час;

$v_{\text{отк}}$ – линейная скорость откачки жидкости из резервуара.

Второй подход [8] в расчете времени выброса учитывает высоту свободного борта резервуара. Разность этих величин представляет собой начальную высоту уровня нефти. Практически эти два выражения тождественны.

Рекомендуемые для расчета значения линейных скоростей выгорания и роста гомותרмического слоя для различных жидкостей представлены в таблице.

На основании представленных подходов был проведен расчет времени выброса для различных высот эксплуатируемых резервуаров, а также для различных высот слоя подтоварной воды. Физическая природа явления выброса горящих нефтепродуктов связана с перегревом и быстрым испарением воды, скопившейся на дне резервуара [9].

Таблица

**Линейные скорости выгорания и роста гомотермического слоя
для различных нефтепродуктов**

Жидкость	Линейная скорость выгорания, м/ч	Линейная скорость роста гомотермического слоя, м/ч
Бензин	До 0,30	До 0,10
Смесь нефти и газового конденсата	До 0,20	До 0,40
Нефть	До 0,15	До 0,40
Мазут	До 0,10	До 0,30

В процессе горения жидкости в резервуаре происходит ее постепенный прогрев на всю глубину слоя горючего, при этом наиболее сложным является образование гомотермического слоя, толщина которого непрерывно увеличивается, если не принять меры для интенсивного отвода тепла от горящего резервуара [10]. Скорость выгорания нефти составляет в среднем 3 мм в минуту, а скорость нарастания гомотермического слоя 9–15 мм/мин, то есть нефть быстрее прогревается по высоте слоя жидкости в резервуаре, чем выгорает с поверхности [11]. Графические зависимости времени выброса от высоты подтоварной воды (для значений 1, 2, 3 и 4 метра) и начальной высоты горючей жидкости показывают линейный характер зависимости. При увеличении высоты слоя подтоварной воды время до выброса закономерно уменьшается, что связано с более быстрым достижением гомотермическим слоем водяной подушки [12].

Необходимо отметить, что представленные расчеты носят теоретический характер и имеют существенные ограничения. Анализ научной литературы и результатов экспериментальных исследований показывает, что существующие формулы не учитывают ряд важных факторов, оказывающих значительное влияние на время выброса [13–16]:

1. Метеорологические факторы:

- скорость и направление ветра, влияющие на интенсивность горения и угол наклона факела пламени (при скорости ветра около 4 м/с отклонение факела от вертикальной оси может составлять 60-70°) [16];
- температура окружающего воздуха и влажность;
- атмосферное давление.

2. Теплофизические факторы [17–19]:

- изменение массовой скорости выгорания в зависимости от характера движения воздушных масс;
- турбулизация процесса горения при перемешивании паров горючего с окислителем, приводящая к увеличению скорости образования гомотермического слоя;
- тепловое излучение от факела пламени, которое может составлять 1-2 диаметра горящего резервуара;

– одновременный нагрев резервуара с внешней и внутренней сторон при горении в обваловании.

3. Физико-химические характеристики нефтепродуктов [5, 20, 21]:

– влажность нефтепродукта и форма существования воды (подтоварная вода на дне или эмульсия в объеме жидкости);

– вязкость и изменение ее при нагреве, влияющие на скорость спуска капли воды вглубь резервуара;

– содержание высокоароматичных соединений и кислородсодержащих компонентов в нефти;

– наличие растворенных газов и легких фракций.

4. Конструктивные особенности резервуаров:

– коррозионный износ стенок резервуара, влияющий на теплопередачу (скорость коррозии может достигать 0,04–1,1 мм/год для равномерной коррозии и 3–8 мм/год для язвенной) [22];

– наличие и состояние теплоизоляции;

– высота свободного борта резервуара (если она превышает толщину прогретого слоя более чем вдвое, жидкость может не переливаться через борт при содержании воды до 1%) [5, с. 13];

– технологические режимы эксплуатации резервуара.

5. Специфические условия современных угроз:

– множественные очаги возгорания при воздействии БПЛА;

– характер повреждения резервуара (место и размер пробоины);

– возможность формирования теплового восходящего потока с скоростью более 110 км/ч;

– образование «окон» в пламени при тотальном пожаре резервуара.

С учетом выявленных ограничений существующих аналитических методов расчета предлагается интегрированный подход к оценке времени выброса, основанный на применении систем компьютерного зрения с использованием тепловизионных камер для мониторинга изменения тепловых полей в процессе горения нефтепродуктов [23, 24].

Современные технологии компьютерного зрения в сочетании с тепловизионной съемкой открывают новые возможности для раннего обнаружения и прогнозирования выброса нефтепродуктов [25]. Тепловизионные камеры способны регистрировать температурные аномалии и отслеживать динамику развития теплового поля в режиме реального времени, что позволяет выявлять ранние признаки формирования гомотермического слоя.

1. Тепловизионные системы обеспечивают непрерывное наблюдение за тепловым полем резервуара, позволяя отслеживать изменение температурных градиентов по глубине слоя нефтепродукта. Интеграция с алгоритмами искусственного интеллекта позволяет обрабатывать тепловые данные в режиме реального времени для различения нормальных температурных колебаний и опасных источников тепла [26].

2. Модели компьютерного зрения на базе сверточных нейронных сетей способны анализировать данные тепловых изображений для обнаружения горячих точек и аномальных зон прогрева, которые могут указывать на приближение гомотермического слоя к подтоварной воде. Системы способны создавать тепловые карты с цветовой кодировкой, позволяющие быстро различать безопасные и потенциально опасные зоны [23].

3. Возможность размещения тепловизионных камер на безопасном расстоянии или на беспилотных летательных аппаратах позволяет осуществлять мониторинг без риска для персонала. Дальность обнаружения при идеальной видимости может достигать 15 километров [27].

Проведенный анализ существующих методических подходов к расчету времени выброса нефти и нефтепродуктов при пожаре в резервуарах показал, что обе рассмотренные методики, несмотря на их практическую значимость, имеют существенные ограничения.

Формулы расчета не учитывают ряд важных факторов:

- метеорологические условия (скорость и направление ветра, температуру и влажность воздуха);
- изменение массовой скорости выгорания;
- турбулизацию процесса горения;
- физико-химические характеристики конкретных нефтепродуктов;
- конструктивные особенности резервуаров (включая коррозионный износ);
- специфические условия воздействия современных средств поражения, таких как БПЛА, способных создавать множественные очаги возгорания.

Для преодоления указанных ограничений предложен инновационный подход к оценке времени выброса, основанный на применении систем компьютерного зрения с использованием тепловизионных камер.

Данная технология позволяет

- осуществлять непрерывный мониторинг изменения тепловых полей в процессе горения нефтепродуктов в режиме реального времени;
- обеспечивает раннее предупреждение о приближении выброса;
- работает в любых погодных условиях и в условиях задымления;
- может интегрироваться с автоматическими установками пожаротушения.

Применение алгоритмов машинного обучения для обработки данных тепловизионных камер открывает возможность прогнозирования времени выброса с точностью 85–99% на основе анализа динамики температурных полей. Интеграция результатов тепловизионного мониторинга с аналитическими методами расчета позволит создать комплексную систему оценки и прогнозирования выброса, значительно повышающую эффективность противопожарной защиты резервуарных парков.

Резюмируя вышеизложенное, необходимо отметить, что для получения корректных данных о времени выброса нефти и нефтепродуктов в условиях

воздействия современных средств поражения необходимо проводить полномасштабные полигонные испытания с применением тепловизионного мониторинга для всестороннего изучения влияния отдельных факторов и их сочетаний. Результаты таких испытаний позволят не только усовершенствовать существующие аналитические методики расчета, но и обучить нейросетевые модели для автоматического прогнозирования выброса, что в конечном итоге обеспечит разработку более эффективных рекомендаций по предупреждению и тушению пожаров в резервуарах с нефтью и нефтепродуктами.

ЛИТЕРАТУРА

1. Минимум 81 раз дроны атаковали российские НПЗ в 2024 году // Северная реальность. – 2025. – URL: <https://www.severreal.org> (дата обращения: 29.10.2025).
2. Объять необъятное: нефтебазы и НПЗ России под прицелом дронов // Neft Capital. – 2024. – URL: <https://oilcapital.ru> (дата обращения: 29.10.2025).
3. Руководство по тушению пожаров на резервуарных парках.– Москва : ВНИИПО МВД России, 1999. – 29 с.
4. Вскипание нефтепродуктов в резервуарах // Пожар.ру. – URL: <https://пожар.рф> (дата обращения: 29.10.2025).
5. Воднев П. П. Расчет параметров пожара, времени вскипания и выброса нефтепродуктов в процессе горения : методические указания / П. П. Воднев. – Ульяновск : УлГТУ, 2014. – 14 с.
6. Клубань В. С. Безопасная откачка нефти из горящих резервуаров / В. С. Клубань // Технологии техносферной безопасности. – 2019. – № 1. – С. 1–8.
7. Руководство по тушению нефти и нефтепродуктов в резервуарах и резервуарных парках. – Москва : ВНИИПО, 1999. – 29 с.
8. Терещнев В. В. Пожарная тактика. Книга 3. Расчет параметров пожаротушения : учеб. пособие. 2-е изд., с изм. / В. В. Терещнев. – Москва : Академия ГПС МЧС России, 2020. – 447 с.
9. Техинфо-М. Гомотермический слой при горении нефтепродуктов. – URL: <https://tehinfo-m.narod.ru> (дата обращения: 29.10.2025).
10. Корольченко А. Я. Физико-химические основы развития и тушения пожаров : учебное пособие/ А. Я. Корольченко. – Москва : Академия ГПС МЧС России, 2014. – 210 с.
11. Сторонкина О. Е. Физико-химические основы горения : учебное пособие / О. Е. Сторонкина, Т. А. Мочалова. – Иваново : ИГПС МЧС России, 2018. – 156 с.

12. Тушение пожаров в резервуарах и резервуарных парках // Пожарная безопасность. – 2010. – URL: <https://gazovik-neft.ru> (дата обращения: 29.10.2025).
13. Физико-химические основы развития и тушения пожара : методические рекомендации. – Новосибирск : Сибирская ПСА, 2020. – 87 с.
14. Методика расчета выбросов вредных веществ в атмосферу при свободном горении нефти и нефтепродуктов. – Самара, 1996. – 42 с.
15. Пожарная безопасность объектов с наличием нефти и нефтепродуктов и их технологических процессов : учебное пособие. – Челябинск : ЮУрГУ, 2021. – 156 с.
16. Руководство по тушению нефти и нефтепродуктов в резервуарах и резервуарных парках. – Москва : ВНИИПО МВД России, 1999. – С. 8–12.
17. Расчет параметров аварийных выбросов опасных веществ / А. С. Софин, О. А. Прокудин, А. А. Агапов, Д. Ю. Сумский // Актуальные проблемы гуманитарных и естественных наук. – 2018. – № 3. – С. 112–118.
18. Алексеев М. М. Применение системы компьютерного зрения для экспериментального изучения движения фронта пламени / М. М. Алексеев, О. Ю. Семенов // Вестник кибернетики. – 2023. – № 2(6). – С. 6–12.
19. Тушение пожаров на нефтехимических объектах : презентация // Fireman Club. – 2023.
20. Давыдов Д. А. Оценка параметров пожара в резервуарах с нефтепродуктами : магистерская диссертация / Д. А. Давыдов. – Тольятти : ТГУ, 2016. – 98 с.
21. Швецов Е. Г. Мониторинг, моделирование и прогнозирование лесных пожаров / Е. Г. Швецов, Е. И. Пономарев. – Красноярск : Институт леса СО РАН, 2017. – 215 с.
22. Причины разрушений и взрывов резервуаров // УралНефтеМаш. – 2019. – URL: <https://uralneftemash.com> (дата обращения: 29.10.2025).
23. Компьютерное зрение для обнаружения пожаров // Ultralytics. 2025. – URL: <https://www.ultralytics.com> (дата обращения: 29.10.2025).
24. Контроль утечек и выбросов с помощью компьютерного зрения // AVI Global. – URL: <https://avi-global.ru> (дата обращения: 29.10.2025).
25. Обзор систем технического зрения в роботизированных установках пожаротушения // FireRobots. – 2024. – URL: <https://firerobots.ru> (дата обращения: 29.10.2025).
26. Компьютерное зрение для обнаружения пожаров с помощью тепловидения, ИИ и прогнозной аналитики // Ultralytics. – 2025. – URL: <https://www.ultralytics.com> (дата обращения: 29.10.2025).
27. Лаптев Н .В. Системы обнаружения лесных пожаров на основе тепловизионных технологий : дисс. канд. техн. наук / Н. В. Лаптев. – Томск : ТПУ, 2023.– С. 89.

СВЕДЕНИЯ ОБ АВТОРАХ

Комраков Петр Владимирович.
Профессор кафедры процессов горения и экологической безопасности.

Кандидат технических наук, доцент.
Академия Государственной противопожарной службы МЧС России.
E-mail: P.Komrakov@academygps.ru.
Россия, 129366, Москва, ул. Бориса Галушкина, 4.

Гудков Максим Андреевич.
Доцент кафедры процессов горения и экологической безопасности.
Кандидат технических наук, доцент.
Академия Государственной противопожарной службы МЧС России.
E-mail: M.Gudkov@academygps.ru.
Россия, 129366, Москва, ул. Бориса Галушкина, 4.

Гапеев Артём Александрович.
Заместитель начальника кафедры процессов горения и экологической безопасности.

Кандидат химических наук, доцент.
Академия Государственной противопожарной службы МЧС России.
E-mail: A.Gapeev@academygps.ru.
Россия, 129366, Москва, ул. Бориса Галушкина, 4.

Калков Дмитрий Юрьевич.
Доцент кафедры радиотехнических систем и комплексов охранного мониторинга.

Кандидат технических наук.
Воронежский институт МВД России.
E-mail: dmitreyrus@mail.ru.
Россия, 394065, Воронеж, проспект Патриотов, 53.

Komrakov Pyotr Vladimirovich.
Professor of the Department of Combustion processes and Environmental Safety.

Candidate of Technical Sciences, Docent.
State Fire Academy of EMERCOM of Russia.
E-mail: P.Komrakov@academygps.ru.
Moscow, 129366, Russia, Borisa Galushkina str., 4.

Gudkov Maxim Andreevich.
Docent of the Department of Combustion processes and Environmental Safety.

Candidate of Technical Sciences, Docent.
State Fire Academy of EMERCOM of Russia.
E-mail: M.Gudkov@academygps.ru.
Moscow, 129366, Russia, Borisa Galushkina str., 4.

Gapeev Artem Alexandrovich.
Deputy head of the Department of Combustion Processes and Environmental Safety.
Candidate of Chemical Sciences, Docent.
State Fire Academy of EMERCOM of Russia.
E-mail: A.Gapeev@academygps.ru.
Moscow, 129366, Russia, Borisa Galushkina str., 4.

Kalkov Dmitry Yurievich.
Associate Professor of the Department of radio engineering systems and security monitoring complexes.
Candidate of Technical Sciences.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: dmitreyrus@mail.ru.
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: выброс нефти; пожар в резервуаре; гомотермический слой; подтоварная вода; БПЛА; компьютерное зрение; тепловизионная съемка; тепловое поле; пожарная безопасность.

Keywords: oil spill; tank fire; homothermal layer; sub-product water; UAV; computer vision; thermal imaging; thermal field; fire safety.

УДК 614.841.12

**ПЕРСПЕКТИВЫ РАЗВИТИЯ СРЕДСТВ ПОРАЖЕНИЯ
БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ**

**PROSPECTS FOR THE DEVELOPMENT
OF UNMANNED AIRCRAFT DEATH DEVICES**

В статье рассматривается проблематика развития беспилотных воздушных судов, используемых нарушителями, физические принципы и технические решения, доступные к применению для их поражения, и рассматриваются перспективы развития комплексов, построенных на этих физических принципах.

The article examines the development of unmanned aircraft used by intruder, the physical principles and technical solutions available for their destruction, and discusses the prospects for the development of complexes based on these physical principles.

Технические средства поражения беспилотных воздушных судов (далее – БВС) в настоящее время становятся неотъемлемыми частями комплексов инженерно-технических средств объекта. В связи с развитием автономных БВС-нарушителей растет значение средств их физического поражения.

Средства поражения БВС достаточно разнообразны, а именно: средства противовоздушной обороны (организационно не входят в состав комплекса инженерно-технических средств охраны), комплексы радиоэлектронного противодействия (далее – РЭП), лазерные комплексы поражения БВС, ультразвуковые генераторы, воздействующие на микрогироскопы БВС, БВС-перехватчики, микроволновые генераторы, взрывомагнитные генераторы, дистанционно-управляемые модули, комплексы засветки оптических и тепловизионных средств видеонаблюдения БВС.

Стоит отметить, что средства ПВО эффективны только против средних и крупных БВС. Классы «малые» и «микро» БВС не являются сферой применения ПВО. Проигрывает ПВО и по критерию стоимости.

В связи с развитием беспилотных авиационных систем, используемых нарушителями, практически полностью дискредитировали себя комплексы РЭП. Причем такое положение дел объясняется не ошибками производителя, а физикой процесса. В настоящее время БВС могут передавать сигналы управления, используя полосу частот от 27 МГц до 7,2 ГГц (причем наблюдается постоянное расширение диапазона этих частот). Таким образом, при мощности передатчика РЭП в 5 кВт, но равномерно распределенного по полосе, спектральная плотность помехи составляет всего порядка $0,7 \times 10^{-6}$ Вт/Гц, что позволяет БВС совершать запланированный полет. Если использовать

генераторы помех на узкие диапазоны частот, но с большой спектральной плотностью помехи, то полет БВС будут осуществлять в частотных «дырах» этого диапазона. Единственно, что ещё может оказать противодействие БВС, так это комбинация генератора с перестройкой частоты с комплексом радиотехнической разведки. Но такие комплексы малоэффективны при применении сигналов с псевдослучайной перестройкой рабочей частоты, шумоподобным сигналом и бесполезны против БВС, использующих телеуправление, осуществляемое по оптоволокну, или осуществляющих полет автономно, ориентируясь при помощи машинного зрения, радиомаякам и меткам. Вместе с тем, РЭП должен быть включен в контур защиты объекта для подавления сигналов глобальных навигационных систем и традиционных (штатных) частот передачи и управления БВС. Если этого не делать, то резко повышается вероятность совершения актов незаконного вмешательства при помощи широкораспространенных дешевых беспилотных воздушных судов, построенных на стандартной элементной базе.

Лазерный физический принцип поражения БВС – характеризуется высокой стоимостью оборудования и существенными ограничениями по погодным условиям применения при ограниченной эффективной дальности поражения.

Ультразвуковые генераторы, воздействующие на микрогироскопы БВС путём создания на них вибрации (в основе большей части микрогироскопов лежат пьезоэлементы), имеют ограниченную дальность эффективного воздействия из-за высокой расходимости луча такого генератора в атмосфере и большом коэффициенте затухания в пространстве. Коэффициент затухания ультразвука зависит также от влажности воздуха и рабочей частоты генератора. Поэтому этот вариант борьбы с БВС является труднореализуемым и дорогостоящим.

Рассмотрим наиболее перспективные способы борьбы с БВС.

1. Использование БВС-перехватчиков.

Одним из определяющих параметров БВС-перехватчиков, при рассмотрении их для противодействия БВС-нарушителям, является способ их запуска: с ручной пусковой установки, одиночные, с открытых площадок и различных направляющих, с дронапортов, использующих комбинированные пусковые установки.

БВС-перехватчики, запускаемые с ручной пусковой установки, концепцию своего применения взяли от пусковых установок зенитных ракет. Использование БВС вместо ракеты снизило стоимость модуля на порядки, но у любого технического решения есть обратная сторона. Обнаружение и захват цели в этом случае осуществляется с помощью теле/теповизионных модулей, установленных на БВС-перехватчике, что ограничивает эффективность их применения.

БВС-перехватчики, стартующие из дронапортов (автоматизированных ангаров, обеспечивающих БВС-перехватчик в готовности к запуску и

инициацию его запуска), могут получать внешнее целеуказание от технических средств обнаружения и наблюдения БВС, но при этом навигационные системы БВС-перехватчика и комплекса внешнего целеуказания должны работать в единых координатных системах.

Другими ограничениями являются скорости перемещения БВС-перехватчика и реализуемые ускорения при атаке на цель. Для БВС-перехватчика перегрузка даже в 5G является запредельной характеристикой (связано это не столько с прочностью корпуса БВС-перехватчика, сколько с энергетическими возможностями двигателя). Видеоролики, выложенные в свободном доступе, показывают, насколько сложно системе наведения БВС-перехватчика удерживать цель в центре прицельной рамки. Данную проблему можно решить, переходя от таранного удара БВС к дистанционному подрыву боеприпаса. Количество и размер поражающих элементов такого боеприпаса определит дистанцию от цели, на которой его следует подрывать. При размещении поражающих элементов впереди боеприпаса сформируется оптимальный конус поражения.

Другим решением вопроса может быть использование БВС-перехватчика вооруженного устройством, метящим дробь или картечь, работающего по принципу пушки Дэвиса. При этом не происходит потери БВС-перехватчика.

Существенным ограничением по эффективности применения БВС-перехватчиков является относительно низкая их скорость полета относительно перехватываемой цели. В редких случаях скорость полета БВС-перехватчика вдвое превышает скорость полета перехватываемой цели, что при проведении простейших геометрических расчетов показывает, что если мы хотим перехватить цель на дистанции в 250 м, то дронапорты с БВС-перехватчиками придется размещать на расстоянии не более 1 км друг от друга (с учетом двух плечей полета БВС-перехватчика из дронапорта).

Комбинация БВС-перехватчиков, расположенных на направляющих комплекса с мортирами с картечными выстрелами, представляется наиболее рациональным решением. Примером такого решения является боевой мобильный комплекс «Антидрон» от НТЦ «ЛЭМТ».

Данное направление развития средств поражения видится перспективным и имеет перспективы по его дальнейшему совершенствованию.

2. Дистанционно-управляемые модули (далее – ДУМ).

ДУМ бывают выполнены на базе гладкоствольного и нарезного оружия. Нарезное оружие обеспечивает большую дальность поражения, но требует создания зоны отчуждения для исключения поражения людей на нисходящей траектории используемых боеприпасов. Для поражения БВС оптимальным боеприпасом является патрон 7,62 x 54R (пристрелочный), а оптимальным оружием – счетверенная установка на основе пулемета Калашникова танкового. Отдельно выполненный ДУМ без средств управления и наведения на цель имеет ограниченную ценность. Поэтому

ДУМ должен быть сопряжен с комплексом средств обнаружения и наблюдения за БВС-нарушителем – радиолокационными средствами обнаружения и сопровождения, теле/тепловизионном комплексом, кроме того лазерным дальномером, баллистическим вычислителем, сервоприводом.

В идеальном случае комплекс борьбы с БВС должен быть многорубежным, с оснащением средствами обнаружения и сопровождения БВС, построенными на разных физических принципах (микроволновое излучение, регистрация ИК-излучения и излучения в оптическом диапазоне длин волн). Наибольшую вероятность поражения цели имеет ДУМ, оснащенный картечными боеприпасами. С учетом максимальной эффективной дальности стрельбы ДУМ с такими зарядами в 300 м, первый рубеж обороны должен проходить по периметру охраняемого объекта, второй рубеж обороны должен быть развернут непосредственно на особо важных и уязвимых узлах объекта. Средства обнаружения и сопровождения целей должны располагаться на высокостоящих зданиях и сооружениях объекта. Все устройства комплекса должны быть объединены в единый АРМ и иметь общую шину данных и протокол передачи информации.

3. Поражение цели микроволновым излучением.

Поражение цели микроволновым излучением является перспективным направлением развития средств поражения БВС. Механизм поражения заключен в генерации наводок на микропроцессоры БВС и линии управления полетными двигателями.

Наилучшие результаты по воздействию на БВС оказывают пачки импульсов высокой мощности, при этом средняя мощность излучения генератора СВЧ будет находиться в диапазоне 2-50 кВт.

Огромным достоинством такого средства поражения является то, что в данном случае не надо точно знать частоты управления БВС, и они могут эффективно воздействовать даже на БВС, управляемые по оптоволокну или осуществляющие полет в режиме радиомолчания.

Такие установки производят: Китай (фирмы CSGC и ORINCO»), США (комплекс PHASER, фирма Raytheon), Великобритания (комплекс RF DEW, фирма Team HERSA), Вьетнам (комплекс V-EMP/S, фирма Viettel). К сожалению, номенклатура отечественных комплексов микроволнового поражения гораздо скромнее, хотя и наблюдается рост таких изделий.

4. Поражение цели электромагнитным импульсом взрывом магнитного генератора (далее – ВМГ).

Взрывом магнитный генератор представляет из себя катушку индуктивности, обложенную взрывчаткой веществом (снаружи или внутри неё), подключенную к мощному конденсатору. При разряде конденсатора на катушку индуктивности в ней возникает магнитное поле. В момент достижения максимального значения магнитного поля происходит подрыв взрывчатки, что приводит к сжатию витков катушки (соответственно магнитного поля катушки). При этом генерируется сильный ток (до 10^8 А).

Можно отметить, что до 20% взрывчатого вещества переходит в энергию электромагнитного излучения. В основе ВМГ лежит принцип превращения магнитной энергии в электрический ток. В упрощенной форме физика процесса приведена ниже.

Она основывается на следующих утверждениях:

- электрическое поле в идеальном проводнике равно нулю, т.е. магнитный поток Φ , заключенный в сжимающейся цилиндрической полости, не меняется в процессе сжатия;

- из формулы (1) вытекает, что ток в контуре обратно пропорционален индуктивности контура;

- энергия магнитного поля также обратно пропорциональна индуктивности, см. формулу (2).

Таким образом, при взрывном уменьшении индуктивности резко возрастает энергия магнитного поля, что приводит к кратковременной генерации сильного тока.

$$\Phi = L \cdot I = \text{const}, I \approx \frac{1}{L} \quad (1)$$

$$W = \frac{L \cdot I^2}{2} = \frac{\phi^2}{2L} \quad (2),$$

где: Φ – магнитный поток; L – индуктивность; I – ток; W – энергия магнитного поля.

Типовые зависимости тока от времени при подрыве ВМГ приведены на рисунке 1 [2] $\times 10^6$ А

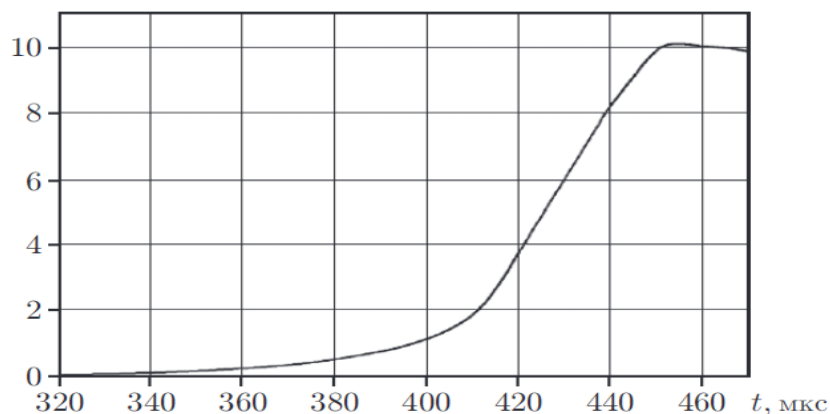


Рис. 1. Зависимость тока от времени при подрыве взрывомагнитного генератора ВМГ-280

Эффективная дальность поражения воздушной цели ВМГ в три раза превышает дальность действия традиционного боеприпаса осколочно-фугасного действия при равенстве масс их боевых частей.

Алгоритм выбора перспективного средства поражения БВС

Для определения преимуществ одного вида средства поражения БВС над другим надо провести оценку совокупности параметров и сделать выбор, основываясь на интегральном коэффициенте. Выпишем типовые

характеристики средств поражения и выставим им оценку по десятибалльной шкале. Сразу заметим, что у вас могут быть другие параметры и другие их оценки.

Сравним лазерный комплекс поражения БВС с комплексом поражения реализованном на основе ДУМ с нарезным оружием (см. табл.).

Таблица

Проведение интегральной оценки параметров лазерного комплекса поражения БВС и комплекса на основе ДУМ

Параметр	Лазерный комплекс	ДУМ
	Значение	Значение
Стоимость комплекса (минимальное значение в этом параметре соответствует максимальной стоимости)	1	6
Эффективность по поражению БВС днём	5	6
Эффективность по поражению БВС ночью	3	6
Эффективность по поражению БВС при плохих погодных условиях ночью	1	5
Дистанция поражения	5	5
Сложность эксплуатации	2	8
Сложность обучения при работе с комплексом (минимальное значение в этом параметре соответствует максимальной сложности)	5	8
Температурный диапазон работы/климатическое исполнение	4	8
Отечественная локализация компонентов	5	10
Включение в перечень Минпромторга	5	5
Необходимость создания зоны отчуждения	7	2
Правовой статус по применению средств поражения	5	5
Энергозатраты (минимальное значение в этом параметре соответствует максимальным энергозатратам)	3	7
Финансовые затраты на поражение единичной цели (минимальное значение в этом параметре соответствует максимальным затратам)	8	5

Поскольку возможность поражения БВС носит вероятностный характер и нюансы развития БВС на долгосрочную перспективу трудно предугадать, защиту необходимо строить, используя различные средства противодействия. На текущий период оптимальной видится защита, состоящая из дронов-перехватчиков, оснащенных боевой частью с дистанционным подрывом (или оснащенных ВМГ), размещенных в дронопортах, комплекса микроволнового излучения и ДУМ.

Стоит отметить, что исходя из тактики применения, технические средства поражения БВС следует рассматривать как неотъемлемую часть комплексов ИТСО и учитывать это при организации системы охраны объекта.



Рис. 2. Интегральная оценка параметров лазерного комплекса поражения и комплекса на основе ДУМ

ЛИТЕРАТУРА

1. Сахаров А. Д. Научные труды. Сборник /А. Д. Сахаров. – Москва : ЦентрКом, 1995. – 528 с.
2. Применение взрывомагнитных генераторов в физике высоких плотностей энергии / В. Д. Селимир, П. Б. Репин, В. А. Демидов [и др.] // Прикладная механика и техническая физика. – 2019. – Т. 60. – № 3(355). – С. 3–14.
3. Михайлов А. А. Определение предельных дальностей обнаружения малогабаритных воздушных объектов с помощью электронно-оптических средств наблюдения/ А. А. Михайлов, А. Д. Гладкова // Системы безопасности. – 2024. – № 2.

СВЕДЕНИЯ ОБ АВТОРЕ

Михайлов Алексей Алексеевич.

Научный сотрудник отдела развития инновационных решений, цифровых технологий и программного обеспечения.

Научно-исследовательский центр «Охрана» Федеральной службы войск национальной гвардии Российской Федерации.

E-mail: vh48905@yandex.ru

Россия, 111539, г. Москва, ул. Реутовская, 12Б.

Mikhailov Alexey Alekseevich.

Researcher of the Department of Innovative Solutions, Digital Technologies and Software Development.

Federal State Institution Research Center «Ohrana» of the Federal Service of the National Guard Troops of the Russian Federation.

E-mail: vh48905@yandex.ru

Russia, 111539, Moscow, Reutovskaya str., 12B.

Ключевые слова: беспилотные воздушные суда; средства поражения беспилотных воздушных судов; радиоэлектронное противодействие; системы охраны.

Keywords: unmanned aerial vehicles; means of destroying unmanned aerial vehicles; and electronic countermeasures; security system.

УДК 623.09

**СОВЕРШЕНСТВОВАНИЕ ЗАЩИЩЕННОСТИ
ОБЪЕКТОВ ОХРАНЫ В УСЛОВИЯХ ПРОТИВОДЕЙСТВИЯ
БЕСПИЛОТНЫМ ВОЗДУШНЫМ СУДАМ**

**IMPROVING THE SECURITY OF PROTECTED FACILITIES
IN THE FACE OF UNMANNED AIRCRAFT**

В данной статье проведен анализ защищенности охраняемых объектов от угроз, связанных с применением беспилотных воздушных судов. Предложены решения и разработаны рекомендации по обеспечению безопасности охраняемых объектов с целью повышения уровня антитеррористической защищенности в условиях противодействия беспилотным воздушным судам.

This article analyzes the security of protected facilities from threats associated with the use of unmanned aircraft. Solutions are proposed and recommendations are developed to ensure the security of protected facilities in order to increase the level of anti-terrorist security in the context of countering unmanned aircraft.

В настоящее время, в связи с осложняющейся внешнеполитической обстановкой, которая неукоснительно сказывается на росте актов терроризма и преступных посягательств, все больше возрастает актуальность и значимость обеспечения безопасности охраняемых объектов различного функционального назначения [1-2].

Основной угрозой для объектов охраны является атака БВС. Данный способ наиболее эффективный для нанесения максимально возможного ущерба, затрачивая на это минимум усилий. Ключевая проблема защиты заключается в системной неэффективности классических методов противодействия. Радарные и оптические системы часто неспособны обнаружить малогабаритные беспилотные воздушные судна (БВС), летящие на предельно малых высотах, а средства перехвата, такие как зенитные комплексы, оказываются малорезультативными против роевых атак или малогабаритных БВС с высокой маневренностью. Данный пробел в безопасности увеличивает риски нанесения значительного ущерба охраняемым объектам.

Сложности в борьбе с БВС возникают по нескольким причинам [2-4]:

1. Высокая скрытность, так как из-за небольшого размера и шума, по сравнению с пилотируемой авиацией, беспилотные судна сложнее обнаружить.

2. Оператор, запускающий и контролирующий полет дрона, может находиться на значительном расстоянии от объекта охраны, прячась за

различными постройками и сооружениями. В зависимости от типа БВС расстояние может варьироваться от нескольких сотен метров до нескольких километров, что значительно снижает шансы на задержание правонарушителя.

3. Высокая скорость движения малогабаритных БВС и короткое время их нахождения над территорией объекта охраны затрудняют организацию перехвата.

4. Низкая стоимость данного типа БВС, например, дрона-камикадзе, намного меньше, чем ракеты или пилотируемого самолета.

5. Возможность создавать и использовать различные тактики нападения на цели, а также гибкость применения, благодаря которой на некоторых видах БВС оператор может менять цель атаки прямо в полете.

6. Высота полета БВС позволяет им легко преодолевать все инженерные барьеры объекта охраны, что делает их труднодоступными для обнаружения с помощью охранных систем и видеонаблюдения.

Ключевыми задачами в борьбе с БВС являются обнаружение, сопровождение, перехват управления и, в критических ситуациях, уничтожение.

Так как разработка новых видов БВС идет постоянно, соответственно и рынок непрерывно пополняется различными средствами защиты от них.

Технические средства защиты можно разделить по следующим принципам действия и решаемым задачам:

– средства разведки и целеуказания – сюда входят радиолокационные станции, оптоэлектронные системы, радиотехнические системы и системы радиоэлектронной разведки, которые помогают обнаружить, идентифицировать найденную цель, определить различные характеристики и передать информацию непосредственно управляющим данными комплексами для дальнейших решений;

– средства поражения – специализированное оборудование, которое отвечает за уничтожение воздушных целей. Сюда входят зенитные ракетные комплексы разных дальностей действия, зенитная артиллерия. Также популярность набирают лазерные комплексы и системы радиоэлектронной борьбы, которые бесшумно выводят летательные аппараты из строя;

– средства радиоэлектронной борьбы – данные системы не уничтожают летательный аппарат, они действуют на объект, подавляя их электронную систему, тем самым делают атаку невозможной или неэффективной.

В настоящее время производители средств обнаружения воздушных целей комбинируют в одном комплексе несколько устройств, объединяя в одном устройстве радары, оптико-электронные и радиотехнические средства. Данное сочетание компенсирует недостатки каждого отдельного

метода, что увеличивает вероятность обнаружения БПЛА, однако интеграция этих технологий значительно увеличивает стоимость оборудования.

Сегодня на рынке достаточно большое количество таких систем, например: подавитель дронов «GroZZa», мобильная система обнаружения БВС «Н1С», «1С» стационарное оборудование обнаружения и позиционирования БВС, комплекс обнаружения БВС «РАДЕСКАН-АНТИДРОН» и другие.

Чтобы определиться с выбором наиболее подходящего оборудования, необходимо провести сравнительный анализ нескольких вариантов противовоздушной защиты объекта. Сначала рассмотрим комплексы, включающие в себя функции обнаружения, подавления и поражения найденных целей: мобильная станция «ЭВЕНК», мобильный комплекс «Сапсан-Бекас» и подавитель «GroZZa» (табл. 1).

Таблица 1

Сравнительная характеристика комплексов противодействия БВС

№ п/п	Параметры	Наименования комплексов		
		«ЭВЕНК»	«Сапсан-Бекас»	«GroZZa»
1.	Дальность обнаружения БПЛА, км	5	5	-
2.	Дальность подавления БПЛА, км	2	1	1,5-2
3.	Диапазон постановки помех, ГГц	1-2	РЧ-диапазон	2,4; 5,8
4.	Назначение	Обнаружение, подавление, поражение	Обнаружение, подавление, перехват сетью БВС	Подавление
5.	Принцип действия	Радар, РЧ-пеленгация, РЭБ, лазер	Радар, РЧ-пеленгация, оптика, РЭБ	РЭБ
6.	Время развертывания, мин	10-15	5-10	1
7.	Рабочий диапазон температур, °С	-40...+50	-40...+50	-20...+50

Для организации мобильного рубежа обнаружения могут использоваться комплексы, приведенные в таблице 2.

Таблица 2

Сравнительная характеристика комплексов противодействия БВС
для организации мобильного рубежа обнаружения

№ п/п	Параметры	Наименования комплексов		
		«НІС»	«Skyeye»	«РАДЕСКАН-АНТИДРОН»
1.	Дальность обнаружения БПЛА, км	5	3	5
2.	Дальность подавления БПЛА, км	-	-	-
3.	Диапазон постановки помех, ГГц	1,2; 2,4; 5,8	2,4; 5,8	0,43; 2,4; 5,8
4.	Назначение	Мобильное обнаружение и сопровождение	Мобильное обнаружение и классификация	Мобильное обнаружение БПЛА
5.	Принцип действия	Радар, РЧ-пеленгация, оптика	РЧ-пеленгация	РЧ-пеленгатор
6.	Время развертывания, мин	3-5	1	2-3
7.	Рабочий диапазон температур, °С	-40...+50	-20...+45	-30...+50

Проведя сравнительный анализ четырех вышеуказанных комплексов, можно сделать вывод о том, что для обеспечения безопасности объектов наиболее перспективными являются комплексы «ЭВЕНК», «РАДЕСКАН-АНТИДРОН» и «НІС», так как они имеют оптимальную дальность обнаружения и подавления, а также широкий частотный диапазон постановки помех.

В отличие от технических средств, которые направлены на противодействие угрозам атаки БВС еще до взаимодействия с объектом, инженерные средства нацелены на то, чтобы защитить непосредственно сам объект и его уязвимые места от атаки БВС, а в случае успешной атаки – минимизировать ущерб. К таким средствам относятся антидроновые сети или защитные ограждающие конструкции (ЗОК). В части нормативно-правового регулирования, существует свод правил [5], в котором дается определение защитным ограждающим конструкциям. Защитная ограждающая конструкция – конструктивная система, позволяющая минимизировать воздействие опасных факторов при атаке беспилотного летательного аппарата (таранный удар БВС, воздействие воздушной ударной волны, кумулятивной струи и осколков) на здания, строения и сооружения, технологическое оборудование на открытом воздухе [5].

Свод правил 542.1325800.2024 определяет функциональные требования, конструктивные решения для защитных конструкций,

производится расчет нагрузок и приводится классификация типов защитных ограждающих конструкций по нескольким признакам:

1. По расположению относительно защищаемого объекта ЗОК классифицируются по следующим типам:

– на независимой опорной конструкции (без опоры на защищаемый объект);

– на зависимой опорной конструкции.

2. По типу элементов, препятствующих контакту БПЛА с защищаемым объектом:

– на основе стальных канатов;

– металлических сеток;

– полимерных сеток;

– железобетонных и габионных конструкций;

– комбинированные.

3. По типу противоосколочных элементов:

– без противоосколочных элементов;

– с противоосколочными элементами на базе железобетонных и габионных конструкций;

– с противоосколочными элементами на базе тюфяков, матрасов, противоосколочных стенок;

– с противоосколочными элементами (шторами, завесами) на базе тканей из композитных материалов.

Конструкция таких приспособлений несложная, однако достаточно эффективная. В состав входят усиливающие сетчатые конструкции, которые препятствуют контакту БВС или переносимого им боевого заряда с защищаемым объектом, и опоры, на которых держатся эти сети. Кроме сеток используют ограждения из стальных тросов, препятствующих пролету БВС.

Конструктивной особенностью является опора, на которой будет держаться сама ЗОК. Существуют опоры двух видов: одиночные колонны/мачты и рамы. Схематично они представлены на рисунке 1.

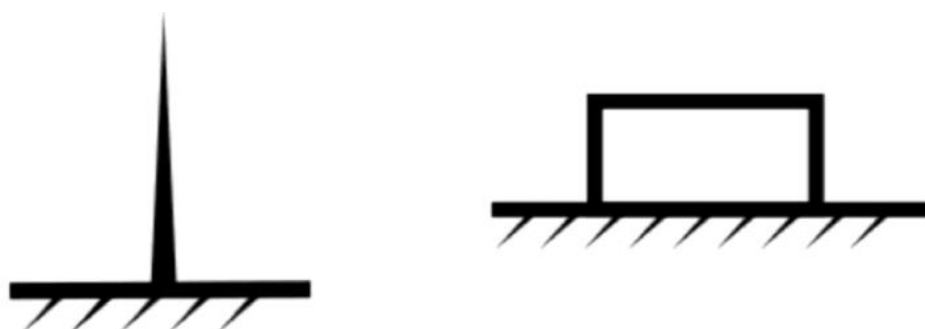


Рис. 1. Схемы опор ЗОК

Для усиления конструкции и лучшей жесткости можно использовать растяжки, сделанные из стальных тросов. Кроме основных ограждений существуют дополнительные, целью которых является улавливание осколочных поражающих элементов боевой части БВС.

На сегодняшний день перспективными системами пассивной защиты от атак БВС являются те, которые применяют композиционные и полимерные материалы в конструкции. Например, компания TENET, изготавливает продукцию из полипропилена и других легких материалов. Благодаря используемым материалам защитные конструкции намного легче металлических, долговечные и легко монтируемые. Легкие сети, согласно своду правил 542.1325800.2024, применяются для 3 и 4 класса защиты. Некоторые характеристики легких сетей ЗОК указаны в таблице 3 [6].

Таблица 3

Характеристики легких сетей ЗОК

Материал	Размер ячейки, см	Вес, г/м ²	Класс горючести	Антистатик	Температурный режим, °С	Нагрузка, кН/м
Полипропилен	40*40	150	Г2 с антипиреном	возможен	-40...+90	12

Тяжелые сети применяются для 1 и 2 класса защиты. Основные характеристики тяжелых сетей указаны в таблице 4 [6].

Таблица 4

Характеристики легких сетей ЗОК

Материал	Размер ячейки, см	Вес, г/м ²	Класс горючести	Антистатик	Температурный режим, °С	Нагрузка, кН/м
Полипропилен	40*40 65*65	650	Г2 с антипиреном	возможен	-50...+100	50

Использование защитных сетей демпфируют удар БВС и лишают его способности передвижения за счет фиксации пропеллеров. Эффективность противодействия металлических конструкции обеспечивается путем крепления несущих тросов с подвешенным противовесом, которые растягиваются при столкновении с летающим объектом, но не рвутся, а гасят кинетическую энергию. Например, ЗОК «Стальной купол» способен выдержать до 30 последовательных попаданий БВС в одну точку, так как сеть самозатягивается [7].

Полимерные барьерные конструкции являются высокотехнологичным решением современных задач обеспечения безопасности критически важных и потенциально опасных объектов. Однако для решения задач обеспечения безопасности объектов охраны от угроз связанных с применением БВС,

целесообразно объединить инженерные и технические системы противодействия в единый комплекс, основанный на применении самых современных технологий и разработок.

ЛИТЕРАТУРА

1. Сидоров А. В. Обеспечение безопасности режимных объектов органов внутренних дел с использованием современных технических средств и технологий / А. В. Сидоров // Охрана, безопасность, связь. – 2024. – № 9-1. – С. 137–145.

2. Сидоров А. В. К вопросу обеспечения безопасности режимных объектов / А. В. Сидоров // Охрана, безопасность, связь. – 2024. – № 9-1. – С. 145–150.

3. Сидоров А. В. Обеспечение безопасности объектов топливно-энергетического комплекса от актов незаконного вмешательства, совершаемых с применением беспилотных воздушных судов / А. В. Сидоров // Охрана, безопасность, связь. – 2025. – № 10-1. – С. 49–54.

4. Сидоров А. В. Совершенствование защищенности объектов уголовно-исполнительной системы в условиях противодействия беспилотным воздушным судам / А. В. Сидоров, Е. Ю. Климок // Техника и безопасность объектов уголовно-исполнительной системы : Сборник материалов Международной научно-практической конференции. В 4-х томах, Воронеж, 14–15 мая 2025 года. – Воронеж : ИП Копыльцов П. И., 2025. – С. 289–292.

5. Защитные и ограждающие конструкции от беспилотных летательных аппаратов. Правила проектирования: свод правил 542.1325800.2024 // СПС «КонсультантПлюс» (дата обращения 25.10.2025)

6. URL: <https://tenet-zavod.ru> – Официальный сайт компании TENET.

7. URL: <https://steel-kupol.ru/> – Официальный сайт компании «Стальной купол».

СВЕДЕНИЯ ОБ АВТОРЕ

Сидоров Александр Викторович.

Заместитель начальника кафедры радиотехнических систем и комплексов охранного мониторинга.

Кандидат технических наук.

Воронежский институт МВД России.

E-mail: asidic@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Sidorov Aleksandr Viktorovich.

Deputy Head of the Department of Radio Engineering Systems and Security Monitoring Complexes.

Candidate of Engineering Sciences.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: asidic@mail.ru.
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: беспилотное воздушное судно; охраняемый объект; защита; меры противодействия; технический комплекс.

Keywords: unmanned aircraft; protected object; protection; counteraction measures; technical complex.

УДК 621.37

**ПРАВОВЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ
БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ В ОХРАНЕ ОБЪЕКТОВ**

**LEGAL ASPECTS OF USING UNMANNED AIRCRAFT
IN PROTECTING OBJECTS**

В статье представлены правовые аспекты, регламентирующие применение беспилотных воздушных судов для организации охраны объектов.

The article presents the legal aspects governing the use of unmanned aerial vehicles for the protection of facilities.

Стремительное развитие технологий делает беспилотные воздушные суда (БВС) все более доступным и эффективным инструментом для обеспечения безопасности. Интеграция БВС в системы охраны объектов представляет собой закономерный этап технологической эволюции в сфере безопасности. Использование технологии БВС предполагает принципиально новые возможности для мониторинга обширных территорий, оперативного реагирования на инциденты и превентивного выявления угроз.

Прежде чем перейти к анализу правовых актов обозначим, почему БВС рассматриваются для обеспечения безопасности объектов:

1. Мобильность: БВС способно быстро достичь любой точки обширной территории, обойти архитектурные преграды и предоставить видео в реальном времени с определенной высоты.

2. Эффективность: один оператор может контролировать периметр и внутреннюю зону объекта, где раньше требовалось несколько патрульных.

3. Автоматизация: маршруты могут быть заранее запрограммированы, а с помощью технологий компьютерного зрения БВС способен автоматически обнаруживать нарушения (проникновение, оставленные предметы).

4. Документирование: запись видео служит доказательством при расследовании инцидентов.

Законодательство Российской Федерации в области беспилотных воздушных судов (БВС) условно можно разделить на две группы: нормативные правовые акты, регламентирующие применение БВС и нормативные правовые акты, регламентирующие противодействие БВС. На рисунке 1 представлены нормативные правовые акты, регламентирующие применение БВС для решения различных задач.

Применение БВС для обеспечения безопасности объекта требует баланса между инновациями и соблюдением законности. Необходимо не только обеспечить безопасность объекта, но и защиту прав граждан и неприкосновенность частной жизни.

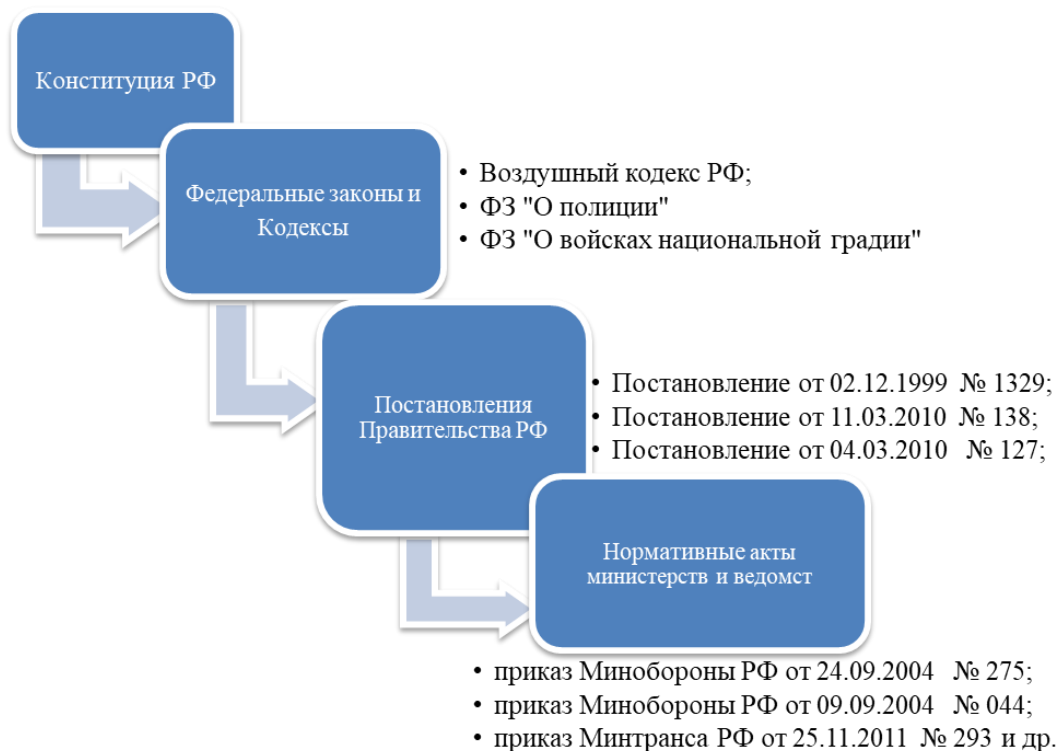


Рис. 1. Нормативные правовые акты в области применения БВС

Исходя из анализа нормативных правовых актов, представленных на рисунке 1 можно сформулировать правовые аспекты, которые необходимо учитывать при использовании БВС для организации охраны объектов.

Основные правовые аспекты можно разделить на несколько блоков:

1. Требования к владельцу дрона и полетам: БВС с взлетной массой более 250 граммов подлежат обязательной регистрации в Росавиации. Дрон получает государственный номер, который должен быть нанесен на его корпус. Для охраны объектов, как правило, используются модели тяжелее этого лимита, поэтому регистрация необходима.

Для проведения полетов необходимо получить разрешение на использование воздушного пространства. Это делается путем подачи плана полета. Исключение составляют полеты в зонах, где это разрешено без подачи плана, но для полетов над охраняемыми объектами такое исключение маловероятно. Категорически запрещены полеты над объектами критической инфраструктуры, режимными территориями, а также вблизи аэропортов без специального согласования.

Использование БВС над городами и поселками регулируется отдельно. Для аэросъемки и наблюдения за объектами в черте города

требуется соблюдение дополнительных требований по безопасности и, как правило, специальное разрешение.

2. Требования к оператору (пилоту): оператор обязан пройти регистрацию в Росавиации как оператор БВС; иметь минимальные знания в области авиации, правил использования воздушного пространства и эксплуатации конкретного типа БВС.

3. Обработка персональных данных. Это один из самых сложных и значимых аспектов в контексте охраны. Любая видеозапись, на которой можно идентифицировать человека (его лицо, фигуру, автомобильный номер), считается обработкой персональных данных согласно 152-ФЗ «О персональных данных». Закон предусматривает исключение: обработка персональных данных без согласия субъекта возможна для осуществления охранной деятельности в соответствии с законодательством (п. 6 ч. 1 ст. 6 152-ФЗ). Однако это право не является абсолютным.

Зоны наблюдения должны быть ограничены охраняемой территорией и периметром. Съемка прилегающих общедоступных территорий (например, тротуара) может быть признана чрезмерной. Необходимо обеспечить защиту этих данных от несанкционированного доступа.

4. Вопросы частной жизни и съемка соседних территорий. Даже если БВС не нарушает правил полетов, его камеры могут захватывать частные владения, находящиеся за пределами охраняемого объекта. Это может быть расценено как вторжение в частную жизнь по ст. 152.2 Гражданского кодекса РФ. Чтобы минимизировать риски, следует: настраивать углы обзора камер так, чтобы минимизировать захват чужих территорий; использовать технологии размытия в реальном времени для областей, не относящихся к объекту охраны.

Интеграция БВС в комплекс охранных мероприятий порождает сложный комплекс правовых коллизий, находящихся на стыке административного, гражданского и информационного права.

Перспективы развития правового регулирования в данной области видятся в создании специализированных норм, учитывающих специфику использования БВС именно в охранной деятельности. Это позволит преодолеть существующий правовой вакуум и создать ясные, понятные правила для всех участников данных правоотношений. Только при условии синхронного развития технологий и права БВС смогут реализовать свой потенциал в сфере охраны объектов, став не просто техническим новшеством, а полноценным и легитимным инструментом обеспечения безопасности.

ЛИТЕРАТУРА

1. Ворона В. А. Концептуальные основы создания и применения системы защиты объектов : учебное пособие / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия-Телеком, 2017. – 196 с.
2. Толстых О. В. Правовое регулирование вопросов противодействия беспилотным воздушным судам на объектах охраны / О. В. Толстых // Научный бюллетень Воронежского института МВД России. – 2024. – № 4. – С. 167–169.
3. Жилин Р. А. Снижение размерности задачи экспертизы при исследовании объектов коалициями экспертов / Р. А. Жилин // Охрана, безопасность, связь. – 2020. – № 5-2. – С. 25–30
4. URL: <http://www.consultant.ru> – Справочно-правовая система «КонсультантПлюс».
5. URL: <http://www.garant.ru> – Справочно-правовая система по законодательству Российской Федерации «Гарант».
6. URL: <http://www.pravo.gov.ru> – Официальный интернет-портал правовой информации «Право».

СВЕДЕНИЯ ОБ АВТОРЕ

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, г. Воронеж, проспект Патриотов, 53.

Tolstykh Olga Vladimirovna.
Associate Professor of the Department of Radio Engineering Systems and Security Monitoring Complexes.
Candidate of Technical Sciences.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: tov48@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: беспилотные воздушные суда; правовое регулирование; охрана объектов; безопасность.

Keywords: unmanned aerial vehicles; legal regulation; object security; safety.

УДК 342.9

А. В. Чаплыгин, А. В. Гребенкин, А. И. Янгиров

**ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ.
НАСУЩНАЯ ПОТРЕБНОСТЬ ИЛИ ВЫНУЖДЕННАЯ МЕРА**

**ELECTROMAGNETIC COMPATIBILITY.
URGENT NEED OR NECESSARY MEASURE**

В статье в доступной форме рассматриваются вопросы, связанные с явлением электромагнитной совместимости, история возникновения проблемы, примеры электромагнитной несовместимости, источники электромагнитных помех и требования к техническим средствам в части ЭМС.

This article examines in an accessible manner the issues related to electromagnetic compatibility. It covers the history of the problem, examples of electromagnetic incompatibility, sources of electromagnetic interference, and requirements for EMC-related technical equipment.

Трагедия на авианосце «Форрестол» развернулась утром 29 июля 1967 года в Тонкинском заливе, где царила идеальная тропическая погода, нарушаемая лишь легким бризом. В это время на палубе корабля авиатехники готовили самолеты к новой бомбардировочной миссии по «тропе Хо Ши Мина».

Катастрофа началась с неожиданного инцидента – самопроизвольного старта ракеты «Zuni» с истребителя F-4 «Фантом II», только что завершившего боевой вылет. Снаряд пронесся над палубой и поразил топливный бак штурмовика A-4 «Скайхок» (борт № 405). Хотя взрывчатое вещество ракеты не детонировало благодаря предохранителю, удар привел к разрыву бака и мгновенному воспламенению выплеснувшегося авиационного топлива. Цепная реакция была стремительной: резкое тепловое воздействие привело к взрывам баков соседних самолетов, а через несколько минут огонь достиг авиационных бомб. Их детонация пробила бронированную палубу, открыв путь огненному потоку в жилые помещения команды и ангар корабля.

Борьба с огнем продолжалась много часов. На летной палубе его удалось обуздать к 12:15, а во внутренних отсеках – только к 13:42. Окончательно пожар был потушен к 4 утра следующего дня. Итогом стали 134 погибших и 161 раненый моряк. В отчаянной попытке остановить катастрофу экипаж был вынужден сбросить за борт множество авиационной техники, из которой 21 самолет был официально списан. Материальный ущерб (без учета потерянных самолетов) составил 72 миллиона долларов. Следствие пришло к выводу, что наиболее вероятной причиной несанкционированного пуска стало электромагнитное излучение корабельного радара, которое через дефектный экранированный кабель вызвало сбой в электронике самолета.

Этот случай, похожий на сценарий голливудского фильма-катастрофы студии Columbia Pictures, но, увы, эта суровая реальность служит ярким примером, почему для электронных устройств, особенно предназначенных для жизнеобеспечения и безопасности, существует одно из важнейших требований – электромагнитная совместимость (ЭМС).

ЭМС – это свойство электронного оборудования работать с заданной эффективностью в определенной электромагнитной обстановке, не генерируя при этом недопустимых для других устройств помех. Под электромагнитной обстановкой подразумевается совокупность всех электромагнитных явлений в конкретной зоне, а помехой считается любое такое явление, которое ухудшает или может ухудшить работу аппаратуры.

Исторически вопросы ЭМС возникли практически одновременно с появлением первых радиотехнических устройств и были связаны в основном с распределением используемых радиочастот и противодействием помехам при приеме полезных радиосигналов, появилась потребность учета ранее игнорируемых видов помех и разработки методов и подходов в борьбе с ними.

С течением времени борьба с помехами получила широкое развитие и обрела отдельное направление в радиоэлектронике. Различные методы подавления помех начали широко использоваться в телевизионных системах, средствах связи (проводных и радио), разнообразных радиоэлектронных комплексах как в быту, так и в промышленности, на транспорте (корабли, самолеты, электропоезда, автомобили).

При современном стремительном росте числа различных информационных и телекоммуникационных систем, повышении объемов передаваемой и принимаемой цифровой информации на фоне увеличения количества и мощности электрооборудования, способного генерировать сильные помехи, проблемы ЭМС будут лишь усугубляться без принятия соответствующих мер.

На рисунке 1 схематично изображены потенциальные источники электромагнитных помех.

Наиболее показательными примерами влияния электромагнитной несовместимости электронных устройств являются:

- нарушение штатного функционирования и полные отказы систем, управляющих оборудованием и технологическими процессами;
- сбои в работе электронных систем контроля и управления, используемых в быту, на производстве и на транспорте, которые вызваны как внешними электромагнитными помехами, так и внутренней несовместимостью компонентов радиоэлектронной аппаратуры;
- отказы критически важных систем для навигации, наведения и посадки летательных аппаратов и другой подобной техники;
- потеря информации в цифровых системах приема и передачи данных.

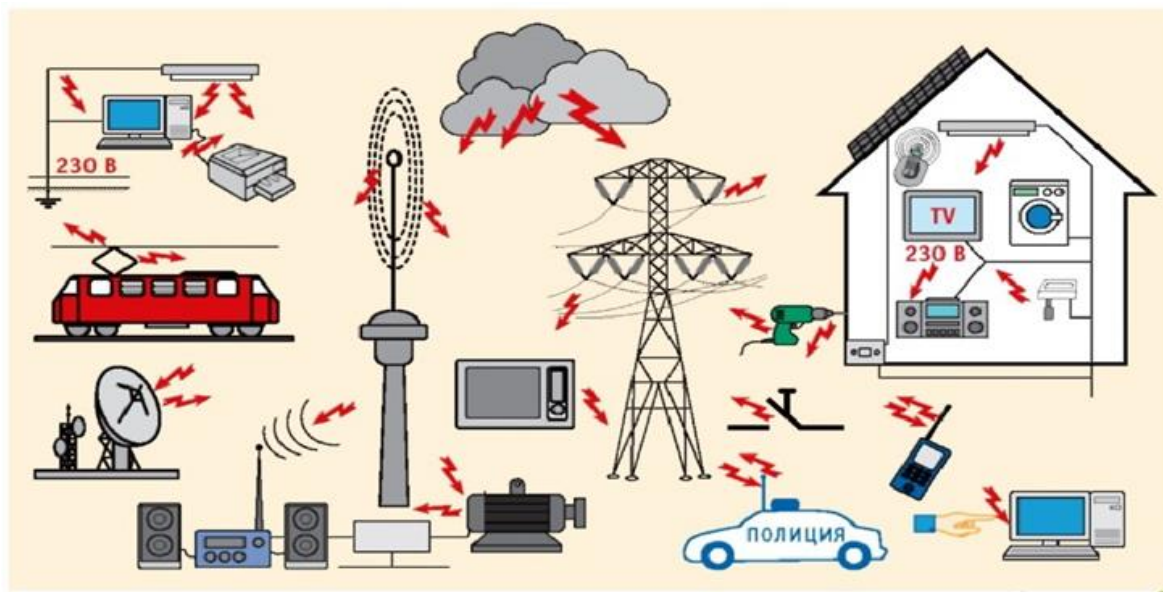


Рис. 1. Потенциальные источники электромагнитных помех

Несоблюдение норм ЭМС может привести к критическим отказам медицинского оборудования, используемого для диагностики и поддержания жизни пациентов. В группе повышенного риска находятся такие устройства, как кардиостимуляторы и аппараты гемодиализа («искусственная почка»). Кроме того, широко распространены данные о негативном влиянии на человеческий организм электромагнитных полей, генерируемых разнообразной радиоэлектронной аппаратурой. Наибольшую опасность представляет высокочастотное излучение от таких источников, как мобильные телефоны, микроволновые печи, радары, а также станции спутниковой и релейной связи. Воздействие электромагнитного излучения на здоровье человека может быть причиной развития различных опухолей, поражения сердца и нервной системы, различных нарушений генного порядка.

Источников электромагнитных помех, способных оказывать влияние на человека и электронную аппаратуру, существует великое множество, но наиболее распространенными являются следующие виды:

1) кратковременные импульсные помехи (наносекундные): их основная причина – коммутационные процессы в механических контактах (реле, выключатели) или искрообразование, например, в коллекторных узлах электродвигателей;

2) мощные импульсные наводки (микросекундные): возникают при коммутации реактивных нагрузок в силовых цепях, таких как катушки индуктивности, соленоиды и конденсаторы, другим частым источником являются интенсивные электромагнитные всплески от грозовых разрядов;

3) помехи от статического электричества: формируются в результате накопления заряда на диэлектриках и его последующего быстрого стекания при контакте с проводящей поверхностью;

4) радиочастотные наводки: их распространенность непрерывно растет в связи с увеличением количества работающих радиопередающих устройств.

Для аналитических целей все эти помехи обычно объединяют в три обобщенные группы:

- кратковременные импульсные (наносекундные);
- мощные импульсные (объединяющие микросекундные и электростатические);
- радиочастотные.

При этом в реальных условиях большинство помех представляет собой сложную комбинацию перечисленных выше видов. Ряд происшествий, вызванных нарушениями ЭМС, приведен в таблице 1 – это как раз случаи, реально создавшие угрозы для людей.

Таблица 1

Инцидент и последствия	Установленная причина
Попадание ракеты «Экзосет» в английский эсминец «Шеффилд» в ходе Фолклендского конфликта. Пожар и гибель корабля	Принудительное отключение радара противоракетной обороны во время сеансов связи
Отказы навигационной аппаратуры на самолетах гражданской авиации США, проявлявшиеся в ошибочном изменении курса	Влияние электронных устройств пассажиров (телефоны, компьютеры, плееры, камеры) на навигационные приборы
Отказы радиоканальных станций, обеспечивающих безопасность полетов, в аэропорту США. Угроза для пассажиров	Воздействие электромагнитного поля от электронной кассовой машины, расположенной в миле от аэропорта
Сбой в компьютеризированном пульте управления клапанами на заводе полупроводников в Великобритании. Утечка хлора	Воздействие на пульт по цепям питания импульсных напряжений от переходных процессов
В США произошли сбои в работе медицинской аппаратуры: в реанимобиле отключились монитор и дефибриллятор, а в больнице некорректно работающие респираторные мониторы стали причиной смерти пациента и несли риски для остальных больных	Влияние электромагнитного излучения от радиопередатчиков и электроинструментов на медоборудование
Остановка автомобилей на автобане в Германии в районе расположения мощной радиостанции. Риск аварий	Воздействие мощного радиосигнала на электронику автотранспорта

Таким образом, очевидны причины повышенного внимания мирового сообщества к вопросам электромагнитной совместимости. Этому способствует развитие и активное применение международных и государственных нормативов, регламентирующих соответствие по ЭМС для широкого спектра технических устройств. Требования ЭМС для различных видов электронной техники установлены множеством стандартов. Одних базовых стандартов порядка 50.

Особое внимание уделяется ЭМС в отношении электронных устройств, предназначенных для работы в системах охраны, безопасности, жизнеобеспечения, в различных производственных процессах, а также в бытовых условиях.

Так, например, в соответствии с «Едиными требованиями к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально-противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации» применяется ГОСТ Р 50009-2000 «Совместимость технических средств электромагнитная. Технические средства охранной сигнализации. Требования и методы испытаний».

Стандарт устанавливает требования, позволяющие всесторонне и эффективно тестировать технические средства охраны (ТСО) на устойчивость к основным электромагнитным помехам. Также им определены максимально допустимые уровни помех, излучаемых данным оборудованием. Номенклатура этих требований к средствам, соответствующим нормам ЭМС, представлена в таблице 2.

Таблица 2

Наименование требования, нормы	Условное обозначение метода испытаний
1. Требование устойчивости к микросекундным импульсным помехам большой энергии.	УК 1
2. Требование устойчивости к наносекундным импульсным помехам.	УК 2
3. Требование устойчивости к кратковременным прерываниям напряжения электропитания переменного тока.	УК 3
4. Требование устойчивости к длительным прерываниям напряжения электропитания переменного тока.	УК 4
5. Требование устойчивости к искажению синусоидальности напряжения электропитания.	УК 5
6. Требование устойчивости к кондуктивным помехам, наведенным радиочастотными электромагнитными полями.	УК 6
7. Требование устойчивости к радиочастотному электромагнитному полю.	УИ 1
8. Требование устойчивости к электростатическим разрядам.	УЭ 1
9. Нормы кондуктивных промышленных радиопомех.	ЭК 1
10. Нормы излучаемых промышленных радиопомех.	ЭИ 1

С целью оценки надежности работы ТСО в разнообразных условиях (таких как уличная среда, помещения с низким энергопотреблением, промышленные объекты и бытовое применение) стандарт определяет уровни интенсивности помеховых воздействий при тестировании, а также критерии исправного функционирования аппаратуры. Действие стандарта распространяется на стационарные, подвижные и переносные (носимые) устройства.

Процедура испытаний включает два ключевых аспекта: воздействие на оборудование нормированными помехами и замер уровня создаваемых им электромагнитных помех. Взаимодействие с внешней электромагнитной средой происходит через специальные интерфейсы, называемые портами. К ним относятся точки соединения: разъемы, клеммы, корпус, стыки кабелей и другие границы раздела. В частности,

порт корпуса представляет собой физический контур технического средства, через который как излучаются создаваемые им электромагнитные поля, так и проникают внешние помехи.

Комплекс испытаний на ЭМС, регламентированный стандартом, может быть представлен в виде схемы. На рисунке 2 с помощью стрелок отображены: конфигурация тестируемого образца, условные обозначения методов испытаний, а также точки приложения помех и проведения измерений.

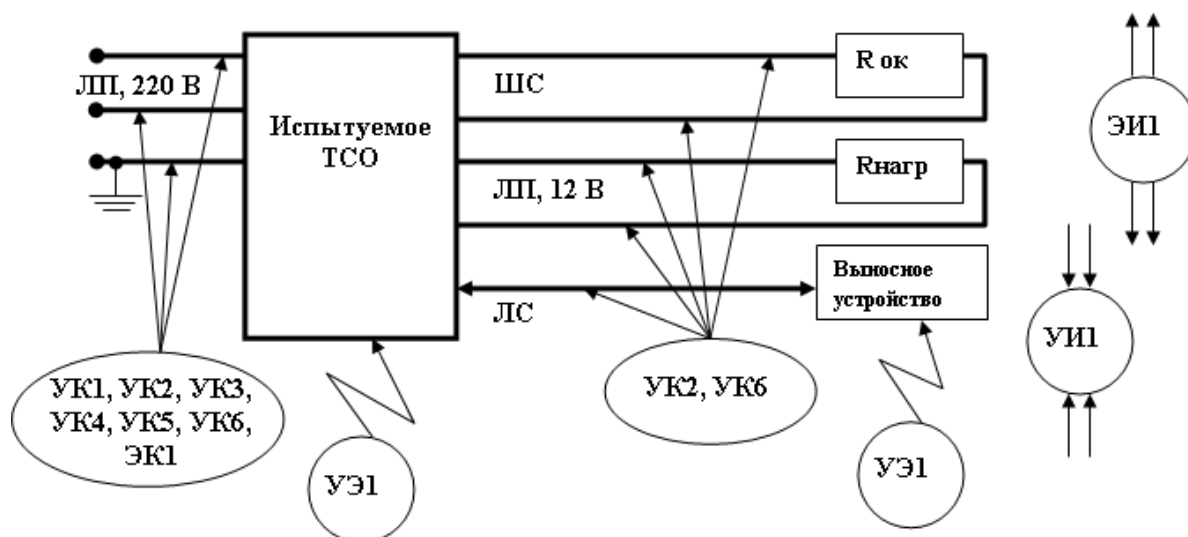


Рис. 2. Конфигурация объекта испытаний

Стандарт определяет нормативные значения для ТСО относительно предельно допустимых уровней промышленных радиопомех: как кондуктивных, то есть распространяющихся по проводящим средам, так и излучаемых в окружающее пространство.

Необходимо отметить, что процедура испытаний ТСО на ЭМС весьма сложна и трудоемка. Во-первых, требуются специальные помещения, так как все измерения радиопомех, излучаемых ТСО должны проводиться в нормированных условиях. Особые требования к помещению предъявляются при испытаниях ТСО на устойчивость к электромагнитным помехам и излучению. Во-вторых, необходимо соответствующее аттестованное испытательное оборудование и поверенные средства измерений.

На рисунке 3 представлена незначительная часть испытательного оборудования для проведения испытаний ТСО на ЭМС.

Самым дорогостоящим оборудованием является экранированная безэховая камера с комплектом генераторов, приемников, передающих и приемных антенн. Стоимость такого испытательного оборудования может составлять десятки миллионов рублей.

Все испытания на ЭМС должны проводиться в специализированных аккредитованных лабораториях или центрах.

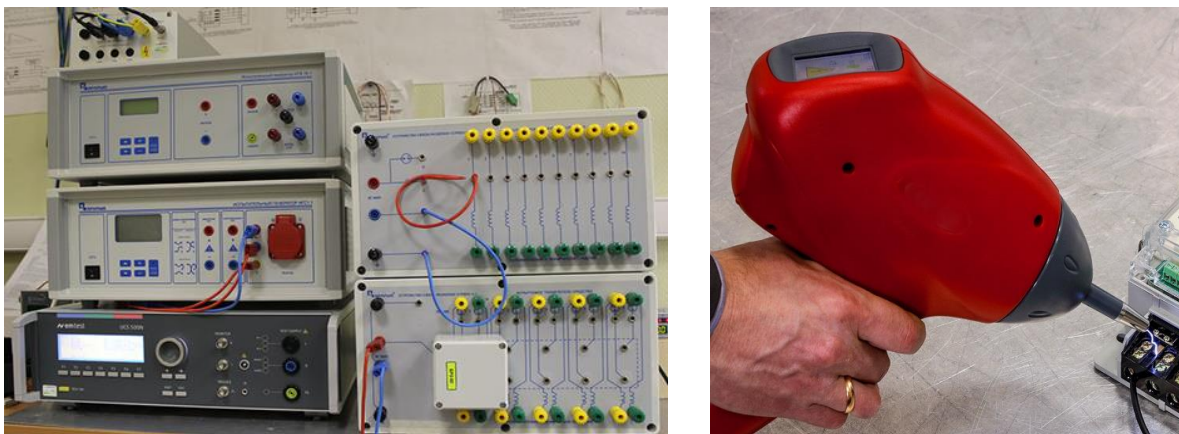


Рис. 3. Испытательное оборудование

В настоящее время ГОСТ Р 50009-2000 входит в перечень стандартов, в результате применения которых на добровольной основе обеспечивается соблюдение требований технического регламента таможенного союза «Электромагнитная совместимость технических средств» ТР ТС 020/2011. Данная ситуация является фактором риска применения недоброкачественной продукции ТСО на отечественном рынке.

ЛИТЕРАТУРА

1. Электромагнитная совместимость. Безопасность электронных систем и аппаратуры, защита окружающей среды и здоровья человека // Электроника: Наука. Технология. Бизнес. – 2000. – № 2. – С. 5–7.
2. Воршевский А. А. Электромагнитная совместимость судовых технических средств / А. А. Воршевский, В. Е. Гальперин // Судовые электроэнергетические комплексы и системы. – 2006. – С. 106–114.
3. Кузнецов Алексей. Об импульсных помехах, приводящих к непредсказуемому поведению цифровых устройств / А. Кузнецов // Схемотехника. – 2004. – № 8, 9.
4. Основные понятия в области ЭМС. Защита от излучений. Электромагнитное экранирование: Alfapol.ru. 17.07.2013.
5. ГОСТ Р 50009-2000. Совместимость технических средств электромагнитная. Технические средства охранной сигнализации. Требования и методы испытаний. – Москва : Стандартинформ, 2020. – 10 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Чаплыгин Андрей Викторович.

Научный сотрудник отделения лабораторных исследований и испытаний.

Научно-исследовательский центр «Охрана» Федеральной службы войск национальной гвардии Российской Федерации.

E-mail: ch-a-v2007@yandex.ru

Россия, 111539, г. Москва, ул. Реутовская, 12Б.

Гребенкин Анатолий Викторович.
Инженер-лаборант отделения лабораторных исследований и испытаний.

Научно-исследовательский центр «Охрана» Федеральной службы войск национальной гвардии Российской Федерации.

E-mail: laboratorianic@yandex.ru

Россия, 111539, г. Москва, ул. Реутовская, 12Б.

Янгиров Адиль Илдарович.

Начальник отделения лабораторных исследований и испытаний.

Научно-исследовательский центр «Охрана» Федеральной службы войск национальной гвардии Российской Федерации.

E-mail: Adil-Yan@yandex.ru

Россия, 111539, г. Москва, ул. Реутовская, 12Б.

Chaplygin Andrey Viktorovich.

Researcher at the Laboratory Research and Testing Department.

Federal State Institution Research Center «Ohrana» of the Federal Service of the National Guard Troops of the Russian Federation.

E-mail: ch-a-v2007@yandex.ru

Russia, 111539, Moscow, Reutovskaya str., 12B.

Grebenkin Anatoly Viktorovich.

Laboratory Engineer at the Laboratory Research and Testing Department.

Federal State Institution Research Center «Ohrana» of the Federal Service of the National Guard Troops of the Russian Federation.

E-mail: laboratorianic@yandex.ru

Russia, 111539, Moscow, Reutovskaya str., 12B.

Yangirov Adil Ildarovich.

Head of the Laboratory Research and Testing Department.

Federal State Institution Research Center «Ohrana» of the Federal Service of the National Guard Troops of the Russian Federation.

E-mail: Adil-Yan@yandex.ru

Russia, 111539, Moscow, 12B Reutovskaya str.

Ключевые слова: электронное устройство; чувствительность к электромагнитным помехам; внешнее электромагнитное поле; требования безопасности; электромагнитная обстановка; электромагнитная совместимость.

Keywords: electronic device; sensitivity to electromagnetic interference; external electromagnetic field; safety requirements; electromagnetic environment; electromagnetic compatibility.

УДК 537.86

**О РАЗРАБОТКЕ МЕТОДА КОЛИЧЕСТВЕННОЙ ОЦЕНКИ
ЗАЩИЩЕННОСТИ ОТКРЫТЫХ ОПЕРАЦИОННЫХ СИСТЕМ
АРМ ОВД РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ON THE DEVELOPMENT OF A METHOD FOR QUANTITATIVE
ASSESSMENT OF THE SECURITY OF OPEN OPERATING SYSTEMS
AUTOMATED WORKSTATIONS OF THE INTERNAL AFFAIRS
AGENCIES OF THE RUSSIAN FEDERATION**

В статье рассматриваются разработанные Метод количественной оценки защищенности открытых операционных систем автоматизированных рабочих мест органов внутренних дел Российской Федерации и программно-методический комплекс количественной оценки защищенности открытых операционных систем автоматизированных систем органов внутренних дел Российской Федерации, а также их эффективность в сравнении с традиционными подходами.

The article discusses the developed Method for quantifying the security of open operating systems of automated workplaces of the internal affairs bodies of the Russian Federation, as well as a software and methodological package for quantifying the security of open operating systems of automated systems of the internal affairs bodies of the Russian Federation, as well as their effectiveness in comparison with traditional approaches.

Бесперебойное функционирование автоматизированных рабочих мест (АРМ) в системе войск национальной гвардии Российской Федерации является важной составляющей для организации управления силами и средствами, обеспечения взаимодействия с другими правоохранительными органами и государственными структурами, а также обеспечения безопасности информации. Уязвимости в защите АРМ создают прямые риски для выполнения войсками национальной гвардии возложенных на них государственных функций. Обеспечение защиты автоматизированных рабочих мест (АРМ) органов внутренних дел Российской Федерации (ОВД) представляет собой сложную многогранную задачу, требующую комплексного применения мер физической, программной и аппаратной защиты.

Правильная оценка защищенности операционных систем (ОС) и её настройка является важной составляющей по защите АРМ. В особенности атакам со стороны злоумышленников подвержены ОС АРМ, в которых не обрабатывается информация, составляющая государственную тайну, так называемые открытые ОС.

Именно подобные АРМ часто становятся первоочередной мишенью для злоумышленников в силу их однотипности и широкой распространенности. Массовый характер использования подобных ОС создает для нарушителей унифицированное поле для атаки, позволяя разрабатывать и применять стандартизированные методы эксплуатации уязвимостей. Относительно меньшая, по сравнению со специализированными защищенными ОС, строгость предъявляемых к ним требований по настройке и сопровождению зачастую приводит к ослаблению режима безопасности, формируя уязвимости в информационной инфраструктуре.

В ранее проведенных исследованиях [1–7] были представлены подходы к формированию методики количественной оценки защищенности открытых ОС. В настоящее время на основе указанных исследований разработаны Метод количественной оценки защищенности открытых ОС АРМ ОВД (Метод), а также программно-методический комплекс количественной оценки защищенности открытых операционных систем автоматизированных систем органов внутренних дел Российской Федерации (ПО) [8].

Разработанные Метод и ПО позволяют оценить защищенность открытых ОС за счет формализованного подхода, который доступен специалистам общего профиля и не требует привлечения узкоспециализированных экспертов. В отличие от традиционных подходов, требующих анализа значительного объема нормативных документов, методических рекомендаций и руководств по эксплуатации ОС, представленные Метод и ПО позволяют свести оценку защищенности ОС к количественному анализу требований безопасности, установленных в документации на сертификацию по «Общим критериям». «Общие критерии» на ОС установлены в серии международных стандартов ISO/IEC 15408 [9-11], в Российской Федерации применяется идентичная серия стандартов ГОСТ Р ИСО/МЭК 15408 [12–14].

В качестве основы для оценки защищенности ОС применяется эталонный профиль защиты (ПЗ) ПЗ ИТ.ОС.А4.ПЗ – наиболее защищенный открытый ПЗ, предназначенный для применения на автоматизированных системах общего назначения (тип «А»). Выбор данного ПЗ обусловлен тем, что данные ОС ориентированы на выполнение разнообразных вычислительных задач и обладают расширенным функционалом, что повышает их универсальность и делает более подходящими для применения в ОВД по сравнению со специализированными ОС категорий «Б» и «В». В целях оценки эффективности разработанных Метода и ПО на базе ФКУ «НИЦ «Охрана» Росгвардии проведены экспериментальные исследования.

Контролируемыми вопросами в рамках экспериментального исследования (проверки) являлись:

- 1) проверка защищенности ОС, установленных на АРМ;

2) проведение мероприятий по повышению защищенности АРМ, сравнительный анализ эффективности традиционного подхода к настройке защищенности ОС и Метода с применением ПО;

3) оценка времени, необходимого для достижения оптимального уровня защищенности ОС различными способами;

4) определение итогового уровня защищенности ОС после настройки.

Экспериментальное исследование (проверка) проводилось комиссионно с участием специалистов по информационной безопасности, независимого специалиста и хронометриста в три последовательных этапа.

На I подготовительном этапе специалистом осуществлялась оценка исходного уровня защищенности ОС АРМ с применением разработанного ПО с фиксацией количественных и лингвистических показателей для последующего сравнения, после чего выполнялась переустановка ОС с учетом специфики решаемых задач и используемых программ.

На всех АРМ был установлен Microsoft Windows 7 Ultimate x64. С учётом потенциальных угроз, которые могут воздействовать на ОС были получены следующие показатели защищенности (табл. 1).

Таблица 1
Результаты I этапа

Усл. ном. АРМ	Показатель защищенности, %	Лингвистический показатель защищенности
1.	Microsoft Windows 7 Ultimate x64 [61%]	[Минимально защищенная система]
2.	Microsoft Windows 7 Ultimate x64 [61%]	[Средне защищенная система]
3.	Microsoft Windows 7 Ultimate x64 [61%]	[Средне защищенная система]
4.	Microsoft Windows 7 Ultimate x64 [61%]	[Средне защищенная система]

На II основном этапе два специалиста по информационной безопасности производили настройку защищенности ОС на четырех АРМ, применяя как традиционный подход, так и разработанные Метод с использованием ПО и документации по «Общим критериям».

Хронометраж работ выполнялся отдельным сотрудником, фиксирующим временные затраты на настройку каждого АРМ.

Результаты, полученные в ходе II этапа экспериментального исследования (проверки), представлены в таблице 2.

Таблица 2
Результаты II этапа

Результаты настройки традиционным способом	Результаты настройки с применением Метода и ПО
Усл. ном. АРМ: 1; Установленная ОС: Red OS 8.0.2; Способ настройки: традиционный; Время настройки: [2 ч. 34 мин.]	Усл. ном. АРМ: 2; Установленная ОС: Windows 10 (22H2); Способ настройки: с применением Метода и ПО; Время настройки: [1 ч. 27 мин.]
Усл. ном. АРМ: 3; Установленная ОС: Windows 10 (22H2); Способ настройки: традиционный; Время настройки: [3 ч. 7 мин.]	Усл. ном. АРМ: 4; Установленная ОС: Red OS 8.0.2; Способ настройки: с применением Метода и ПО; Время настройки: [1 ч. 44 мин.]

На III заключительном этапе осуществлялась перекрестная проверка качества выполненных работ посредством взаимного аудита настроек защищенности с использованием ранее разработанного перечня требований безопасности, состоящего из 24 пунктов и предоставленного специалистам в момент проведения аудита.

Результаты проведенного экспериментального исследования (проверки) демонстрируют, что в сравнении с традиционным способом время настройки ОС сократилось примерно на час, качество настройки ОС улучшилось на 3-4 пункта. Таким образом, применение разработанных Метода и ПО позволяет упростить процессы оценки и настройки открытых ОС АРМ ОВД.

ЛИТЕРАТУРА

1. Разработка автоматизированной системы расчета оценки защищенности операционных систем информационных систем на основе анализа требований безопасности / А. И. Янгиров, Е. А. Рогозин, Е. Ю. Никулина, А. В. Калач // Вестник Воронежского института ФСИН России. – 2022. – № 4. – С. 182–188. – EDN VNBXNZ.

2. Янгиров А. И. Расчет оценки защищенности открытых операционных систем на основе анализа требований безопасности по ГОСТ Р ИСО/МЭК 15408 / А. И. Янгиров, Е. А. Рогозин // Вопросы обеспечения безопасности в киберпространстве: Материалы Всероссийской научно-технической конференции, Махачкала, 16 декабря 2022 года. – Махачкала : Дагестанский государственный технический университет, 2022. – С. 243–248. – EDN EDHNEY.

3. Янгиров А. И. К вопросу оценки защищенности операционных систем, использующихся в автоматизированных информационных системах органов внутренних дел / А. И. Янгиров // Охрана, безопасность, связь. – 2023. – № 8-3. – С. 83–90. – EDN SLCGLG.

4. Алгоритмизация расчета оценки защищенности операционных систем АИС ОВД, разработанного на основе анализа требований безопасности ГОСТ Р ИСО/МЭК 15408 и возможных угроз / А. И. Янгиров, Е. А. Рогозин, О. И. Бокова, С. Б. Ахлюстин // Вестник Дагестанского

государственного технического университета. Технические науки. – 2023. – Т. 50, № 3. – С. 167–171. – DOI 10.21822/2073-6185-2023-50-3-167-171. – EDN QIOPPE.

5. К вопросу проведения количественной оценки защищенности открытых операционных систем АС ОВД РФ на основе теории нечеткой логики / А. И. Янгиров, И. М. Янгиров, Е. А. Рогозин, С. Б. Ахлюстин // Охрана, безопасность, связь. – 2024. – № 9-1. – С. 163–170. – EDN FKQAIL.

6. Методический подход к количественной оценке защищенности открытых операционных систем АС ОВД / А. И. Янгиров, И. М. Янгиров, Е. А. Рогозин, С. Б. Ахлюстин // Вестник Дагестанского государственного технического университета. Технические науки. – 2024. – Т. 51, № 3. – С. 163–171. – DOI 10.21822/2073-6185-2024-51-3-163-171. – EDN PPUULY.

7. Математическая модель количественной оценки защищенности открытых операционных систем при их выборе в АС ОВД / А. И. Янгиров, Е. А. Рогозин, П. М. Дуплякин [и др.] // Вестник Дагестанского государственного технического университета. Технические науки. – 2025. – Т. 52, № 2. – С. 169–179. – DOI 10.21822/2073-6185-2025-54-2-180-189. – EDN SZBLQY.

8. Свидетельство о государственной регистрации программы для ЭВМ № 2025685462 Российская Федерация. Программно-методический комплекс количественной оценки защищенности открытых операционных систем автоматизированных систем органов внутренних дел Российской Федерации: № 2025685462: заявл. 15.09.2025: опубл. 23.09.2025 / А. И. Янгиров, Е. А. Рогозин [и др.] ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Воронежский государственный университет инженерных технологий».

9. ISO/IEC 15408-1:2022 «Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model».

10. ISO/IEC 15408-2:2022 « Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 2: Security functional components».

11. ISO/IEC 15408-3:2022 « Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 3: Security assurance components».

12. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

13. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.

14. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты оценки доверия к безопасности.

СВЕДЕНИЯ ОБ АВТОРАХ

Янгиров Адиль Илдарович.
Начальник отделения лабораторных исследований и испытаний.
Научно-исследовательский центр «Охрана» Федеральной службы войск национальной гвардии Российской Федерации.
E-mail: Adil-Yan@yandex.ru
Россия, 111539, г. Москва, ул. Реутовская, 12Б.

Рогозин Евгений Алексеевич.
Профессор кафедры автоматизированных информационных систем ОВД.
Доктор технических наук, профессор.
Воронежский институт МВД России.
E-mail: evgenirogozin@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Yangirov Adil Ildarovich.
Head of the Laboratory Research and Testing Department.
Federal State Institution Research Center «Ohrana» of the Federal Service of the National Guard Troops of the Russian Federation.
E-mail: Adil-Yan@yandex.ru
Russia, 111539, Moscow, Reutovskaya str., 12B.

Rogozin Evgeny Alekseevich.
Professor of the Department of Automated Information Systems of the Interior Ministry.
Doctor of Technical Sciences, Professor.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: evgenirogozin@yandex.ru
Russia, 394065, Voronezh, Prospekt Patriotov, 53.

Ключевые слова: количественная оценка защищенности; операционные системы; автоматизированное рабочее место; экспериментальное исследование.

Keywords: quantitative assessment of security, operating systems, automated workplace, experimental research.

УДК 004.056

ВСЕРОССИЙСКИЙ КРУГЛЫЙ СТОЛ
ПРОБЛЕМЫ АДАПТАЦИИ СОТРУДНИКОВ
ПОДРАЗДЕЛЕНИЙ ПО ДЕЛАМ НЕСОВЕРШЕННОЛЕТНИХ
НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ ПРОФЕССИОНАЛЬНОЙ
ДЕЯТЕЛЬНОСТИ И ПУТИ ИХ РЕШЕНИЯ

Д. В. Вечерникова

К ВОПРОСУ О НЕКОМПЛЕКТЕ ШТАТНОЙ ЧИСЛЕННОСТИ
ПОДРАЗДЕЛЕНИЙ ПО ДЕЛАМ НЕСОВЕРШЕННОЛЕТНИХ
ОРГАНОВ ВНУТРЕННИХ ДЕЛ И МИНИМИЗАЦИЕЙ
УВОЛЬНЕНИЙ В ПЕРВЫЕ ГОДЫ СЛУЖБЫ

ON THE ISSUE OF UNDERSTAFFING IN JUVENILE AFFAIRS UNITS
OF INTERNAL AFFAIRS BODIES AND MINIMIZING DISMISSALS
IN THE FIRST YEARS OF SERVICE

В статье рассматриваются некоторые вопросы некомплекта численности кадров в подразделениях по делам несовершеннолетних в органах внутренних дел. На основе анализа статистических данных МВД России автором отмечается, что основной проблемой профессиональной деятельности сотрудников по делам несовершеннолетних является некомплект личного состава, который существенно увеличивает общую рабочую нагрузку, тем самым снижает качество профилактической работы среди несовершеннолетних.

The article discusses some issues related to the shortage of personnel in the juvenile affairs units of the internal affairs bodies. Based on the analysis of statistical data from the Ministry of Internal Affairs of the Russian Federation, the author notes that the main problem in the professional activities of juvenile affairs officers is the shortage of personnel, which significantly increases the overall workload and thus reduces the quality of preventive work among minors.

В условиях продолжающейся специальной военной операции, возникновением новых вызовов и угроз усилением санкционного давления со стороны недружественных стран, Министерство внутренних дел Российской Федерации сосредоточило внимание на ряде критических важных задач. Одной из таких задач является минимизация кадрового оттока, обеспечения сохранности личного состава и поддержания высокого уровня морально-психологического состояния сотрудников, повышения их профессиональной грамотности. Согласно статистической отчетности МВД России число некомплекта личного аттестованного состава ВД России составило 145,0 тыс. ед. или 18,7% (2023 г.: 14,9%), федеральных

государственных гражданских служащих и работников – 27,6 тыс. ед. или 18,3% (2023 г.: 16,7%) [1]. При этом количество уволенных в 2024 году составило 74,5 тыс. единиц, что значительно превышает число принятых на службу, а количество уволенных на первом году службы составило 2 693 человек [1]. Уволенных сотрудников по делам несовершеннолетних от штатной численности службы по сравнению в 2023 годом увеличилось с 9,8% до 10,7% в 2024 году. Статистика же прошлых лет показывает не утешающую динамику: так, если в 2020 году было уволено 5,6%, то в 2024 году цифра уволенных возросла до 7,6% [1]. Таким образом, имеющийся кадровый некомплект существенно увеличивает рабочую нагрузку на инспектора по делам несовершеннолетних вследствие перераспределения между сотрудниками «свободных» участков. И такая дополнительная нагрузка не всегда оплачивается. Сотрудник, вынужденный тратить время на обслуживание дополнительных территорий, сталкивается не только с существенным увеличением временных, но и психолого-энергетических затрат, что в конечном счете приводит к эмоциональному выгоранию и снижению его работоспособности. Двойной режим работы часто вызывает физическое и психическое истощение, а недостаток времени для восстановления приводит к мысли о завершении службы в органах внутренних дел. Согласно статистике кадровой службы МВД России основными причинами увольнения участковых уполномоченных и сотрудников подразделений по делам несовершеннолетних 37,5% от общего числа составили уволенные по выслуге лет, дающей право на получение пенсии, а 45,7% по инициативе самого сотрудника [1]. И в данном аспекте возникает еще один проблемный вопрос о передаче опыта молодым сотрудникам. Если сотрудник подразделения по делам несовершеннолетних в силу неопытности не заметил, не обратил внимание на девиантное, делинквентное поведение подростка, далее будут вынуждены включаться в работу сотрудники оперативных служб, следствия и дознания, да, собственно, и вся правоохранительная система в целом. Если же сотрудник грамотно и профессионально выполняет свои обязанности, знает о неблагополучных семьях, о криминогенной обстановке и оперативно влияет на нее, он самостоятельно решает большинство потенциальных проблем в отношении данной категории и осуществляет профилактику правонарушений среди несовершеннолетних. Таким образом, задачи и полномочия инспектора по делам несовершеннолетних характеризуются как многофункциональные и комплексные, которые охватывают весь комплекс административной и служебной деятельности органов внутренних дел. Сотрудник подразделения по делам несовершеннолетних является не только представителем власти, но и юристом, и психологом, и педагогом, и наставником.

Обозначенная статистика свидетельствует о том, что некомплект кадров в органах внутренних дел представляет собой комплексную проблему, которая обусловлена рядом социально-экономических факторов. Необходимо отметить снижение привлекательности службы в органах внутренних дел как с экономической, так и социальной значимости. Наблюдается рост альтернативных предложений, заманчивых по своей сути для молодого сотрудника, таких как предложения более высокого уровня заработной платы и социальные пакеты (ранее были предусмотрены льготы по оплате коммунальных услуг, проезда в общественном транспорте и т.д., что являлось существенной поддержкой для сотрудника и тем более молодого специалиста, что также способствует оттоку кадров).

Для эффективного решения обозначенной проблемы необходимо внедрение комплекса мер, направленных на улучшение условий труда, повышение квалификации, а также обеспечение социальной поддержки.

Кроме того, необходимо повышать престиж профессии сотрудника органов внутренних дел – проведение информационных кампаний, направленных на формирование положительного общественного мнения о важности и значимости профессии, целесообразно организовывать встречи, в том числе с использованием средств массовой информации, с представителями профессии, которые могут поделиться своим опытом и достижениями, продемонстрировать высокое профессиональное мастерство.

Одним из основных факторов, влияющих на некомплект состава органов внутренних дел, является социальная поддержка. В связи с этим целесообразно расширить программы социальной поддержки, включая доступ к медицинским услугам и другим социальным гарантиям.

Это лишь некоторые предложения, которые будут способствовать улучшению ситуации с некомплектом в органах внутренних дел Российской Федерации, привлечению квалифицированных специалистов и повышению эффективности их труда.

ЛИТЕРАТУРА

1. Сведения о состоянии работы с кадрами органов внутренних дел Российской Федерации в 2024 году: Главное управление по работе с личным составом МВД России // Издано на оборудовании типографии ГУРЛС МВД России Москва, 2025 год

СВЕДЕНИЯ ОБ АВТОРЕ

Вечерникова Дина Васильевна.
Доцент кафедры административной деятельности органов
внутренних дел.

Кандидат юридических наук.
Краснодарский университет МВД России.
E-mail: kadovd@yandex.ru
Россия, 350005, г. Краснодар, ул. Ярославская, 128

Vechernikova Dina Vasilievna.
Associate Professor of the Department of Administrative Activities
of Internal Affairs Bodies.

Candidate of Law.
Krasnodar University of the Ministry of Internal Affairs
of the Russian Federation.
E-mail: kadovd@yandex.ru
Russia, 350005, Krasnodar, Yaroslavskaya str., 128.

Ключевые слова: подразделения по делам несовершеннолетних органов внутренних дел; профилактическая работа с несовершеннолетними; некомплект личного состава; материально-техническое обеспечение службы.

Keywords: juvenile affairs units of internal affairs bodies; preventive work with minors; shortage of personnel; logistics support for the service.

УДК 342.92

**ПРОФЕССИОНАЛЬНАЯ АДАПТАЦИЯ СПЕЦИАЛИСТОВ,
ВПЕРВЫЕ ПРИБЫВШИХ НА СЛУЖБУ В СИСТЕМЕ
ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ**

**PROFESSIONAL ADAPTATION OF SPECIALISTS WHO HAVE
ARRIVED FOR THE FIRST TIME TO WORK
IN THE LAW ENFORCEMENT SYSTEM**

В настоящей статье исследуются некоторые проблемы, возникающие у специалистов, впервые прибывших на службу в системе правоохранительных органов, после прохождения ими обучения, а также вопросы, касающиеся особенностей прохождения службы в органах внутренних дел.

This article explores some of the challenges faced by first-time employees in the internal affairs department of law enforcement agencies after completing their training, as well as the specific features of serving in the internal affairs department.

Одним из главных направлений по совершенствованию организации службы в органах внутренних дел, обеспечению эффективной деятельности и выполнению возложенных на данные органы задач является грамотный подбор кадров. В свою очередь адаптация сотрудников, принятых на службу в правоохранительные органы, играет наиболее важную роль в системе формирования кадров, поскольку грамотно обученные и подготовленные сотрудники будут наиболее эффективно выполнять возложенные на них задачи, обеспечивать авторитет и уважение к органам внутренних дел и формировать новое поколение будущих специалистов, располагая необходимым опытом, а в современных реалиях в принципе любое подразделение или организация, реализующая в своей основе управленческие и организационные функции, должна быть заинтересована в совершенствовании своей структуры и персонала [2, с. 99].

Следует отметить, что существует множество факторов, влияющих на эффективную адаптацию сотрудников, впервые прибывших на службу в системе правоохранительных органов, к которым можно отнести: содержание, характер, временные рамки процесса адаптации и др., на которые влияет ряд особенностей:

1. Особенность и определенный характер служебной деятельности, заключающийся в выполнении сотрудниками органов внутренних дел обязанностей, возложенных на них государством по обеспечению общественного порядка, общественной безопасности, профилактической

работе, пресечению и предупреждению административных правонарушений и уголовных преступлений в различных сферах и областях.

2. Четко выстроенная нормативно-правовая база, устанавливающая жесткий порядок служебной деятельности сотрудников органов внутренних дел, осуществляемой в строгом соответствии с Федеральным законодательством Российской Федерации и установленными локальными нормативными правовыми актами территориальных подразделений МВД России при проведении процессуальных действий и оперативно-розыскных мероприятий. За любое действие должностные лица правоохранительных органов несут ответственность, а контроль за грамотным выполнением их служебных обязанностей возложен на органы прокуратуры и суда.

3. Государственная и служебная тайна, обладающая определенной степенью секретности при осуществлении служебной деятельности должностных лиц, уполномоченных проводить предварительное расследование и осуществлять оперативно-розыскные мероприятия, также является особенностью, поскольку до момента поступления на службу молодые специалисты не сталкивались с таким понятием и некоторыми ограничениями и ответственностью, возлагаемыми на них в случае ее разглашения.

4. Наделение должностных лиц правоохранительных органов определенными государственными властными полномочиями, например, наделение должностных лиц, уполномоченных проводить предварительное расследование правом применения меры пресечения в отношении подозреваемого или обвиняемого в виде домашнего ареста или заключения под стражу по решению суда, если есть основание полагать, что данное лицо может скрыться, а также использовать меры пресечения в виде обязательства о явке для различных целей [1].

5. Оказание надлежащего противодействия лицам, которые не заинтересованы в том, чтобы предварительное расследование по уголовным делам проходило на должном уровне и в полном объеме. Одной из главных проблем, возникающих при нейтрализации последствий, которые могут возникнуть при негативном влиянии подозреваемых или обвиняемых, является конфликтный характер взаимодействия, что плохо сказывается на адаптации молодых специалистов сотрудников органов внутренних дел, впервые прибывших на службу, в силу отсутствия практического опыта.

6. Тяжелые условия труда, отражающиеся, в частности в ненормированном труде, недостатке свободного времени из-за того, что большинство процессуальных действий, проводимых уполномоченными должностными лицами, имеют строгие временные сроки, установленные действующим законодательством. Таким образом, сотрудник должен не только качественно выполнить свою работу (своевременно, объективно и

полно осуществлять расследование, соблюдать все предписания закона, охранять права и законные интересы граждан), но и осуществлять все мероприятия в строго ограниченные временные отрезки, а недостаток свободного времени плохо сказывается на отдыхе и восстановлении сотрудников, что непосредственно влияет на качество и своевременность выполнения поставленных задач.

7. Наличие профессионального риска и опасности. Деятельность сотрудников правоохранительных органов часто сопряжена с информационной неопределенностью, необходимостью быстрого выбора способа осуществления деятельности в той или иной ситуации, невозможностью прогнозирования последствий данного выбора.

Приведенные особенности подчёркивают необходимость повышения эффективности программ адаптации сотрудников, во многом определяющей дальнейшее осуществление профессиональной деятельности [3, с. 27].

Профессиональная адаптация молодого сотрудника в подразделениях органов внутренних дел раскрывается в подготовке и приспособлению к характеру, особенностям, режиму и условиям службы в правоохранительных органах, а также в должном уровне овладения профессиональными навыками и умениями, в формировании необходимых служебных и профессиональных качеств личности сотрудника необходимых для успешного выполнения возложенных на них обязанностей по обеспечению общественного порядка, общественной безопасности, реализации внутренней защиты государства, осуществлению предварительного расследования и др.

В качестве главных проблем при вхождении в должность молодых специалистов органов внутренних дел можно определить: недостаточную информированность молодых специалистов об истории и традициях службы органов внутренних дел; низкую степень удовлетворенности сотрудников различными аспектами своей трудовой деятельности; недостаточную эффективность работы назначенных наставников, вплоть до полного устранения от выполнения функции наставника.

Для решения указанных проблем и ускорения процесса адаптации молодых специалистов в системе правоохранительных органов по окончании процесса обучения требуется усиление практикоориентированного подхода в программах подготовки в системе высшего образования, частичного изменения учебных планов в соответствии с запросом потенциального работодателя, активное участие в разработке основных образовательных программ и в учебном процессе практических сотрудников правоохранительных органов.

ЛИТЕРАТУРА

1. Уголовно-процессуальный кодекс Российской Федерации от 18 дек. 2001 г. №174-ФЗ : в ред. от 13 июля 2015 г. №174-ФЗ. – URL: http://www.consultant.ru/document/cons_doc.
2. Магомедов К. О. Профессионально-адаптационные проблемы в муниципальной службе / К. О. Магомедов // Вопросы государственного и муниципального управления. – 2012.– № 1. – С. 99–103.
3. Шуклин М. С. Психологические особенности работы по повышению уровня адаптации молодых специалистов в подразделениях ОВД [Текст] / М. С. Шуклин // Психопедагогика в правоохранительных органах. – 2008. – № 1. – С. 26–28.
4. Жилин Р. А. Особенности использования программы для формирования высокосогласованных групп экспертов на основе численного метода предварительной экспертизы / Р. А. Жилин // Вестник Воронежского института ФСИИ России. – 2022. – № 1. – С. 40–45.

СВЕДЕНИЯ ОБ АВТОРЕ

Губарев Иван Сергеевич.
Преподавать кафедры административного права.
Кандидат юридических наук.
Воронежский институт МВД России.
E-mail: vanechka.gubarev2015@gmail.com
Россия, 394065, Воронеж, проспект Патриотов, 53.

Gubarev Ivan Sergeevich.
Lecturer of the Department of Administrative Law.
Candidate of Law Sciences.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: vanechka.gubarev2015@gmail.com
Russia, 394065, Voronezh, Prospekt Patriotov, 53.

Ключевые слова: правоохранительные органы, процесс адаптации, молодые сотрудники, служба в ОВД.

Keywords: law enforcement agencies, adaptation process, young employees, service in the police department.

УДК 342.9

**НЕКОТОРЫЕ ВОПРОСЫ РЕАЛИЗАЦИИ
ПРАВОВЫХ И СОЦИАЛЬНЫХ ГАРАНТИЙ
КАК ФАКТОР ПОВЫШЕНИЯ ПРИВЛЕКАТЕЛЬНОСТИ СЛУЖБЫ
ДЛЯ МОЛОДОГО СПЕЦИАЛИСТА
ПОДРАЗДЕЛЕНИЯ ПО ДЕЛАМ НЕСОВЕРШЕННОЛЕТНИХ**

**SOME ISSUES OF IMPLEMENTING
LEGAL AND SOCIAL GUARANTEES AS A FACTOR
INCREASING THE ATTRACTIVENESS OF THE SERVICE
FOR YOUNG SPECIALISTS IN MINORITY AFFAIRS**

В статье рассматриваются актуальные вопросы обеспечения правовых и социальных гарантий для молодых специалистов подразделений по делам несовершеннолетних органов внутренних дел Российской Федерации. Анализируется действующее законодательство, регламентирующее правовой статус и меры социальной поддержки сотрудников органов внутренних дел. Выявляются системные проблемы и противоречия, снижающие эффективность реализации предоставленных гарантий на практике. На основе проведенного анализа предлагается комплекс мер, направленных на совершенствование механизмов реализации прав и социальной защищенности молодых сотрудников подразделений по делам несовершеннолетних, что является ключевым фактором повышения престижа службы и закрепления кадров в указанных подразделениях.

This article examines current issues related to ensuring legal and social guarantees for young specialists in juvenile affairs units of the Russian Federation's internal affairs agencies. It analyzes current legislation regulating the legal status and social support measures for employees of internal affairs agencies. It identifies systemic problems and inconsistencies that reduce the effectiveness of the implementation of these guarantees in practice. Based on this analysis, a set of measures is proposed to improve mechanisms for realizing the rights and social protection of young employees of juvenile affairs units, which is a key factor in enhancing the prestige of the service and retaining personnel in these units.

Эффективность деятельности подразделений по делам несовершеннолетних (далее – ПДН) органов внутренних дел в значительной степени обусловлена уровнем профессиональной подготовки и стабильностью кадрового состава. В этой связи особую актуальность приобретает проблема закрепления на службе молодых специалистов, которые, обладая современными знаниями и высокой мотивацией, нередко сталкиваются с

комплексом трудностей, приводящих к их увольнению в первые годы службы. Одним из действенных инструментов решения данной проблемы является создание системы реализации предусмотренных законодательством правовых и социальных гарантий, направленных на адаптацию, профессиональное становление и обеспечение достойного уровня жизни сотрудников.

Правовой основой статуса сотрудников органов внутренних дел, включая молодых специалистов ПДН, выступают Федеральный закон от 30 ноября 2011 № 342-ФЗ «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» [1] (далее – ФЗ № 342), Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» [2] (далее – ФЗ № 3), Федеральный закон от 19.07.2011 № 247-ФЗ «О социальных гарантиях сотрудникам органов внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» [3] (далее – ФЗ № 247), Приказ МВД России от 23.08.2017 № 845 «Об утверждении Инструкции по организации работы подразделений по делам несовершеннолетних органов внутренних дел Российской Федерации» [4] (далее – Приказ № 845), а также иные нормативные правовые акты, регламентирующие вопросы прохождения службы, денежного довольствия, социального обеспечения и жилищного обеспечения. Указанными нормативными правовыми актами установлен широкий спектр гарантий, таких как денежное довольствие (ст. 66 ФЗ № 342), ежегодные оплачиваемые отпуска (глава 8 ФЗ № 342), гарантии социальной защиты (глава 9 ФЗ № 342), медицинское обеспечение (ст. 11 ФЗ № 247), жилищные гарантии и иные меры социальной поддержки. Указанные меры поддержки призваны обеспечить социальную защищенность сотрудников и компенсировать риски и расходы, связанные с исполнением служебных обязанностей. Например, ст. 11 ФЗ № 247 гласит, что сотрудник имеет право на бесплатное получение медицинской помощи, в том числе на изготовление и ремонт зубных протезов, бесплатное обеспечение лекарственными препаратами для медицинского применения по рецептам на лекарственные препараты, бесплатное обеспечение медицинскими изделиями по назначению врача в медицинских организациях федерального органа исполнительной власти в сфере внутренних дел. Согласно ст. 8 ФЗ № 247, сотруднику, не имеющему жилого помещения в населенном пункте по месту службы, и совместно проживающим с ним членам его семьи может предоставляться служебное жилое помещение или жилое помещение в общежитии, относящиеся к жилым помещениям специализированного жилищного фонда. Несмотря на достаточную законодательную регламентацию, в практической деятельности процесс реализации многих социально-правовых гарантий для молодых специалистов ПДН сопряжен с рядом системных проблем. Так, ключевой проблемой, существенно снижающей

привлекательность службы, остается нерешенность жилищного вопроса. Несмотря на существование жилищных фондов МВД России, очередь на получение служебного жилья, особенно в крупных городах, может растягиваться на годы, что создает серьезное материальное и психологическое давление на молодого специалиста и его семью, вынужденного нести расходы по аренде жилья.

Еще одной значимой проблемой является диспропорция между высоким уровнем эмоциональной и физической нагрузки, характерной для работы в ПДН, и уровнем денежного довольствия, особенно в начальный период службы. Работа с несовершеннолетними правонарушителями, неблагополучными семьями, проведение профилактических мероприятий требует от сотрудника не только глубоких профессиональных знаний, но и значительных психоэмоциональных ресурсов. Факторами, усугубляющими диспропорцию, могут выступать еще ненормированный рабочий день – работа в вечернее и ночное время, высокий уровень ответственности – за жизнь и здоровье несовершеннолетних, необходимость постоянного психологического напряжения, большой объем документооборота. Действующее законодательство не предусматривает специальных надбавок за работу с несовершеннолетними правонарушителями, повышенных коэффициентов за психоэмоциональные нагрузки, что усугубляет проблемы текучести кадров в подразделениях ПДН, снижения мотивации молодых специалистов, профессионального выгорания.

В этой связи, существующая система оплаты труда, не всегда в полной мере учитывающая специфику и интенсивность служебной деятельности в ПДН, может не соответствовать ожиданиям молодого специалиста. Важно отметить, что необходимость совершенствования системы оплаты труда в органах внутренних дел в последние годы особенно актуальна и получила признание на законодательном уровне. В постановлении Совета Федерации Федерального Собрания РФ от 3 июля 2024 г. № 203-СФ «О предложениях Совета Федерации Федерального Собрания РФ по формированию концепции федерального бюджета на 2025 год и на плановый период 2026 и 2027 годов» рекомендовано Правительству РФ при формировании проекта федерального бюджета на 2025 год и на плановый период 2026 и 2027 годов рассмотреть вопрос о совершенствовании оплаты труда в Министерстве внутренних дел РФ и повышении уровня оплаты труда низкооплачиваемых сотрудников [5].

Кроме того, на стадии адаптации молодой сотрудник нередко сталкивается с организационными барьерами, такими как недостаточность или формализация института наставничества, отсутствие четкого механизма карьерного планирования и перспектив профессионального роста. Правовая гарантия на повышение квалификации может быть реализована несвоевременно, что тормозит процесс интеграции нового

сотрудника в профессиональную среду и снижает его уверенность в завтрашнем дне.

Для повышения привлекательности службы в ПДН и эффективной реализации социально-правовых гарантий необходим комплексный подход.

Во-первых, представляется целесообразным разработать и внедрить ведомственные целевые программы, которые бы консолидировали существующие и новые меры поддержки.

В рамках таких программ можно предусмотреть:

- установление специализированной надбавки за специфику службы в ПДН для сотрудников, имеющих стаж службы до 5 лет;
- упрощение процедуры предоставления служебного жилья именно для молодых специалистов ПДН, в том числе через создание целевого фонда;
- развитие программы аренды жилья с последующей компенсацией части затрат и др.

Во-вторых, требуется совершенствование организационных механизмов. Необходимо формализовать и наполнить практическим содержанием институт наставничества, закрепив за опытным сотрудником обязанность по курированию молодого специалиста не только в оперативно-служебной деятельности, но и в вопросах реализации его прав и гарантий. Целесообразно разработать индивидуальные планы профессионального развития для каждого молодого сотрудника ПДН, четко определяющие этапы карьерного роста, условия и сроки повышения квалификации.

В-третьих, важным направлением является развитие непрофильных мер социальной поддержки. Это может включать в себя организацию корпоративного отдыха для семей сотрудников, создание системы психологической разгрузки и реабилитации, обеспечение возможности получения дополнительного образования за счет средств ведомства. Подобные меры способствуют формированию чувства социальной защищенности и корпоративной солидарности.

Таким образом, существующая система правовых и социальных гарантий для сотрудников органов внутренних дел требует адресной корректировки применительно к нуждам молодых специалистов подразделений по делам несовершеннолетних. Предложенные меры, направленные на усиление материальной поддержки, решение жилищной проблемы, совершенствование организационных и развитие дополнительных социальных механизмов, в своей совокупности позволят существенно повысить привлекательность службы в ПДН, снизить уровень текучести кадров и, как следствие, повысить эффективность работы по предупреждению правонарушений и безнадзорности несовершеннолетних.

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 // СПС «КонсультантПлюс».
2. О полиции : Федеральный закон от 07.02.2011 № 3-ФЗ// СПС «КонсультантПлюс».
3. О социальных гарантиях сотрудникам органов внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 19.07.2011 № 247-ФЗ// СПС «КонсультантПлюс».
4. Об утверждении Инструкции по организации работы подразделений по делам несовершеннолетних органов внутренних дел Российской Федерации : приказ МВД России от 23.08.2017 № 845// СПС «КонсультантПлюс».
5. О предложениях Совета Федерации Федерального Собрания РФ по формированию концепции федерального бюджета на 2025 год и на плановый период 2026 и 2027 годов : постановление Совета Федерации Федерального Собрания РФ от 3 июля 2024 г. № 203-СФ // СПС «Гарант».

СВЕДЕНИЯ ОБ АВТОРЕ

Динисламова Айза Зубаировна.

Преподаватель кафедры административной деятельности органов внутренних дел.

Краснодарский университет МВД России.

E-mail: ayza.dinislamova@mail.ru

Россия, 350005, г. Краснодар, ул. Ярославская, 128.

Dinislamova Ayza Zubairovna.

Lecturer in the Department of Administrative Activities of Internal Affairs Bodies.

Krasnodar University of the Ministry of Internal Affairs of Russia

Email: ayza.dinislamova@mail.ru

Russia, 350005, Krasnodar, Yaroslavskaya st., 128.

Ключевые слова: молодой специалист; подразделение по делам несовершеннолетних; правовые гарантии; социальные гарантии; кадровое обеспечение; органы внутренних дел.

Keywords: young specialist; juvenile affairs unit; legal guarantees; social guarantees; personnel support; internal affairs bodies.

УДК 342.92

**ИНДИВИДУАЛЬНЫЕ АДАПТАЦИОННЫЕ МАРШРУТЫ
ВЫПУСКНИКОВ МВД РОССИИ:
ПРАВОВЫЕ ВОЗМОЖНОСТИ И ОГРАНИЧЕНИЯ**

**INDIVIDUAL ADAPTATION ROUTES FOR GRADUATES
OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA:
LEGAL OPPORTUNITIES AND RESTRICTIONS**

В настоящей статье акцентируется внимание на возрастающей потребности в дифференцированном подходе к адаптации выпускников образовательных организаций МВД России, особенно ярко проявляющейся в условиях трансформации системы подготовки кадров для органов внутренних дел Российской Федерации (далее – ОВД). Анализируются нормативно-правовые основы, допускающие гибкость в организации адаптационного процесса, выявляются правовые барьеры внедрения индивидуальных адаптационных маршрутов и формулируются предложения по их преодолению в рамках действующей административно-правовой системы.

This article focuses on the growing need for a differentiated approach to the adaptation of graduates of educational institutions of the Ministry of Internal Affairs of the Russian Federation, which is particularly evident in the context of the transformation of the system of training personnel for the Ministry of Internal Affairs of the Russian Federation (hereinafter referred to as the Ministry of Internal Affairs). The author analyzes the legal and regulatory framework that allows for flexibility in the organization of the adaptation process, identifies the legal barriers to the implementation of individual adaptation routes, and formulates proposals for overcoming these barriers within the existing administrative and legal system.

Сегодня проблематика настоящей статьи не вызывает сомнений в ее актуальности, особенно в контексте современных тенденций персонализации государственной службы и повышения эффективности кадровой политики. Особое внимание уделяется начальному этапу служебной деятельности – периоду адаптации выпускников образовательных организаций системы МВД России. Именно от успешности этого этапа во многом зависит не только личностно-профессиональное становление молодого специалиста, но и общая стабильность кадрового состава, а также качество выполнения соответствующих функций на местах.

В условиях усложнения социальной составляющей полицейской деятельности, цифровизации служебных процессов и повышения требований к компетенциям сотрудников всё более очевидной становится

неэффективность универсальных, «усреднённых» подходов к адаптации. На первый план выходит необходимость дифференцированного сопровождения молодых кадров с учётом их профессиональной подготовки, личностных особенностей, региональной специфики и задач конкретного подразделения ОВД. В связи с этим всё большую актуальность приобретает идея внедрения индивидуальных адаптационных маршрутов (далее – ИАМ) – гибких, персонализированных программ, направленных на поэтапное и целенаправленное вхождение выпускника образовательной организации системы МВД России в служебную среду.

И прежде всего отметим, что под ИАМ в контексте настоящей статьи следует понимать комплекс административно-организационных и правовых мер, разрабатываемых с учётом индивидуальных особенностей выпускника образовательной организации системы МВД России и специфики служебной деятельности подразделения [1].

В отличие от универсальных программ, ИАМ предполагает правовую возможность дифференциации сроков, содержания и форм адаптации. Однако реализация такого подхода сталкивается с рядом административно-правовых проблем.

С одной стороны, действующее законодательство о службе в ОВД, а также подзаконные акты МВД России формально допускают элементы индивидуализации в организации служебной деятельности. Например, посредством разработки индивидуальных планов повышения квалификации (п. б) ч. 1 ст. 76 ФЗ «О службе в ОВД» [2]), установления наставничества (ст. 11. ФЗ «О службе в ОВД»). При этом нормативная правовая база, непосредственно закрепляющая ИАМ как самостоятельное административно-правовое явление института прохождения государственной службы в ОВД, на сегодняшний день отсутствует.

С другой стороны, принципы единоначалия, равенства сотрудников перед служебным законодательством и жёсткая регламентация кадровых процедур создают объективные правовые ограничения для широкомасштабного внедрения индивидуального подхода к сотрудникам. Например, предоставление одному сотруднику льготных условий адаптации может быть расценено как нарушение принципа равенства.

В этих условиях возникает научно и практически значимая проблема: в каких правовых рамках возможно формирование индивидуальных адаптационных маршрутов, не нарушающих основ административно-правового регулирования, и какие нормативные барьеры необходимо преодолеть?

И для того чтобы ответить на этот вопрос, необходимо обратиться к зарубежной практике.

Так, в США предусмотрена программа так называемого полевого обучения (Field Training Officer Program (FTOP)). После окончания полицейской академии в течение обычно 4–6 месяцев новобранцы проходят

указанную программу под руководством более опытного офицера. Программа регулируется локальными нормативными актами (руководствами департаментов полиции), но основана на стандартах трудоустройства и обучения сотрудников правоохранительных и исправительных органов, установленных уполномоченной организацией (International Association of Directors of Law Enforcement Standards and Training (IADLEST)). Адаптация индивидуализирована: офицер составляет ежедневный план обучения новоиспеченного сотрудника и оценивает его прогресс по более чем 30 компетенциям (от общения с гражданами до применения оружия) [3].

В Германии полицейские проходят трехлетнее обучение, состоящее из теоретической подготовки и практики, после чего назначаются на должность с испытательным сроком от 1 до 3 лет в зависимости от административно-территориального образования (земли). Рассматриваемый испытательный срок регулируется нормативными правовыми актами административно-территориальных образований (законами земель) и положениями об обучении. Каждому молодому сотруднику назначается куратор по обучению, который: проводит регулярные встречи; оценивает служебное поведение и профессиональные навыки; подготавливает отчеты для руководства. Наиболее интересными являются несколько фактов. Во-первых, адаптация включает ротацию по подразделениям (патруль, следствие, административная работа) для формирования у сотрудника универсальных компетенций [4]. Во-вторых, в ФРГ основой подготовки полицейских кадров является принцип пожизненного найма, поэтому обучение и профессиональная деятельность сотрудника осуществляется в расчете на перспективу. Постоянное повышение квалификации выступает неотъемлемой частью карьерного роста.

Французская система подготовки полицейских кадров является одной из старейших в мире. Первичная (начальная) подготовка рядовых полицейских составляет 1 год, за который слушатели получают базовые знания, а также проходят стажировку (практику) под руководством опытного наставника. Подготовка сотрудников среднего звена носит дифференцированный характер. Обучение полицейских на должности инспекторов проходит в течение 16 месяцев в Высшей школе инспекторов Национальной полиции в г. Канн-Экюз. Офицеры же проходят 18-месячное обучение в высшей школе офицеров национальной полиции в г. Ницца. После выпуска сотрудник еще год считается стажером и работает под руководством наставника, который составляет индивидуальную карточку сопровождения. Оценка стажировки включает три компонента: профессиональные навыки, этическое поведение, способность к командной работе [5].

Итак, зарубежный опыт, хотя и рассмотрен фрагментарно, убедительно демонстрирует: ИАМ – важнейший фактор обеспечения высокого качества подготовки правоохранительных кадров. Возвращаясь к современной российской практике, выделим три основные группы ограничений,

препятствующих формированию системного правового подхода к индивидуальной адаптации выпускников в органах внутренних дел:

1. Нормативно-правовые: отсутствие прямого упоминания ИАМ в федеральном законодательстве о прохождении службы в ОВД и ведомственных приказах; отсутствие типового положения об ИАМ.

Отметим, что подобный ведомственный нормативный правовой акт, регулирующий организацию наставничества в органах внутренних дел Российской Федерации, был разработан и действовал до 2017 года [6]. В настоящее время указанный документ утратил силу.

2. Институциональные: отсутствие должного уровня взаимодействия и координация между образовательными организациями системы МВД России и иными образовательными организациями, осуществляющими подготовку по правоохранительным специальностям и направлениям подготовки, и территориальными ОВД; отсутствие единой методики разработки ИАМ.

3. Ценностно-культурные: доминирование скорее формального подхода к адаптации, нежели личностно-ориентированного; недоверие к «индивидуализации» как потенциальному источнику неравенства среди молодых сотрудников.

Несмотря на декларируемую открытость к инновациям в кадровой политике, действующая административно-правовая система МВД России сохраняет инерционный характер, ориентированный на единообразие, а не на персонализацию служебного развития. Вместе с тем возможная разработка и последующее нормативное закрепление наиболее общих принципов и порядка организации ИАМ – не исключение из правил, а развитие существующих правовых механизмов, направленное на повышение эффективности кадровой политики ОВД.

В продолжение анализа отметим возможные предложения по нормативному правовому оформлению ИАМ.

Полагаем, следует вернуться к идее разработки ведомственного типового положения, которое было бы построено на основе практико-ориентированного подхода и включало бы в себя следующие блоки:

– четко определенное понятие «индивидуального адаптационного маршрута»;

– обязательные и факультативные компоненты ИАМ (наставничество, обучение, психологическая поддержка, конкретные служебные задачи);

– критерии разработки маршрута с учетом профиля подготовки выпускника, рекомендаций выпускающей образовательной организации и специфики подразделения, в котором молодой специалист будет проходить службу;

– форму «Индивидуального адаптационного плана» как приложения к приказу о назначении на должность;

– механизм контроля и оценки эффективности прохождения ИАМ в рамках испытательного срока.

Таким образом, несмотря на отсутствие в российском законодательстве прямого закрепления ИАМ как самостоятельного административно-правового института, действующая нормативно-правовая база содержит достаточные основания для их правомерного внедрения. Анализ зарубежного опыта подтверждает: персонализированный подход к адаптации не только повышает эффективность профессиональной социализации выпускников образовательных организаций МВД России и иных образовательных организаций высшего образования, но и способствует устойчивости кадрового состава ОВД. Убеждены, для реализации этого потенциала в системе МВД России требуется разработка ведомственного типового положения об ИАМ, построенного на практико-ориентированных принципах с учетом норм действующего законодательства. Только системное нормативное оформление ИАМ позволит перейти к устойчивой, эффективной модели адаптации новой генерации полицейских. Полагаем, необходимо продолжить более глубокое исследование правовых, организационных и управленческих аспектов внедрения ИАМ в систему государственной службы в ОВД.

ЛИТЕРАТУРА

1. Маюров Н. П. Особенности профессиональной адаптации молодых сотрудников ОВД к службе / Н. П. Маюров, П. Н. Маюров, О. Д. Ороева // Ленинградский юридический журнал. – 2018. – № 4. – С. 45–50.

2. О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 30.11.2011 № 342-ФЗ (ред. от 28.11.2025) // СПС «КонсультантПлюс». – URL : <https://www.consultant.ru> (дата обращения: 01.10.2025).

3. Field Training Officer FTO Program. – URL : <https://www.madisonal.gov/514> (дата обращения: 01.10.2025).

4. How much training to be a cop in germany. – URL : <https://germanyfocusguide.com/blog> (дата обращения: 01.10.2025).

5. Куркина И. Н. Базовые стандарты и модели подготовки полицейских кадров за рубежом / И. Н. Куркина // Ведомости УИС. – 2012. – № 10 (125). – С. 51–56.

6. Об утверждении Положения об организации наставничества в органах внутренних дел Российской Федерации : приказ МВД России от 24.12.2008 № 1139 (документ утратил силу) // СПС «КонсультантПлюс». – URL: <https://www.consultant.ru> (дата обращения: 01.10.2025).

СВЕДЕНИЯ ОБ АВТОРЕ

Курашова Мария Михайловна.
Преподаватель кафедры административного права.
Воронежский институт МВД России.
E-mail: km4498@
Россия, 394006, г. Воронеж, пр-т Патриотов, д. 53.

Kurashova Maria Mikhailovna.
Lecturer of the Department of Administrative Law.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: km4498@
Russia, 394065, Voronezh, Prospekt Patriotov, 53.

Ключевые слова: индивидуальный адаптационный маршрут; выпускники образовательных организаций системы МВД России; административное право; персонализация государственной службы; нормативно-правовое регулирование; кадровая политика.

Keywords: individual adaptation route; graduates of educational organizations of the Russian Ministry of Internal Affairs; administrative law; personalization of public service; legal regulation; personnel policy.

УДК 342.9

**ОБ АДАПТАЦИИ И НЕКОТОРЫХ АДАПТАЦИОННЫХ БАРЬЕРАХ
МОЛОДЫХ СПЕЦИАЛИСТОВ ПОДРАЗДЕЛЕНИЙ
ПО ДЕЛАМ НЕСОВЕРШЕННОЛЕТНИХ, ОКОНЧИВШИХ
ОБРАЗОВАТЕЛЬНЫЕ ОРГАНИЗАЦИИ СИСТЕМЫ МВД РОССИИ**

**ABOUT ADAPTATION AND SOME ADAPTATION BARRIERS
OF YOUNG SPECIALISTS OF JUVENILE AFFAIRS UNITS
WHO HAVE GRADUATED FROM EDUCATIONAL ORGANIZATIONS
OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA**

В статье проанализированы проблемные вопросы адаптации выпускников образовательных организаций МВД России, проходящих службу в подразделениях по делам несовершеннолетних. Автором научно обоснованы сущность и необходимость адаптации. Рассмотрены отдельные адаптационные барьеры, возникающие в деятельности молодых специалистов.

The article analyzes the problematic issues of adaptation of graduates of educational institutions of the Ministry of Internal Affairs of the Russian Federation who serve in juvenile affairs units. The author scientifically substantiates the essence and necessity of adaptation. Some adaptation barriers arising in the activities of young specialists are considered.

Профессиональное становление молодых сотрудников является важным этапом успешного прохождения ими службы в органах внутренних дел (далее – ОВД). Его эффективность не только предопределяет позитивное, добросовестное отношение к выполнению должностных обязанностей, но и влияет на длительность служебной деятельности как в рамках одного подразделения, так в ОВД в целом.

МВД России заинтересовано в подготовке компетентных и грамотных специалистов, осуществляемой в ведомственных образовательных организациях: институтах, университетах, академиях. Пополнение полицейских рядов ответственной, целеустремленной, квалифицированной молодежью особенно важно в условиях кадрового голода, ставшего устойчивой проблемой современности с ее негативной тенденцией к ежегодному усложнению.

Как отмечал на расширенном заседании коллегии МВД России В. А. Колокольцев, по состоянию на март 2025 г. неуккомплектованность органов внутренних дел составила более 172 тыс. должностей, при этом более 33 тыс. вакансий стали свободными только за минувший год. Равным образом увольняются не только опытные сотрудники со стажем

службы от 10 лет и более, но и молодые специалисты, только пришедшие в профессию [1].

Расторжение контракта происходит в том числе в первые месяцы после окончания ведомственных образовательных организаций. Не удерживает молодых сотрудников и обязательство по возмещению МВД России значительных материальных средств, затраченных на их подготовку и обучение.

Сложившаяся тенденция затронула и подразделения по делам несовершеннолетних (далее – ПДН). Так, по результатам наблюдения среди выпускников Воронежского института МВД России 2024 года выпуска, обучившихся по специальности «Правоохранительная деятельность» (узкая специализация – сотрудник подразделения по делам несовершеннолетних), в течение первого года службы более 20% молодых специалистов уволилось, а 60% перевелось на должности в иные службы и подразделения ОВД. Среди выпускников 2025 года выпуска, обучавшихся по той же специализации, несмотря на отсутствие фактов увольнения, лишь 30% остались в рядах инспекторов ПДН. Преобладающая же часть молодых специалистов предпочло службу в качестве участковых уполномоченных полиции, сотрудников уголовного розыска, подразделений дознания и иных. Серьезность такой ситуации обусловлена множеством факторов.

Во-первых, подразделения по делам несовершеннолетних не пополняются специально подготовленными кадрами: основную часть сотрудников составляют лица «старой закалки», имеющие стаж службы в ОВД более 15-20 лет и, как правило, служащие до появления возможности реализовать право на пенсию по выслуге лет, либо сотрудники, изначально не имеющие «полицейского образования», прошедшие обучение по программам профессиональной подготовки кадров в образовательных организациях МВД России, но обычно «не задерживающиеся на службе». Иными словами, опытные сотрудники постепенно уходят из профессии, а среди молодых распространена постоянная текучесть кадров.

Во-вторых, не реализуется потенциал молодых инспекторов ПДН, обучившихся по соответствующей специальности и прошедших профессиональную теоретико-практическую подготовку в стенах ведомственного учреждения, ориентированную на формирование необходимого уровня компетенции, воспитание личных и морально-деловых качеств, получение знаний, умений и навыков, отвечающим современным требованиям.

Действительно, образовательный процесс в институтах, университетах, академиях МВД России отличается особой спецификой. Курсанты, а затем слушатели не только осваивают образовательные программы, но и привлекаются к несению службы в нарядах как в пределах обеспечивающих нужд организации, так и в качестве приданных сил совместно с

действующими сотрудниками ОВД, в том числе в городских, районных, областных и иных мероприятиях по охране общественного порядка. Кроме того, с первого курса обучения курсанты присягают на верность Российской Федерации, получают специальное звание рядового полиции, вступают в множественные субординационные отношения, а вместе с тем в целом получают правовой статус сотрудника органа внутренних дел, включая значительный объем не только прав, но и обязанностей, требований, ограничений и ответственности. В таких условиях с первых дней обучения начинается служебный путь молодых сотрудников, а сами они становятся неотъемлемой частью ведомства.

Однако на практике, как было отмечено выше, затраченные Министерством внутренних дел России средства на подготовку профессиональных кадров, в том числе инспекторов ПДН, зачастую не оправдываются, а сама суть специализированного и в большинстве случаев целевого обучения теряет свой смысл и ценность. Одной из причин такой ситуации выступает неэффективная профессиональная адаптация молодых сотрудников.

Само понятие адаптация имеет различные значения. Оно используется в многочисленных научных дисциплинах, сферах и отраслях общественной жизни. С учетом предметной области можно выделить, в частности, биологическую адаптацию к условиям среды и воздействию внешних факторов, физиологическую адаптацию организма к умственным и физическим нагрузкам, культурную, языковую, социально-психологическую и другие виды. Например, в медицине под адаптацией понимают привыкание к действию конкретного лекарственного препарата или терапии в целом, в психологии общения – «выстраивание стиля коммуникации с учетом ожиданий и особенностей аудитории», в литературе – «упрощение текста для малоподготовленных читателей» [2].

Содержательные особенности адаптации предельно широки, однако в сущности все виды адаптационных процессов объединяет один термин – приспособление (привыкание) к условиям существования. В рамках настоящей статьи наиболее существенны социально-психологические и профессиональные аспекты адаптации.

Так, отечественный ученый С. Д. Артемов рассматривает в качестве адаптации «процесс приспособления личности к существующим общественным отношениям, нормам, образцам, традициям общества, в котором живет и действует человек» [3, с. 135].

В свою очередь, рассматривая профессиональную адаптацию, П. Е. Венгер полагает, что она представляет собой «процесс достижения молодым специалистом профессионально-личностного развития, соответствия требованиям своей профессии за счет поддержания профессионально-ценностных ориентаций и успешной профессиональной деятельности, при этом сохраняется спокойствие и комфорт сотрудника».

Автор называет адаптацию своеобразным «испытательным сроком», который определяет успешность профессиональной деятельности в будущем [4, с. 3].

Профессиональная адаптация молодого инспектора по делам несовершеннолетних является комплексной категорией, включающей аспекты приспособления к коллективу, его внутренним корпоративным нормам, к режиму служебного времени и отдыха, особенностям и сложностям несения службы, характеру выполняемых задач, контингенту общения. Она выступает очень важным этапом становления служебной деятельности молодого специалиста, и может быть даже решающим. Именно начало профессионального пути определяет, состоится ли сотрудник как профессионал, и останется ли вообще служить в ОВД.

Так, только адаптированный сотрудник способен самостоятельно и качественно выполнять должностные и служебные обязанности, быть уверенным в своих способностях как в личностном, так в профессионально-деловом смысле, признавать и осознанно соблюдать предусмотренные правовые и социальные нормы поведения, проявлять преимущественную готовность к преодолению трудностей и эмоционально-стрессовых ситуаций, не испытывая существенного физического и психологического давления и психологически не избегая своей принадлежности к службе в ОВД. Срок профессиональной адаптации индивидуален. Оптимально для выпускников ведомственных образовательных организаций он должен составлять до нескольких месяцев.

Это лежит и в основе некоторых особенностей прохождения службы в ОВД. В частности, в соответствии с п. 123-126 Приказа МВД России от 1 февраля 2018 г. № 50 «Об утверждении Порядка организации прохождения службы в органах внутренних дел Российской Федерации» за сотрудником, назначенным на должность по окончании ведомственной образовательной организации, закрепляется наставник, который обязан оказывать ему консультативно-разъяснительную, методическую и практическую помощь. Цель наставничества заключается в подготовке молодого специалиста к самостоятельному выполнению служебных обязанностей при этом срок выполнения им задания для индивидуального обучения нормативно регламентирован и устанавливается на период от одного до трех месяцев [5].

Однако на практике срок профессиональной адаптации выпускников ОВД превышает указанные нормативные пределы, а у отдельных молодых специалистов ПДН в целом обнаруживается неспособность преодолеть возникающие адаптационные барьеры.

Категория «адаптационный барьер» представляет собой некоторую условную границу, за пределами которой адекватная адаптация невозможна. Это различного рода внутренние и внешние факторы, индивидуально воспринимаемые как преграды для профессионального закрепления.

Как справедливо отмечает П. Е. Венгер, адаптационный процесс является активным и зачастую сопровождается самоизменением, самокоррекцией, направленными на достижение цели соответствия требованиям социума, социальным нормам и условиям среды [4, с. 2]. Действительно, адаптация изначально связана с усилиями по преодолению различий между привычным и новым, личными установками и профессиональными требованиями.

Оригинальность адаптационных барьеров обусловлена их личностной принадлежностью. Так, одни и те же условия среды для некоторых сотрудников ОВД будут являться оптимальными, а для других непригодными.

Несмотря на названную субъективную обусловленность, выделим отдельные наиболее существенные адаптационные барьеры, возникающие в деятельности молодых инспекторов ПДН.

В частности, к их числу относятся:

– специфика профессиональной деятельности, обусловленная необходимостью работы с неблагополучными семьями, девиантными детьми и подростками. Учитывая, что большинство инспекторов ПДН являются представителями женского пола, важно отметить, что они склонны испытывать серьезную эмоциональную и психологическую напряженность в работе, ежедневно сталкиваясь с правонарушениями, совершенными несовершеннолетними, а также в отношении них. Для некоторых молодых сотрудниц наблюдаемые жилищно-бытовые условия, в которых вынуждены жить дети, маргинальный социальный контингент, ненормированность служебного времени, необходимость участия в мероприятиях по лишению и ограничению родительских прав являются травмирующими профессиональными факторами, в силу чего с учетом своих морально-деловых качеств они не находят в себе силы продолжать служебную деятельность в качестве инспектора по делам несовершеннолетних;

– формальность института наставничества, отсутствие реальной методической и практической помощи со стороны руководителя. Безусловно, нельзя судить о повсеместном распространении данного феномена, однако он нередко обнаруживается при анализе первоначального этапа прохождения службы в подразделениях по делам несовершеннолетних. В частности, молодые специалисты зачастую выполняют задание для индивидуального обучения и конструктивно взаимодействуют с наставником лишь «на бумаге», в том числе ввиду высокой загруженности последних. Они самостоятельно приступают к исполнению служебных обязанностей, пытаясь использовать знания и умения, полученные в ходе обучения, что не всегда успешно удается из-за отсутствия практического опыта на первоначальном этапе службы;

– неконкурентный уровень денежного содержания молодых

сотрудников ПДН и его несоответствие объему и характеру возлагаемых на них обязанностей. Так, курсанты и слушатели ведомственных образовательных организаций ежемесячно получают денежное содержание, которое увеличивается от года к году с учетом индексации, повышением стажа службы в ОВД, а также присвоением на последнем курсе обучения специального звания «младший лейтенант полиции». Выпускаясь из образовательного учреждения, степень личной ответственности молодых полицейских сильно возрастает, появляется множество новых обязанностей и задач, а размер денежного содержания при этом увеличивается незначительно, что особенно сильно ощущается в первые годы службы;

– адаптационные трудности, обусловленные процессом вхождения в служебный коллектив. Они имеют двойственную природу, поскольку могут быть спровоцированными как новоиспеченным сотрудником, так и более опытными членами подразделения. Оказавшись в новом подразделении, молодому специалисту важно ощущать себя частью коллектива, не стать отвергнутым, изолированным, брошенным, непонятым. В то же время ему самому важно избегать пассивность, игнорирования корпоративных норм и ценностей сослуживцев, проявления неуважительного отношения и самоуверенности;

– личностно-психологические особенности, несоответствующие требованиям к компетенции инспектора по делам несовершеннолетних (депрессивность, излишняя уступчивость, доверчивость, эмоциональная неустойчивость, жестокость, застенчивость).

Таким образом, под адаптационным барьером следует понимать совокупность субъективно воспринимаемых факторов, условий профессиональной деятельности, а также познавательные-когнитивные, эмоционально-волевые, морально-деловые качества личности молодого инспектора по делам несовершеннолетних, препятствующие проявлению адаптационных возможностей или исключают возможность адаптации в целом, что вызывает объективную необходимость в выработке научно-практических рекомендаций по их преодолению.

ЛИТЕРАТУРА

1. Выступление Владимира Колокольцева на расширенном заседании коллегии МВД России от 5 марта 2025 года. – URL: <https://мвд.рф/news> (дата обращения: 25.11.2025).

2. Толковый словарь Ожегова. – URL: <https://slovarozhegova.ru/> (дата обращения: 25.11.2025).

3. Артемов С. Д. Социальные проблемы адаптации / С. Д. Артемов. – Москва : Просвещение, 1990. – 180 с.

4. Венгер П. Е. Адаптация молодого специалиста в сфере профессиональной деятельности / П. Е. Венгер // Политехнический молодежный журнал. – 2023. – № 7(84). – С. 1–12.

5. Об утверждении Порядка организации прохождения службы в органах внутренних дел Российской Федерации : приказ МВД России от 01.02.2018 № 50 (с изм. и доп., вступ. в силу с 30.01.2023) // Официальный сайт МВД России. – URL: <https://mvd.consultant.ru/documents/24078> (дата обращения: 28.11.2025).

6. Амеджанова Т. Ц. Наставничество как механизм закрепления молодых сотрудников в правоохранительных органах / Т. Ц. Амеджанова // Вестник Бурятского государственного университета. Образование. Личность. Общество. – 2024. – № 3. – С. 29–36.

СВЕДЕНИЯ ОБ АВТОРЕ

Павленко Ольга Сергеевна.

Адъюнкт института.

Воронежский институт МВД России.

E-mail: olinon@mail.ru

Россия, 394065, г. Воронеж, проспект Патриотов, д. 53.

Olga Sergeevna Pavlenko.

Postgraduate.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: olinon@mail.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: адаптация; адаптационный барьер; профессиональное становление; наставничество; инспектор по делам несовершеннолетних.

Keywords: adaptation; adaptation barrier; professional development; mentoring; juvenile inspector.

УДК 159.99

Научное издание

НАУЧНЫЙ БЮЛЛЕТЕНЬ
ВОРОНЕЖСКОГО ИНСТИТУТА МВД РОССИИ

Сборник

Выпуск 4

В авторской редакции

Компьютерная верстка Н. В. Крючковой

Объем 1,8 Мб

Воронежский институт МВД России,
394065, Воронеж, просп. Патриотов, 53