

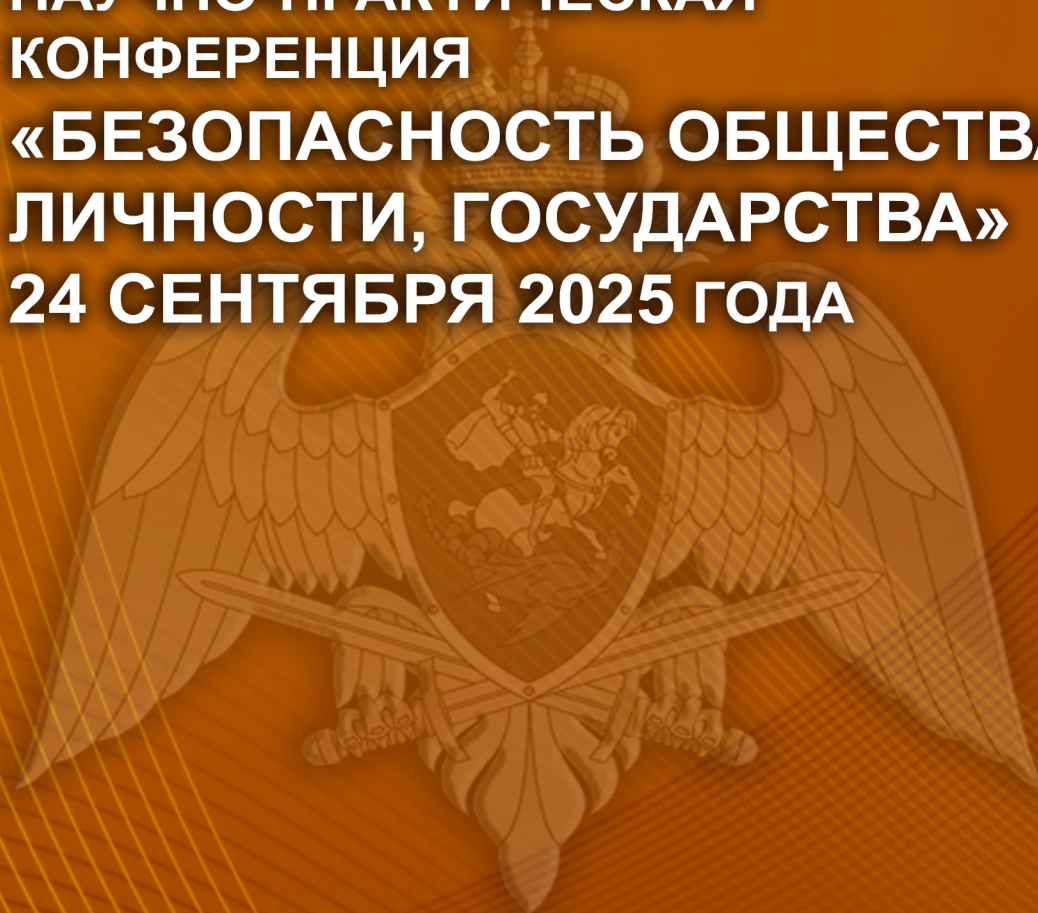
СБОРНИК СТАТЕЙ

**ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК
НАЦИОНАЛЬНОЙ ГВАРДИИ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
«ОХРАНА»**

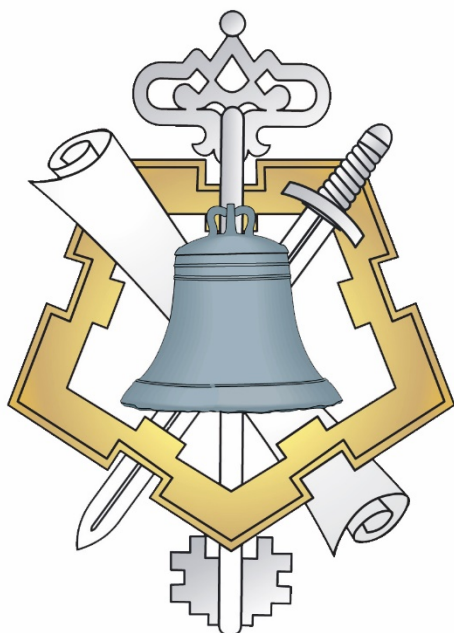
**ВЕДОМСТВЕННАЯ
НАУЧНО-ПРАКТИЧЕСКАЯ
КОНФЕРЕНЦИЯ
«БЕЗОПАСНОСТЬ ОБЩЕСТВА,
ЛИЧНОСТИ, ГОСУДАРСТВА»
24 СЕНТЯБРЯ 2025 ГОДА**

**ВЫП. 2
МОСКВА 2026**



**ФЕДЕРАЛЬНАЯ СЛУЖБА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР «ОХРАНА»**



СБОРНИК СТАТЕЙ

**ВЕДОМСТВЕННАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ
«БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА»
24 СЕНТЯБРЯ 2025 ГОДА**



МОСКВА 2026 г.



СБОРНИК СТАТЕЙ

**ВЕДОМСТВЕННАЯ
НАУЧНО-ПРАКТИЧЕСКАЯ
КОНФЕРЕНЦИЯ
«БЕЗОПАСНОСТЬ
ЛИЧНОСТИ, ОБЩЕСТВА,
ГОСУДАРСТВА»
30 ОКТЯБРЯ 2024 ГОДА**
Вып. 2. – Москва:
Федеральное казенное
учреждение «Научно-
исследовательский центр
«Охрана» Федеральной
службы войск
национальной гвардии
Российской Федерации,
2026 г. – 135 с.
ББК 32.844
60.82

Редакционная коллегия:

**Председатель
В.Н. Демин**

**Заместитель
председателя
В.С. Зарубин**

**Ответственный
секретарь
А.Н. Морозов**

Члены редакционной коллегии:

**В.С. Зарубин
А.Р. Фамильнов
А.Н. Морозов**

**Технический редактор
М.А. Гасанов**

СОДЕРЖАНИЕ

Алексеев А.И. Проблемные вопросы оборудования объектов (территорий) системами оповещения и управления эвакуацией при угрозе совершения или совершении террористического акта	4
Антышев А.А. О вопросах цифровой трансформации деятельности участкового уполномоченного полиции.	8
Анюхин С.Г. К вопросу совершенствования технических требований нормативных документов с учетом расширения практики применения радиоволновых извещателей	12
Баринев И.А. Пути и методы повышения информативности систем централизованного наблюдения	16
Великклад Т.П. Подготовка специалистов беспилотной авиации. Проблемы и пути решения	20
Вихирев А.А. Вопросы дистанционного управления объектовыми устройствами	24
Гапоненко В.А. Вопросы совершенствования нормативного правового обеспечения регулирования охранной деятельности в Российской Федерации	28
Губарь Д.С. Уголовно-правовые меры обеспечения антитеррористической защищенности объектов и территорий	33
Дмитриев Р.С. Об основных технических требованиях к средствам обнаружения, основанным на трибоэлектрическом принципе действия	42
Здоровцов А.Г. К вопросу скрытой передачи тревожного сигнала в мобильных (быстроразвертываемых) технических средствах охраны	46
Каханов С.А. Опыт защиты объектов от противоправного применения беспилотных воздушных судов в современных условиях, участия в организации оборудования охраняемых объектов специальными техническими средствами противодействия БВС	50
Квасов В.Б. Особенности реализации пропускного режима охраняемого объекта	53
Колосков А.А. Перспективы применения преобразователей кинетической энергии в качестве источников автономного электропитания технических средств безопасности	55
Красилич А.А. Применение систем формирования тревожных сообщений с использованием видеоаналитики и искусственного интеллекта для централизованной охраны объектов и территорий (площадок)	60
Левин А.И. О применении технологий искусственного интеллекта для выявления признаков серийности преступлений	64
Лялевич В.Г. Перспективы применения суперконденсаторов для обеспечения автономности и надежности технических средств охраны	69
Михайлов А.А. Лазерные комплексы поражения БВС, их особенности, достоинства и ограничения, вытекающие из физического принципа функционирования	73
Мороз И.В. Оборудование объектов инженерно-техническими средствами охраны (ИТСО): актуальные технологии и нормативные требования	78
Пархаев А.В., Михайлов А.А. Проблемы оценки и тестирования современной видеоаналитики	81
Проскурин Р.А. Инновационные подходы к повышению эффективности управления во вневедомственной охране на основе технологий искусственного интеллекта	86

СОДЕРЖАНИЕ

Прошутинский Д.А. Угрозы противоправного применения беспилотных воздушных судов и методы противодействия на объектах (территориях) различной ведомственной принадлежности	91	В сборнике содержатся материалы
Рябцев Н.А. О некоторых вопросах создания и применения звуковых извещателей системы охранной сигнализации	95	II межведомственной научно-практической конференции
Сбродов А.С. Перспективы применения беспилотных летательных аппаратов в системе охраны важных государственных объектов	98	«Безопасность личности, общества, государства – 2025», проведенной
Семенов К.П. Цифровизация военных образовательных организаций высшего образования войск национальной гвардии Российской Федерации: современное состояние и перспективы	102	Федеральным казенным учреждением «Научно-исследовательский центр
Сорочинский Я.Л. Проблемные вопросы осуществления контрольных мероприятий по антитеррористической защищенности объектов (территорий) различной ведомственной принадлежности	108	«Охрана» Федеральной службы войск
Сорочинский Я.Л. Участие Подразделений Вневедомственной Охраны Росгвардии В Электронных Торгах: Стратегия Роста на Конкурентном Рынке Охранных Услуг	112	национальной гвардии Российской Федерации
Фирсов А.Г. Основные результаты работы систем охранно-пожарной сигнализации по обеспечению пожарной безопасности объектов защиты в 2024 г.	116	24 сентября 2025 года. Издание представляет интерес для специалистов
Шипулин А.В. Проблемы и решения при использовании биометрических данных в системах безопасности и охране общественного порядка	122	вневедомственной охраны Росгвардии, сотрудников
Юдина С.М. Спорные вопросы определения объектов (территорий), подлежащих антитеррористической защите	126	правоохранительных органов, предприятий и организаций,
Янгиров А.И. Подход к распределению ресурсов безопасности для обеспечения защищенности автоматизированных систем	132	работающих в сфере обеспечения безопасности

УДК 006.05:654.92
ББК 30ц/3стд2-053

**АЛЕКСЕЕНКО АНАТОЛИЙ ИВАНОВИЧ, НАУЧНЫЙ СОТРУДНИК ОТДЕЛА РАЗРАБОТКИ
НОРМАТИВНО-МЕТОДИЧЕСКИХ ДОКУМЕНТОВ ФКУ НИЦ «ОХРАНА» РОСГВАРДИИ**

**ПРОБЛЕМНЫЕ ВОПРОСЫ ОБОРУДОВАНИЯ ОБЪЕКТОВ (ТЕРРИТОРИЙ)
СИСТЕМАМИ ОПОВЕЩЕНИЯ И УПРАВЛЕНИЯ ЭВАКУАЦИЕЙ ПРИ УГРОЗЕ
СОВЕРШЕНИЯ ИЛИ СОВЕРШЕНИИ ТЕРРОРИСТИЧЕСКОГО АКТА**

Аннотация. В настоящей статье рассмотрены вопросы нормативного регулирования обеспечения защиты критически важных объектов инфраструктуры и жизнеобеспечения, мест массового пребывания людей от террористических угроз и оборудования объектов (территорий) системами (комплексами) оповещения и эвакуации при угрозе совершения террористического акта.

Ключевые слова: антитеррористическая защита, защита объектов, системы оповещения, функциональная независимость, сигналы оповещения.

**ALEKSEYENKO ANATOLY IVANOVICH, RESEARCHER OF THE DEPARTMENT OF DEVELOPMENT
OF NORMATIVE AND METHODOLOGICAL DOCUMENTS FSI «SRC «OKHRANA» OF THE FEDERAL
SERVICE OF NATIONAL GUARD OF RUSSIA**

**PROBLEM ISSUES OF EQUIPPING FACILITIES (TERRITORIES) WITH WARNING AND
EVACUATION MANAGEMENT SYSTEMS IN THE EVENT OF A THREAT OR COMMITMENT
OF A TERRORIST ACT**

Annotation. This article discusses the issues of regulatory regulation of ensuring the protection of critical infrastructure and life support facilities, places of mass stay of people from terrorist threats and equipment of facilities (territories) with warning and evacuation systems (complexes) in case of threat of a terrorist act.

Keywords: anti-terrorist protection, protection of facilities, warning systems, functional independence, warning signals.

Защита объектов и населения от угроз террористического характера является первоочередной задачей государства. Законодательство Российской Федерации ориентировано на охрану прав личности и обеспечение деятельности государственных институтов.

Политика государства в данной сфере формируется Концепцией противодействия терроризму в Российской Федерации [1], определяющей основные принципы политики государства в области противодействия террористическим угрозам, а также цель, задачи и пути развития системы противодействия терроризму.

Для обеспечения безопасности граждан, защиты объектов инфраструктуры и жизнеобеспечения от антитеррористических проявлений Концепцией определены меры, направленные на противодействие террористическим угрозам, начиная от предупреждения (профилактики) и заканчивая непосредственным реагированием на такие угрозы.

В целях предупреждения (профилактики) террористических проявлений необходимо совершенствование правовой базы, а также

введение в действие типовых требований, направленных на защиту объектов инфраструктуры и жизнеобеспечения от террористических угроз путем оборудования их комплексами технических средств охраны и обеспечения безопасности.

Обязательное наличие на объектах таких комплексов предусмотрено действующими нормативными правовыми актами, устанавливающими требования к антитеррористической защите в отношении ряда ведомств, такими как Федеральный закон от 6 марта 2006 года № 35-ФЗ «О противодействии терроризму» [2], а также разработанными в его продолжение подзаконными актами, конкретизирующими его положения.

Так, в соответствии с требованиями, предъявляемыми к антитеррористической защите мест массового пребывания людей и объектов, подлежащих обязательной охране войсками национальной гвардии [3], и требованиями к защите от террористических угроз объектов Минпросвещения России [4] предусмотрено обязательное наличие комплексов, обеспечивающих информирование людей при угрозе возникновения предпосылок совершения террористических актов, при этом, акцент сделан на их функциональной независимости.

Обеспечение безопасности на сегодняшний день является одним из важнейших и актуальных вопросов, требующих постоянного развития комплекса мер реагирования на террористические угрозы. В этих целях ФКУ «НИЦ «Охрана» Росгвардии была реализована задача по разработке и введению в действие национального стандарта ГОСТ Р 71934-2025 «Системы тревожной сигнализации. Системы оповещения при угрозе совершения или совершении террористического акта. Общие технические требования. Методы испытаний» [5] (далее – ГОСТ Р 71934 или стандарт), в рамках которого реализован единообразный понятийный аппарат в области систем оповещения при угрозе совершения или совершении террористического акта (далее – СО при УСТА). При этом понятийный аппарат, используемый для данного класса технических средств, и основные характеристики учитывают уже введенные понятия и характеристики в отношении существующих видов комплексов оповещения, например, систем оповещения и управления эвакуацией при пожаре (далее – СОУЭ при пожаре).

Установленные в стандарте требования к СО при УСТА в технической части согласованы с основными требованиями, предъявляемыми к СОУЭ при пожаре, для возможности использования на объектах номенклатуры технических средств, применяемых в СОУЭ при пожаре.

Вместе с тем практика применения стандарта в области СО при УСТА сформировала ряд проблемных вопросов как юридического (в части нормативного регулирования применения системы СО при УСТА), так и технического характера (реализация способов информирования при возникновении угрозы и возможность использования оборудования СОУЭ при пожаре).

Так, изменением № 1 к Своду правил (СП 484.1311500.2020) [6], введенным в действие МЧС России с 1 сентября 2025 года, предусмотрена возможность использования оборудования СОУЭ при пожаре для целей информирования при возникновении предпосылок совершения террористического акта.

В марте текущего года завершено публичное обсуждение нового проекта Свода правил (СП 3.13130) [7], вводимых взамен СП 3.13130-2009 [8]. Новая редакция документа допускает применение технических средств, предназначенных для речевого оповещения о пожаре, в том числе в целях информирования об угрозе совершения террористического акта и мерах антитеррористического характера. Однако, противоречия в законодательстве в части требований, предъявляемых к функциональной независимости комплексов, обеспечивающих передачу звуковой информации при возникновении угрозы совершения террористического акта,

не позволяют в полной мере реализовать указанные изменения.

Законодательно установленная обязательная функциональная независимость СОУЭ при пожаре на объектах, подлежащих обязательной охране войсками национальной гвардии [3], а также на объектах Минпросвещения России [4] делает невозможным ее совместное использование с СО при УСТА.

Одновременно, требованиями, предъявляемыми к защите от возникающих террористических угроз на объектах Минобрнауки России [9], определены лишь обязательные мероприятия по их оборудованию комплексами для информирования и координации действиями людей при эвакуации, при этом функциональная независимость таких комплексов не устанавливается.

В текущем году были утверждены требования по защите объектов Федерального агентства по делам национальностей от угроз антитеррористической направленности [10], которые также не устанавливают функциональную независимость используемых на объектах СО при УСТА.

Таким образом, различие требований в части обязательного наличия отдельных комплексов на объектах, находящихся в ведении различных государственных органов, затрудняют скоординированную реализацию мер по обеспечению антитеррористической защиты объектов. Также имеется ряд нерешенных вопросов технической направленности, затрагивающих возможность совместной работы СО при УСТА и СОУЭ при пожаре. Так, ввиду наличия принципиально различных подходов к предупреждению и реагированию на чрезвычайные ситуации, вызванные различными видами угроз (террористические, пожары, стихийные бедствия или иные), остается довольно проблематичной возможность однозначного разрешения порядка взаимодействия нескольких комплексов, применяемых при таких угрозах. Поскольку СО при УСТА должны быть автономными, а СОУЭ при пожаре иметь безусловный приоритет срабатывания, то в чрезвычайной ситуации они будут работать одновременно.

Вместе с тем стандартом [5] предусмотрена возможность применения в качестве СО при УСТА иных комплексов и устройств в их составе при условии соблюдения нормативных требований в данной области. Положения стандарта сфокусированы на установлении требований к техническим характеристикам СО при УСТА и устройствам в их составе, обеспечивающих своевременное информирование об угрозе нападения или внезапном нападении в целях совершения террористического акта.

В тоже время, возможность использования оборудования СОУЭ при пожаре для целей информирования об угрозе возникновения предпосылок для совершения террористического акта при безусловном приоритете ее срабатывания может привести к противоречию в части действий, направленных на спасение людей. Тактика действий по спасению при пожаре предполагает незамедлительное перемещение людей в безопасную зону, чтобы исключить получение термических травм и отравление продуктами горения, тогда как действия по спасению при совершающемся террористическом акте напрямую зависят от действий злоумышленников, которые практически не поддаются прогнозированию, а указание на незамедлительную эвакуацию в сторону выхода, где могут находиться террористы, может стать принципиальной и фатальной тактической ошибкой, которая неизбежно приведет к трагическим последствиям.

Также следует учитывать вероятность поведенческих сценариев злоумышленников. Со стороны террористов могут быть предприняты действия, направленные на скопление людей в ходе эвакуации, например, путем поджога или просто включения СОУЭ при пожаре. Ярким примером этому служит террористическая атака, совершенная группой лиц в марте 2024 года в «Крокус Сити Холл», в ходе которой террористы подожгли концертный зал и стали расстреливать пытавшихся спастись людей на выходе из него.

Становится очевидным, что в случае срабатывания нескольких установленных одинаковых по принципу действия звуковых и световых оповещателей, работающих в системах разного назначения, потребуются определенные знания для правильного понимания и реагирования на формируемые ими сигналы: к какой именно системе относится прибор и что делать при его срабатывании. В экстренной ситуации, в условиях стресса и дефицита времени такая

неопределенность может стоить жизни, и поэтому должна быть полностью исключена.

Решение данной задачи может быть возможно включением в систему оповещения модулей управления эвакуацией, что не противоречит требованиям ГОСТ Р 71934 [5]. Так, стандартом предусмотрены способы оповещения путем трансляции через СО при УСТА сообщений, проговариваемых в микрофон или посредством световых указателей. Такие варианты потребуют проведения особой организации рабочего места должностного лица, передающего необходимую информацию, гарантирующего его безопасность, а также обеспечивающего по возможности визуальный контроль перемещения злоумышленников.

Именно поэтому требования стандарта [5] ориентированы, в первую очередь, на функциональную надежность СО при УСТА и гарантированное доведение речевой информации на территории объекта. Необходимость учета ситуации при реализации террористической угрозы указывает на целесообразность сохранения за лицами и службами, ответственными за антитеррористическую защиту объектов, вариативности транслируемых речевых сообщений. В данном случае решающей организационной задачей со стороны ответственных служб является создание условий для однозначного понимания людьми, находящимися на объекте, в первую очередь – персоналом, сигналов оповещения.

Таким образом, для точного определения характера угрозы требуется постоянная организационная подготовка персонала и служб, ответственных за антитеррористическую защиту конкретного объекта, что позволит сохранить жизни и здоровье людей даже при трансляции противоречивой информации, поступающей от СО при УСТА и СОУЭ при пожаре.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Концепция противодействия терроризму в Российской Федерации: утверждена Президентом Российской Федерации 5 октября 2009 года // Официальный сайт «Российская газета» (<https://rg.ru>) – 20.10.2009 – № 198.
2. О противодействии терроризму: федеральный закон от 6 марта 2006 г. № 35-ФЗ // Собрание законодательства Российской Федерации – 13.03.2006 – № 11 – Ст. 1146.
3. Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии Российской Федерации, и форм паспортов безопасности таких мест и объектов (территорий): постановление Правительства Российской Федерации от 25 марта 2015 года № 272 // Собрание законодательства Российской Федерации – 14.04.2015 – № 14 – Ст. 2119.
4. Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий): постановление Правительства Российской Федерации

от 2 августа 2019 года № 1006 // Собрание законодательства Российской Федерации – 12.08.2019 – № 32 – Ст. 4716.

5. ГОСТ Р 71934-2025 «Системы тревожной сигнализации. Системы оповещения при угрозе совершения или совершении террористического акта. Общие технические требования. Методы испытаний» утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 27 января 2025 г. № 27-ст: дата введения – 2025-03-01 // Официальный интернет-портал Росстандарта (info@rst.gov.ru) – 1.03.2025 – № 27-ст.

6. Изменение № 1 СП 484.1311500.2020 Системы противопожарной защиты. Системы пожарной сигнализации и автоматизация систем противопожарной защиты. Нормы и правила проектирования: утверждены приказом Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий бедствий от 27.03.2025 № 252: дата введения – 2025-09-01 // Официальный сайт МЧС России (mchs.gov.ru).

7. СП 3.13130 «Системы противопожарной защиты. Система оповещения и управления эвакуацией людей при пожаре. Требования пожарной безопасности»: проект: уведомление о сводах правил от 03.09.2024 // Официальный сайт Росстандарта (st.gov.ru).

8. СП 3.13130-2009 «Системы противопожарной защиты. Система оповещения и управления эвакуацией людей при пожаре. Требования пожарной безопасности» от 25.03.2009 №173: дата введения – 2009-05-01 // Официальный сайт МЧС России (mchs.gov.ru).

9. Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства науки и высшего образования Российской Федерации и подведомственных ему организаций, объектов (территорий), относящихся к сфере деятельности Министерства науки и высшего образования Российской Федерации, формы паспорта безопасности этих объектов (территорий) и признании утратившими силу некоторых актов Правительства Российской Федерации: постановление Правительства Российской Федерации от 7 ноября 2019 г. № 1421 // Собрание законодательства Российской Федерации – 14.11.2019 – № 46 – Ст. 6491.

10. Об утверждении требований к антитеррористической защищенности объектов (территорий) Федерального агентства по делам национальностей, его территориальных органов, подведомственных организаций и формы паспорта безопасности этих объектов (территорий): постановление Правительства Российской Федерации от 24 февраля 2025 года № 209 // Собрание законодательства Российской Федерации – 09.03.2015 – № 9 – Ст. 941.

УДК 351.74:004

**АНТЫШЕВ АЛЕКСАНДР АЛЕКСАНДРОВИЧ, ВЕДУЩИЙ НАУЧНЫЙ СОТРУДНИК
НАПРАВЛЕНИЯ ПО ВЗАИМОДЕЙСТВИЮ С ВОЕННО-ПРОМЫШЛЕННОЙ КОМИССИЕЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ ФКУ НПО «СТИС» МВД РОССИИ**

**СОЛДАТЕНКОВА НАДЕЖДА АЛЕКСЕЕВНА, ВЕДУЩИЙ НАУЧНЫЙ СОТРУДНИК
НАПРАВЛЕНИЯ ПО ВЗАИМОДЕЙСТВИЮ С ВОЕННО-ПРОМЫШЛЕННОЙ КОМИССИЕЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ ФКУ НПО «СТИС» МВД РОССИИ**

О ВОПРОСАХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ДЕЯТЕЛЬНОСТИ УЧАСТКОВОГО УПОЛНОМОЧЕННОГО ПОЛИЦИИ

Аннотация. В статье рассмотрены основные потребности участкового уполномоченного полиции (УУП) в специальной технике при выполнении оперативно-служебных задач. Описан опыт применения передовых технологий в международной практике. Сформулированы научно-технические предложения по развитию материально-технического обеспечения для деятельности УУП с учётом применения инновационных технических решений. Представленные рекомендации согласуются с тенденциями развития науки и техники и нацелены на оптимизацию деятельности УУП.

Ключевые слова: участковый уполномоченный полиции, умный (цифровой) пункт полиции, специальная техника.

Повседневная служба участковых уполномоченных полиции (УУП) обусловлена многообразием функциональных обязанностей. Успешное выполнение возложенных на УУП обязанностей является залогом хорошего состояния оперативной обстановки на обслуживаемом территории. По своему содержанию должность УУП выполняет задачи как работник оперативной службы, осуществляет поручения по линии работы дознавателей и следователей, ведет учёт и осуществляет проверки по соблюдению миграционного и регистрационного режима, контроль поднадзорного контингента, оказывает содействие в предупреждении безнадзорности и правонарушений среди несовершеннолетних, ведет профилактическую работу с населением, а также оказывает содействие другим службам и органам, в том числе не находящимся в подчинении МВД России. [2]

Центральное положение УУП среди сотрудников территориальных подразделений МВД России вызывает потребность в проработке мер, ориентированных на снижение нагрузки, оптимизации временных затрат и повышении результативности при реализации оперативно-служебных задач.

Достижение этих целей возможно при автоматизации процессов служебной деятельности, оптимизации документооборота, создание условий для осуществления технического обслуживания, оснащением данных сотрудников современными специальными техническими средствами.

Мировой опыт показывает, что перспективными направлением развития по линии цифровых технологий является внедрение «умных»

технологий, основанных на технологиях «больших данных», искусственного интеллекта, робототехнических системах [3-4]. На сегодняшний день в Китае, Южной Корее, США, Японии, и Израиле широко применимы технологии искусственного интеллекта и робототехнические комплексы в правоохранительной и правоприменительной практике, а публикации о внедрении передовых технологий в деятельность полицейских подразделений позволяет сделать вывод о внедрении VR и AR-технологий (виртуальная и дополненная реальность).

Направления развития отечественной промышленности совпадают с мировыми тенденциями. Российские предприятия проводят разработки по развитию новых технологий, в том числе в части создания отечественной электронной компонентной базы и перспективных разработок вооружения, военной и специальной техники в интересах силовых ведомств в рамках Программы развития оборонно-промышленного комплекса и государственной программы вооружения.

Внедрение цифровых технологий должны быть интуитивно-понятными в эксплуатации, а их разработка должна основываться на анализе процессов, происходящих в подразделениях.

Сотрудниками ФКУ НПО «СТИС» МВД России проводятся исследования, направленные на выявление потребностей, в том числе УУП, в материально-техническом обеспечении, информационных сервисах и ресурсах, с учётом перспективы применения средств и систем основанных на инновационных технологиях, а также учёта специфики функциональных обязанностей и оперативно-служебных задач

участковых уполномоченных полиции, мест расположения впервые разворачиваемых участковых пунктов полиции (УПП)(климатические, физико-географические условия), других особенностей.

Предварительные результаты исследования показали, что наибольший интерес у УУП для перспективного оснащения показали беспилотные аппараты (далее – БПА) как летательного типа, так и наземного, в том числе работающих в автономном режиме. БПА помогут УУП в проведении мониторинга обслуживаемой территории для обеспечения безопасности граждан и объектов, при проведении массовых мероприятий, оперативно-розыскных мероприятий, поисково-спасательных работах на местности. Безусловно, применение БПА обеспечит безопасность и личного состава органов внутренних дел, повысит оперативность реагирования на правонарушения, а также поспособствует их пресечению.

Также для решения задач мониторинга в деятельности УУП существенную поддержку может оказать интегрированная система видеонаналитики поступающей информации с персональных носимых устройств видеофиксации, правоохранительного сегмента системы «Безопасный город» и других контролирующих видеокамер, расположенных на объектах обслуживаемой территории. Работа такой системы может быть реализована на основе алгоритмов искусственного интеллекта и выполнять функции по распознаванию типовых ситуаций, требующих реагирования.

В дополнение к БПА для поисково-спасательных операций УУП выражают необходимость в обеспечении специальными поисковыми средствами: тепловизорами, приборами ночного видения, очками дополненной реальности с системой интеллектуального распознавания.

Для сельских населенных УПП, важен вопрос служебного транспорта, когда проезд на легковом автомобиле бывает затруднен из-за природных особенностей (отсутствие дорог, сезонные разливы водоемов, схождение снежных масс и т.д.), тогда в перспективе предлагается оснащение специальными транспортными средствами: квадроциклами, маломерными судами, снегоходами. Такой автотранспорт повысит мобильность УУП вне зависимости от погодных условий. В городской местности будет актуально обеспечение УУП средствами индивидуальной мобильности электрические самокаты, гироскутеры, электровелосипеды. Вместе с тем, такое решение подойдет и для УУП не имеющих водительского удостоверения.

Продолжая тему различия в материально-техническом обеспечении участковых пунктов

полиции (УПП) в зависимости от характера обслуживаемой территории, необходимо отметить, что для сельских УУП является актуальным наличие аппаратно-программного комплекса (далее – АПК) для работы на местах преступления. Сотрудники экспертно-криминалистической службы не всегда могут оперативно прибыть на место преступления, тогда УУП с помощью «умного» АПК сканирует место преступления и направляет цифровую копию для предварительного анализа. Подобный прибор позволит обнаруживать, выявлять и фиксировать следы и иную криминалистически значимую информацию и передавать данные для соответствующего анализа и поиска по базам данных и учетам. Целесообразно также предусмотреть возможность устанавливать такой прибор как полезную нагрузку на БВС или робототехнический комплекс; высокотехнологичных нейросетей, интегрирование которых в систему криминалистических учетов позволит осуществлять проверку и сравнительный анализ полученной информации даже в случае с малоинформативным объектом (например, смазанного следа пальца руки).

Особое внимание заслуживают средства радиосвязи. Разнородность стандартов радиосвязи и самого оборудования порождает ряд трудностей при взаимодействии с другими оперативными подразделениями. Решением этой проблемы видится оснащение УПП средствами радиосвязи разработанных в рамках Единой национальной платформы радиосвязи. Это комплекс технических решений на основе доверенного и защищенного российского оборудования, программного и информационного обеспечения, соответствующих комплексу национальных стандартов ГОСТ Р 71586 «Цифровая профессиональная подвижная радиосвязь». Создание масштабируемых многозоновых многоканальных отечественных систем профессиональной радиосвязи поспособствует повышению эффективности и оперативности межведомственного взаимодействия на различных уровнях управления при проведении мероприятий, связанных с обеспечением общественной безопасности, предупреждением и ликвидацией чрезвычайных ситуаций и террористических угроз.

Вопрос совершенствования деятельности УУП это не только «умный участковый пункт полиции», наличие современной специальной техники, но и экипировка самого участкового. УУП отмечена высокая потребность в различных средствах индивидуальной защиты. В рамках межведомственной работы по экипировке полицейского будущего по прогнозам аналитиков должна состоять из следующих систем:

система защиты;
система управления и связи;
система жизнеобеспечения;
система энергообеспечения;
система робототехнического обеспечения;
система поражения.

Подобнее об этих системах, их техническом составе и функциональных возможностях отражено в работах [5].

Для работы с гражданским населением также требуется внедрение новых цифровых решений. Обращаясь к международному опыту, приведем в пример полицейских в г. Дубай (Объединенные Арабские Эмираты), где на основе передовых технологии работает «умный» полицейский участок. Граждане самостоятельно регистрируют обращения в полицию в электронном виде, по видеосвязи обсуждают с полицейскими его суть, что позволяет заявителю получить информацию о принимаемых мерах в срок до 7 дней. Кроме того, в г. Дубай существуют подразделения называемые - «Департамент счастья», которые осуществляют оценку запросов населения, относящихся к повседневной деятельности полиции и предоставлению государственных услуг через сеть многофункциональных центров [4].

Расширить применение такого цифрового помощника можно путем установки на улицах и в общественных местах информационных порталов с голосовым ассистентом. Граждане смогут обратиться за помощью, а также принять и оформить заявление (в какой пункт полиции и к какому сотруднику обратиться, автоматически внося эту информацию в информационную систему/запись в электронную очередь).

Развитие информационных технологий и информационных сервисов обеспечения повседневной деятельности МВД России также является неотъемлемой частью цифровой трансформации УПП. Здесь, важно указать, что данное направление согласно Концепции развития информатизации деятельности по охране общественного порядка в системе МВД России до 2030 года является приоритетным. Концепцией предусмотрена разработка мобильного приложения для планшета, включающего базу данных и знаний с целью оказания помощи сотруднику, системы видеонаблюдения и видеоаналитики информации, поступающей с различных устройств видеofиксации, а также патрульных робототехнических комплексов. Таким образом, планируется создание единого информационного пространства с доступностью данных в соответствии с ролевой моделью.

Введение в отдельных местностях Российской Федерации военного положения, режимов повышенных уровней реагирования или готовности объективно привносит в порядок несения службы указанными сотрудниками определенные особенности. Относительно материально-технического обеспечения эти особенности нашли отражение в потребности подразделений в служебном автотранспорте бронированного исполнения, средствах обнаружения и противодействию БПЛА, средствах оказания первой медицинской помощи.

Специальный транспорт в данном случае это автомобили с модульной архитектурой защиты кузова от поражающих факторов стрелкового оружия и взрывных устройств различного типа, оснащенные бортовой информационно-управляющей системой, автоматизированной системой управления средствами поражения; дистанционно управляемыми боевыми модулями с различным вооружением летального и нелетального воздействия (в том числе скрытого исполнения), средством обнаружения направления ведения огня; блокиратором радиоуправляемых взрывных устройств; беспилотными робототехническими и роботизированными средствами обнаружения и противодействия БВС.

Исследование потребностей УУП в материально-техническом оснащении будущего УПП наглядно продемонстрировало контрастность потребностей в зависимости от оперативной обстановки на обслуживаемой территории, физико-географического положения, а также человеческих факторов. Общим остаётся запрос на цифровую трансформацию рутинных функциональных обязанностей УУП, автоматизацию процессов и повышение оперативности. Реализация указанных потребностей возможна при проведении научных изысканий, в том числе при взаимодействии с передовыми отечественными предприятиями и организациями.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Тепляков С.В. Перспективы инновации в МВД России // Актуальные исследования. 2021 №4 (31). С. 15-17.
2. Организация деятельности участкового уполномоченного полиции. Авторский коллектив: Аврутин Р.Ю., Беженцев А.А., Ваганов А.Э., Ермолаев В.Г., Кулаков Н.А., Лампадова С.С., Лиховенков С.И., Паук Н.Н., Сахарова Т.А., Стульнова Т.В., Тарасов А.В., Ткачук В.Н., Холманский В.И., Шельпяков А.А. Учебно-практическое пособие – СПб. 2020. – 427 с.
3. Лукашов Н.В. Организационные и правовые основы применения полицейских робототехнических комплексов в органах внутренних дел Российской Федерации // Труды академии управления МВД России. 2020. №3 (55). С. 210-221.
4. Садыков М.Б. Внедрение автономных систем в Объединенных Арабских Эмиратах на примере полиции Дубая: правовые и технические аспекты// В сборнике: Технологии XXI века в юриспруденции. 2022. С.162-173.
5. Облик сотрудника полиции будущего: отчет о НИР/ руководитель А.А. Антышев; исполнители: В.В. Бородай, Ю.А. Волобринская, Ю.А. Лекарь, Ю.В. Синютин; ФКУ НПО «СТиС» МВД России. - М., 2024. – 65 с. Рег. № НИОКТР 01241837.

УДК 654.9

ББК 30ц

АНЮХИН СЕРГЕЙ ГЕОРГИЕВИЧ, СТАРШИЙ НАУЧНЫЙ СОТРУДНИК ОТДЕЛА РАЗВИТИЯ СРЕДСТВ ОБНАРУЖЕНИЯ ФЕДЕРАЛЬНОГО КАЗЕННОГО УЧРЕЖДЕНИЯ «НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР «ОХРАНА» РОСГВАРДИИ

РЯБЦЕВ НИКОЛАЙ АЛЕКСЕЕВИЧ, НАЧАЛЬНИК ОТДЕЛА РАЗВИТИЯ СРЕДСТВ ОБНАРУЖЕНИЯ ФЕДЕРАЛЬНОГО КАЗЕННОГО УЧРЕЖДЕНИЯ «НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР «ОХРАНА» РОСГВАРДИИ, КАНДИДАТ ТЕХНИЧЕСКИХ НАУК

ДМИТРИЕВ РОМАН СЕРГЕЕВИЧ, НАЧАЛЬНИК СЕКТОРА ОТДЕЛА РАЗВИТИЯ СРЕДСТВ ОБНАРУЖЕНИЯ ФЕДЕРАЛЬНОГО КАЗЕННОГО УЧРЕЖДЕНИЯ «НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР «ОХРАНА» РОСГВАРДИИ, КАНДИДАТ ТЕХНИЧЕСКИХ НАУК

КУЛИКОВА ЕЛЕНА ВАДИМОВНА, ВЕДУЩИЙ ИНЖЕНЕР-ИССЛЕДОВАТЕЛЬ АО «НИИ КП» ГП РОСКОСМОС, КАНДИДАТ ТЕХНИЧЕСКИХ НАУК

К ВОПРОСУ СОВЕРШЕНСТВОВАНИЯ ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ НОРМАТИВНЫХ ДОКУМЕНТОВ С УЧЕТОМ РАСШИРЕНИЯ ПРАКТИКИ ПРИМЕНЕНИЯ РАДИОВОЛНОВЫХ ИЗВЕЩАТЕЛЕЙ

Аннотация. В статье рассмотрены вопросы совершенствования технических требований нормативных документов с учетом расширения практики применения радиоволновых извещателей. Представлены основные нормативные документы в области стандартизации, касающиеся производства, порядка проведения испытаний и методов контроля средств обнаружения, основанных на радиоволновом физическом принципе действия. Описаны вновь введенные положения, затрагивающие технические параметры радиоволновых извещателей.

Ключевые слова: охрана, средство обнаружения, радиоволновый извещатель, стандартизация, технические требования, нормативно-правовой акт.

ANYUKHIN SERGEY GEORGIEVICH, SENIOR RESEARCHER OF THE DETECTION TOOLS DEVELOPMENT DEPARTMENT OF THE FEDERAL STATE INSTITUTION «SCIENTIFIC RESEARCH CENTER «OKHRANA» OF THE FEDERAL SERVICE OF NATIONAL GUARD OF THE RUSSIAN FEDERATION

RYABTSEV NIKOLAY ALEKSEEVICH, HEAD OF THE DETECTION TOOLS DEVELOPMENT DEPARTMENT OF THE FEDERAL STATE INSTITUTION «SCIENTIFIC RESEARCH CENTER «OKHRANA» OF THE FEDERAL SERVICE OF NATIONAL GUARD OF THE RUSSIAN FEDERATION, CANDIDATE OF TECHNICAL SCIENCES

DMITRIEV ROMAN SERGEEVICH, HEAD OF THE SECTOR OF THE DETECTION TOOLS DEVELOPMENT DEPARTMENT OF THE FEDERAL STATE INSTITUTION «SCIENTIFIC RESEARCH CENTER «OKHRANA» OF THE FEDERAL SERVICE OF NATIONAL GUARD OF THE RUSSIAN FEDERATION, CANDIDATE OF TECHNICAL SCIENCES

KULIKOVA ELENA VADIMOVNA, LEADING RESEARCH ENGINEER AT JSC RESEARCH INSTITUTE OF SPACE TECHNOLOGIES OF THE ROSCOSMOS STATE CORPORATION, CANDIDATE OF TECHNICAL SCIENCES

ON THE ISSUE OF IMPROVING THE TECHNICAL REQUIREMENTS OF THE REGULATORY DOCUMENTS, TAKING INTO ACCOUNT THE EXPANSION OF THE PRACTICE OF USING RADIO WAVES DETECTORS

Annotation. The report discusses the issues of improving the technical requirements of regulatory documents, taking into account the expansion of the practice of using radio wave detectors. The main normative documents are presented standardization documents related to the production, testing procedures, and control methods of detection devices based on the radio wave physical principle of operation. The newly introduced provisions affecting the technical parameters of radio wave detectors are described.

Keywords: security, detection device, radio wave detector, standardization, technical requirements, regulatory legal act.

Средства обнаружения, основанные на радиоволновом физическом принципе действия (далее – РВ-извещатели) подразделяются на два типа – линейные РВ-извещатели для охраны периметра и объемные РВ-извещатели. В связи с рядом преимуществ перед аналогичными по области применения средствами обнаружения РВ-извещатели в последнее время получили широкое распространение при организации охраны различных объектов. Так линейные РВ-извещатели могут контролировать прямолинейные протяженные участки периметров объектов длиной до 300 м, объемные РВ-извещатели, предназначенные для охраны помещений и открытых площадок, имеют более широкий диапазон обнаруживаемых скоростей и антропологических параметров нарушителя, также у них отсутствует зависимость обнаружительной способности от направления движения нарушителя в зоне обнаружения извещателя.

Преимущества РВ-извещателей связаны с особенностями радиоволнового физического принципа, повышающих параметры их помехоустойчивости и обнаружительной способности.

При охране открытых площадок, извещателями большой дальности действия, для выделения на фоне помех полезных сигналов, возникающих при перемещении нарушителя в зоне обнаружения, применяется метод линейной частотной модуляции излучаемой энергии. Данный метод позволяет выделить величину разности фаз между излученным и отраженным от нарушителя сигналами.

В этом случае величина этой разности фаз зависит от дистанции, которую прошел нарушитель по направлению к извещателю.

Для анализа возможного появления помех в зоне обнаружения или сигнала от перемещения нарушителя полученные значения разности фаз сравниваются с заданными параметрами, по которым определяется появление полезного сигнала. Если измеренные значения фаз превышают установленный порог, это определяется извещателем, как перемещение нарушителя и формируется извещение о срабатывании.

Высокая степень устойчивости РВ-извещателей к внешним воздействующим факторам окружающей среды, таких как атмосферные осадки (дождь, снег), природные помехи (раскачивание деревьев и кустов от ветровых нагрузок), вибрация

предметов обеспечиваются физическим принципом их функционирования.

Также минимизируется риск возникновения ложных срабатываний из-за перемещения объектов с небольшой площадью поверхности, отражающей радиоволны, таких как мелкие животные (например, крысы или кошки).

Также РВ-извещатели способны обнаруживать современные угрозы в том числе такие, как проникновение на охраняемый объект (территорию) дистанционно управляемых аппаратов.

Положительный опыт, полученный в ходе разработки и эксплуатации РВ-извещателей был закреплен в новых нормативных документах, с учетом положений действующих стандартов, например, национального стандарта Российской Федерации [1], определяющего общие технические и функциональные требования технических средств охранной сигнализации, а также их классификацию в зависимости от наличия дополнительных функций. Кроме того, необходимо учитывать положения иных нормативно-правовых актов, затрагивающих данную предметную область, например, постановление [2], которым определены радиоэлектронные приборы и устройства, не требующие регистрации. Также постановлением установлены допустимые параметры диапазона рабочих частот и максимальной излучаемой мощности РВ-передатчика.

При непосредственном участии авторов в период с 2020 по 2023 годы в соответствии с утвержденными программами стандартизации внесены изменения в действующие нормативные документы:

- национальный стандарт на линейные РВ-извещатели для охраны периметров объектов;
- национальный стандарт на объемные РВ-извещатели для закрытых помещений и открытых площадок [3] (таблица 1).

Изменения в национальном стандарте на линейные РВ-извещатели проведены с целью поддержки импортозамещающих технологий, введения требований к ширине полосы излучаемых частот, уровню внеполосных излучений радиопередатчиков, а введенная функция автоматического мониторинга уровня принимаемого радиосигнала учитывает воздействие климатических и природных условий (сугробы снега, высокий травяной покров), что повышает надежность функционирования.

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

Национальный стандарт на объемные РВ-извещатели пересмотрен с целью установления конкретных требований, условий и методов испытаний для контроля параметров, выполнение которых расширяет их функциональные возможности в части выявления перемещения нарушителя в пределах помещения или на территории, а также попыток проникновения на транспортных средствах или дистанционно

управляемых аппаратов наземным, водным или воздушным путями.

Также в рассмотренных нормативных документах проведена актуализация ссылочной нормативной базы и в связи с возникновением дополнительных рисков введен новый понятийный аппарат, приведенный в соответствие с действующими терминами и определениями.

Таблица 1 – Изменения, внесенные в нормативные документы на РВ-извещатели

	Наименование нормативных документов	
Наименование актуализируемого нормативного документа	ГОСТ Р 52651-2006. Национальный стандарт Российской Федерации. Извещатели охранные линейные радиоволновые для периметров. Общие технические требования и методы испытаний	ГОСТ Р 50659-2012. Национальный стандарт Российской Федерации. Извещатели радиоволновые доплеровские для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний
Наименование актуализированного нормативного документа	ГОСТ Р 52651-2022. Национальный стандарт Российской Федерации. Извещатели охранные линейные радиоволновые для периметров. Общие технические требования и методы испытаний	ГОСТ Р 50659-2024. Национальный стандарт Российской Федерации. Извещатели радиоволновые доплеровские для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний
Внесенные изменения	<ul style="list-style-type: none"> - определены области применения стандарта; - сформирован перечень стандартов, на которые даются ссылки в национальном стандарте; - установлены основные термины с соответствующими определениями; - введены новые технические требования к полосе излучаемых частот; - введены новые технические требования к ширине полосы радиочастот и внеполосным излучениям радиопередатчиков; - введены новые технические требования к автоматическому контролю величины запаса уровня принимаемого радиосигнала; - введены новые методы испытаний 	<ul style="list-style-type: none"> - определены области применения стандарта; - сформирован перечень стандартов, на которые даются ссылки в национальном стандарте; - установлены основные термины с соответствующими определениями; - введены новые технические требования к обнаружению дистанционно управляемых аппаратов; - введены новые методы испытаний
Год разработки	2020–2022	2023
Дата вступления в действие	01.01.2023	01.06.2024

Разработанные национальные стандарты [4, 5] позволяют предприятиям-изготовителям средств обнаружения разрабатывать и поставлять на отечественный рынок технических средств безопасности РВ-извещатели, отвечающие требованиям нормативно-правовых актов Российской Федерации, обладающие высокими техническими и функциональными параметрами, а также отвечающие современному состоянию науки и техники.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р 52435–2015 Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний // «Консультант Плюс»: справочно-правовая система: [сайт]. - URL: <https://hq-cnsdb-01.rosgvard.ru> (дата обращения: 5 августа 2025 года).
2. О порядке регистрации радиоэлектронных средств и высокочастотных устройств: постановление Правительства РФ от 20.10.2021 № 1800 (ред. от 01.07.2024) // «Консультант Плюс»: справочно-правовая система: [сайт]. - URL: <https://hq-cnsdb-01.rosgvard.ru> (дата обращения: 5 августа 2025 года).
3. Рябцев Н.А., Анюхин С.Г., Куликова Е.В. Актуализация требований к извещателям охраняемым радиоволновым // Мягкие измерения и вычисления, 2024, том 81, № 8, с. 73-79.
4. ГОСТ Р 50659-2024. Национальный стандарт Российской Федерации. Извещатели радиоволновые доплеровские для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний // «Консультант Плюс»: справочно-правовая система : [сайт]. - URL: <https://hq-cnsdb-01.rosgvard.ru> (дата обращения: 6 августа 2025 года).
5. ГОСТ Р 52651-2022. Национальный стандарт Российской Федерации. Извещатели охранные линейные радиоволновые для периметров. Общие технические требования и методы испытаний // «Консультант Плюс»: справочно-правовая система: [сайт]. - URL: <https://hq-cnsdb-01.rosgvard.ru> (дата обращения: 6 августа 2025 года).

УДК 654.949

ББК 32.99

БАРИНОВ ИГОРЬ АЛЕКСАНДРОВИЧ, НАУЧНЫЙ СОТРУДНИК ФКУ «НИЦ «ОХРАНА» РОСГВАРДИИ

ГАПОНЕНКО ВАДИМ АЛЕКСАНДРОВИЧ, СТАРШИЙ НАУЧНЫЙ СОТРУДНИК ФКУ «НИЦ «ОХРАНА» РОСГВАРДИИ

КУЗЬМИНА ЕКАТЕРИНА НИКОЛАЕВНА, МЛАДШИЙ НАУЧНЫЙ СОТРУДНИК ФКУ «НИЦ «ОХРАНА» РОСГВАРДИИ

ПУТИ И МЕТОДЫ ПОВЫШЕНИЯ ИНФОРМАТИВНОСТИ СИСТЕМ ЦЕНТРАЛИЗОВАННОГО НАБЛЮДЕНИЯ

Аннотация. В статье представлен анализ алгоритмов работы объектового оборудования и пультового программного обеспечения и возможности их изменения с целью повышения информативности систем централизованного наблюдения.

Ключевые слова: системы централизованного наблюдения, информативность, объективное охранное оборудование, охранные извещатели, автоматизированные рабочие места.

BARINOV IGOR ALEXSANDROVICH, RESEARCHER AT THE FSI «SRC «OKHRANA» OF THE FEDERAL SERVICE OF THE NATIONAL GUARD OF THE RUSSIA

GAPONENKO VADIM ALEKSANDROVICH, SENIOR RESEARCHER AT THE FSI «SRC «OKHRANA» OF THE FEDERAL SERVICE OF THE NATIONAL GUARD OF THE RUSSIA

KUZMINA EKATERINA NIKOLAEVNA, JUNIOR RESEARCHER AT THE FSI «SRC «OKHRANA» OF THE FEDERAL SERVICE OF THE NATIONAL GUARD OF THE RUSSIA

WAYS AND METHODS OF INCREASING THE INFORMATION CONTENT OF CENTRALIZED SURVEILLANCE SYSTEMS

Annotation. The article presents an analysis of algorithms for the operation of object equipment and remote-control software and the possibility of changing them in order to increase the information content of centralized surveillance systems by.

Keywords: centralized monitoring system, informativeness, object security equipment, security detectors, automated workplaces.

Информативность систем централизованного наблюдения (далее – СЦН), применяемых для организации охраны объектов, определяется количеством типов, формируемых объектовым оборудованием тревожных, служебных и диагностических сообщений. Этот технический параметр является важным показателем данных систем в части обеспечения безопасности и защищенности охраняемых объектов – чем он выше, тем больше вероятность обнаружения несанкционированного проникновения либо оперативного реагирования на преступные посягательства. Её можно решать различными способами: посредством установки на объектах дополнительных средств обнаружения (извещателей), интеграции с объектовыми системами охраны, системами охранного видеонаблюдения и т.д. Однако, существует техническое решение, реализация которого не требует привлечения и установки дополнительных подсистем и технических средств

охраны (далее – ТСО), – это реализация незадействованных возможностей объектового оборудования и пультового программного обеспечения посредством изменения алгоритмов их функционирования.

Проведенный анализ режимов функционирования объектового оборудования различных СЦН, а также имеющийся опыт разработки и применения ТСО показали, что существует возможность повышения их информативности путем отслеживания перемещений по охраняемому объекту лиц, осуществивших незаконное проникновение. Это реализуемо посредством изменения алгоритмов функционирования объектового оборудования и пультового программного обеспечения в режиме тревоги, то есть после фиксации проникновения и передачи соответствующего тревожного извещения на пульт централизованного наблюдения (далее – ПЦН).

В настоящее время подразделениями вневедомственной охраны Росгвардии и частными охранными организациями для охраны объектов и мест проживания и хранения имущества граждан (далее – МПХИГ) применяются СЦН, в которых объективное оборудование может функционировать в трех основных режимах:

режим «снято с охраны» (объект не охраняется);
режим «взято под охрану» (объект охраняется);
режим «тревога» (охранным оборудованием зафиксировано несанкционированное проникновение на объект).

Анализ технической документации показал, что в СЦН реализовано несколько вариантов режимов функционирования объектового оборудования в режиме тревоги. При этом в большинстве СЦН объектовые приборы после фиксации нарушения шлейфа сигнализации (далее – ШС) и передачи информации на ПЦН либо прекращают контроль их состояния до снятия/повторного взятия объекта с охраны/под охрану, либо осуществляют ограниченное по количеству (времени) число попыток их контроля. Среди реализованных в объектовом оборудовании различных СЦН алгоритмов функционирования в режиме тревоги можно выделить следующие основные:

- объектовый прибор прекращает контроль ШС до момента получения команды на снятие с охраны;

- объектовый прибор осуществляет однократную попытку контроля ШС после фиксации тревоги через фиксированный интервал времени и, если он в состоянии «норма», производит взятие его под охрану с передачей соответствующего извещения на ПЦН;

- объектовый прибор осуществляет ограниченное число попыток контроля ШС, которое можно установить в его настройках, либо установить временной интервал, в течении которого будут осуществляться попытки контроля и взятия ШС под охрану.

- прибор все время от фиксации тревоги до получения команды на снятие/повторное взятие ШС с охраны/под охрану анализирует его состояние и в случае изменения передает соответствующее извещение на ПЦН.

Последний из перечисленных вариантов, реализованный у ряда производителей СЦН, является оптимальным алгоритмом работы объектовых приборов, он позволяет предоставить персоналу следующую дополнительную информацию по охраняемому объекту,

находящемуся в режиме тревоги: о месте нахождения лиц, осуществивших незаконное проникновение, их примерном количестве, возможном уходе с объекта, повторном проникновении в охраняемую зону и т.д.

Однако, и в этих СЦН в настройках объектовых приборов имеется опция отключения функции постоянного контроля ШС. Наличие её связано с необходимостью обеспечения работы с проводными безадресными охранными извещателями, наиболее часто используемыми в качестве средств обнаружения на охраняемых объектах и МПХИГ. Большинство типов данных извещателей имеют специфику в алгоритме функционирования в режиме тревоги. Эта специфика алгоритма работы извещателей заключается в следующем.

При появлении в зоне обнаружения нарушителя извещателем формируется сигнал «тревога» посредством разрыва ШС, в случае работы с нормально замкнутыми контактами реле либо замыканием ШС в случае работы с нормально разомкнутыми контактами реле. Время размыкания (замыкания) цепи ШС извещателями при формировании сигнала «тревога» и его гарантированной фиксации объектовым прибором должно составлять не менее 2 с.

После формирования сигнала тревоги извещателю необходимо время для восстановления в нормальное состояние (время на нормализацию чувствительного элемента), длительность которого в соответствии с ГОСТ на различные типы извещателей может лежать в диапазоне от 10 до 70 с.

На этот период времени извещатель не контролирует зону обнаружения, однако возвращает ШС в состояние «норма».

Указанный алгоритм функционирования не является корректным и не позволяет формировать достоверные извещения. Так, в случае контроля ШС объектовым прибором в течении временного периода восстановления извещателя и нахождения нарушителя в зоне обнаружения на ПЦН будет передано сообщение о восстановлении ШС, то есть о покидании нарушителем охраняемого помещения. При этом в случае постоянного нахождения нарушителя на объекте объектовый прибор будет формировать чередующиеся последовательно извещения «тревога» и «норма».

Оптимальным решением проблемы будет учет особенности функционирования проводных безадресных извещателей в алгоритме работы

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

объектовых приборов посредством временного интегрирования значений измеренных параметров ШС с целью исключения передачи на ПЦН неподтвержденных извещений.

Таким образом, для повышения информативности СЦН необходима реализация в алгоритмах функционирования объектового оборудования режима постоянного контроля ШС в режиме тревоги с обеспечением временного интегрирования параметров ШС при работе с проводными безадресными извещателями. Это потребует внесения изменений в программный код объектовых приборов и обновление прошивок, установленных на охраняемых объектах и МПХИГ изделий. Осуществление указанных мероприятий, учитывая реализованный во многих СЦН режим дистанционного обновления программной памяти, не вызовет серьёзных проблем.

Полученная на ПЦН информация о месте нахождения и перемещениях по объекту нарушителей должна представляться оперативному персоналу ПЦО. Это потребует изменения алгоритма работы автоматизированных рабочих мест (далее – АРМ) комплексов средств автоматизации пунктов централизованной охраны (далее – КСА ПЦО) и оснащение их функциями, которые будут использовать полученную информацию для её визуализации.

Важной составной частью служебной информации по объектам и МПХИГ, хранимой в базах данных серверов КСА ПЦО, являются графические планы их помещений, на которых указывается расположение установленных ТСО и описание уязвимых в части возможного проникновения мест.

В СЦН для визуализации обстановки на охраняемых объектах на основе полученной информации необходимо обеспечить возможность работы АРМ КСА ПЦО с указанными графическими планами. Для работы с базами данных СЦН в составе КСА ПЦО имеются отдельные АРМ: АРМ «Инженер», «Администратор базы данных» либо «Администратор», функции которых заключаются в создании карточек новых и редактирования существующих объектов и МПХИГ, создании и редактировании справочной и служебной информации, информации об установленных и используемых ТСО и т.д. Указанные АРМ, должны быть оснащены функцией разметки графических планов объектов и установления на них границ разделов и размещения входящих в их состав охраняемых зон.

При разметке границ разделов и входящих в их состав зон охраны структура охраняемого

объекта в виде иерархического выпадающего списка может располагаться в левой части окна АРМ «Инженер», а графический план охраняемого объекта в правой части. Это позволит обеспечить удобство

при осуществлении программной привязки разделов и охраняемых зон к помещениям объекта.

Для этих целей в АРМ должен быть реализован графический редактор (либо специальный режим работы), позволяющий размечать на планах объектов разделы и зоны охраны с их границами в виде графических компонент, имеющих индивидуальную цветовую окраску. Так как охраняемые объекты могут иметь различную планировку и зачастую сложную конфигурацию, графический редактор должен обеспечивать нанесение границ охраняемых зон и разделов произвольной формы, а также выбор цвета фона внутри границ для каждой зоны.

АРМ дежурного пульта управления (далее – ДПУ) на основе анализа информации, поступающей с охраняемых объектов, должно обеспечивать:

при возникновении тревожной ситуации на охраняемом объекте автоматический вывод на экран его графического плана;

выделение цветом (например, красным) зон охраны и границ разделов, на которых совершено проникновение;

нанесение на графический план маршрута и направления перемещения по объекту лиц, осуществивших незаконное проникновение на объект, посредством выделения цветом (отличным от «тревожного» цвета) разделов и охраняемых зон, которые они покинули.

В КСА ПЦО, кроме того, может быть реализован алгоритм определения примерной численности нарушителей посредством анализа количества зон охраны, одновременно находящихся в состоянии тревоги и отслеживания временных интервалов, в течение которых на них фиксировалось проникновение. На основе проведенного анализа пультовое программное обеспечение должно формировать извещения в протокол событий о предполагаемой численности нарушителей.

Еще одним важным элементом в ряду мероприятий по повышению информативности СЦН является передача сотрудникам групп задержания графического плана объекта, на который совершено незаконное проникновение, с нанесённой на него средствами АРМ текущей обстановкой, отражающий перемещения и нахождение лиц, осуществивших незаконное проникновение. Это также потребует реализации

в КСА ПЦО новых функций, обеспечивающих защищенное взаимодействие с мобильными устройствами сотрудников групп задержания. В настоящее время в составе ряда СЦН, применяемых подразделениями вневедомственной охраны, таких как СЦН «Приток-А», «Центавр Проксима» и «Струна-5», имеются мобильные приложения для собственников, в которых реализованы возможности получения информации с охраняемых объектов и управления объектовым оборудованием. Доработка указанных мобильных приложений с целью получения с АРМ КСА ПЦО графических планов объектов иной служебной информации и предоставление их для использования сотрудникам групп задержания позволит решить данную задачу.

Резюмируя изложенное, можно говорить о том, что в настоящее время существует реальная

возможность повышения информативности СЦН без установки дополнительных ТСО либо интеграции с другими системами охраны, реализуемая посредством проведения доработки программного обеспечения и модернизации объектового охранного оборудования, изменения алгоритмов работы и оснащения новыми функциями АРМ КСА ПЦО. Проведение указанных мероприятий не только обеспечит дополнительной оперативной информацией персонал ПЦО подразделений вневедомственной охран и мониторинговых центров частных охранных организаций, но и повысит уровень личной безопасности сотрудников групп задержания, эффективность их действий на охраняемых объектах, при реагировании по сигналам тревоги.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Автоматизированное рабочее место администратора базы данных Руководство по эксплуатации ФИДШ.425688.100 - 1 РЭ.
2. Комплекс пультового программного обеспечения «Ладога». Руководство по эксплуатации БФЮК. 425629.001 РЭ.
3. Межгосударственный стандарт ГОСТ 26342 Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры.
4. ГОСТ Р 52436 Приборы приемно-контрольные охранные. Классификация. Общие технические требования и методы испытаний.
5. ГОСТ Р 52435 Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний.
6. ГОСТ Р 56102.1 Системы централизованного наблюдения. Часть 1. Общие положения.

УДК 351.861

ВЕЛИКОКЛАД ТАТЬЯНА ПИМЕНОВНА

ПОДГОТОВКА СПЕЦИАЛИСТОВ БЕСПИЛОТНОЙ АВИАЦИИ.

ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

Аннотация. Статья посвящена актуальной проблеме, касающейся подготовки операторов беспилотных авиационных систем, с учетом сегодняшних требований к квалификации таких специалистов.

Ключевые слова: беспилотные авиационные системы, оператор, образовательные программы, подготовка специалистов, учебные центры.

TRAINING OF UNMANNED AVIATION SPECIALISTS.

PROBLEMS AND SOLUTIONS

Annotation. The article is devoted to the current issue of training operators of unmanned aerial systems, taking into account the current requirements for the qualifications of such specialists.

Keywords: unmanned aerial systems, operator, educational programs, training specialists, training centers.

Квалифицированные специалисты по эксплуатации беспилотных авиационных систем (далее - БАС) сегодня востребованы не только для решения военных задач, но и гражданских с целью оптимизации производственных процессов и обеспечения безопасности человека в современном мире. Важно напомнить, что в декабре 2022 года В.В. Путин поручил Агентству стратегических инициатив сформировать систему подготовки разных специалистов в сфере БАС. При этом необходимо подчеркнуть, что Министерством науки и высшего образования РФ, в рамках федерального проекта «Кадры для БАС», входящего в состав национального проекта «Беспилотные авиационные системы», запланировано к 2030 году подготовить не менее одного миллиона таких специалистов [1].

Безусловно, основная цель проекта - обеспечить российские компании и государственные учреждения квалифицированными кадрами, способными эффективно работать в стремительно развивающейся индустрии беспилотных технологий.

Стоит отметить, что проект «Кадры для беспилотных авиационных систем» включает в себя несколько ключевых задач:

- разработка и внедрение образовательных программ для общего и среднего профессионального образования, а также программ дополнительного профессионального обучения, с включением модулей по обучению навыкам проектирования, разработки, производства и эксплуатации БАС;

- создание образовательных программ высшего образования с внедрением модулей по БАС и поддержке развития гибких образовательных траекторий;

- обучение не менее 65 000 человек по дополнительным профессиональным программам с государственной поддержкой;

- подготовка педагогических кадров для образовательных организаций общего и среднего профессионального образования;

- создание цифрового реестра кадров БАС с разработкой информационно-аналитической системы, которая будет содержать данные о потребностях в кадрах, квалификациях и опыте специалистов;

- организация соревнований и популяризация профессий в сфере БАС, для повышения престижности этих профессий и привлечения новых специалистов.

Вместе с тем, нельзя не признать, что в современных реалиях, с учетом развития беспилотной авиации, острой проблемой является именно уровень подготовки специалистов в этой области. Важно отметить, что на основании статистических данных, выявленные нарушения правил использования воздушного пространства при применении БАС, в большинстве случаев происходят в связи с отсутствием соответствующей подготовки и переподготовки операторов управления беспилотных летательных аппаратов. Кроме того, БАС включает в себя не только летательный аппарат, но и наземные технические средства, оборудования навигации и связи, поэтому степень подготовки специалистов

по их техническому обслуживанию напрямую влияет на безопасность гражданской и военной авиации, а процесс эксплуатации зависит от исправности БАС в соответствии с требованием технической документации[2].

Очевидно, что в настоящее время, профессиональная подготовка специалистов беспилотной авиации, это дорогое удовольствие, которое включает в себя содержание большого учебного центра, технику, тренажерное оборудование, педагогов и инструкторов с большим опытом работы. При этом необходимо подчеркнуть, что у желающих пройти обучение не всегда есть возможность получить качественную подготовку, так как образовательный процесс в этом направлении, должным образом не регламентирован с учетом сегодняшних требований к квалификации таких специалистов. Почему? Да потому, что любая компания или ИП получив лицензию на дополнительное профессиональное образование (далее - ДПО), выполнив формальные требования, создает сайт, запускает рекламную кампанию и продает за 15-25 тысяч рублей теоретический курс подготовки «Оператор БАС с максимальной взлетной массой до 30 кг и менее». К тому же, основным документ, в соответствии с которым осуществляется подготовка специалистов БАС - это профессиональный стандарт «Специалист по эксплуатации беспилотных авиационных систем, включая в себя одно или несколько беспилотных воздушных судов максимальной взлетной массой 30 кг. и менее» [3,4]. Таким образом, человек дистанционно прослушав теорию, пройдя формальный тест, получает удостоверение «Оператор БАС с максимальной взлетной массой до 30 кг и менее», не пройдя при этом очную предполетную и полетную практики, так как профессиональный стандарт позволяет это делать. Причем, после такого дистанционного обучения, уже можно поднимать БАС весом 29,9 кг, который летит со скоростью 72 км. в час на высоте 1100 метров.

В связи с тем, что в большинстве случаев, существует огромный разрыв между учебным процессом ДПО и реальными задачами, такое формальное, дистанционное обучение, направленное на освоение минимальных знаний, нужно жестко регламентировать, начиная с нормативно-правового регулирования, а так же и с повышения требований к выдаче лицензий в зависимости от формы осуществления образования. Ведь на сегодняшний день, если

организация или ИП планирует осуществлять ДПО только в форме онлайн-образования, им для этого нужно предоставить сведения о наличии электронной информационно-образовательной среды. В свою очередь, если организация получает лицензию на очное образование, то лицензиат в последующем может осуществлять и онлайн образование. Очевидно, что после прохождения подобных курсов ДПО, у так называемых операторов беспилотных авиационных систем отсутствуют практические навыки, ведь обучаться пилотированию на одной теории, тем более только в дистанционном формате невозможно, так как слушатель должен прочувствовать управление беспилотного летательного аппарата, соотнося все это со знанием о механике полета.

Вместе с тем, хотелось бы напомнить, что у нас есть опыт подготовки пилотов большой авиации, а также международный опыт, где при обучении, весомое количество часов отводится на авиатренажерную практику. Можно с уверенностью сказать, что такой подход, необходимо внедрять и для подготовки операторов БАС с целью отработки навыков выполнения штатных полетов, полетов в сложных метеоусловиях, а также отработки действий при отказах и в особых случаях. Безусловно, для этого нужно создавать специальные учебные центры с авиатренажерами и действующими беспилотными комплексами, включать в программу подготовки практические часы налета обучающихся, что позволит сформировать устойчивые навыки пилотирования. Также необходимо ввести выдачу летных книжек с подтверждением освоенных типов БАС и часов налета, и выдавать их вместе с удостоверениями оператора БАС. Кроме того, отдельного внимания заслуживает и вопрос квалификации преподавательского и инструкторского состава, которые зачастую не имеют практических навыков в этой области.

Нельзя не признать, что и образовательные программы, нуждаются в серьезной доработке, так как они должны составляться на основе квалификационных требований и компетенций в соответствии с сегодняшними реалиями, охватывая не только теоретическую подготовку, но и практические занятия на авиатренажерах и современных типах БЛА, для получения практических устойчивых навыков самостоятельного выполнения полетов.

При этом теоретическая часть подготовки, в том числе должна включать в себя и изучение

нормативно-правового регулирования в области беспилотной авиации, а также реальные кейсы для анализа сложных, нестандартных задач. Необходимо в учебную программу включить и изучение специального профессионального программного обеспечения по управлению БАС, чтобы обучающийся мог самостоятельно создавать полётные задания. В тоже время, в программы подготовки обязательно нужно включать тему: «Действия оператора БАС при попадании в зону действия радиоэлектронной борьбы», ведь в Российской Федерации практически все объекты гражданской инфраструктуры прикрыты системой радиоэлектронной борьбы. Все эти моменты, несомненно, нужно учитывать при разработке обучающих программ.

Следует принять во внимание и тот факт, что при подготовке специалистов БАС, недостаточно часов уделяется регламенту совместного использования воздушного пространства БАС и пилотируемых воздушных судов. На каждый полет нужно получать разрешение в соответствии с требованием законодательства, проводить предполетный анализ местности [5]. Ведь только четкое выполнение техники безопасности и стандартных операционных процедур являются гарантом исключения ошибок.

Итак, для эффективной организации учебного процесса в области беспилотной авиации, необходимо:

- создавать специальные учебные центры, включающие инновационное, материально-

техническое оснащение, с целью теоретической подготовки специалистов, а также обязательной отработки навыков выполнения штатных полетов, полетов в сложных метеоусловиях, и отработки действий при отказах и в особых случаях;

- усилить контроль и ответственность за разработку, утверждение образовательных программ обеспечивающих достижение планируемых результатов с учетом сегодняшних реалий;

- запретить формальное, дистанционное обучение, направленное только на освоение минимальных теоретических знаний, без практической подготовки;

- нужно жестко регламентировать требования выдачи лицензий в зависимости от формы осуществления образования;

- после успешного окончания обучения, специалистам наравне с удостоверением «Оператор БАС с максимальной взлетной массой до 30 кг. и менее», необходимо выдавать и летную книжку внешнего пилота с указанием часов налета, типов БАС для того, чтобы работодатель видел документальное подтверждение квалификации кандидата на вакансию.

Очевидно, что современная эпоха характеризуется быстрым технологическим и общественным развитием, требующая знаний в данной области, поиска правильных решений, и только комплексный подход поспособствует надлежащей подготовки высококвалифицированных специалистов в области беспилотной авиации, для решения задач, поставленных государством.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Автоматизированное рабочее место администратора базы данных Руководство по эксплуатации ФИДШ.425688.100 - 1 РЭ.
2. Комплекс пультового программного обеспечения «Ладога». Руководство по эксплуатации БФЮК. 425629.001 РЭ.
3. Межгосударственный стандарт ГОСТ 26342 Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры.
4. ГОСТ Р 52436 Приборы приемно-контрольные охранные. Классификация. Общие технические требования и методы испытаний.
5. ГОСТ Р 52435 Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний.
6. ГОСТ Р 56102.1 Системы централизованного наблюдения. Часть 1. Общие положения.

LIST OF SOURCES

1. Velikoklad T.P. Training of Unmanned Aerial Vehicle Specialists for Solving Civilian Tasks // Problems of Emergency Safety. 2025. No.1. Pp.68-72.

2. Velikoklad T.P. Problems Arising in the Training of Specialists for Unmanned Aerial Vehicles // Collection of Materials on the Development of Robotics in the Russian Ministry of Emergency Situations (within the framework of the XV International Salon of Security Equipment "Integrated Security -2024"). Moscow, 2024. pp.43-50.
3. Order of the Ministry of Labor and Social Protection of the Russian Federation dated July 5, 2018 No. 447n "On approval of the professional standard "Specialist in the operation of unmanned aircraft systems, including one or more unmanned aircraft with a maximum take-off weight of 30 kg. and less" dated July 23, 2018, to be declared invalid// The guarantor.ru: inf.-right. the portal. – URL: <https://clck.ru/34X4rc> (accessed on 08.09.2025).
4. Order of the Ministry of Labor and Social Protection of the Russian Federation dated 09/14/2022 No. 526n "On approval of the professional standard "Specialist in the operation of unmanned aircraft systems, including one or more unmanned aircraft with a maximum take-off weight of 30 kg. and less", entered into force on 03/01/2023// Garant.ru: inf.-right. the portal. – URL: <https://clck.ru/34X4rc> (date of application: 09/08/2025).
5. Decree of the Government of the Russian Federation dated 03/11/2010 N 138 (as amended on 12/02/2020) "On Approval of the Federal Rules for the Use of the Airspace of the Russian Federation" (as amended and supplemented, intro. effective from 06/09/2021)// Federal Law of the Russian Federation 2010. - No. 1.

УДК 004.38

ВИХИРЕВ АНАТОЛИЙ АЛЕКСАНДРОВИЧ, ПОДПОЛКОВНИК ПОЛИЦИИ,
ЗАМЕСТИТЕЛЬ НАЧАЛЬНИКА ОТДЕЛА ФКУ «НИЦ «ОХРАНА» РОСГВАРДИИ

СЕРЕБРЯКОВ СЕРГЕЙ ВЛАДИМИРОВИЧ, ПОДПОЛКОВНИК ПОЛИЦИИ,
ЗАМЕСТИТЕЛЬ НАЧАЛЬНИКА ОТДЕЛА ФКУ «НИЦ «ОХРАНА» РОСГВАРДИИ

К ВОПРОСУ ФОРМИРОВАНИЯ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ МОБИЛЬНЫХ УСТРОЙСТВ СОТОВОЙ СВЯЗИ ДЛЯ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ ОБЪЕКТОВЫМИ УСТРОЙСТВАМИ

Аннотация. В статье рассматриваются вопросы формирования функциональных требований к программному обеспечению мобильных устройств сотовой связи (смартфоны, планшетные компьютеры), предназначенному для организации дистанционного управления техническими средствами охраны и исполнительными устройствами, установленными на объектах, а также получения на мобильные устройства собственников (пользователей) информации о состоянии и событиях, произошедших на охраняемых объектах.

Ключевые слова: мобильное устройство сотовой связи, дистанционное управление, объектовые устройства, система передачи извещений.

Annotation. The article discusses the issues of forming functional requirements for the software of mobile cellular communication devices (smartphones, tablet computers), designed to organize remote control of security equipment and actuators installed at facilities, as well as receiving information on the status and events that occurred at protected facilities on mobile devices of owners (users), of information about the status and events that occurred at the protected facilities.

Keywords: mobile cellular communication device, remote control, object devices, notification transmission system.

Введение. В настоящее время автоматизированное управление режимами централизованной охраны объектов и мест проживания и хранения имущества граждан (охраняемых объектов) осуществляется собственниками или уполномоченными на то лицами (Пользователями) непосредственно на самих объектах, с использованием возможностей устройств объектовых (УО).

Вместе с тем, благодаря широкому и повсеместному внедрению УО, работающих с пультовым оборудованием пунктов централизованной охраны (ПЦО) подразделений вневедомственной охраны войск национальной гвардии Российской Федерации (Подразделений ВО) по цифровым каналам связи, появились иные возможности дистанционного взаимодействия Пользователей с техническими средствами охраны (ТСО) в части управления режимами охраны, а также оперативного уведомления о произошедших на охраняемом объекте событиях.

Основная часть. Следует отметить, что на отечественном рынке охранных услуг уже предлагаются приложения для мобильных устройств сотовой связи, реализующие функции дистанционного управления объектовым оборудованием, такие как: «Охрана Приток-А» для работы с СПИ «Приток-А»,

производства ООО ОБ «Сократ», г. Иркутск [1], «Proxyma Assistant 2» для работы с СПИ «Центавр Проксима», производства «Компания Проксима», г. Тула [2], «My Alarm» из состава системы безопасности «Центр Охраны» производства ООО «НТКФ «Си Норд» г. Санкт-Петербург [3], «GEO.RITM Mobile» из состава СПИ «Ритм» производства ООО «НПО «Ритм» г. Санкт-Петербург [4].

Однако, указанные приложения не в полной мере удовлетворяют условиям использования на охраняемых объектах, в частности, недостаточен уровень защищенности от постороннего вмешательства и возможного саботажа УО.

С целью совершенствования существующих приложений для мобильных устройств сотовой связи с функциями дистанционного управления УО ГУВО Росгвардии принято решение о разработке на базе ФКУ «НИЦ «Охрана» Росгвардии приложений, совместимых с УО, включённых в Список технических средств безопасности, удовлетворяющих «Единым требованиям...» [5].

Принципиально взаимодействие мобильных устройств Пользователя с УО возможно посредством двух схем организации каналов связи.

Первая схема предполагает организацию прямого канала связи мобильного устройства Пользователя с объектовым оборудованием, установленным и функционирующим на охраняемом объекте (рис. 1).

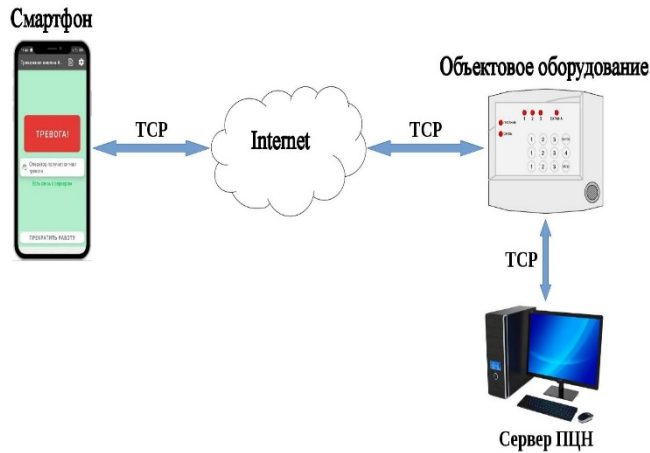


Рисунок 1

Применение данной схемы требует доработки существующего протокола обмена информацией между объектовым оборудованием и пультом централизованного наблюдения (ПЦН), а также встроенного программного обеспечения (ПО) данного оборудования. С учетом последующей обязательной процедуры перепрограммирования УО, данное решение представляется трудоемким и затратным.

Более приемлемой представляется вторая схема организации канала связи (рис. 2), при которой Пользователь со своего мобильного устройства взаимодействует не напрямую с объектовым оборудованием, а через дополнительное звено – Web-сервер с использованием стандартных Интернет - протоколов (SMTP, FTP, HTTP, IMAP, RTCP, Telnet и ряда других).

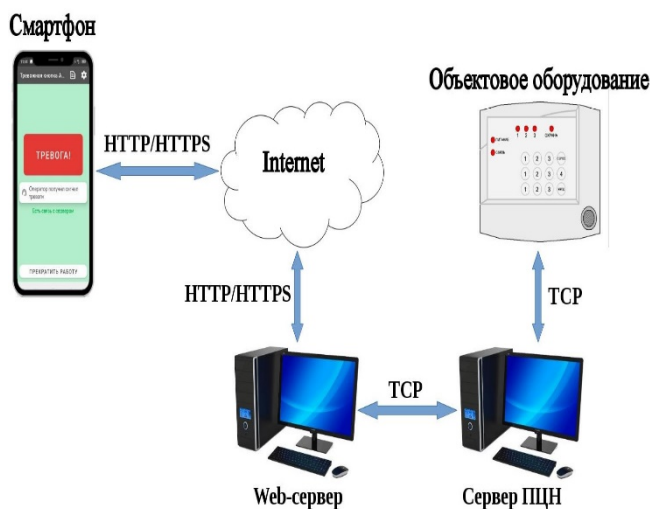


Рисунок 2

Web-сервер обеспечивает связь с сервером ПЦН и является по отношению к нему клиентским приложением, таким как ПО автоматизированного рабочего места (АРМ) дежурного ПЦН. При этом взаимодействие между Web-сервером и сервером ПЦН должно осуществляться по проприетарному (внутрифирменному) протоколу обмена данными по локально-вычислительной сети ПЦО. При использовании указанной схемы отпадает необходимость доработки указанного протокола обмена, так как команды управления объектовым оборудованием и команды запросов информации с сервера ПЦН реализованы во всех проприетарных протоколах СПИ.

Для организации взаимодействия мобильного устройства сотовой связи Пользователя с Web-сервером могут быть использованы как распространённые Web-браузеры, например, Google Chrome, Mozilla Firefox, Safari и др., так и специальное ПО, которое является более предпочтительным в плане удобства и скорости пользования.

Важным элементом при реализации функции дистанционного управления объектовым оборудованием является криптографическая защита передаваемой информации между приложением Пользователя и Web-сервером ПЦО. Это связано с тем, что перехват злоумышленниками посредством специальных программ и изменение пакетов данных, содержащих команды дистанционного УО, в лучшем случае приведут к снижению уровня надежности охраны, а в худшем – к несанкционированному проникновению на охраняемый объект. Наиболее надежным и распространенным методом защиты информационных потоков в сети Интернет на сегодняшний день является применение протокола TLS. Криптографический протокол защиты транспортного уровня TLS обеспечивает защищенную передачу данных между узлами в сети Интернет, используя при этом асимметричное шифрование для аутентификации и симметричное шифрование при передаче данных. В то же время, по требованию отечественного законодательства на территории Российской Федерации возможно использование протокола с криптографическими алгоритмами по ГОСТ Р 34.10-2012 [6] и ГОСТ Р 34.11-2012 [7].

Анализ приложений для мобильных устройств сотовой связи различных компаний – разработчиков охранных систем позволяет сформулировать функциональные требования к ПО для управления объектовым оборудованием, установленном на охраняемых объектах.

К основным функциональным требованиям можно отнести следующие:

установка на мобильные устройства сотовой связи, функционирование под управлением ОС iOS и Android и др.;

взаимодействие с Пользователем в интерактивном режиме;

возможность ввода доменного имени Web-сервера для организации связи с ПЦО;

возможность входа в приложение по логину и паролю Пользователя либо посредством функций TouchID/FaceID;

подключение и взаимодействие с Web-сервером ПЦО по защищенному протоколу HTTPS;

передача на ПЦН через Web-сервер сформированных Пользователем команд управления на взятие/снятие объекта (разделов объекта) под охрану/с охраны, управление исполнительными устройствами, подключенными к объектовому оборудованию посредством реле и силовых ключей;

получение с ПЦН извещений о взятии/снятии объекта (разделов объекта) под охрану/с охраны, тревожных извещений сохраняемых объектов, сформированных объектовым оборудованием, и информирование о них Пользователя звуковым, световым, вибросигналами;

возможность формирования и передачи Пользователем на ПЦН запросов о состоянии охраняемого объекта, шлейфов охранной, тревожной сигнализации и технологических датчиков;

возможность формирования и передачи Пользователем на ПЦН запросов на получение из базы данных сервера ПЦН архива событий по охраняемым объектам (дата и время постановки под охрану, снятия с охраны, возникновения тревожных событий и т. д.);

наличие понятной и логичной структуры (ПО должно быть максимально простым и понятным в использовании).

К дополнительным функциональным требованиям приложений можно отнести следующие:

наличие возможности бесплатного пробного ознакомления вне зависимости от бизнес-модели его распространения;

обеспечение возможности выбора места хранения данных (облачное хранилище, память устройства или SD-карта);

обеспечение поддержки сервисов и расширений операционной системы (ОС), соответствующих целевой функциональности приложения;

использование стандартных навигационных компонентов платформы (навигационных панелей, элементов управления страницами, панелей вкладок)

и неизменность системных навигационных функций. Если платформа поддерживает кнопку

«Назад», нажатие на нее всегда должно вести на предыдущий экран. Если платформа поддерживает кнопку «Домой», то нажатие на нее всегда должно вести на домашний экран мобильного устройства;

использование стандартных жестов, принятых в ОС: нажатие «Tap», произвольный перенос «Drag», горизонтальный перенос за пределы экрана «Flick», горизонтальный перенос в пределах экрана «Swipe», двойное нажатие «Doubletap», перемещение двух пальцев в разные стороны по диагонали «Pinch», нажатие с удержанием «Tap and Hold», встряхивание устройства «Shake». В приложениях под ОС iOS должна быть реализована поддержка 3D Touch. При этом следует не прибегать к использованию стандартных жестов для выполнения нестандартных действий;

соответствие руководствам (рекомендациям) по дизайну и удобству пользования ОС для работы, на которой оно создано. Мобильное приложение для ОС iOS должно соответствовать руководствам компании Apple, а мобильное приложение для ОС Android должно соответствовать руководствам компании Google;

наличие раздела «Помощь», содержащего информацию по правилам пользования функциями приложений. Раздел «Помощь» должен быть доступен из основного меню приложения или находиться в легкодоступной и видимой пользователями части экрана;

наличие раздела «О приложении», где должны быть указаны название приложения, его текущая версия, предприятие-разработчик и его контактные данные;

поддержка (по возможности) как книжной, так и альбомной ориентации экрана;

наличие возможности очистки кеша и удаления загруженных файлов.

Заключение. Решение поставленной перед ФКУ «НИЦ «Охрана» Росгвардии задачи по разработке ПО мобильных устройств сотовой связи с функциями дистанционного управления объектовым оборудованием позволит повысить качество оказываемых Пользователям услуг за счёт предоставления возможности дистанционного управления режимами охраны объектов и оперативного доступа к информации об их состоянии, и, как следствие, повысит конкурентоспособность вневедомственной охраны войск национальной гвардии Российской Федерации на рынке предоставления охранных услуг.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Сайт ООО ОБ «Сократ», г. Иркутск – <https://www.sokrat.ru/>.
2. Сайт «Компания Проксима», г. Тула – <https://www.proxyma.ru/>.
3. Сайт ООО «НТКФ «Си Норд» г. Санкт-Петербург – <https://www.cnord.ru/>.
4. Сайт ООО «НПО «Ритм» г. Санкт-Петербург – <https://www.cnord.ru/>.
5. Список технических средств безопасности, удовлетворяющих «Единым требованиям 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» [Текст]. – М.: НИЦ «Охрана», 2022. – 97 с. – Режим доступа <http://nicohrana.ru/engine/download.php?id=1456&area=static>.
6. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», введен 2013-01-01, взамен ГОСТ Р 34.10-2001 – М.: Стандартинформ, переиздание сентябрь 2018.
7. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования», введен 2013-01-01, взамен ГОСТ Р 34.11-94 – М.: Стандартинформ, 2013.

УДК 654.9

ББК 67.0

**ГАПОНЕНКО ВАДИМ АЛЕКСАНДРОВИЧ, СТАРШИЙ НАУЧНЫЙ СОТРУДНИК ФКУ
«НИЦ «ОХРАНА» РОСГВАРДИИ**

ВОПРОСЫ СОВЕРШЕНСТВОВАНИЯ НОРМАТИВНОГО ПРАВОВОГО РЕГУЛИРОВАНИЯ ОХРАННОЙ ДЕЯТЕЛЬНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. Статья посвящена выработке путей совершенствования нормативного правового регулирования охранной деятельности в Российской Федерации, обеспечивающих соответствие юридических норм характеру и уровню экономического и социального развития страны. Для решения данной задачи проведен анализ законодательства Российской Федерации, в результате которого определены основные субъекты, участвующие в осуществлении охранной деятельности в нашей стране. Также установлено, что в стране отсутствует нормативно правовой акт, регулирующий правоотношения в сфере охранной деятельности, и, как следствие, нет законодательно закрепленного понятия «Охранная деятельность». Предложено в целях совершенствования нормативного правового регулирования охранной деятельности в Российской Федерации принять федеральный закон, регулирующего правоотношения в этой сфере. На основе анализ возможных подходов к формулированию понятия «Охранная деятельность» разработана его дефиниция.

Ключевые слова: государственная охрана, нормативное правовое регулирование, орган государственной власти, охранная деятельность, субъект, участвующий в осуществлении охранной деятельности, физические и юридические лица.

GAPONENKO VADIM ALEKSANDROVICH, **SENIOR RESEARCHER OF THE FEDERAL STATE
INSTITUTION «SCIENTIFIC RESEARCH CENTER «OKHRANA» OF THE FEDERAL SERVICE OF
NATIONAL GUARD OF RUSSIA**

ISSUES OF IMPROVING THE LEGAL REGULATION OF SECURITY ACTIVITIES IN THE
RUSSIAN FEDERATION

Annotation. The article is devoted to the development of ways to improve the normative legal regulation of security activities in the Russian Federation, ensuring compliance of legal norms with the nature and level of economic and social development of the country. To solve this problem, an analysis of the legislation of the Russian Federation was carried out, as a result of which the main entities participating in the implementation of security activities in our country were identified. It was also established that there is no normative legal act in the country regulating legal relations in the field of security activities, and, as a result, there is no legislatively enshrined concept of "Security Activity". It is proposed to adopt a federal law regulating legal relations in this area in order to improve the normative legal regulation of security activities in the Russian Federation. Based on the analysis of possible approaches to the formulation of the concept of "Security Activity", its definition has been developed.

Keywords: state security, normative legal regulation, state authority, security activities, subject participating in the implementation of security activities, individuals and legal entities.

Введение. В своей эволюции охрана, как сфера деятельности человека, прошла долгий путь от простейшего способа ее осуществления – «выставления часового», еще во времена первобытно-общинного строя для предотвращения нападения диких животных, до использования в настоящее время сложнейших, наделенных искусственным интеллектом, робототехнических систем и средств для противодействия противоправным посягательствам объекты,

находящиеся как в государственной (муниципальной), так и в частной собственности.

В настоящее время, с учетом современного развития общества, охрану и всякую деятельность по ее осуществлению (далее – охранная деятельность) можно рассматривать в двух аспектах:

Первый – как взаимодействие потребителя услуг (выступающего в роли заказчика), и исполнителя, осуществляющего данные услуги.

При этом как заказчик, так и исполнитель могут быть физическими и юридическими лицами в любой комбинации.

Второй – деятельность государства по обеспечению защиты критически важных объектов от противоправных посягательств. В этом случае в роли заказчика выступают органы государственной власти или уполномоченные ими организации, а выполнение услуг по охране данных объектов выступают только юридические лица, имеющие различную форму собственности.

Независимо кто является заказчиком охранной услуги, между ним и субъектом ее осуществляющей возникают общественные отношения, требующие целенаправленного регулирования через механизм правового воздействия, для которого одним из ключевых условий результативности является эффективность правовых предписаний, установленных или санкционированных государством, определяемая степенью достижения поставленной цели. При этом максимальная эффективность правовых предписаний достигается при условии соответствия юридических норм характеру и уровню экономического и социального развития страны.

Поэтому выработка путей совершенствования нормативного правового регулирования охранной деятельности в Российской Федерации для обеспечения соответствия юридических норм характеру и уровню экономического и социального развития страны является актуальным.

Для определения путей совершенствования нормативного правового регулирования охранной деятельности в Российской Федерации в первую очередь необходимо определить:

- а) субъекты, которым законодательно разрешено осуществлять охранную деятельность;
- б) нормы права, которыми руководствуются субъекты, участвующие в осуществлении охранной деятельности (далее – Субъекты).

Основная часть. Проведенный анализ законодательства Российской Федерации показал, что в настоящее время законодательно определены следующие Субъекты:

1. Федеральная служба безопасности Российской Федерации (далее – ФСО России) – обеспечивает государственную охрану в соответствии с Федеральным законом от 27 мая 1997 г. № 57-ФЗ [4].

2. Федеральная служба войск национальной гвардии Российской Федерации (далее – Росгвардия), которая в соответствии с частью

1 статьи 2 Федерального закона от 03 июля 2016 г. № 226-ФЗ [7], обеспечивает охрану:

важных государственных объектов, специальных грузов, сооружений на коммуникациях в соответствии с перечнями, утвержденными Правительством Российской Федерации;

особо важных и режимных объектов, объектов, подлежащих обязательной охране войсками национальной гвардии, в соответствии с перечнем, утвержденным Правительством Российской Федерации;

собственных объектов;
имущества физических и юридических лиц по договорам;

3. Министерство внутренних дел Российской Федерации (далее – МВД России) – охрана дипломатических представительств, консульских учреждений, иных официальных представительств иностранных государств, представительств международных организаций в соответствии с пунктом м) ст. 1 Указа Президента РФ от 01 марта 2011 г. № 250 [11].

4. Частные охранные организации, функционирующие в соответствии с Законом Российской Федерации от 11 марта 1992 г. № 2487-1 [3] (с 1 сентября 2026 г. их деятельность будет регулироваться Федеральным законом от 30 ноября 2024 г. № 427-ФЗ [10]).

5. Подразделения ведомственной охраны, подпадающие по действие Федерального закона «О ведомственной охране» от 14 апреля 1999 г. № 77-ФЗ [6].

6. Подразделения охраны юридических лиц с особыми уставными задачами, определенные в части 2 статьи 4 Федерального закона № 150-ФЗ [5].

Кроме того, указанные выше Субъекты имеют:

1. Различные формы собственности, а именно:

а) ФСО России, Росгвардия и МВД России являются федеральными органами исполнительной власти;

б) подразделения ведомственной охраны и подразделения охраны юридических лиц с особыми уставными задачами являются организациями (структурными подразделениями) принадлежащим федеральным органам исполнительной власти (ФГУП «Охрана» Росгвардии [12]), государственным корпорациям (Ростех [8]) или акционерным обществам со значительной долей акций у государства (ОАО «Газпром» [9]);

г) частные охранные организации, находящиеся в частной собственности.

2. Присущие только им субъективные права и юридические обязанности в отношении различных объектов, которые подлежат охране в Российской Федерации.

В ходе анализа законодательства Российской Федерации установлено, что в стране отсутствует нормативно правовой акт, регулирующий правоотношения в сфере охранной деятельности (деятельность рассмотренных выше Субъектов регламентируется конкретными федеральными законами, определяющими их субъективные права и юридические обязанности [3 – 11]), и как следствие нет законодательно закрепленного понятия «Охранная деятельность».

Таким образом, по мнению автора, совершенствование нормативного правового регулирования охранной деятельности в Российской Федерации в первую очередь связано с принятием федерального закона (опыт регулирования охранной деятельности с использованием такого правового акта имеется в Республике Беларусь [14]), устанавливающего:

правовую основу осуществления охранной деятельности;

основные понятия в сфере охранной деятельности;

организационные основы осуществления охранной деятельности;

полномочия органов государственной власти (Президента Российской Федерации, Федерального собрания Российской Федерации, Правительства Российской Федерации и федеральных органов исполнительной власти);

порядок взаимодействия Субъектов охранной деятельности;

компетенции и порядок контроля за выполнением Субъектами охранной деятельности законодательства Российской Федерации.

Первым шагом на пути разработки предлагаемого проекта федерального закона является формулирование отсутствующей в настоящее время дефиниции «Охранная деятельность».

В ходе анализа законодательных и нормативных актов установлено, что в Российской Федерации существует два подхода к формулированию дефиниции «Охранная деятельность».

Первый подход. Техническим комитетом по стандартизации «Средства автоматизации и системы управления» (ТК 439) 1 августа 2002 г. был введен в действие руководящий документ «Системы охраны и безопасности объектов. Термины и определения» РД 25.03.001-2002 (далее

– РД 25.03.001-2002) [13], в котором дано определение охранной деятельности, как действия по обеспечению неприкосновенности собственности и личности от преступных посягательств.

Данная дефиниция определяет охранную деятельность как действие по обеспечению неприкосновенности, то есть сохранения в целостности, защиты от всякого посягательства со стороны кого-либо [15].

В свою очередь в Конституции Российской Федерации [2] определено:

1. Неприкосновенность территории Российской Федерации (ч. 3 ст. 4).

2. Личная неприкосновенность (ч. 1 ст. 22).

3. Неприкосновенность частной жизни (ч. 1 ст. 23).

4. Неприкосновенность жилища (ст. 25).

5. Президент Российской Федерации обладает неприкосновенностью (ст. 91, ч. 1 ст. 92.1).

6. Сенаторы Российской Федерации и депутаты Государственной Думы обладают неприкосновенностью (ч. 1 ст. 98).

7. Судьи неприкосновенны (ч. 1 ст. 122).

Таким образом, в соответствии с Конституцией Российской Федерации неприкосновенностью обладают: территория страны; личность и ее частная жизнь; некоторые категории должностных лиц, а также жилище, как элемент частной жизни личности.

При этом в Российской Федерации, в соответствии с Венской конвенция о дипломатических сношениях [1], которая инкорпорирована в российскую правовую систему ч. 4 ст. 15 Конституции Российской Федерации, неприкосновенностью пользуются дипломаты (ст. 31) и дипломатические представительства (ст. 22).

Также в Конституции Российской Федерации установлено, что право частной собственности охраняется законом (ч. 1 ст. 35), при этом частной собственностью может являться имущество (ч. 2 ст. 35), земля (ч. 1 ст. ст. 36), природные ресурсы (ч. 1 ст. ст. 36) и интеллектуальная собственность (ч. 1 ст. 44). Кроме того, в Российской Федерации существует государственная, муниципальная и иные формы собственности (ч. 2 ст. 8).

При этом, в юриспруденции понятие неприкосновенность используется как термин, определяющий некое правовое положение или элемент правового статуса [16].

Исходя из положений Конституции Российской Федерации и принятом в юриспруденции узкого понимания неприкосновенности, как правового положения или статуса, можно сделать следующие выводы:

1. Собственность не может обладать каким-либо статусом и тем более статусом неприкосновенности.

В Российской Федерации действует только охрана права на собственность (ч. 1 ст. 35 Конституции Российской Федерации).

Жилище (как возможный предмет собственности) обладает неприкосновенностью только как воля проживающих в нем лиц (ст. 25 Конституции Российской Федерации).

2. Неприкосновенность личности – принцип, согласно которому человек не может быть произвольно лишён свободы.

В праве Российской Федерации содержание принципа неприкосновенности личности заключается в следующем (ч. 2 ст. 22 Конституции Российской Федерации):

ограничение личной свободы возможно только по определённым основаниям;

заключение под стражу возможно лишь в соответствии с процессуальным законодательством;

до судебного решения лицо может быть подвергнуто задержанию до 48 часов.

Кроме того, в определении «Охранная деятельность» данном в РД 25.03.001-2002 отсутствует указание кто обеспечивает неприкосновенность, то есть не определен круг субъектов охранной деятельности.

Второй подход. Определения дефиниции «Охранная деятельность» через понятия «охрана» и «защита».

Анализ большого числа источников, в которых обосновывались подходы к формулированию дефиниции «Охранная деятельность» через понятия «охрана» и «защита» проведен Квасовым В.Б. [17], который делает вывод, что охрана является деятельностью определенных субъектов, направленной на обеспечение состояния защищенности охраняемых объектов (объектов охраны) от противоправных посягательств.

На основании данных выводов Квасов В.Б. дает следующее определение: «Государственная охранная деятельность (государственная охрана) – это деятельность реализующих публичные интересы специально уполномоченных субъектов, осуществляемая с целью обеспечения состояния защищенности охраняемых объектов путем использования специальных правовых, организационных, технических и иных мер».

При этом позиция автора имеет существенный недостаток, так как в дефиниции упор делается на то, что охранная деятельность является государственной деятельностью. Этот недостаток приводит к тому, что охранная деятельность может

осуществляется только государством, то есть субъектами правоотношения могут выступать только государственные органы или организации, принадлежащие исключительно государству. То есть не учитывается, что в Российской Федерации важную роль в осуществлении охранной деятельности играют частные охранные организации.

Кроме того, в формулировке определения при осуществлении охранной деятельности защищаются только объекты от противоправных посягательств, то есть отсутствует охрана лиц (граждан и должностных лиц Российской Федерации; иностранных граждан, должностных лиц и дипломатов, а также лиц без гражданства, находящихся на территории Российской Федерации).

Из рассмотренных выше подходов к формулированию понятия «Охранная деятельность» можно сделать следующие выводы:

1. Формулирование дефиниции «Охранная деятельность» через понятие неприкосновенности личности определяет, что действия по ее обеспечению в соответствии со ст. 22 Конституции Российской Федерации включают в себя недопустимость вмешательства извне в сферу индивидуальной жизнедеятельности человека, а именно свободу и личную неприкосновенность, которая включает физическую, психическую и моральную неприкосновенность. То есть охранная деятельность в таком случае должна обеспечивать права и свободы человека и гражданина в том числе, например, свободу вероисповедания. Следовательно, принятый в РД 25.03.001-2002 подход не приемлем для формулирования понятия «Охранная деятельность».

2. Формулирование дефиниции «Охранная деятельность» через понятия «охрана» и «защита», предложенное Квасовым В.Б., позволяет перейти к формулированию правоотношений, которые можно урегулировать нормами права, что является основной целью введения данной дефиниции в законодательство Российской Федерации. Однако, как говорилось выше, предложенная Квасовым В.Б. дефиниция не лишена недостатков.

С учетом определенных в Российской Федерации Субъектов охранной деятельности, субъективных прав и юридических обязанностей Субъектов в отношении различных объектов, которые подлежат охране в Российской Федерации, а также предложенного Квасовым В.Б.

подхода предлагается следующая формулировка: «охранная деятельность – деятельность субъектов, определенных законодательством Российской Федерации, направленная на обеспечение защиты жизни и здоровья граждан Российской Федерации, иностранных граждан, лиц без гражданства и должностных лиц всех уровней власти Российской Федерации, а также объектов различной формы собственности от противоправных посягательств на них».

Заключение. В статье на основе результата анализа законодательства Российской Федерации: определен перечень субъектов, которым законодательно разрешено осуществлять

охранную деятельность, и источники права, определяющие их субъективные права и юридические обязанности [3 – 11];

сделан вывод, что совершенствования нормативного правового регулирования охранной деятельности в Российской Федерации связано с принятием федерального закона, регулирующего правоотношения в сфере охранной деятельности.

В целях разработки федерального закона, регулирующего правоотношения в сфере охранной деятельности, предложена структура данного закона, а также разработана дефиниция «Охранная деятельность».

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Венской конвенция о дипломатических сношениях, принятая 18 апреля 1961 г [Электронный ресурс] // Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/dip_rel.shtml (дата обращения 05.04.2024).
2. Конституция Российской Федерации от 12 декабря 1993 г. (с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Собрание законодательства РФ. – 2014. – № 31. – Ст. 4398
3. Закон Российской Федерации от 11 марта 1992 г. № 2487-1 «О частной детективной и охранной деятельности в Российской Федерации».
4. Федеральный закон Российской Федерации от 27 мая 1996 г. № 57-ФЗ «О государственной охране».
5. Федеральный закон Российской Федерации от 13 декабря 1996 г. № 150-ФЗ «Об оружии».
6. Федеральный закон Российской Федерации от 14 апреля 1999 г. № 77-ФЗ «О ведомственной охране».
7. Федеральный закон Российской Федерации от 3 июля 2016 г. № 226-ФЗ «О войсках национальной гвардии Российской Федерации».
8. Федеральный закон от 23 ноября 2007 г. № 270-ФЗ «О Государственной корпорации по содействию разработке, производству и экспорту высокотехнологичной промышленной продукции «Ростех».
9. Федеральный закон 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса».
10. Федерального закона от 30 ноября 2024 г. № 427-ФЗ «О частной охранной деятельности» // ГАРАНТ.РУ информационно-правовой портал [Электронный ресурс]. 22.05.2025. – URL: <https://www.garant.ru/hotlaw/federal/1771098/> (дата обращения 22.05.2025).
11. Указ Президента Российской Федерации от 1 марта 2011 г. № 250 «Вопросы организации полиции».
12. Приказ Росгвардии от 12.05.2021 № 165 «Об утверждении Устава федерального государственного унитарного предприятия «Охрана» Федеральной службы войск национальной гвардии Российской Федерации и некоторых вопросах организации его деятельности».
13. Руководящий документ «Системы охраны и безопасности объектов. Термины и определения» РД 25.03.001-2002. [Электронный ресурс] // Режим доступа: https://standartov.ru/norma_doc/47/47809/index.htm (дата обращения 05.04.2024).
14. Закон Республики Беларусь от 8 мая 2009 г. № 16-3 «О государственной охране» Источник: <https://pravo.by/document/?guid=11031&p0=N10900016> – Национальный правовой Интернет-портал Республики Беларусь.
15. Ожегов С.И. Толковый словарь русского языка: 80000 слов и фразеологических выражений / С.И. Ожегов, Н.Ю. Шведова. 4-е изд., дополненное. М.: ЛД ИНВЕСТ, Азбуковник. 2003. С. 486 [Электронный ресурс] // Режим доступа: <https://gufo.me/dict/ozhegov> (дата обращения 05.04.2024)
16. Большая российская энциклопедия - электронная версия. [Электронный ресурс] // Режим доступа: <https://bigenc.ru/> (дата обращения 05.04.2024)
17. Квасов В. Б. Административно-правовое регулирование государственной охранной деятельности: дис. канд. юрид. наук: 5.1.2 – ННГУ, Н. Новгород, 2023 – 235 с.

УДК 343.34
ББК 67.408.1

ГУБАРЬ ДМИТРИЙ СТАНИСЛАВОВИЧ, ВЕДУЩИЙ ЮРИСКОНСУЛЬТ

УГОЛОВНО-ПРАВОВЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ И ТЕРРИТОРИЙ

Аннотация. Материал посвящен анализу уголовно-правовых мер обеспечения антитеррористической защищенности объектов и территорий в Российской Федерации. Рассматривается практика применения статей 217.1 и 217.3 Уголовного кодекса Российской Федерации, а также их концептуальные недостатки, включая формализованность правовых конструкций и зависимость от административной преюдиции.

Ключевые слова: терроризм, антитеррористическая защищенность, критическая инфраструктура, топливно-энергетический комплекс, объекты и территории, уголовно-правовые меры, статьи 217.1 и 217.3 Уголовного кодекса Российской Федерации.

GUBAR DMITRIY STANISLAVOVICH, **SENIOR LEGAL COUNSEL**

CRIMINAL LAW MEASURES TO ENSURE THE ANTI-TERRORIST SECURITY OF FACILITIES AND TERRITORIES

Annotation. The article examines criminal law measures ensuring the anti-terrorist security of facilities and territories in the Russian Federation. It analyzes the practice of applying Articles 217.1 and 217.3 of the Criminal Code of the Russian Federation, as well as their conceptual shortcomings, including the excessive formalism of legal constructs and dependence on administrative prejudice.

Keywords: terrorism, anti-terrorist security, critical infrastructure, fuel and energy sector, facilities and territories, criminal law measures, Articles 217.1 and 217.3 of the Criminal Code of the Russian Federation.

Вступление. Современный этап общественного развития сопровождается нарастанием террористических угроз, принимающих все более комплексный и гибридный характер, а также активизацией террористических сообществ, ведущих антироссийскую пропаганду, которая усиливается на фоне проведения специальной военной операции.

Вспоминая трагические события последнего десятилетия в России, в числе которых резонансные нападения с огнестрельным оружием в образовательных учреждениях Казани и Челябинска, концертном зале Crocus City Hall, можно с уверенностью констатировать, что на сегодняшний день вопросы обеспечения защищенности объектов и территорий требуют от государства адекватного и многоуровневого реагирования.

Еще одним серьезным инцидентом является диверсия на газопроводах «Северный поток», последствия которой вышли далеко за рамки национальных границ и наглядно показали необходимость принятия согласованных мер по обеспечению антитеррористической защищенности объектов топливно-энергетического комплекса [21].

Среди приоритетов государственной политики, зафиксированных в Указах Президента Российской Федерации от 26.12.2015 № 664 «О мерах по совершенствованию государственного управления в области противодействия терроризму» [6], от 13.05.2019 г. № 216 «Об утверждении Доктрины энергетической безопасности Российской Федерации» [7] и от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [8], указаны меры по достижению требуемого уровня защищенности объектов топливно-энергетического комплекса, иных объектов и территорий от террористических угроз, совершенствованию правовых механизмов обеспечения антитеррористической защищенности.

В соответствии с Федеральным законом от 06.03.2006 № 35-ФЗ «О противодействии терроризму» [3], а также Федеральным законом от 21.07.2011 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» [4]:

антитеррористическая защищенность объекта (территории) определяется как состояние защищенности здания, строения, сооружения, иного объекта, места массового пребывания людей, препятствующее совершению

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

террористического акта (пункт 6 статьи 3 Федерального закона № 35-ФЗ, пункт 2 статьи 2 Федерального закона № 256-ФЗ);

требования к антитеррористической защищенности различных объектов и территорий, категории объектов и критерии категорирования утверждаются Правительством Российской Федерации (пункт 4 части 2 статьи 5 № 35-ФЗ, часть 1 статьи 7 Федерального закона № 256-ФЗ).

В настоящее время изданы 49 постановлений Правительства Российской Федерации, предусматривающих требования к антитеррористической защищенности различных объектов и территорий, в числе которых:

от 25.03.2015 № 272 [11] – устанавливает требования к антитеррористической защищенности мест массового пребывания людей, а также объектов и территорий, подлежащих обязательной охране войсками национальной гвардии Российской Федерации;

от 19.10.2017 № 1273 [12] – регулирует порядок обеспечения безопасности торговых объектов и прилегающих к ним территорий;

от 02.08.2019 № 1006 [13] – определяет меры по обеспечению безопасности объектов и территорий, находящихся в ведении Министерства просвещения Российской Федерации.

Отдельного внимания заслуживает нормативное регулирование вопросов антитеррористической защищенности объектов топливно-энергетического комплекса, включающее следующие постановления Правительства Российской Федерации:

от 05.05.2012 № 459 [9] – определяет порядок категорирования объектов топливно-энергетического комплекса, критерии отнесения их к соответствующим категориям, а также перечень исходных данных, необходимых для проведения такой процедуры;

от 05.05.2012 № 460 [10] – содержит правила актуализации паспорта безопасности объекта топливно-энергетического комплекса.

Еще ряд постановлений Правительства Российской Федерации, предусматривающих требования к антитеррористической защищенности объектов топливно-энергетического комплекса, имеет гриф «для служебного пользования».

Выполнение указанных требований является обязательным для органов (организаций), являющихся правообладателями объектов и территорий, а также физических и юридических лиц в отношении объектов, находящихся

в их собственности или принадлежащих им на ином законном основании.

Антитеррористическая защищенность объектов и территорий обеспечивается за счет применения комплекса инженерных, технических и организационно-правовых мер, направленных на предотвращение совершения террористических актов.

При этом указанные меры дифференцируются в зависимости от категории объекта (территории), присвоенной с учетом потенциального количества возможных пострадавших, а также предполагаемого объема материального ущерба в случае совершения террористического акта [17].

Одни меры осуществляются вне зависимости от категории объекта и территории, другие же, наоборот, применяются с учетом потенциальных рисков масштабных негативных последствий.

Данные меры носят комплексный организационный характер, отмечают важнейшую практическую значимость инженерно-технической укрепленности охраняемых объектов и территорий, а также оборудования их инженерно-техническими средствами обеспечения антитеррористической защищенности [15].

К числу таких инженерно-технических средств относятся система видеонаблюдения, система охранной сигнализации, система контроля и управления доступом, система охранного освещения, система оповещения и управления эвакуацией, система обеспечения вызова экстренных оперативных служб, системы досмотра, а также различные замки, заграждения, ограждения, защитные конструкции объектов и территорий.

Условия проектирования, установки и эксплуатации инженерно-технических средств регламентированы рядом межгосударственных и национальных стандартов [14].

Антитеррористическая защищенность обеспечивается выполнением следующих требований: наличием организационно-распорядительных документов, назначением должностных лиц, ответственных за защиту объекта (территории), разработкой порядка взаимодействия должностных лиц и служб объекта с органами исполнительной власти и аварийно-спасательными службами, организацией охраны силами вневедомственной охраны войск национальной гвардии Российской Федерации или частных охранных организаций, обеспечением контрольно-пропускного режима, выполнением требований положений и инструкций,

регламентирующих порядок обеспечения охраны, пропускного, внутреннего режимов и безопасной работы объекта.

Еще одним значимым механизмом в системе обеспечения антитеррористической защищенности является контрольная деятельность, которая осуществляется уполномоченными органами в форме плановых и внеплановых проверок хозяйствующих субъектов, эксплуатирующих объекты и территории, ориентированная на оценку эффективности соответствующего обеспечения и своевременное выявление проблем организации антитеррористической защищенности.

Вместе с тем на практике возникает множество ситуаций, в которых игнорируются вышеуказанные законодательные требования [23], что в свою очередь существенно повышает угрозу антитеррористической защищенности объектов и территорий.

В этой связи в системе мер противодействия актам незаконного вмешательства на объектах, в отношении которых действуют требования антитеррористической защищенности, особое значение приобретают уголовно-правовые средства, как наиболее строгая форма правового реагирования на угрозу национальной безопасности.

Основная часть. Еще в 2017 году Совет Безопасности Организации Объединенных Наций принял резолюцию, призывающую государства рассмотреть возможность разработки или дальнейшего совершенствования своих стратегий уменьшения рисков террористических нападений на объекты критической инфраструктуры. При этом в документе отдельно указывается на необходимость обеспечения уголовной ответственности за подобные преступления [26].

Традиционный подход уголовного законодательства акцентирует внимание на привлечении к ответственности за совершенные террористические акты либо за действия, непосредственно предшествующие их реализации.

Однако исключительно карательные меры, основанные на принципе устрашения, оказываются недостаточно эффективными в контексте противодействия терроризму. Это обусловлено, в частности, тем, что исполнители террористических актов нередко осознанно жертвуют собственной жизнью во имя реализации экстремистских и античеловеческих целей, что делает угрозу наказания для них несущественной.

В связи с этим наибольшую практическую значимость приобретает предупреждение террористических угроз, поэтому российские законодатели криминализируют действия, направленные против защитных мер, или неспособность их реализовать.

В частности, статьи 217.1 и ст. 217.3 Уголовного кодекса Российской Федерации [1] устанавливают уголовную ответственность за нарушение требований к антитеррористической защищенности объектов топливно-энергетического комплекса, а также иных объектов и территорий, если это деяние повлекло по неосторожности причинение тяжкого вреда здоровью человека или причинение крупного ущерба.

При этом статья 217.3 введена в Уголовный кодекс Российской Федерации относительно недавно с вступлением в силу с 1 июля 2024 года Федерального закона от 31.07.2023 № 398-ФЗ [5] и по словам инициаторов законопроекта должна иметь серьезное профилактическое значение для предотвращения новых трагедий [25].

Квалифицированным видом преступлений обеих статей выступает нарушение требований антитеррористической защищенности, повлекшее по неосторожности смерть человека, а особо квалифицированным – смерть двух

и более лиц, при этом размер причиненного ущерба для квалификации преступлений уже не имеет значения.

Статья 217.3 Уголовного кодекса Российской Федерации, в отличие от 217.1, имеет специфическую правовую конструкцию: уголовная ответственность по ней наступает лишь в случае, если лицо ранее дважды и более раз в течение 180 дней привлекалось к административной ответственности за правонарушение, предусмотренное статьей 20.35 Кодекса Российской Федерации об административных правонарушениях «Нарушение требований к антитеррористической защищенности объектов (территорий) и объектов (территорий) религиозных организаций» [2].

Основными деяниями, составляющими объективную сторону нарушения требований к антитеррористической защищенности, которые предусмотрены постановлениями Правительства Российской Федерации, могут являться:

непроведение категорирования объектов (территорий), несоставление паспорта безопасности объекта (территории);

несоблюдение сроков категорирования и (или) паспортизации объекта (территории);

непринятие организационно-распорядительных документов по вопросам антитеррористической защищенности;

необеспечение пропускного и внутриобъектового режимов, физической охраны;

неоснащение объекта (территории) системами видеонаблюдения, охранной сигнализации, средствами оповещения и управления эвакуацией, иными инженерно-техническими средствами и системами охраны.

С субъективной стороны рассматриваемый состав преступлений по обоим статьям характеризуется смешанной формой вины: по отношению к деянию это может быть умысел (прямой или косвенный), либо неосторожность (легкомыслие или небрежность), по отношению к последствиям – только неосторожность (легкомыслие или небрежность). В целом такие преступления следует признать неосторожными, поскольку определяющим в данном случае является психическое отношение субъекта к последствиям.

Исходя из сути предъявляемых требований по обеспечению антитеррористической защищенности, следует констатировать, что их нарушение может быть совершено как в активной форме, т.е. совершение запрещенных действий, так и в пассивной, то есть в неисполнении установленных действий (бездействии) [22].

Таким образом, в уголовном праве созданы условия привлечения к уголовной ответственности лиц, игнорирующих действующие законодательные требования к антитеррористической защищенности объектов и территорий, что позволяет назначить им справедливое и соразмерное наказания в случае возникновения серьезных негативных последствий [18].

Однако имеется ряд проблемных аспектов, которые существенно затрудняют правоприменительную деятельность.

Статья 217.1 Уголовного кодекса Российской Федерации с момента ее введения в законодательство демонстрирует ряд концептуальных недостатков, на которые еще в 2011 году обращали внимание российские исследователи в сфере уголовного права [16].

По своей конструкции состав преступления, предусмотренный указанной статьей, относится к материальным: он предполагает наличие обязательного последствия, без наступления которого деяние не может считаться оконченным.

Состав преступления в данном случае формируется лишь при условии причинения

тяжкого вреда здоровью человека либо причинения крупного имущественного ущерба.

При отсутствии таких последствий деяние подлежит квалификации не в рамках уголовного права, а как административное правонарушение, предусмотренное статьей 20.30 Кодекса Российской Федерации об административных правонарушениях.

Квалифицированный состав статьи 217.1 (ч. 2) Уголовного кодекса Российской Федерации предусматривает ответственность за нарушение правил безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса, повлекшее по неосторожности смерть человека, а особо квалифицированный состав (ч. 3) – смерть двух и более лиц.

Данная законодательная логика представляется оправданной: здесь дифференциация ответственности осуществляется по критерию увеличения тяжести физического вреда.

Вместе с тем объекты топливно-энергетического комплекса часто представляют собой крупные градообразующие производства, со сложным многоступенчатым производственным процессом, в котором задействуется большое количество сложных механизмов и установок, и посягательства на такие объекты как раз и имеют своей целью причинить значительный имущественный ущерб.

В этой связи для обеспечения баланса и последовательности уголовно-правовой конструкции представляется обоснованным закрепить дифференциацию ответственности также с учетом имущественного вреда.

Субъективная сторона состава рассматриваемого преступления отличается повышенной сложностью.

Ключевым элементом здесь выступает установление причинно-следственной связи между нарушением специальных правил и наступившими вредными последствиями. Отсутствие такой связи исключает возможность квалификации содеянного по статье 217.1 Уголовного кодекса Российской Федерации.

Вина должна быть установлена не только в отношении самого деяния, выражающегося в нарушении требований антитеррористической защищенности, но и в отношении наступивших последствий.

Аналогично статье 217.1, состав преступления по статье 217.3 Уголовного кодекса Российской Федерации также формируется лишь при условии причинения тяжкого вреда здоровью человека либо причинения крупного имущественного ущерба.

При отсутствии таких последствий деяние подлежит квалификации не в рамках уголовного права, а как административное правонарушение, предусмотренное статьей 20.35 Кодекса Российской Федерации об административных правонарушениях.

Отдельную правовую проблему в статье 217.3 Уголовного кодекса Российской Федерации представляет предусмотренное в ее диспозиции условие обязательного предшествующего неоднократного привлечения лица к административной ответственности за аналогичные нарушения.

Так, уголовное преследование становится возможным лишь в случае, если лицо в течение 180 дней дважды и более раз привлекалось к ответственности по статье 20.35 Кодекса Российской Федерации об административных правонарушениях.

В результате уголовная ответственность может быть исключена именно в тех случаях, когда несоблюдение требований к антитеррористической защищенности повлекло тяжкие последствия, но при этом отсутствуют ранее зафиксированные административных правонарушения.

Для сравнения, нормы уголовного законодательства, регламентирующие ответственность за нарушение требований пожарной безопасности (статья 219 Уголовного кодекса Российской Федерации) и охраны труда (статья 143 Уголовного кодекса Российской Федерации), не содержат административной преюдиции.

В соответствии с указанными статьями, уголовная ответственность наступает непосредственно при наличии последствий – причинения тяжкого вреда здоровью или гибели человека, вне зависимости от наличия предшествующих административных правонарушений.

Это означает, что нарушение требований пожарной безопасности или охраны труда влечет уголовную ответственность уже с момента наступления опасных последствий, тогда как в сфере обеспечения антитеррористической защищенности действует дополнительный фильтр в виде административной преюдиции.

Некоторые исследователи в сфере уголовного права даже предлагают привести диспозицию статьи к виду, аналогичному ст. 219 Уголовного кодекса Российской Федерации, исключив из нее слова «совершенное лицом после его

неоднократного привлечения к административной ответственности за аналогичное деяние» [20].

Еще более парадоксальным явлением выступает невозможность приобретения отдельными лицами, систематически не исполняющими установленные требования к антитеррористической защищенности, криминообразующего признака неоднократной привлеченности к административной ответственности.

Так, по смыслу ст. 2.5 Кодекса Российской Федерации об административных правонарушениях лица, имеющие специальные звания, не несут административной ответственности, а следовательно, они не могут быть привлечены к уголовной ответственности за нарушение требований к антитеррористической защищенности объектов (территорий) [20].

Далее необходимо отметить, что правовые конструкции обеих статей позволяют избежать уголовной ответственности за несоблюдение требований к антитеррористической защищенности, если в ходе нападения на объект причинен ущерб меньше, установленного в примечаниях к статьям 217.1 и 217.3 Уголовного кодекса Российской Федерации, где законодатель конкретизировал размер крупного ущерба – свыше одного миллиона рублей.

Однако такой подход нарушает системность уголовного законодательства, поскольку в статье 216 Уголовного кодекса Российской Федерации, регулирующей смежный состав, крупный ущерб установлен в размере свыше 500 тысяч рублей.

Очевидно, что более логичным решением было бы унифицировать данные положения, распространив примечание статьи 216 Уголовного кодекса Российской Федерации на статьи 217.1 и 217.3.

В этой связи представляется целесообразным установить норму об «особо крупном ущербе» в размере свыше одного миллиона рублей, а может быть и в еще более крупном размере, по аналогии с преступлениями против собственности.

Такой шаг позволит не только устранить внутренние противоречия, но и дифференцировать ответственность, закрепив особо крупный ущерб в качестве квалифицирующего или особо квалифицирующего признака.

Следует отметить, что при квалификации преступлений по обеим статьям законодателем абсолютно проигнорирована существующая классификация объектов и территорий по степени их значимости и присвоенной категории.

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

Так, для объектов топливно-энергетического комплекса и иных объектов (территорий), подлежащих антитеррористической защищенности, может предусматриваться до четырех категорий опасности.

Такая градация позволяет дифференцировать требования к обеспечению безопасности объектов с учетом степени потенциальной опасности совершения террористического акта и его возможных последствий, учитывать важность объекта для инфраструктуры, масштабы возможных социально-экономических последствий.

Одновременно с этим, нельзя обойти и проблематику обоснованности квалификации преступного деяния по обеим статьям Уголовного кодекса Российской Федерации.

Некоторые из перечисленных нарушений способны существенно снизить защищенность объекта (территории) от террористических угроз: например, необеспечение здания физической охраной и системой видеонаблюдения уменьшает оперативность выявления подозрительных лиц, а необорудование объекта средствами оповещения и управления эвакуацией создает панику и дезорганизует действия людей, что в случае совершения террористического акта может повлечь увеличение размеров ущерба и количества жертв.

Другие же нарушения антитеррористических требований, в частности, связанные с отсутствием необходимой документации по вопросам антитеррористической защищенности носят в большей степени формальный характер нарушения, за которое должна быть предусмотрена административная или дисциплинарная ответственность.

Поэтому квалификация преступного деяния обоснована не во всех случаях, а лишь когда недопущение нарушения соответствующих требований к антитеррористической защищенности создавало реальную возможность предупредить террористический акт, исключить либо минимизировать причинение вреда жизни, здоровью, имуществу граждан и (или) имуществу организаций вследствие совершения террористического акта.

Уголовная ответственность должна применяться в случаях, когда нарушение требований к антитеррористической защищенности хотя и было допущено, однако напрямую не способствовало причинению вреда чьему-либо здоровью или имуществу: например, когда запасной выход не оборудован видеокамерами, но

террористы проникли в здание через парадный вход [20].

По данным Судебного департамента при Верховном Суде Российской Федерации и Агентства правовой информации [27] за период с 2021 по 2024 годы уголовное преследование по статьям, непосредственно регламентирующим нарушение требований антитеррористической защищенности, носит крайне ограниченный характер.

В частности, за период с 2021 по 2024 годы по статье 217.1 Уголовного кодекса Российской Федерации был осужден лишь один гражданин, получивший условное лишение свободы. В 2024 году также зафиксирован единичный случай прекращения уголовного дела по данной статье.

Статья 217.3 Уголовного кодекса Российской Федерации, устанавливающая ответственность за неисполнение обязанностей по обеспечению антитеррористической защищенности, в судебной практике за весь период своего действия с 1 июля 2024 года вовсе не применялась.

Для сопоставления обратимся к статистике по другим составам преступлений, имеющим смежную природу, но более широкое применение.

Так, в 2024 году по статье 219 Уголовного кодекса Российской Федерации («Нарушение требований пожарной безопасности») по части 1 осуждены 3 человека, по части 2 (деяния, повлекшие тяжкий вред здоровью) – также 3 человека, по части 3 (повлекшие смерть двух и более лиц) – 10 человек.

В 2023 году количество осужденных по данной статье было выше: по частям 1, 2 и 3 – 2, 5 и 17 человек соответственно.

Еще более показательна статистика по статье 143 Уголовного кодекса Российской Федерации («Нарушение требований охраны труда»).

В 2023 году по части 1 осуждены 32 человека, по части 2 (смерть одного человека) – 95 человек, по части 3 (смерть двух и более лиц) – 11 человек.

В 2024 году эти показатели увеличились: по частям 1, 2 и 3 – 37, 132 и 15 человек соответственно.

Такая судебная статистика в совокупности с вышеперечисленными недостатками правовых конструкций статей 217.1 и 217.3 Уголовного кодекса Российской Федерации свидетельствует о неэффективности уголовно-правовых мер обеспечения антитеррористической защищенности объектов и территорий.

Об этом свидетельствуют и публикации авторов, отмечая, что несмотря на активное совершенствование в последние годы

антитеррористической защищенности различных объектов (территорий), до недавнего времени в рамках заявленной проблематики не используется потенциал уголовной ответственности [18].

В последнее время в международной практике противодействия терроризму прослеживается тенденция к усилению уголовно-правового реагирования на нарушения требований антитеррористической защищенности объектов и территорий.

В большинстве стран мира нарушение требований к антитеррористической защищенности не является самостоятельным уголовным преступлением, а становится таковым только в случае прямой связи с подготовкой или совершением террористического акта. Вместе с тем отдельное зарубежное законодательство имеет уникальное стратегическое значение.

Так, принципиально новый подход к обеспечению антитеррористической защищенности закреплён в законодательстве Великобритании. 3 апреля 2025 года был принят Закон «О защите объектов от терроризма» (Terrorism (Protection of Premises) Act 2025), также известный как *Martyn's Law* [28].

Закон закрепляет требования по антитеррористической защищенности в качестве самостоятельного объекта правовой охраны, распространяется на объекты, расположенные на территории Англии, Шотландии, Уэльса и Северной Ирландии, и вводит дифференцированный подход к мерам безопасности в зависимости от потенциальной вместимости объекта: от 200 человек – стандартный уровень требований, от 800 человек – повышенный.

К числу обязательных мер относятся назначение уполномоченного лица или ответственной организации, разработка и реализация процедур по эвакуации, укрытию, блокировке территории, а также обеспечению внутренних и внешних коммуникаций в случае террористической угрозы.

Для объектов, подпадающих под повышенный уровень, дополнительно предусмотрено внедрение технических и организационных средств защиты, включая системы видеонаблюдения, контрольно-пропускные режимы, охрану периметра, а также меры по информационной безопасности.

За неисполнение установленных требований предусмотрена административная ответственность в виде штрафов, а в случае злостного уклонения –

лишение свободы на срок, не превышающий двух лет, или штраф (или оба вида наказания).

При этом закон рассматривает нарушение требований антитеррористической защищенности как самостоятельное преступление, не связывая его с фактическими последствиями, будь то имущественный ущерб или причинение вреда жизни и здоровью. Преступным признается само по себе неисполнение предписания уполномоченного органа, что подчеркивает превентивный характер ответственности и направлено на предупреждение потенциальной опасности до наступления реального вреда.

Указанный закон требует отдельного, внимательного и детального изучения – как в части правовых конструкций и условий привлечения к уголовной ответственности, так и в аспекте анализа правоприменительной практики, а также систематического выявления положительных примеров.

Заключение. Проведенные исследования позволяют сделать вывод, что уголовно-правовые нормы, регулирующие ответственность за нарушение требований к антитеррористической защищенности, не в полной мере отвечают задачам уголовного законодательства.

Их чрезмерная формализованность, а в некоторых случаях – зависимость от административной преюдиции смещают фокус правоприменения на анализ последствий уже совершенного преступления, тогда как непосредственное нарушение требований антитеррористической защищенности остается вне должного внимания.

Некоторые исследователи в сфере уголовного права считают, что несмотря на отсутствие в Особенной части Уголовного кодекса Российской Федерации иных статей, специально направленных на охрану объектов, такая охрана обеспечивается иными уголовно-правовыми нормами, имеющими широкий спектр действия [19].

В отдельных ситуациях действительно возможно применение иных уголовно-правовых норм, опосредованно обеспечивающих охрану объектов, например, предусматривающих ответственность за причинение вреда здоровью по неосторожности или за халатность, однако при этом антитеррористическая защищенность сама по себе не получает статуса самостоятельного объекта уголовно-правовой охраны.

В этой связи существует необходимость не просто точечной корректировки норм,

а концептуального переосмысления подхода к уголовно-правовой охране антитеррористической защищенности, как правового состояния, отражающего устойчивость объекта и территории к возможным угрозам.

Развитие института антитеррористической защищенности в качестве самостоятельного объекта уголовно-правовой охраны будет соответствовать формированию уголовной практики, ориентированной на превенцию террористических угроз, а не только на реагирование по факту их реализации.

В свою очередь, перспектива неизбежного наступления уголовной ответственности будет побуждать к неукоснительному соблюдению требований к антитеррористической защищенности объектов и территорий [24].

При реформировании национального законодательства следует непременно учесть британский опыт. Его превентивная направленность и дифференцированный подход могут стать примером для создания более эффективного уголовно-правового механизма, ориентированного не только на реагирование, но и на предупреждение террористических угроз.

Полноценное и глубокое раскрытие новых правовых конструкций статей 217.1 и 217.3 Уголовного кодекса Российской Федерации возможно лишь в рамках комплексного научного

исследования, организованного российским научным сообществом.

Важно подчеркнуть, что центральным направлением исследования должно стать выявление противоречий и пробелов в действующем регулировании, снижающих уровень антитеррористической защищенности объектов и территорий. Одновременно необходимо научно обосновать потребность в дифференциации уголовной ответственности, с учетом значимости и установленной категории опасности объектов и территорий.

Такой подход позволит учесть объективные различия между, например, объектами критической инфраструктуры федерального уровня и объектами локального значения, что принципиально важно для построения справедливой и эффективной модели уголовной ответственности.

Совершенствование российского уголовного права в указанной сфере будет способствовать выполнению резолюций Совета Безопасности Организации Объединенных Наций, приоритетным направлениям государственной политики в области противодействия терроризму, укреплению антитеррористической защищенности объектов и территорий, а также созданию правовых стимулов для добросовестного исполнения ответственными лицами установленных требований.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.
2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 24.06.2025) // Собрание законодательства Российской Федерации. 2002. № 1 (ч. I). Ст. 1.
3. Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму» // Собрание законодательства Российской Федерации. 2006. № 11. Ст. 1146.
4. Федеральный закон от 21.07.2011 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» // Собрание законодательства Российской Федерации. 2011. № 30 (ч. I). Ст. 4604.
5. Федеральный закон от 31.07.2023 № 398-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 14.07.2025).
6. Указ Президента Российской Федерации от 26.12.2015 № 664 «О мерах по совершенствованию государственного управления в области противодействия терроризму» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 14.07.2025).
7. Указ Президента Российской Федерации от 13 мая 2019 г. № 216 «Об утверждении Доктрины энергетической безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2019. № 20. Ст. 2421.
8. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СПС Консультант плюс // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 14.07.2025).

9. Постановление Правительства Российской Федерации от 05.05.2012 № 459 // Собрание законодательства Российской Федерации. 2012. № 20. Ст. 2556.
10. Постановление Правительства Российской Федерации от 05.05.2012 № 460 // Собрание законодательства Российской Федерации. 2012. № 20. Ст. 2557.
11. Постановление Правительства Российской Федерации от 25.03.2015. № 272 // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 14.07.2025).
12. Постановление Правительства Российской Федерации от 19.10.2017 № 1273 // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 14.07.2025).
13. Постановление Правительства Российской Федерации от 02.08.2019 № 1006 // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 14.07.2025).
14. Приказ Ростехрегулирования от 31.10.2006 № 236-ст, приказ Ростехрегулирования от 17.12.2008 № 430-ст, приказ Росстандарта от 22.11.2012 № 1034-ст, приказ Росстандарта от 22.10.2014 № 1371-ст, приказ Росстандарта от 28.10.2015 № 1659-ст, приказ Росстандарта от 09.11.2016 № 1628-ст, приказ Росстандарта от 16.05.2022 № 300-ст, приказ Росстандарта от 27.01.2025 № 27-ст // СПС Консультант плюс (дата обращения: 14.07.2025).
15. Багринцева О.В., Никитина Ю.С., Абросимова Е.М., Сошнева Д.А. Технические системы антитеррористической и противокриминальной защиты. Воронеж: Воронежский институт Министерства внутренних дел Российской Федерации. 2023. ISBN: 978-5-00229-029-1.
16. Закомолдин Р.В. Преступные нарушения специальных правил и требований безопасности: монография. М-во образования и науки Российской Федерации. Фил. федерального гос. бюджетного образовательного учреждения высш. проф. образования «Российский гос. социальный ун-т» в г. Тольятти Самарской обл. - Тольятти: Фил. РГСУ в г. Тольятти, 2013. ISBN 978-5-903795-49-9.
17. Труфанов А.Ю. О проблемных вопросах категорирования объектов в целях обеспечения их антитеррористической защищенности // Актуальные проблемы противодействия экстремизму и терроризму на современном этапе: Сборник научных статей Всероссийской научно-практической конференции с международным участием, 17-18 февраля 2022 года. Новосибирск: Новосибирский военный институт имени генерала армии И.К. Яковлева войск национальной гвардии Российской Федерации. ISBN: 978-5-6048320-1-1.
18. Аккаева Х.А. К вопросу об уголовной ответственности за нарушение требований к антитеррористической защищенности объектов (территорий) // Пробелы в российском законодательстве. 2024. Т. 17. № 4. EDN: IMULMJ.
19. Борисов С.В., Будило Н.Н. Топливо-энергетический комплекс как объект уголовно-правовой охраны // Криминологический журнал. 2021. № 4. DOI: <https://doi.org/10/24412/2687-0185-2021-4-14-19>.
20. Глуздак Г.Н. Проблемы уголовно-правовой регламентации ответственности за нарушение требований к антитеррористической защищенности объектов (территорий) // Мировой судья. 2024. № 11. DOI: 10.18572/2072-4152-2024-11-26-31.
21. Гончар В.С., Ширяев Ю.Е. Юридическая ответственность за преступления против объектов топливно-энергетического комплекса // Образование и право. 2023. № 4. DOI: 10.24412/2076-1503-2023-4-300-302.
22. Закомолдин Р.В. О некоторых новеллах уголовного законодательства, направленных на обеспечения специальных требований и правил безопасности // Вестник Самарской гуманитарной академии. Серия «Право». 2011. № 2 (10).
23. Теуважев З.А. Некоторые особенности антитеррористической защищенности // Право и управление. 2024. № 2. DOI: 10.24412/2224-9133-2024-2-174-176.
24. Чулкина Э.Ю. Уголовно-правовые нормы с двойной превенцией: понятие, механизм превентивного воздействия и виды // Актуальные проблемы российского права. 2023. Т. 18. № 5. DOI: 10.17803/1994-1471.2023.150.5.107-122.
25. Информационное агентство «РБК». В России ввели уголовную ответственность за нарушение мер защиты объектов // Электронное издание. URL: <https://www.rbc.ru/politics/01/07/2024/6681210f9a79472fd775fe40> (дата обращения: 03.08.2025).
26. Информационное агентство ТАСС. СБ ООН принял резолюцию о защите критической инфраструктуры от нападений террористов // Электронное издание. URL: <https://tass.ru/mezhdunarodnaya-panorama/4019713?ysclid=mdyzt571i339501411> (дата обращения: 05.08.2025).
27. Сайт Судебного департамента при Верховном Суде Российской Федерации // Электронный ресурс. URL: <https://cdep.ru> (дата обращения 25.07.2025); Электронное издание «Агентство правовой информации», зарегистрировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, свидетельство № ФС 77–6332 // Электронный ресурс. URL: <https://stat.апи-пресс.рф> (дата обращения 25.07.2025).
28. Patrick Rogers. The Terrorism (Protection of Premises). Act 2025. Martyn's Law // Электронный сайт. URL: https://www.wtwco.com/en-gb/insights/2025/04/the-terrorism-protection-of-premises-act-2025?utm_source (дата обращения: 03.08.2025).

УДК 654.9

ББК 30ц

ДМИТРИЕВ РОМАН СЕРГЕЕВИЧ, НАЧАЛЬНИК СЕКТОРА ОТДЕЛА РАЗВИТИЯ СРЕДСТВ ОБНАРУЖЕНИЯ ФЕДЕРАЛЬНОГО КАЗЕННОГО УЧРЕЖДЕНИЯ «НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР «ОХРАНА» РОСГВАРДИИ, КАНДИДАТ ТЕХНИЧЕСКИХ НАУК

РЯБЦЕВ НИКОЛАЙ АЛЕКСЕЕВИЧ, НАЧАЛЬНИК ОТДЕЛА РАЗВИТИЯ СРЕДСТВ ОБНАРУЖЕНИЯ ФЕДЕРАЛЬНОГО КАЗЕННОГО УЧРЕЖДЕНИЯ «НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР «ОХРАНА» РОСГВАРДИИ, КАНДИДАТ ТЕХНИЧЕСКИХ НАУК

ОБ ОСНОВНЫХ ТЕХНИЧЕСКИХ ТРЕБОВАНИЯХ К СРЕДСТВАМ ОБНАРУЖЕНИЯ, ОСНОВАННЫМ НА ТРИБОЭЛЕКТРИЧЕСКОМ ПРИНЦИПЕ ДЕЙСТВИЯ

Аннотация. В докладе рассмотрены средства обнаружения, основанные на трибоэлектрическом принципе действия. Представлены их основные преимущества, а также сформированные технические требования к данным средствам обнаружения. Описан возможный положительный эффект от их практического применения в деятельности подразделений вневедомственной охраны войск национальной гвардии Российской Федерации при организации охраны объектов.

Ключевые слова: охрана, периметр, средство обнаружения, извещатель, трибоэлектрический эффект, технические требования.

DMITRIEV ROMAN SERGEEVICH, HEAD OF THE SECTOR OF THE DETECTION TOOLS DEVELOPMENT DEPARTMENT OF THE FEDERAL STATE INSTITUTION «SCIENTIFIC RESEARCH CENTER «OKHRANA» OF THE FEDERAL SERVICE OF NATIONAL GUARD OF THE RUSSIAN FEDERATION, CANDIDATE OF TECHNICAL SCIENCES

RYABTSEV NIKOLAY ALEKSEEVICH, HEAD OF THE DETECTION TOOLS DEVELOPMENT DEPARTMENT OF THE FEDERAL STATE INSTITUTION «SCIENTIFIC RESEARCH CENTER «OKHRANA» OF THE FEDERAL SERVICE OF NATIONAL GUARD OF THE RUSSIAN FEDERATION, CANDIDATE OF TECHNICAL SCIENCES

ABOUT THE BASIC TECHNICAL REQUIREMENTS FOR DETECTION TOOLS BASED ON BASED ON THE TRIBOELECTRIC PRINCIPLE OF OPERATION

Annotation. This report examines detection systems based on the triboelectric principle. Their key advantages are presented, along with the technical requirements for these systems. The potential positive impact of their practical application by non-departmental security units of the Russian National Guard troops in securing facilities is described.

Keywords: security, perimeter, detection device, detector, triboelectric effect, technical requirements.

Одной из основных задач подразделений вневедомственной охраны войск национальной гвардии Российской Федерации (далее – подразделения) является охрана особо важных и режимных объектов, объектов подлежащих обязательной охране в соответствии с перечнем объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации, утвержденным Правительством Российской Федерации [1], собственных объектов, а также объектов физических и юридических лиц по договорам (далее – объекты) [2].

Безопасность объектов зависит от совокупности принимаемых организационных мер и безотказной

работы технических систем охраны, включающих в себя системы видеонаблюдения, контроля и управления доступом, освещения, а также систему охранной сигнализации, включающей в себя различные средства обнаружения (далее – СО). При этом организация охраны периметра объекта выходит на передний план, так как раннее обнаружение проникновения способствует минимизации возможного ущерба от действий нарушителей и повышает общую защищенность объекта.

Для построения системы охраны периметра объекта широко применяются различные СО, основанные на магнитоконтактном, оптико-

электронном (активном и пассивном), радиоволновом и трибоэлектрическом принципах действия, область и специфика применения которых обусловлены их функциональными особенностями.

Так магнитоконтактные СО используют для блокировки калиток и въездных ворот, пассивные оптико-электронные СО применяют для охраны участков периметров протяженностью до 70 м, радиоволновые и активные оптико-электронные СО устанавливают на прямых участках периметров протяженностью до 300 м, СО, основанные на трибоэлектрическом принципе действия (далее – СОТП), – на полотне ограждения периметров.

Стоит отметить, что для организации охраны периметров значимых объектов, в том числе важных государственных объектов, объектов промышленности, критической инфраструктуры и транспорта, таких как атомные электростанции, объекты топливно-энергетического комплекса, аэропорты и т.п., применяются СОТП.

При этом в случае взятия под охрану подобных объектов подразделениями возникает проблема выбора СОТП, так как на сегодняшний день отечественными предприятиями-изготовителями технических средств охраны производятся множество типов данных СО, отличающихся друг от друга техническими и функциональными характеристиками.

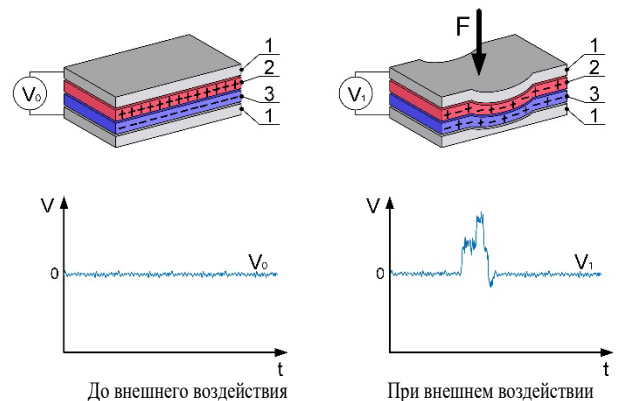
Для решения данной проблемы ФКУ «НИЦ «Охрана» Росгвардии по заданию ГУВО Росгвардии проведена научно-исследовательская работа в рамках которой выявлены преимущества СОТП перед радиоволновыми и активными оптико-электронными СО, такие как:

- возможность охраны периметров со сложной конфигурацией – имеющих повороты и изгибы, а также где имеет место изменение рельефа участков местности (уклоны и подъемы);
- высокая помехоустойчивость – имеют низкую чувствительность к осадкам, электромагнитным помехам, наличию близко растущих кустарников и деревьев;
- отсутствие «мертвых зон» и низкое энергопотребление.

Данные преимущества обусловлены использованием в СОТП одноименного трибоэлектрического эффекта, рисунок 1.

Физика трибоэлектрического эффекта основана на межатомном взаимодействии: если у одного из материалов притяжение атомов сильнее, то электроны второго начинают сдвигаться в сторону первого, так происходит возникновение статических зарядов, то есть один из материалов теряет электроны, а другой их приобретает [3]. Трибоэлектрический эффект проявляется при трении следующих пар: диэлектрик-диэлектрик, полупроводник-полупроводник, металл-металл (разной плотности), металл-диэлектрик, жидкий

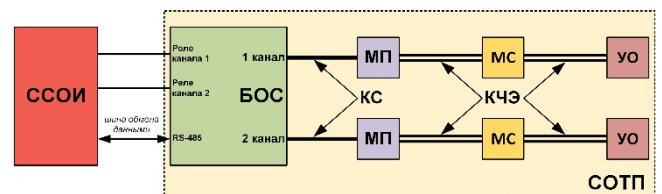
диэлектрик-металл и другие варианты сочетаний различных материалов [4].



1 – внешняя токопроводящая оболочка; 2, 3 – разнородные диэлектрики; F – внешнее воздействие; V_0 – начальное напряжение между разнородными диэлектриками; V_1 – напряжение между разнородными диэлектриками при внешнем воздействии; «+» – положительный заряд; «-» – отрицательный заряд.

Рисунок 2 - Трибоэлектрический эффект

Кроме того, в ходе работы сформирована общая структурная схема СОТП, состоящая из блока обработки сигнала (далее – БОС) и чувствительного элемента. Общая структурная схема СОТП, имеющего два канала (фланга) обнаружения, представлена на рисунке 2.



ССОИ – система сбора и обработки информации; БОС – блок обработки сигналов; КС – кабель соединительный; КЧЭ – кабельный чувствительный элемент (трибоэлектрический кабель); МП – муфта переходная; МС – муфта соединительная; УО – устройство оконечное (резистор и конденсатор).

Рисунок 2 - Общая структурная схема СОТП, имеющего два канала (фланга) обнаружения

В качестве чувствительного элемента в СОТП применяется трибоэлектрический кабель, принцип действия которого заключается в наведении электрического заряда, возникающего при трении, друг о друга разнородных диэлектриков. Кабель крепят либо непосредственно к полотну ограждения, либо к специальному легкому металлическому козырьку над ним.

Сигналы, поступающие от кабеля, обрабатываются БОС, который в соответствии с заданным алгоритмом работы формирует извещение о тревоге и передает его в систему сбора и обработки информации путем замыкания реле или передачи кодовой комбинации по шине обмена данными с использованием различных интерфейсов, например, по асинхронному интерфейсу RS-485.

Кроме того, для формирования требований авторами проведен анализ ряда

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

межгосударственных и национальных стандартов Российской Федерации, определяющих основные технические и функциональные требования к вышеуказанным СО [5-11]. Результаты проведенного анализа показали, что данные стандарты, не регламентируют ряд особенностей таких, как способы крепления, устройство и структура трибоэлектрических чувствительных кабелей, способы сопряжения БОС и ССОИ.

При этом данные особенности необходимо учитывать при применении СОТП в подразделениях, т.к. СО должны обладать, как высокими техническими параметрами, так и высокими эксплуатационными характеристиками, превышающими требования стандартов.

В результате исследования вышеуказанная проблема ФКУ «НИЦ «Охрана» Росгвардии решена путем формирования основных технических требований к средствам обнаружения, основанным на трибоэлектрическом принципе действия и предназначенным для применения в подразделениях (таблица 1), определяющих требования к функциональному назначению и тактико-техническим характеристикам, помехоустойчивости и электропитанию, устойчивости и прочности к внешним воздействующим факторам, защите от несанкционированных воздействий и контролю функционирования, конструкции, электромагнитной совместимости и надежности, а также к интерфейсу и безопасности.

Таблица 1 – Основные технические требования к средствам обнаружения, основанным на трибоэлектрическом принципе действия

1 Требования к функциональному назначению и тактико-техническим характеристикам
2 Требования по помехоустойчивости
3 Требования к электропитанию
4 Требования устойчивости и прочности к внешним воздействующим факторам
4.1 Открытое пространство окружающей среды
4.2 Сухое тепло
4.3 Холод
4.4 Повышенная влажность
4.5 Синусоидальная вибрация
4.6 Импульсный механический удар
4.7 Прочность к воздействию внешних факторов при транспортировании
5 Требования защиты от несанкционированных воздействий
5.1 Защита от вскрытия корпуса
5.2 Защита соединительных линий
5.3 Контроль целостности чувствительного элемента
6 Требования к интерфейсу
6.1 Общие требования
6.2 Информационные выходы
6.3 Адресные и беспроводные извещатели
6.4 Информативность
7 Требования контроля функционирования
7.1 Формирование извещения о неисправности
7.2 Автоматический самоконтроль функционирования
7.3 Удаленный (дистанционный) контроль функционирования
7.4 Компенсация уменьшения чувствительности
7.5 Сезонная подстройка чувствительности
8 Требования к конструкции
9 Требования электромагнитной совместимости
10 Требования надежности
11 Требования безопасности
12 Требования к технической документации

Необходимо отметить, что требования сформированы с учетом анализа технической и эксплуатационной документации наиболее широко распространенных на рынке СОТП ведущих Российский производителей технических средств безопасности и дополняют требования стандартов на данный вид СО.

Разработанные требования легли в основу сформированного авторами проекта соответствующего раздела «Единых требований 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» [12].

Применение на практике сформированных технических требований позволяет осуществлять разработку, модернизацию и квалифицированный отбор образцов СОТП с высокими тактико-техническими характеристиками и широкими функциональными возможностями, что в свою очередь позволяет подразделениям обеспечить высокую надежность охраны объектов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. О перечне объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации: распоряжение Правительства РФ от 15.05.2017 № 928-р (ред. от 24.06.2025) // «Консультант Плюс»: справочно-правовая система : [сайт]. - URL: <https://hq-cnsdb-01.rosguard.ru> (дата обращения: 12 августа 2025 года).
2. О войсках национальной гвардии Российской Федерации: Федеральный закон от 03.07.2016 № 226-ФЗ (ред. от 31.07.2025) // «Консультант Плюс»: справочно-правовая система: [сайт]. - URL: <https://hq-cnsdb-01.rosguard.ru> (дата обращения: 12 августа 2025 года).
3. Люблинский К.А., Малышева А.А., Адамович К.А., Василевский А.Г. Извещатель охранный трибоэлектрический, устройство и особенности применения // Новые направления развития приборостроения: материалы 17-й Международной научно-технической конференции молодых ученых и студентов, 17-19 апреля 2024 года, Минск, Республика Беларусь/ Белорусский национальный технический университет; редкол. О.К. Гусев (пред. редкол. [и др.] – Минск: БНТУ, 2024. – С. 86: [сайт]. - URL: <https://rep.bntu.by> (дата обращения: 13 августа 2025 года).
4. Трибоэлектрические средства защиты периметра. Прогноз на завтра. [сайт]. - URL: <https://triz-cable.ru> (дата обращения : 13 августа 2025 года).
5. ГОСТ Р 52435–2015 Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний // «Консультант Плюс»: справочно-правовая система: [сайт]. - URL: <https://hq-cnsdb-01.rosguard.ru> (дата обращения: 12 августа 2025 года).
6. ГОСТ Р 71322–2024 Извещатели линейные трибоэлектрические для охраны периметров территорий. Общие технические требования и методы испытаний // «Консультант Плюс»: справочно-правовая система: [сайт]. - URL: <https://hq-cnsdb-01.rosguard.ru> (дата обращения: 12 августа 2025 года).
7. ГОСТ Р 52860–2007 Технические средства физической защиты. Общие технические требования // «Консультант Плюс»: справочно-правовая система: [сайт]. - URL: <https://hq-cnsdb-01.rosguard.ru> (дата обращения: 12 августа 2025 года).
8. ГОСТ Р 54455–2011 Системы охранной сигнализации. Методы испытаний на устойчивость к внешним воздействующим факторам // «Консультант Плюс»: справочно-правовая система: [сайт]. - URL: <https://hq-cnsdb-01.rosguard.ru> (дата обращения: 12 августа 2025 года).
9. ГОСТ 15150–69 Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды // «Консультант Плюс»: справочно-правовая система: [сайт]. - URL: <https://hq-cnsdb-01.rosguard.ru> (дата обращения: 12 августа 2025 года).
10. ГОСТ 26342–84 Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры // «Консультант Плюс»: справочно-правовая система: [сайт]. - URL: <https://hq-cnsdb-01.rosguard.ru> (дата обращения: 12 августа 2025 года).
11. ГОСТ 14254–2015 Степени защиты, обеспечиваемые оболочками (Код IP) // «Консультант Плюс»: справочно-правовая система: [сайт]. - URL: <https://hq-cnsdb-01.rosguard.ru> (дата обращения: 12 августа 2025 года).
12. Единые требования к системам передачи извещений, объектовым техническим средствам охраны и сигнальным охранно-противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации.: утверждены решением расширенного заседания Технического совета ГУВО Росгвардии (Протокол № 2 от 14–17 октября 2024 года) // Федеральное казенное учреждение «Научно-исследовательский центр «Охрана» Росгвардии: официальный сайт. - 2025. URL: <https://nicohrana.ru/wp-content/uploads/2024/11/et-2024.pdf> (дата обращения: 12 августа 2025 года).

УДК 654.9

**ЗДОРОВЦОВ АНАТОЛИЙ ГЕННАДЬЕВИЧ, КАНДИДАТ ТЕХНИЧЕСКИХ НАУК,
ПРЕПОДАВАТЕЛЬ КАФЕДРЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ
ФАКУЛЬТЕТА (ИНЖЕНЕРНОГО ОБЕСПЕЧЕНИЯ) ПЕРМСКОГО ВОЕННОГО ИНСТИТУТА
ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**К ВОПРОСУ СКРЫТОЙ ПЕРЕДАЧИ ТРЕВОЖНОГО СИГНАЛА В МОБИЛЬНЫХ
(БЫСТРОРАЗВЕРТЫВАЕМЫХ) ТЕХНИЧЕСКИХ СРЕДСТВАХ ОХРАНЫ**

Аннотация. В статье проведен анализ стоящих на вооружении мобильных технических средств охраны обрывного принципа действия, каналов передачи данных и выдвинуты требования, которым должны соответствовать такие современные средства для выполнения задачи по сохранению жизни и здоровья личного состава войск национальной гвардии Российской Федерации и гражданского персонала.

Ключевые слова: система охраны; мобильное техническое средство охраны; быстроразвертываемое средство охраны; извещатель; тревога; режим охраны; зона охраны; радиосигнализатор.

**ZDOROVTSOV ANATOLY GENNADYEVICH, CANDIDATE OF TECHNICAL SCIENCES,
LECTURER OF THE DEPARTMENT OF ENGINEERING AND TECHNICAL MEANS OF SECURITY OF THE
FACULTY (ENGINEERING SUPPORT) OF THE PERM MILITARY INSTITUTE OF THE NATIONAL GUARD
TROOPS OF THE RUSSIAN FEDERATION**

**ON THE QUESTION OF HIDDEN TRANSMISSION OF ALARM SIGNAL IN MOBILE (RAPID-
DEPLOYABLE) TECHNICAL SECURITY MEANS**

Annotation. The article analyzes the mobile technical security equipment of the breakaway principle of action, data transmission channels in service and puts forward the requirements that such modern means must meet to perform the task of preserving the life and health of the personnel of the troops of the National Guard of the Russian Federation and civilian personnel.

Keywords: security system; mobile technical security device; rapidly deployable security device; detector; alarm; security mode; security zone; radio alarm.

На Федеральную службу войск Национальной гвардии Российской Федерации (далее – Росгвардия) возлагаются различного рода задачи, некоторыми из которых являются охрана важных государственных и собственных объектов, специальных грузов, сооружений на коммуникациях, а также объектов, подлежащих обязательной охране войсками национальной гвардии, в соответствии с перечнями, утверждёнными Правительством Российской Федерации [1], а также участие в оборудовании важных государственных и собственных объектов охраняемых войсками, мест несения боевой службы караулов (войсковых нарядов) инженерно-техническими средствами охраны (далее – ИТСО), а также организация их эксплуатации и ремонта.

Пресечение противозаконных действий со стороны нарушителей, проникших на территорию Российской Федерации, – одна из главных проблем в стране. За последние годы противозаконные действия приобрели глобальный характер, угрожая интересам граждан, общественной безопасности и стабильности государства. Наибольший интерес для таких нарушителей вызывают сведения, которые составляют государственную, служебную и коммерческие тайны. Как правило, такие

сведения хранятся на персональных компьютерах (далее – ПК) и бумажных носителях в сейфах и ящиках на важных объектах. Вследствие этого в настоящее время актуальной задачей безопасности важных объектов является обеспечение физической защиты таких помещений [1].

По опыту участия Росгвардии в специальной военной операции существует необходимость в охране полевых городков, полевых складов с оружием и комнат для хранения оружия. Отсюда следует, что выполнение возложенных задач в отрыве от пункта постоянной дислокации (далее – ППД) является приоритетным направлением, при этом существует необходимость частой передислокации полевых городков из одного места в другое, оборудуя каждый раз новые пункты временной дислокации (далее – ПВД). В условиях агрессии противника своевременность выполнения служебно-боевых задач (далее – СБЗ) по оборудованию объектов комплексом инженерно-технических средств охраны (далее – ИТСО) способствует сохранению жизни и здоровья личного состава при размещении в ПВД.

Неотъемлемой частью выполнения вышеуказанных задач является своевременное и скрытое оборудование охраняемых объектов

в ПВД комплексом ИТСО. В связи с этим, успешное выполнения СБЗ обеспечит устройство рубежей обнаружения обрывными техническими средствами охраны (далее – ОТСО).

В соответствии с требованиями нормативно-правовых актов (далее – НПА) Росгвардии при расположении воинских частей (организаций) в пунктах временной дислокации места размещения оборудуются ИТСО с применением быстроразвертываемых инженерных и технических систем (средств) охраны, после чего размещается личный состав, вооружение, военная \ и специальная техника, а также другое имущество. Количество и расположение инженерных \ и технических систем (средств) охраны должно обеспечивать сохранность вооружения, военной и специальной техники, а также другого имущества [3].

Приоритетом при выполнении СБЗ всегда является безопасность личного состава, а применение мобильных технических средств охраны (далее - МобТСО) существенно облегчит выполнение задач по оборудованию объектов ИТСО, что повысит значение данного показателя, а также уменьшит требуемое для этого время. Актуальность проблемы внедрения на вооружение МобТСО возрастает с каждым годом, а для повышения безопасности личного состава очевидно применение МобТСО со скрытой передачей сигнала тревоги на средство сбора и обработки информации (далее – ССОИ). С их использованием уменьшится число привлечения личного состава к оборудованию объектов в ПВД, что позволит заблаговременно приступить к выполнению других СБЗ. Исходя из этого, можно однозначно сказать, что ПВД очень

нуждаются в МобТСО, которые находят широкое применение при оборудовании охраняемых войсками объектов в условиях отрыва частей и подразделений Росгвардии от ППД, при выполнении ими СБЗ.

Актуальным и открытым вопросом остается скрытая передача МобТСО тревожного сигнала на ССОИ, так как все современные охранные мобильные комплексы передают данный сигнал по радиоканалу, который обнаруживается противником. Следствием раскрытия места нахождения МобТСО является обнаружение нахождения ПВД, что приводит к высокой вероятности уничтожения данного пункта ракетными и беспилотными комплексами. Исходя из вышесказанного, можно утверждать, что приоритетной целью является разработка такого мобильного технического средства охраны обрывного принципа действия, который передавал бы тревожное извещение по проводной линии связи, а радиоканал оставался как резервный, это увеличит степень надежности охраняемых рубежей и всего ПВД в целом.

На вооружении войск национальной гвардии стоят такие обрывные МобТСО, как «Алмаз», «Трепанг», «Кувшинка», «Кувшинка-М» – произведенные в Союзе Советских Социалистических Республик (далее – СССР), так и современные – сигнализационный комплекс (далее – СК) «Паутина», СК «Радиобарьер», в состав которых входят обрывные сигнализаторы [3-9]. Анализ тактико-технических характеристик существующих мобильных технических средств охраны находящихся на вооружении войск национальной гвардии представлены в таблице 1.

Таблица 1 – Существующие мобильные технические средства охраны, находящиеся на вооружении войск национальной гвардии

Параметр	Алмаз	Трепанг	Кувшинка	Кувшинка-М	Леер-Р	СК Паутина	РС-У СК «Радиобарьер»
Определение места обрыва	Нет	Нет	Нет	Да	Нет	Да	Да
Канал передачи данных на ССОИ	Нет	Нет	Нет	Нет	Радиоканал	Радиоканал	Радиоканал
Дальность передачи тревожного извещения, м	Нет	Нет	Нет	Нет	До 500	До 1500	До 1000
Скрытая передача «тревожного сигнала»	Нет	Нет	Нет	Нет	Нет	Нет	Нет
Шифрование при передаче данных по радиоканалу	Нет	Нет	Нет	Нет	Нет	Да	Да
Максимальная протяженность блокируемого участка, м	До 4400	До 13200	До 800	До 500	До 3000	До 500	До 400
Длительность непрерывной работы (в среднем), дней	До 104	До 10	До 7	До 5	До 365	До 5	До 1825
Напряжение питания, В	3,5-4,5	3,4-4,5	2,4-3	6	3,6	12	12
Диапазон рабочих температур, С°	От -20 до +35	От -20 до +35	От -10 до +40	От -15 до +40	От -40 до +65	От -40 до +55	От -40 до +50

Анализ существующих мобильных ТСОС обрывного принципа действия (табл. 1) показывает, что данные существующие средства передают «тревожный сигнал» на ССОИ по радиоканалу, либо не передают вообще, что делает их «видимыми» на сканерах радиоэлектронных излучений противника или же приходится заводить

чувствительный элемент к оператору вместе с блоком обработки и отображения «тревожного сигнала». Такой подход приводит к тому, что личный состав находится под угрозой поражения артиллерийскими и беспилотными комплексами противника.

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

Путем решения данной проблемы является вывод «тревожного сигнала» от мобильного технического средства охраны обрывного принципа действия на средство сбора и обработки информации по проводным каналам связи, который будет являться основным каналом и радиоканалу – который будет являться резервным каналом передачи «тревожного извещения».

Для обеспечения выполнения задачи по обеспечению скрытой передачи тревожного сигнала от разрабатываемого мобильного технического средства охраны обрывного принципа действия на средство сбора и обработки информации, и с целью отображения и хранения информации о тревожном извещении, проведен анализ способов передачи таких извещений, а также виды каналов и физических линий предназначенных для этого. Самыми распространенными физическими линиями передачи данных являются: кабель «Витая пара», «Полевой кабель», «Оптическое волокно» (табл. 2) [10].

Исходя из показателей, можно сделать вывод, что все рассматриваемые кабели имеют свои достоинства и недостатки (табл. 2). Несмотря на указанные достоинства, при оборудовании МобТСО воинских частей в пунктах временной дислокации, нужно понимать, что иметь специальные оборудование и навыки по коммутации витой пары и оптоволоконно практически невозможно. Ждать поставки оборудования занимает много времени. Исходя из цели, задачу возможно решить путем

применения полевого кабеля. Данный кабель присутствует в любой воинской части, имеет достаточно большую прочность и хорошо маскируемый.

Проведенный анализ разработанности вопроса о применении мобильных технических средств охраны обрывного принципа действия и физических каналов передачи тревожного извещения применяемых в войсках национальной гвардии Российской Федерации можно сделать вывод, что в соответствии с НПА Росгвардии при расположении воинских частей в пунктах временной дислокации, места их размещения оборудуются ИТСО с применением мобильных (быстроразвертываемых) технических средств охраны, которые разработаны в Союзе Советских Социалистических Республик (далее – СССР). Современные МобТСО также имеют большое количество недостатков, а именно проблемным вопросом является скрытая передача МобТСО тревожного сигнала на ССОИ, так как все современные охранные мобильные комплексы передают данный сигнал по радиоканалу, который обнаруживается противником. Следствием раскрытия места нахождения МобТСО является обнаружение нахождения ПВД, что приводит к высокой вероятности уничтожения данного пункта ракетными и беспилотными комплексами. Отсюда следует необходимость обосновать требования, которым должно соответствовать мобильное техническое средство охраны обрывного принципа действия.

Таблица 2 – Сравнительный анализ параметров физических каналов передачи тревожного извещения

Параметр	Витая пара	Полевой кабель	Оптическое волокно
Устойчивость к внешним воздействиям	Средняя	Высокая	Низкая
Дальность передачи тревожного извещения, м	До 1000	До 30 000	До 20 000
Возможность скрытой передачи тревожного извещения	Нет	Нет	Да
Возможность считать информацию с кабеля	Да	Да	Нет
Сложность коммутации	Да	Нет	Да
Необходимость специального оборудования для монтажа кабеля	Да	Нет	Да
Необходимость специальных навыков для монтажа кабеля	Да	Нет	Да
Стоимость монтажа и эксплуатации кабеля	Высокая	Низкая	Высокая
Диапазон рабочих температур, С°	От +5 до +40	От +5 до +40	От –30 до +65

Таблица 2 – Сравнительный анализ параметров физических каналов передачи тревожного извещения

Параметр	Значение
Канал передачи данных на ССОИ	Проводной, радиоканал (резервный)
Интерфейс передачи данных по проводной связи	П-274М
Частота радиоканала передачи данных, МГц	433-435
Дальность передачи тревожного извещения, м	До 1000
Скрытая передача «тревожного сигнала»	Да
Шифрование при передаче данных по радиоканалу	Да
Максимальная протяженность блокируемого участка, м	До 500
Определение места до обрыва	Да
Длительность непрерывной работы (в среднем), дней	До 365
Напряжение питания, В	12
Диапазон рабочих температур, °С	От –40 до +50

Таким образом, при соответствии требованиям, представленным в таблице 3, МобТСО позволит выполнить стоящую задачу по скрытой передаче тревожного извещения на ССОИ и достичь цели по сохранению жизни и здоровья личного состава. Исходя из этого, перспективным направлением является исследование вопроса, заключающегося

в возможности разработки МобТСО с двумя каналами передачи тревожного извещения:

основной – физическая линия передачи данных (полевой кабель П-274М);

резервный – радиоканал (частота 433-435 МГц).

Также рассмотреть возможность универсального подключения его к ССОИ любого типа по данным канал связи.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Указ Президента РФ от 30 сентября 2016 г. № 510 «О Федеральной службе войск национальной гвардии Российской Федерации».
2. Здоровцов, А. Г. К вопросу повышения системы физической защиты важных объектов / А. Г. Здоровцов // Альманах Пермского военного института войск национальной гвардии. – 2025. – № 1(17). – С. 11-34. – EDN MNKEUG.
3. Электроконтактное средство обнаружения «Алмаз». – Техническое описание. – М.: ПОССТАТ, 1980. – 28 с.
4. Быстроразвертываемое техническое средство охранной сигнализации «Трепанг». – Техническое описание. – М.: ПОССТАТ, 1982. – 31 с.
5. Сигнализатор охранный обрывного типа «Кувшинка». – Техническое описание. – М.: ПОССТАТ, 1984. – 37 с.
6. Сигнализатор охранный обрывного типа «Кувшинка-М». – Техническое описание. – М.: ПОССТАТ, 1986. – 57 с.
7. Быстроразвертываемый (мобильный) комплект обрывного средства обнаружения «Леер-Р». – Техническое описание. – М.: Аргус-Спектр, 2017. – 61 с.
8. «Обрывное средство обнаружения» мобильного быстроразвертываемого сигнализационного комплекса «ПАУТИНА». – Техническое описание. – М.: Охранные системы, 2005. – 129 с.
9. Сигнализационный комплекс Радиобарьер: учебное пособие // Учебный центр ООО «Полюс-СТ». Rev. 1.1/06.14.1. – 268 с.
10. Магауенов, Р. Г. Системы охранной сигнализации: основы теории и принципы построения / Р. Г. Магауенов. – Учебное пособие. – 3-е изд., стереотип. – М.: Горячая линия – Телеком, 2019. – 494 с.

**КАХАНОВ СЕРГЕЙ АЛЕКСАНДРОВИЧ, НАЧАЛЬНИК ОТДЕЛЕНИЯ-ЗАМЕСТИТЕЛЬ
НАЧАЛЬНИКА ОТДЕЛА ОХРАНЫ ВАЖНЫХ ГОСУДАРСТВЕННЫХ ОБЪЕКТОВ
УПРАВЛЕНИЯ БОЕВОЙ СЛУЖБЫ ЦЕНТРАЛЬНОГО ОКРУГА ВОЙСК НАЦИОНАЛЬНОЙ
ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

ПУТИ СОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ ВЗАИМОДЕЙСТВИЯ В ЦЕЛЯХ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ, ПОДЛЕЖАЩИХ ОХРАНЕ В ПРИГРАНИЧНЫХ РЕГИОНАХ

Аннотация. в статье проведен анализ современного состояния существующей системы взаимодействия на основе изучения нормативных правовых актов Российской Федерации, регламентирующих взаимодействие органов безопасности с подразделениями Росгвардии и научных исследований в сфере охраны и защиты государственной границы, а также объектов, расположенных в приграничном регионе. Предложены пути совершенствования существующей системы взаимодействия в целях повышения защищенности объектов с учетом степени угрозы нападения на них в современных формирующихся условиях.

Ключевые слова: взаимодействие, безопасность, защищенность объектов, классификация объектов, модель угроз, модель нарушителя, требования к защищенности объектов, противодействие современных формирующихся условиях.

В настоящее время обстановка вблизи границ Российской Федерации остается неустойчивой, что требует усиления мер по обеспечению безопасности и защиты важных государственных объектов (ВГО), особенно в приграничных регионах. Это обусловлено обострением угрозы военного характера, включая провокации вдоль западных границ, заброску диверсионно-разведывательных формирований и другие формы вооруженного воздействия.

Обеспечение безопасности на приграничной территории осуществляется пограничными органами Федеральной службы безопасности Российской Федерации (ФСБ России) во взаимодействии с Вооруженными Силами Российской Федерации, войсками национальной гвардии и другими воинскими формированиями Российской Федерации, оказывающими в рамках своих полномочий во взаимодействии исполнение возложенных задач по защите и охране государственной границы Российской Федерации.

Правовой основой взаимодействия органов безопасности ФСБ России с Федеральной службой войск национальной гвардии Российской Федерации (Росгвардия) в сфере защиты и охраны государственной границы являются Конституция Российской Федерации, законодательные и иные нормативные правовые акты, ведомственные (межведомственные) и совместные правовые акты.

Порядок взаимодействия органов безопасности ФСБ России при реализации предоставленных им полномочий в сфере защиты и охраны государственной границы определен межведомственными нормативными актами,

регламентирующими взаимодействие пограничных органов, Вооруженных Сил Российской Федерации, войск национальной гвардии Российской Федерации и органов внутренних дел Российской Федерации (полиции).

В рамках данного взаимодействия подразделения Росгвардии оказывают содействие пограничным органам ФСБ России в охране государственной границы путём обмена информацией о деятельности и местоположении подразделений (войсковых нарядов), а также применения беспилотных аппаратов и комплексов для повышения защищенности охраняемых объектов.

В целях своевременного принятия решения по повышению защищенности объектов и реагированию всех имеющихся сил и средств войск национальной гвардии, задействованных в обеспечении их безопасности, пограничными органами по оперативной линии доводится информация до подразделений Росгвардии о вооруженном вторжении (подготовке к вооруженному вторжению) на территорию Российской Федерации со стороны сопредельного государства, а также о выявленных мероприятиях, выполняемых вооруженными силами сопредельного государства на территории сопредельного государства.

Согласно нормативным правовым актам Росгвардии, объектами войск национальной гвардии являются собственные объекты, здания, строения и сооружения, принадлежащие на праве оперативного управления воинским частям (организациям) войск, а также пункты

их временного размещения в полевых условиях, в том числе объекты, расположенные на территории ВГО, особо важных и режимных объектов, подлежащих охране войсками национальной гвардии.

Документами, регламентирующими реализацию требований к обеспечению безопасности и антитеррористической защищенности объектов, подлежащих охране территориальными органами и их подразделениями Росгвардии, определен порядок взаимодействия должностных лиц администраций охраняемых объектов с органами безопасности по разработке и утверждению перечня основных угроз и модели нарушителя в отношении ВГО, а также согласованию паспортов безопасности и антитеррористической защищенности ВГО, включенных в перечни, утвержденные Правительством Российской Федерации.

В отношении территориальных органов, воинских частей, подразделений и объектов Росгвардии, расположенных в том числе на территории ВГО и подлежащих охране в приграничном регионе, согласно действующей нормативной правовой базе и полученным в ходе проведенных научных исследований результатов в установленной системе взаимодействия органов безопасности с территориальными органами (подразделениями) Росгвардии не определен порядок и методика разработки такой модели угроз и модели нарушителя для повышения их безопасности и антитеррористической защищенности, что затрудняет оценку степени и характера угроз, оперативно выработать требования к системе охраны и защиты объектов, в том числе определить необходимые дополнительные силы и средства для эффективного противодействия угрозам в реальных условиях.

Для повышения защищенности ВГО в приграничном регионе необходимо разработать и внедрить систему категорирования этих объектов

с учётом степени угрозы и характера возможных воздействий. Это позволит дифференцировать требования к системам охраны и защиты каждого объекта, определить необходимые дополнительные силы и средства для эффективного противодействия угрозам.

Таким образом, необходимо совершенствовать существующую систему взаимодействия органов безопасности с подразделениями Росгвардии для повышения защищенности ВГО в приграничном регионе. Это должно включать разработку предложений по порядку разработки и применения методики определения модели угроз и нарушителей, подготовку системы категорирования объектов, а также определение требований к системам охраны и защиты каждого объекта.

Пути решения этой задачи могут включать:

1. Углублённое изучение и анализ существующих угроз и методов их реализации в приграничных регионах.

2. Разработка методических рекомендаций по оценке степени угрозы для каждого типа ВГО с учётом их особенностей и местоположения, а также поддержки принятия решения по применению сил и средств для противодействия сформированным угрозам в определенный момент времени.

3. Создание системы мониторинга и прогнозирования угроз, которая позволит оперативно реагировать на изменения обстановки и корректировать меры охраны.

4. Взаимодействие между органами безопасности, Росгвардией и другими силовыми структурами для обмена информацией и координации действий при угрозе нападения на ВГО.

Реализация этих мер позволит обеспечить более высокий уровень защищенности объектов в приграничном регионе и эффективно противостоять современным угрозам в кризисных ситуациях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Конституция Российской Федерации. – М.: Юрид. лит. 1993. – 64 с.
2. Федеральный закон от 03.04.1995 г. № 40-ФЗ (ред. от 28.06.2014) «О Федеральной службе безопасности» (с изм. и доп., вступ. в силу с 30.09.2014) // Российская газета. – 2014.
3. Федеральный закон Российской Федерации от 03.07.2016 № 226 «О войсках национальной гвардии Российской Федерации».
4. Федеральный закон Российской Федерации от 06.03.2006 N 35-ФЗ «О противодействии терроризму».

5. Закон Российской Федерации от 01.04.1993 г. № 4730–1 «О Государственной границе Российской Федерации» // Ведомости съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. – 1993. – № 17, ст. 594.
6. Указ Президента Российской Федерации от 3.09.2016 г. N 510 «О Федеральной службе войск национальной гвардии Российской Федерации».
7. Постановление Правительства Российской Федерации от 19.01.2005 г. № 30 «О типовом регламенте взаимодействия федеральных органов исполнительной власти».
8. Постановление Правительства Российской Федерации от 25 марта 2015 г. № 272 «Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии Российской Федерации, и форм паспортов безопасности таких мест и объектов (территорий)».
9. Постановление Правительства Российской Федерации от 19.07.2007 г. № 456 «Об утверждении Правил физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов».
10. Постановление Правительства Российской Федерации от 27.05.2017 г. № 646 «Об утверждении требований к оборудованию инженерно-техническими средствами охраны важных государственных объектов, специальных грузов, сооружений на коммуникациях, подлежащих охране войсками национальной гвардии Российской Федерации».
11. Постановление Правительства Российской Федерации от 15 мая 2017 г. № 928-р «О перечне объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации».
12. Приказ ФС ВНГ РФ от 27 мая 2019 г. № 177дсп «Об утверждении требований к оборудованию ИТСО собственных объектов войск национальной гвардии Российской Федерации и Руководства по организации оборудования ИТСО собственных объектов войск национальной гвардии Российской Федерации. Издание ИУ ЦА ВНГ РФ, 2019 г.
13. Временное наставление по инженерному обеспечению войск национальной гвардии Российской Федерации. Приказ ФСВНГ РФ от 27 марта 2019 № 108дсп.
14. Методические рекомендации по подготовке сил и средств войск национальной гвардии Российской Федерации к охране и обороне мест своего размещения (собственных объектов). Издание ЦА ВНГ РФ, 2017 г.
15. Методические рекомендации участия подразделений вневедомственной охраны войск национальной гвардии Российской Федерации в мероприятиях по антитеррористической защищенности объектов различной ведомственной принадлежности. Р078-2018 г.
16. Системы физической защиты. Методические рекомендации по проведению анализа уязвимости ядерно-опасных объектов. Утверждены распоряжением № 167-р Минатома России от 10 мая 2001 г. М.: Минатом, 2001.
17. Приказ Минатома России от 22.01.2004. № 221-222дсп «Системы физической защиты ядерно-опасных объектов. Методические рекомендации по оценке эффективности».
18. Пензин А.А. Методика проведения оценки эффективности системы физической защиты ядерно-опасных объектов /А.А. Пензин //Сборник научных трудов академии. – М.: ВУНЦ СВ «ОВА ВС РФ». – 2012. - № 45. - С. 78-85.

УДК 35.078.42

КВАСОВ В.Б., ЗАМЕСТИТЕЛЬ НАЧАЛЬНИКА ФГУП «УВО ВНГ РОССИИ ПО ЯМАЛО-НЕНЕЦКОМУ АВТОНОМНОМУ ОКРУГУ», ПОЛКОВНИК ПОЛИЦИИ, КАНДИДАТ ЮРИДИЧЕСКИХ НАУК

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ПРОПУСКНОГО РЕЖИМА ОХРАНЯЕМОГО ОБЪЕКТА

Основным элементом, организации системы безопасности объекта любой сложности является пропускной режим, включающий в себя основные требования по организации и осуществлению пропускного и внутриобъектового режимов на объекте.

Пропускной режим, как следует из его названия, регулирует исключительно «пропуск» через границы охраняемого объекта. Однако для комплексной охраны необходим контроль за тем, что происходит непосредственно на территории объекта, поэтому параллельно с пропускным обеспечивается и внутриобъектовый режим.

Внутриобъектовый режим устанавливает внутри границ охраняемого объекта особый порядок, необходимый для обеспечения его защищенности. Законом «О ведомственной охране» внутриобъектовый режим определен как порядок, обеспечиваемый совокупностью мероприятий и правил, выполняемых лицами, находящимися на охраняемых объектах, в соответствии с требованиями внутреннего трудового распорядка и пожарной безопасности. [1, с. 3]

Таким образом, пропускной режим охраняемого объекта, по нашему мнению, представляет собой комплекс организационных мероприятий (административно-ограничительных), инженерно-технических решений и действий службы охраны, которые направлены на контроль за пропуском на охраняемые объекты и с охраняемых объектов сотрудников, посетителей, транспорта, материальных средств [2, с.124].

В случае выявления фактов нарушения внутриобъектового и (или) пропускного режима сотрудниками (работниками) требований внутренней инструкции работники охраны фиксируют различными способами от докладных записок до принятых внутренних актов нарушения режима, выявленное нарушение и передают руководителю предприятия (организации).

Дисциплинарные взыскания на сотрудника (работника) предприятия (организации) могут налагаться руководителем данного предприятия (организации) с оформлением соответствующего

приказа по предприятию (организации) или руководителем структурного подразделения с оформлением распоряжения по структурному подразделению. Уменьшение размера премии или невыплата премии полностью оформляется приказом руководителя данного предприятия (организации) на основании документов, подтверждающих факт нарушения.

Всем сотрудникам (работникам) предприятия (организации), сторонних организаций и посетителям должно быть запрещено как правило:

- находиться на объектах и передвигаться по территории без пропуска; передавать кому-либо, свои личные пропуска, отмечать на контрольно-пропускном пункте чужой пропуск или проводить на территорию (выпускать с территории) по своему личному пропуску другое лицо;

- пытаться проходить (проезжать) на территорию объектов вне контрольно-пропускного пункта;

- проводить с собой на территорию объектов детей;

- проходить на территорию объектов в состоянии какого-либо опьянения;

- распивать алкогольную продукцию и принимать наркотические вещества;

- курить в не установленных местах, разжигать костры, выжигать траву, а также осуществлять огневые работы без оформления соответствующего разрешения на их производство;

Изменения в режиме работы персонала оформляются приказом руководителя предприятия (организации).

Список сотрудников (работников) организации (предприятия), имеющих право прохода (проезда) на территорию организации (предприятия) без регистрации на КПП и без осмотра автотранспорта, утверждается локальным нормативно-правовым актом руководителя организации (предприятия). Все иные обязаны иметь пропуск (временный, постоянный, материальный и т.д.) дающий право посещения объекта (тов) или территории (й).

Сотрудники (работники) подразделения охраны при проверке пропуска имеют право не пропускать

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

на территорию объекта сотрудника (работника), при отсутствии идентификации личности. При увольнении работник обязан сдать пропуск.

Временные пропуска выдаются только при наличии в списке работников организации (предприятия), письменной информации руководителя подразделения или письменной информации руководителя сторонней организации (предприятия) отметки о проведении инструктажа по пропускному и внутри объектовому режимам. Функционал данного документа также описывается в инструкции по обеспечению пропускного режима.

На территорию объектов организации (предприятия) без оформления пропусков и без осмотра автотранспорта пропускаются лица в сопровождении руководителя организации (предприятия), и уполномоченных им должностных лиц.

Отдельного внимания заслуживает порядок въезда-выезда железнодорожного транспорта:

Железнодорожные ворота постоянно должны находиться в закрытом положении. Открытие ворот производится работниками охраны только по указанию уполномоченного руководителя.

Тепловозы перед выездом и въездом через железнодорожные ворота подлежат осмотру на общих основаниях.

Члены локомотивно-составительской бригады постоянно должны иметь при себе личный пропуск и предъявлять его в руки работнику охраны по его требованию. В тепловозах запрещается провоз через железнодорожные ворота Предприятия

пассажиров, кроме состава бригады, и провоз любых товароматериальных ценностей.

Физическим основанием для вывоза (выноса) продукции и других материальных средств с территории организации (предприятия) служат сопроводительные документы и материальный пропуск. Данные документы должны соответствовать требованиям безопасности.

Материальный пропуск оформляется в структурном подразделении. Непосредственно перед вывозом (выносом) товароматериальных ценностей ответственное лицо подразделения согласовывает материальный пропуск с охраной.

Таким образом, осуществление пропускного режима на охраняемый объект осуществляется непосредственно в период пересечения периметра охраняемого объекта, после его пересечения и нельзя не отметить такой важный фактор как предупредительные мероприятия в непосредственной близости от охраняемого объекта. Указанные мероприятия в соответствии с действующим законодательством могут осуществляться только сотрудниками правоохранительных органов. Сотрудники (работники) иных ведомств предприятий, организаций могут вести лишь наблюдение с использованием технических средств либо визуальное. Осуществлять реагирование на противоправные действия также могут лишь в рамках действующего законодательства. Тем не менее, данный рубеж является наиболее важным с точки зрения безопасности охраняемого объекта.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Приказ Министерства образования, науки и молодежной политики Республики Коми от 1 июня 2018 г. № 209-п «Об утверждении положения об организации пропускного и внутриобъектового режимов на объекте (территории) образовательной организации Республики Коми» // <https://base.garant.ru/48670436/?ysclid=m6otesw5r9925560127>.
2. Квасов В.Б. Административно-правовое регулирование государственной охранной деятельности: дис. канд. юрид. наук: 5.1.2 – Нижегородский государственный университет им. Н.И. Лобачевского, Нижний Новгород, 2023 – 235 с.

УДК 621.311.6
ББК 31.25

КОЛОСКОВ АЛЕКСЕЙ АНАТОЛЬЕВИЧ, НАУЧНЫЙ СОТРУДНИК ФКУ «НИЦ «ОХРАНА»
РОСГВАРДИИ

ВИХИРЕВ АНАТОЛИЙ АЛЕКСАНДРОВИЧ, НАУЧНЫЙ СОТРУДНИК ФКУ «НИЦ
«ОХРАНА» РОСГВАРДИИ

ТАЛЫШЕВ НИКОЛАЙ ВАСИЛЬЕВИЧ, КАНДИДАТ ТЕХНИЧЕСКИХ НАУК, ДОЦЕНТ,
НАЧАЛЬНИК ОТДЕЛА ФКУ «НИЦ «ОХРАНА» РОСГВАРДИИ

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ПРЕОБРАЗОВАТЕЛЕЙ КИНЕТИЧЕСКОЙ ЭНЕРГИИ В КАЧЕСТВЕ ИСТОЧНИКОВ АВТОНОМНОГО ЭЛЕКТРОПИТАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ БЕЗОПАСНОСТИ

Аннотация. В работе проанализирована применимость принципов преобразования кинетической энергии в электрическую для построения на их основе источников автономного электропитания технических средств безопасности. Предложены направления использования таких преобразователей для замены гальванических элементов, а также рассмотрены перспективы расширения области их практического применения.

Ключевые слова: техническое средство безопасности, преобразователь, кинетический модуль, автономное электропитание.

KOLOSKOV ALEXSEY ANATOLYEVICH, RESEARCHER AT THE FSI «SRC «OKHRANA»
OF ROSGVARDIYA

VIKHIREV ANATOLIY ALEXSANDROVICH, RESEARCHER AT THE FSI «SRC «OKHRANA»
OF ROSGVARDIYA

TALYSHEV NIKOLAY VASILYEVICH, CANDIDATE OF SCIENCES (TECHNICAL), ASSISTANT
PROFESSOR, HEAD OF DEPARTMENT AT THE FSI «SRC «OKHRANA» OF ROSGVARDIYA

PROSPECTS FOR USING CONVERTERS KINETIC ENERGY AS SOURCES AUTONOMOUS
POWER SUPPLY OF TECHNICAL SECURITY MEANS

Annotation. The paper analyzes the applicability of principles conversion of kinetic energy into an electrical signal for constructing on their basis sources of autonomous electric power supply of technical means of safety. Directions of use of such converters for replacement of galvanic elements are proposed, and also prospects of expanding of the area of their practical application are considered.

Keywords: technical safety device, converter, kinetic module, autonomous electrical wiring.

Одной из немаловажных организационно-технических составляющих обеспечения безопасности объекта является оснащение персонала и сотрудников подразделений охраны техническими средствами тревожной сигнализации. Значительная часть данных средств, основанных на применении беспроводных технологий обмена данными, укомплектована автономными источниками электропитания, в качестве которых применяются гальванические элементы (химические источники тока) [1]. На практике широко используются два вида источников: перезаряжаемые (аккумуляторы) и перезаряжаемые элементы. Они имеют

разнообразные физико-химические принципы работы и технологические особенности при изготовлении, но при этом обладают рядом недостатков, в том числе:

а) необходимость непрерывного контроля электрических параметров, так как сам принцип работы гальванических элементов (получение электрической энергии посредством химической реакции) подразумевает ограниченность запасаемой ими энергии. Выработка ресурса для перезаряжаемых элементов или разряд аккумуляторов приводит к невозможности выполнения ими своих функций;

б) саморазряд, то есть постепенное снижение электрической емкости гальванических элементов, происходящее в процессе хранения, вследствие постоянно протекающих внутренних химических реакций. И если для аккумуляторов саморазряд можно компенсировать периодическим подзарядом, то для перезаряжаемых элементов этот процесс необратим;

в) высокая зависимость от температурного режима эксплуатации, которая связана с тем, что использование гальванических элементов в условиях повышенных температур окружающего воздуха (выше плюс 35 оС) значительно сокращает их ресурс, а негативное влияние пониженных температур (ниже минус 10 оС) выражается как в снижении электрической емкости гальванических элементов, так и в значительном замедлении химических реакций, происходящих в процессе заряда аккумуляторов, что приводит к невозможности их полноценного заряда;

г) чувствительность к неблагоприятным воздействиям внешней среды, обусловленная тем, что эксплуатация в условиях повышенной влажности воздуха или наличия в нем агрессивных веществ, приводит к окислению контактов гальванических элементов, и как следствие к отказу работоспособности технического средства;

д) высокая токсичность веществ, входящих в состав гальванических элементов, поэтому устройства на их основе отнесены к отходам II класса опасности [2], что означает, что они представляют опасность для здоровья людей и окружающей среды и требуют специальной технологии утилизации.

В качестве альтернативы гальваническим элементам, для электропитания отдельных видов технических средств безопасности предлагается использовать элементы автономного питания, лишенные перечисленных выше недостатков, – устройства, преобразующие кинетическую энергию движения в электрическую энергию (далее – кинетические модули или модули).

Ключевым преимуществом использования кинетических модулей является отсутствие в их составе элементов, предназначенных для длительного хранения электроэнергии, так как электроэнергия в кинетическом модуле вырабатывается непосредственно в момент физического воздействия на него. Отсутствие элементов, имеющих ограниченный ресурс, значительно повышает надежность питаемых ими технических средств безопасности. Кроме того, при условии соблюдения правил эксплуатации кинетических модулей, срок их службы практически не ограничен.

Проанализируем применимость известных физических принципов преобразования кинетической энергии движения в электрическую для построения на их основе источников автономного электропитания технических средств безопасности. Отправной точкой для выбора принципа преобразования энергии для таких модулей служит оценка их способности соответствовать требованиям по электропитанию и сохранению размеров и массы технических средств безопасности при замене гальванических элементов.

Кинетические модули рассматриваются как альтернатива традиционным гальваническим элементам, которые используются в различных портативных устройствах безопасности [3]. К таким устройствам относятся беспроводные кнопки тревожной сигнализации, активные вещественные идентификаторы (брелоки) и другие. Они отличаются малой длительностью информационного сигнала и низким энергопотреблением. Это создает теоретические предпосылки для использования модулей в качестве источника питания для таких устройств.

В качестве физических принципов преобразования кинетической энергии в электрическую при разработке модулей могут быть использованы:

- а) прямой пьезоэлектрический эффект;
- б) обратный магнитострикционный эффект;
- в) электростатическая индукция;
- г) электромагнитная индукция.

Одним из ключевых технических параметров, определяющих пригодность кинетического модуля, работающего на определенном физическом принципе, для использования в качестве источника электропитания для технических средств безопасности, являются вольтамперные характеристики и временные параметры процесса генерации электроэнергии. Для кинетических модулей, преобразующих энергию на основе прямого пьезоэлектрического или обратного магнитострикционного эффектов, это энергия дискретного импульса. При этом, напряжение прямого пьезоэлектрического эффекта, в зависимости от конструктивных особенностей кристалла и силы механического воздействия, может составлять от десятков до сотен вольт [4]. Однако, длительность генерируемого кинетическим модулем импульса недостаточна для выработки автономным источником питания мощности, необходимой для формирования и передачи извещения. Аналогичная ситуация наблюдается и с обратным магнитострикционным эффектом (эффект Виллари) [5].

Для модулей, использующих электростатическую и электромагнитную индукцию, – это значения напряжения и тока, генерируемые в течение всего времени физического воздействия на него. Благодаря отсутствию временных ограничений и возможности накопления энергии, при их использовании может быть обеспечено автономное питание практически любого портативного технического средства безопасности.

Важным техническим параметром при выборе автономного источника электропитания технических средств безопасности является массогабаритный показатель. Наименьшими размерами и весом обладает модуль, основанный на прямом пьезоэлектрическом эффекте. Чуть больше по этим характеристикам имеют модули с обратным магнитострикционным эффектом. Третье место уверенно занимают модули с электромагнитной индукцией. А самые крупные и тяжелые – это модули с электростатической индукцией. Это связано с необходимостью использования в них таких крупных элементов, как коллектор и индуктор.

К важным критериям при выборе физического принципа преобразования энергии, используемого в кинетическом модуле, относятся не только технические характеристики, но и его стоимость. Пьезоэлектрические и магнитно-индукционные модули относительно недороги, так как их производство не требует сложных технологий и дорогих материалов. В тоже время электростатические модули стоят дороже из-за сложной конструкции и большого количества деталей. Самые дорогие – это преобразователи, созданные на основе обратного магнитострикционного эффекта.

Анализируя технико-экономические параметры, можно сделать вывод, что для портативных средств безопасности лучше всего подходят модули, основанные на электромагнитной индукции, то есть использующие явление возникновения электрического тока, электрического поля или электрической поляризации при изменении магнитного поля во времени или при движении материальной среды в магнитном поле [6]. При этом с точки зрения функциональности использования в технических средствах безопасности для выработки электрической энергии наиболее применимы модули линейного, роторного или коммутационного типов.

Если приведение в действие технического средства безопасности сопряжено

с поступательным движением, то наиболее целесообразно осуществлять генерацию электрической энергии с помощью кинетических модулей линейного типа. На рисунке 1 приведено графическое представление принципа работы кинетического модуля линейного типа. В тоже время при проектировании такого модуля в составе устройства необходимо учитывать, что эффективность преобразования энергии линейного движения напрямую зависит от скорости перемещения силовых линий магнитного поля через витки катушки, а также от степени плотности данного поля при пересечении проводов. То есть наибольшая электродвижущая сила при равных скоростях возникает при входе магнита в соленоид и выходе из него и тем более значительную результирующую энергию можно получить, чем выше скорость движения магнита будет обеспечена.

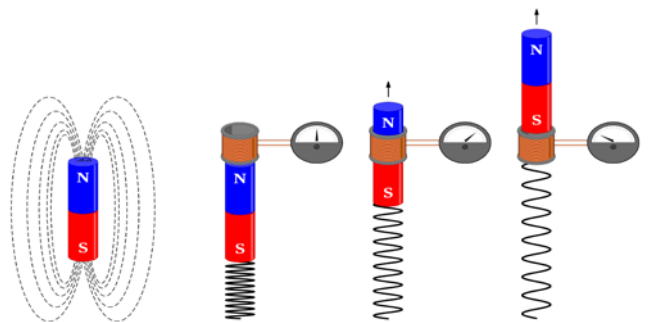


Рисунок 1 – Принцип работы кинетического модуля линейного типа

Если механика технического средства безопасности предполагает вращательное движение, то наиболее целесообразно осуществлять генерацию электрической энергии с помощью кинетических модулей роторного типа. Схемы таких модулей, преобразующих энергию в электрическую посредством использования электромагнитной индукции, приведена на рисунке 2. В качестве кинетических модулей выступают генераторы переменного (слева) и постоянного тока (справа).

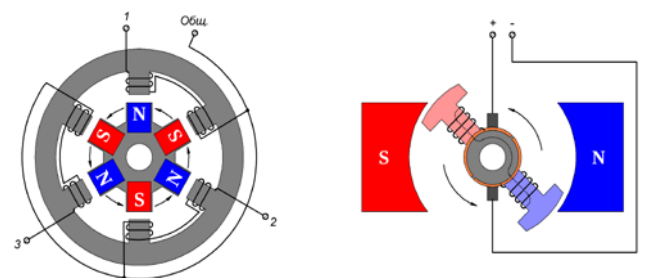


Рисунок 2 – Схемы построения кинетических модулей роторного типа

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

Энергоэффективность данных модулей зависит не только от скорости вращения роторной части, но и динамичности смены намагничивания. Поэтому в целях получения более высокого значения электродвижущей силы при одинаковой угловой скорости ротора рациональнее использовать схему, приведенную в левой части рисунка 2.

В случае, если габаритные размеры технического средства безопасности ограничивают вращательное движение ротора, то рационально для автономного преобразования энергии использовать кинетический модуль коммутационного типа, принцип работы которого приведен на рисунке 3.

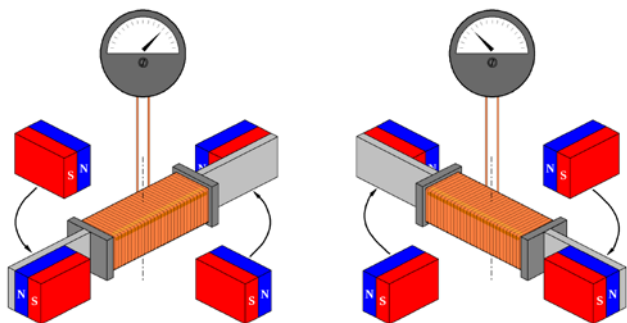


Рисунок 3 – Принцип работы кинетического модуля коммутационного типа

В связи с тем, что в данном модуле нарастание магнитного потока через катушку индуктивности возникает в результате изменения намагниченности сердечника при его касании одной из разнополярно ориентированных пар магнитов, то повышение эффективности преобразования энергии может быть достигнуто путем увеличения количества витков в соленоиде, а также использованием магнитов с более высоким значением магнитной индукции.

В контексте разработки автономных источников электропитания для технических средств безопасности, кинетический модуль представляет собой инновационное решение, обладающее высокой эффективностью, широким спектром применения и имеющее ряд преимуществ перед используемыми в портативных беспроводных устройствах гальваническими элементами.

Наиболее перспективным видится применение кинетического модуля в беспроводной кнопке тревожной сигнализации при ее эксплуатации в условиях, когда температура окружающей среды ниже минус 10 °С. Как показывает практика, традиционные гальванические элементы при таких значениях температуры подвержены быстрому разряду, что может привести к отказу в работе устройства. Кинетический модуль, напротив,

обеспечивает стабильное электропитание, что делает его идеальным для эксплуатации в холодных климатических условиях.

Еще одно достоинство использования кинетических модулей заключается в отсутствии в их составе элементов, требующих периодической замены, что позволяет обеспечивать полную герметизацию корпуса значительно более простыми способами, чем в ином случае. Это позволяет создать устройства, предназначенные для эксплуатации в условиях повышенной влажности и воздействия агрессивных сред, в которых одной из причин отказа работоспособности технических средств безопасности является окисление электрических контактов или замыкание дорожек платы.

Кроме того, необслуживаемые кнопки тревожной сигнализации могут быть реализованы как в носимом варианте, так и в стационарном исполнении. Стационарные версии найдут свое применение на объектах исторического и культурного наследия, где установка проводных систем может нарушить эстетическое восприятие или повредить архитектурные элементы интерьера. Кинетический модуль позволяет интегрировать данные устройства в инфраструктуру без необходимости прокладывания кабелей, что особенно важно для сохранения исторического облика зданий.

Еще одним направлением применения кинетических преобразователей энергии в технических средствах безопасности может стать их использование в социальных, медицинских и образовательных учреждениях. Ограниченность выделяемых ресурсов на непрофильные для данных учреждений текущие расходы по техническому обслуживанию систем безопасности, очень низкая предсказуемость выхода из строя гальванических элементов и необходимость времени на их закупку и своевременную замену, а иногда и просто разгильдяйство приводит к тому, что существующая система тревожной (вызывной) сигнализации оказывается неработоспособна, что ставит под угрозу жизни и здоровье сотрудников, посетителей и пациентов. Использование кинетических модулей в беспроводных кнопках тревожной сигнализации исключает возможность возникновения такой проблемы и гарантированно обеспечивает инициирование тревожного извещения. А создание системы адресных приемников во всех помещениях данных учреждений позволит решить проблему с определением места нахождения сотрудника или

пациента, нажавшего кнопку тревожной сигнализации (кнопку вызова помощи).

Кинетический модуль также может найти применение в активных вещественных идентификаторах, таких как брелоки для систем контроля и управления доступом. Зачастую отказ гальванического элемента, питающего брелок, в силу его разряда, происходит в самый неподходящий, а иногда и критический момент, что приводит к блокировке доступа. Кинетический преобразователь энергии, благодаря своей автономности, обеспечивает гарантированное электропитание брелоков, повышая надежность системы безопасности и снижая вероятность отказов.

С помощью предлагаемых кинетических модулей можно обеспечивать работу автономных замков с идентификацией на основе электронных ключей Touch-Memory или бесконтактных идентификаторов RFID. При повороте ручки такого замка посредством шестереночной передачи происходит вращение ротора микроэлектрогенератора, вырабатывающего электропитание для контроллера электронных ключей (идентификаторов). После принятия им решения на допуск, энергия, вырабатываемая в результате дальнейшего вращения ручки данного замка, подается на исполнительный элемент, осуществляющий деблокировку запирающего устройства. Автономные замки с идентификацией могут найти применение в случаях, когда подключение элементов системы контроля

и управления доступом с помощью проводов затруднительно из-за особенностей открывающихся или смежных конструкций, например, для стеклянных дверей.

Неожиданным может оказаться эффект от размещения совокупности технических средств безопасности с источниками электропитания на основе кинетических модулей в элементах напольных покрытиях. Это позволит осуществлять позиционирование и контроль за перемещением объектов в охраняемых помещениях, формировать траектории движения нарушителей.

Кроме того, применение кинетических модулей для питания извещателей-ловушек [7] позволит повысить их автономность, то есть обеспечит возможность смены места их размещения на объекте в зависимости от необходимости, что снизит вероятность их предварительного обнаружения злоумышленником и последующего обхода при проникновении.

Таким образом использование модулей, преобразующих кинетическую энергию в электрическую, формирует новые возможности для создания универсальных и высокоэффективных решений по осуществлению электропитания различных беспроводных устройств, обеспечивая их надежную работу в экстремальных условиях, а также открывая новые возможности для повышения их автономности и расширяя области практического применения технических средств безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р 58593-2019. Национальный стандарт Российской Федерации. Источники тока химические. Термины и определения (утв. и введен в действие приказом Росстандарта от 7 октября 2019 г. № 964-ст) – М.: Стандартинформ, 2019.
2. Об утверждении требований при обращении с группами однородных отходов I – V классов опасности: приказ Минприроды России от 11 июня 2021 г. № 399 (ред. от 04.04.2023).
3. ГОСТ Р 54455-2011 (МЭК 62599-1:2010). Национальный стандарт Российской Федерации. Системы охранной сигнализации. Методы испытаний на устойчивость к внешним воздействующим факторам (утв. и введен в действие Приказом Росстандарта от 28 сентября 2011 г. № 411-ст) – М.: Стандартинформ, 2012.
4. Дугиева Д.А. Изучение пьезоэлектрического эффекта в кварце // Молодой ученый. – 2020. – № 34 (324). – С. 4-6.
5. Мащенко И.П., Мащенко А.И. Теоретические основы эффекта Виллари // Известия вузов. Северо-Кавказский регион. Технические науки. – 2005. – № 3. – С. 4-8.
6. Избранные главы физики для учителей: учебное пособие / А.А. Шаповалов. – Барнаул: АлтГПУ. – 2018. – 155 с.
7. ГОСТ Р 52551-2016. Национальный стандарт Российской Федерации. Системы охраны и безопасности. Термины и определения (утв. и введен в действие приказом Росстандарта от 22 ноября 2016 г. № 1743-ст) – М.: Стандартинформ, 2012.

УДК 654.9

**КРАСИЛИЧ АЛЕКСАНДР АЛЕКСАНДРОВИЧ, ПОЛКОВНИК ПОЛИЦИИ, ЗАМЕСТИТЕЛЬ
НАЧАЛЬНИКА
ФГКУ «УВО ВНГ РОССИИ ПО Г. САНКТ-ПЕТЕРБУРГУ И ЛЕНИНГРАДСКОЙ ОБЛАСТИ»**

**ПРИМЕНЕНИЕ СИСТЕМ ФОРМИРОВАНИЯ ТРЕВОЖНЫХ СООБЩЕНИЙ
С ИСПОЛЬЗОВАНИЕМ ВИДЕОАНАЛИТИКИ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА
ДЛЯ ЦЕНТРАЛИЗОВАННОЙ ОХРАНЫ ОБЪЕКТОВ И ТЕРРИТОРИЙ (ПЛОЩАДОК)**

Аннотация. Применение систем формирования тревожных сообщений на основании использования современных возможностей видеоаналитики и искусственного интеллекта при осуществлении централизованной охраны объектов подразделениями вневедомственной охраны приведет к существенному увеличению их объемов и надежности, а также значительно упростит реализацию многих задач, указанных в «Программе технического перевооружения подразделений вневедомственной охраны», ГУВО Росгвардии на 2025 год.

Ключевые слова: тревожные сообщения, сформированные на основе видеоаналитики и искусственного интеллекта; возможность организации реагирования нарядами полиции.

В мае 2024 года в адрес ФГКУ «УВО ВНГ России по г. СПб и ЛО» (далее – «ФГКУ УВО») поступили первые предложения о рассмотрении возможности реагирования нарядов полиции групп задержания ФГКУ УВО на формируемые тревожные извещения аппаратно-программным комплексом (далее – «АПК») «Безопасный город» ГКУ «Городской мониторинговый центр» (далее – «ГМЦ») Комитета по информатизации и связи Правительства г. Санкт-Петербурга с использованием видеоаналитики и искусственного интеллекта на детских и спортивных площадках города Санкт-Петербурга.

Учитывая важную социальную функцию по обеспечению безопасности мест, предназначенных для отдыха и развития детей, по созданию комфортной и безопасной среды их обитания, а также с целью дальнейшего развития инновационных технологий в сфере охраны, ФГКУ УВО было признано, что реализация указанной программы с участием подразделений вневедомственной охраны является перспективным направлением.

С учётом этого, а также в соответствии с письмом ГУВО Росгвардии от 12.07.2024 №8/4076 «О проведении тестовой эксплуатации» и согласно подпункту 5.7 решения расширенного заседания Технического совета ГУВО Росгвардии, проведённого в мае 2024 года в г. Магасе, начиная с августа 2024 года по настоящее время под руководством ФКУ НИЦ «Охрана» Росгвардии в ФГКУ УВО проводится соответствующий эксперимент по выводу сигналов от систем видеонаблюдения детских спортивных площадок, формирующих тревожные извещения на основании

видеоаналитики и искусственного интеллекта, непосредственно в Центры оперативного управления (далее – «ЦОУ») нарядами полиции групп задержания филиалов ФГКУ УВО, в целях выработки Единой технической политики в сфере вневедомственной охраны, утвержденной распоряжением Росгвардии от 07 июня 2023 г. № 1/1107-р».

Данный эксперимент показал, что система формирования тревожных извещений на основании использования возможностей видеоаналитики и искусственного интеллекта с объектов охраны, в том числе открытых спортивных и детских площадок, при противодействии кражам, умышленному уничтожению или повреждению имущества на них, а также при обеспечении общественного порядка, способна организовать обмен информацией (тревожными извещениями и приёмом команд управления), как с АРМ систем централизованного наблюдения (далее – «СЦН») подразделений вневедомственной охраны по сетям GSM и/или Интернет/Ethernet 10/100 Мбит/с, так и программно-аппаратным комплексом взаимодействия с мониторинговыми компаниями (далее – «ПАК ВcМК»). При этом указанные системы видеонаблюдения имеют возможность распознавать лица людей, фиксировать в сцене обзора оружие, драки, человека, лежащего без движения или подающего жесты о помощи. Видео и аудио потоки с камер, расположенных на детских и спортивных площадках, поступают в аппаратно-программный комплекс (далее – «АПК») «Безопасный город» и обрабатываются нейросетями с целью распознавания

противоправных действий, далее сигнал передаётся на реагирование в подразделения вневедомственной охраны посредством ПАК ВсМК.

Следует отметить, что в ходе проведения эксперимента в ЦОУ филиалов ФГКУ УВО не поступило ни одного ложного срабатывания. При этом при формировании тестового тревожного сообщения при имитации в секторе обзора средств видеонаблюдения попытки повреждения (перемещения) имущества объекта, демонстрации предметов похожих на оружие, драки, лежащего без движения человека или подающего жесты о помощи, тревожные сообщения были сформированы в течение одной минуты и переданы на ПЦО ОВО. Учитывая изложенное, в настоящее время ход проводимого эксперимента следует считать удачным.

Вместе с тем, с целью определения полного спектра возможных проблем при организации реагирования на указанные объекты в случае поступления сигналов от указанных систем видеонаблюдения, в настоящее время ФГКУ УВО совместно с ГКУ «ГМЦ» в рамках АПК «Безопасный город» проведено расширение данного эксперимента путём принятия их установленным порядком на реагирование посредством ПАК ВсМК с применением действующего тарифа, предусмотренного действующим приказом ФГКУ УВО от 22.05.2018 №215, на услуги «...по реагированию при поступлении сигналов на автоматизированное рабочее место пункта централизованной охраны, сформированных с помощью комплекса технических средств охраны системы мониторинга, предоставляемые ФГКУ УВО и его филиалами, организациям, финансируемым из бюджетов всех уровней, коммерческим организациям и индивидуальным предпринимателям» в размере 2608 руб. в месяц с каждого объекта.

Здесь справочно следует отметить, что доступом к АПК «Безопасный город» обладают также и другие правоохранительные органы г. Санкт-Петербурга. Оператор дежурной службы АПК анализирует ситуативную картинку и в случае тревоги передает сигнал на пульт Росгвардии для вызова группы задержания и принятия мер реагирования.

Исследуя перспективы применения таких Систем формирования тревожных сообщений на основе видеоналитики и искусственного интеллекта в различных сферах охраны объектов, в том числе крупных централизованно охраняемых учреждений, нельзя не заметить, что они

существенно расширяют функциональные возможности существующих комплексных систем охраны таких объектов. Так, с помощью них появляется возможность обнаружения нарушителей на большой дальности путем наблюдения за ними вне зоны охраны и обзора основной системы сигнализации и видеонаблюдения. Такой комплекс наблюдения может обеспечивать обнаружение, определение количественного состава нарушителей и контроль при перемещении их по территории охраняемых объектов, в том числе объектов большой площади и с протяженным периметром. Кроме того, с помощью использования современных возможностей видеоналитики и искусственного интеллекта при осуществлении централизованной охраны объектов подразделениями вневедомственной охраны появляется возможность осуществить идентификацию собственника (владельца имущества), а также определение нештатной ситуации, при постановке (снятие) объекта под централизованную охрану.

Вместе с тем, следует также отметить, что в ходе изучения действующей нормативной документации при проведении данного эксперимента выявлен ряд организационных вопросов, требующих внимания в вопросах обеспечения централизованной охраны объектов и имущества, а именно:

1. При заключении договоров охраны требуется чёткое определение предмета договора охраны по проведению комплекса мероприятий по контролю над объектами граждан и организаций (далее – «Объект») и пресечению противоправных посягательств в отношении находящегося на нём имущества граждан и организаций путем реагирования силами нарядов групп задержания ФГКУ УВО.

Пояснение: в настоящее время к комплексу мероприятий по контролю над Объектами и пресечению противоправных посягательств на них, в том числе, относится оборудование Объекта техническими средствами охраны согласно Р 093-2024 «Методические рекомендации. Обследование объектов, охраняемых или принимаемых под охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации». При этом к охраняемым объектам относятся – здания, строения, сооружения (части здания, строения, сооружения и помещения), водные объекты, прилегающие к ним территории и акватории, имущество граждан и организаций, охраняемые на договорной основе

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

подразделениями вневедомственной охраны и оборудованные техническими средствами охраны (охранно-пожарной, охранной, тревожной сигнализацией), подключенных на ПЦО подразделений вневедомственной охраны, посредством реагирования на сигналы «тревога» группами задержания подразделений вневедомственной охраны. Но в проводимом эксперименте Объект, является открытой площадкой, которая оборудованию привычными средствами сигнализации не подлежит, тревожное извещение будет формироваться на основании видеоаналитики исходя из заданных параметров, что по смыслу Р 093-2024, что не в полном объеме позволяет отнести его к категории «охраняемый объект».

2. В соответствии с п. 21 ст. 9 Главы 2 Федерального закона от 3 июля 2016 г. № 226-ФЗ «О войсках национальной гвардии Российской Федерации» в полномочия войск национальной гвардии входит охрана на договорной основе особо важных и режимных объектов, объектов на коммуникациях, объектов, подлежащих обязательной охране в соответствии с перечнем, утверждаемым Правительством Российской Федерации, имущества граждан и организаций, а также обеспечение оперативного реагирования на сообщения о срабатывании охранной, охранно-пожарной и тревожной сигнализации (далее – ОПТС) на подключенных к пультам централизованного наблюдения подразделений войск национальной гвардии объектах, охрана которых осуществляется с помощью технических средств охраны, в этих целях незамедлительно прибывать на место совершения преступления, административного правонарушения, место происшествия, пресекать противоправные деяния, устранять угрозы безопасности граждан и общественной безопасности, документировать обстоятельства совершения административного правонарушения, обстоятельства происшествия, обеспечивать сохранность следов преступления, административного правонарушения, происшествия. Учитывая это, а также то, что в соответствии с рекомендациями ФКУ «НИЦ Охрана» Росгвардии Р 093-2024 «Техническое средства охраны(далее – «ТСО») – конструктивно законченное устройство, выполняющее самостоятельные функции в составе системы, предназначенной для обеспечения охраны и безопасности объекта», что полностью подходит под определение и к системам видеоаналитики с использованием искусственного интеллекта, при проработке в дальнейшем нормативно-

технической документации по использованию систем необходимо предусмотреть отождествление терминов ОПТС и ТСО в данном контексте;

3. Взаимодействие оперативных дежурных АПК «Безопасный город», Мониторинговых компаний и ФГКУ УВО осуществляется в строгом соответствии с действующей Инструкцией по взаимодействию, согласно которой действия нарядов полиции групп задержания ФГКУ УВО регламентируются нормативными документами войск национальной гвардии Российской Федерации, предусматривающими отработку сигнала «тревога» с охраняемого объекта. С учетом особенностей данного объекта (открытые площадки) указанной Инструкцией не предусмотрен порядок действия нарядов полиции при отсутствии на объекте заявителя в случае задержания правонарушителей, для их последующего доставления в дежурные службы ОВД и установления причин формирования тревожного извещения.

При этом следует отметить, что организация реагирования нарядов полиции на сигналы, поступающие с комплексов и систем формирования тревожных сообщений, осуществляющих использование элементов видеоаналитики и искусственного интеллекта, направленно на исполнение Указа Президента РФ от 10.10.2019 №490 «О развитии Искусственного интеллекта в РФ» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») и полностью вписывается в Указание Росгвардии 6 июня 2025 № 8/3571 «О направлении проекта Концепции и концептуальных положений» и существующую Концепцию построения и развития АПК «Безопасный город», утвержденную Распоряжением Правительства РФ от 03.12.2014 № 2446-р, целью которой является повышение общего уровня общественной безопасности, правопорядка и безопасности среды обитания за счет существенного улучшения координации деятельности сил и служб, ответственных за решение этих задач, путем внедрения на базе муниципальных образований комплексной информационной системы.

Применение систем, формирующих тревожные сообщения на основе видеоаналитики и искусственного интеллекта, позволяет обрабатывать и фиксировать на открытых площадках и других централизованно охраняемых объектах такие правонарушения, как:

- разрушения строительных конструкций;

- повреждение оборудования и инвентаря;
- определение положения в позиции стрельбы, поднятые руки, наличие опасных предметов;
- опасное сближение людей;
- оставленные предметы;
- и другие.

На основании вышеизложенного можно утверждать, что применение видеоаналитики с искусственным интеллектом в системе централизованной охраны неминуемо приведет к увеличению объемов услуг вневедомственной охраны объектов и мест проживания и хранения имущества граждан, а также значительно упростит реализацию единой технической политики по реализации многих задач, указанных в «Программе технического перевооружения подразделений вневедомственной охраны», ГУВО Росгвардии на 2025 год, в том числе таких, как:

- Использование в организации и обеспечении централизованной охраны подразделениями вневедомственной охраны современных технических средств охраны и наблюдения, не требующих размещения их на площадях сторонних организаций;
- Сокращение непроизводительных расходов за счет оптимизации оборудования на площадях операторов связи;
- Проведение комплекса мер, направленных на снижение ложных срабатываний.

С этой целью считаю целесообразным продолжить проведение полноценной опытной эксплуатации указанных выше систем формирования тревожных сообщений на основе видеоаналитики и искусственного интеллекта.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Указ Президента РФ от 10 октября 2019 № 490 (в редакции от 15 февраля 2024) «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»);
2. Распоряжение Росгвардии от 07 июня 2023 г. № 1/1107-р «О единой технической политике в сфере вневедомственной охраны»;
3. Протокол расширенного заседания Технического совета Главного управления вневедомственной охраны Федеральной службы войск национальной гвардии Российской Федерации от 27-30 мая 2024 года №1;
4. Р 093-2024 «Методические рекомендации. Обследование объектов, охраняемых или принимаемых под охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации»;
5. «Программа технического перевооружения подразделений вневедомственной охраны на 2025 год» (исх. ГУВО Росгвардии от 18.02.2025 № 8/845);
6. Указание Росгвардии 6 июня 2025 № 8/3571 «О направлении проекта Концепции и концептуальных положений».

УДК 004.8

ЛЁВИН АНДРЕЙ ИВАНОВИЧ, ВЕДУЩИЙ НАУЧНЫЙ СОТРУДНИК ОТДЕЛА СИСТЕМ СВЯЗИ ЦЕНТРА СРЕДСТВ И СИСТЕМ СВЯЗИ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОГО ИНСТИТУТА СПЕЦИАЛЬНОЙ ТЕХНИКИ ФКУ НПО «СТИС» МВД РОССИИ КАНДИДАТ ТЕХНИЧЕСКИХ НАУК ПРОФЕССОР АКАДЕМИИ ВОЕННЫХ НАУК

О ПРИМЕНЕНИИ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ВЫЯВЛЕНИЯ ПРИЗНАКОВ СЕРИЙНОСТИ ПРЕСТУПЛЕНИЙ

Аннотация. В статье кратко изложены некоторые практики применения технологий искусственного интеллекта в правоохранительной деятельности органов внутренних дел Российской Федерации. Освещены постулаты применения искусственного интеллекта для выявления признаков серийности преступлений. Показана необходимость применения и сущность деятельностного подхода для идентификации серийных преступлений, имеющих существенные отличия от других взаимосвязанных преступлений. Акцентируется внимание на необходимости формализации криминалистических признаков преступлений с целью формирования комплексного фактора, отражающего тип многоэпизодного преступления. Описан порядок выбора комплекса признаков классификации для выявления системообразующих признаков серийного преступления и механизм детализации признаков преступной деятельности. Приведена схема модели формирования версии о серийном преступлении с использованием технологии искусственного интеллекта.

Ключевые слова: технологии искусственного интеллекта, серийные преступления, признаки преступлений, деятельностный подход, классификация, детализация, версия, датасет, искусственная нейронная сеть, криминалистическая модель, машинное обучение, генетические алгоритмы.

LEVIN ANDREY IVANOVICH, LEADING RESEARCHER OF THE DEPARTMENT OF COMMUNICATION SYSTEMS CENTER FOR COMMUNICATION EQUIPMENT AND SYSTEMS RESEARCH INSTITUTE OF SPECIAL EQUIPMENT FEDERAL STATE UNITARY ENTERPRISE NPO "STIS" OF THE MINISTRY OF INTERNAL AFFAIRS OF THE RUSSIAN FEDERATION CANDIDATE OF TECHNICAL SCIENCES PROFESSOR OF THE ACADEMY OF MILITARY SCIENCES

ON THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES TO DETECT SIGNS OF SERIAL CRIMES

Annotation. The article briefly outlines some practices of using artificial intelligence technologies in the law enforcement activities of the Internal Affairs bodies of the Russian Federation. The postulates of using artificial intelligence to identify signs of serial crimes are highlighted. The necessity of using and the essence of the activity-based approach for identifying serial crimes that have significant differences from other interrelated crimes is shown. Attention is focused on the need to formalize the forensic features of crimes in order to form a complex factor that reflects the type of multi-episode crime. The article describes the procedure for selecting a set of classification features to identify the system-forming features of a serial crime and the mechanism for detailing the features of criminal activity. The article also provides a diagram of a model for generating a version of a serial crime using artificial intelligence technology

Keywords: artificial intelligence technologies, serial crimes, signs of crimes, activity-based approach, classification, detailing, version, dataset, artificial neural network, forensic model, machine learning, genetic algorithms.

В соответствии с Указом Президента Российской Федерации от 10 октября 2019 г. № 490 в Российской Федерации реализуется Национальная стратегия развития искусственного интеллекта на период до 2030 года [1]. Данные технологии активно внедряются во все сферы деятельности, в том числе и в практическую

деятельность органов внутренних дел Российской Федерации (далее – ОВД РФ) и постоянно находятся в поле зрения руководства ведомства.

Реализуемый в настоящее время план по внедрению технологий искусственного интеллекта в ОВД РФ на 2023-2025 характеризуется следующим:

для проведения идентификации и оперативного поиска лица по его фотоизображению в МВД России разработана и используется подсистема «Опознавание (биометрическая идентификация)» программно-технического комплекса «ИБД-Ф»;

разработан прототип программного обеспечения, позволяющий в автоматическом режиме создавать нейросетевые модели для решения таких задач технического зрения, как классификация изображений, обнаружение

и распознавание объектов, сегментация изображений, выделение ключевых точек объекта;

для прогнозирования вероятности раскрытия преступления на основе имеющихся первичных данных о преступлениях введена в опытную эксплуатацию интеллектуальная модель прогнозирования «Виктория»;

для поиска деструктивного контента в открытых источниках в сети Интернет и анализа социальных сетей используются специализированные программные комплексы, предназначенные для обработки и анализа больших данных (программный комплекс «Виток-OSINT», программные комплексы «Демон Лапласа» и «Крибрум»);

по направлению применения искусственного интеллекта в сфере МВД России постоянно проводятся научно-исследовательские и опытно-конструкторские работы.

Серийные преступления являются специфическим видом преступной деятельности, который имеет сходные криминалистически значимые признаки. Они и являются основанием для объединения определённого количества преступлений в едином уголовном деле. Как правило, данные виды преступной деятельности связаны с наличием некоторого множества однотипных «по почерку» преступлений, совершаемых одним и тем же лицом (или группой лиц) на протяжении определённого периода [2].

Таким образом, серийное преступление можно определить, как многоэпизодное преступное деяние, совершаемые субъектом или субъектами по неочевидным мотивам, в ходе которых объектом посягательств оказывается человек или имущество, ранее не знакомые субъекту, а время между эпизодами преступлений превышает интервал, необходимый для эмоционального охлаждения субъекта после совершения деяния.

Принятие решений в процессе идентификации типов и характерных признаков преступлений связано с созданием, передачей, хранением и обработкой больших объёмов информации,

что в большинстве реальных случаев не представляется возможным без применения современных аппаратно-программных средств. В этой связи применение технологий искусственного интеллекта имеет особенное значение для выявления признаков многоэпизодных преступных деяний, когда возникают ситуации, сочетающие в себе различные виды информационной неопределённости.

Термин «серийная преступность» начал использоваться для описания серийных убийств в семидесятых годах прошлого столетия, когда появились первые публикации на эту тему [3]. Для идентификации серийных преступлений, имеющих существенные отличия от других взаимосвязанных преступлений, целесообразно применять деятельностный подход [3, 4]. Такой подход строится на основе формирования групп системообразующих признаков, которые характеризуют состав преступления.

Можно выделить следующие группы таких признаков:

1) Объект преступления – охраняемые уголовным законом общественные отношения, на которые осуществлено преступное посягательство;

2) Объективная сторона преступления – это внешняя характеристика преступления, то есть то, как преступление проявляется в реальной действительности.

3) Субъект преступления – это физическое лицо, достигшее возраста уголовной ответственности, совершившее общественно опасное деяние, предусмотренное уголовным законом во вменяемом состоянии.

4) Субъективная сторона преступления – т.е. психическая деятельность лица, непосредственно связанная с совершением преступления.

Выбор комплекса признаков классификации должен производиться в соответствии с требованиями существенности каждого из признаков (веса признака) и определения априорных корреляционных зависимостей между признаками. Значимость признака определяется степенью влияния того или иного элемента для формирования частной версии в деятельности по расследованию соответствующего вида преступлений.

Необходимо отметить, что вопросы применения технологий искусственного интеллекта для выявления признаков серийности преступления в настоящее время исследованы не в полной мере. Это связано с тем, что научные исследования

в сфере применения систем искусственного интеллекта в правоохранительной деятельности в нашей стране начали вестись сравнительно недавно, в связи с чем можно констатировать относительно низкую разработанность вопросов, связанных с их внедрением в расследование преступлений.

Вместе с тем российскими учёными подробно исследованы технологии создания искусственного интеллекта на базе искусственной нейронной сети для последующего его использования в правоохранительной деятельности [5], определены этапы компьютеризации криминалистических учётов с их последующим использованием в системах искусственного интеллекта

в криминалистической регистрации [6].

Учеными, внесшими существенный вклад в разработку вопросов внедрения технологий искусственного интеллекта в правоохранительную деятельность, являются А.Б. Арзуманян, Г.Н. Андреева, А.В. Бахтеев, И.Р. Бегишев, А.А. Бессонов, В.В. Бычков, В.Р. Волкова, Р.И. Дремлюга, Р.Е. Жихорева, Г.Г. Камалова, С.А. Ковалев, Н.В. Кравчук, О.С. Лейнова, Е.Н. Макарова, Н.В. Мишина, И.Н. Мосечкин, А.В. Нестеров, А.Л. Осипенко, С.В. Петрикова, В.В. Поляков, Т.А. Полякова, Б.В. Псарева, О.А. Решняк, О.Л. Романова, А.Г. Себякин, И.А. Семенцова, В.С. Соловьев, Д.Н. Сретенцев, Ю.А. Цветков, И.А. Филиппова, Т.Н. Юдина и другие.

Теоретическое изучение технологии разработки искусственного интеллекта на базе искусственной нейронной сети для его использования в правоохранительной деятельности указывает на то, что на первом этапе необходимо сформировать «датасет» – базу данных, которая будет использована для обучения нейронной сети. В последующем необходимо создать алгоритм обучения искусственной нейронной сети. При этом данный алгоритм может содержать условия окончания обучения, порядок предъявления примеров обучающей выборки, коэффициенты погрешностей, количество возможных ошибок перед сменой установок.

На следующем этапе системе предлагаются размеченные данные для «запоминания» нейросетью свойств классов объектов, с которыми в последующем ей придется столкнуться. После этого перед искусственной нейросетью ставятся задачи, аналогичные поставленным в процессе обучения в условиях неизвестности «правильных ответов».

Оценка эффективности результатов обучения осуществляется на основе ряда показателей, основополагающими из которых выступают точность и правильность. Точность при этом отражает повторяемость результатов, правильность, в свою очередь, подразумевает соответствие результатов валидации поставленным разработчиком задачам. При возникновении необходимости искусственную нейронную сеть «дообучают».

На сегодняшний день наиболее развитыми и полными среди всех имеющихся исследований в области использования искусственного интеллекта для раскрытия и расследования преступлений являются разработки по изучению материалов уголовных дел о серийных преступлениях, совершённых в период существования СССР и современной России с 1973-го по 2018 год [7, 8].

В результате проделанной работы было установлено, что перспективным направлением совершенствования научно-технической составляющей криминалистического обеспечения их расследования является разработка эффективных технологий искусственного интеллекта для построения поискового портрета серийного преступника.

Примером применения технологии искусственного интеллекта для выявления признаков серийности преступлений можно считать созданную акционерным обществом «РАМЭК-ВС» в процессе выполнения НИР «Серия» [7] цифровую криминалистическую модель серийных преступлений, содержащую двадцать семь признаков с различным числом градаций, которые к тому же связаны между собой как элементы единой системы. Применение данной модели позволило на основе закономерностей изученных преступлений определить те признаки из выявленных, на основе которых возможно установить серийный характер преступлений. Такими признаками являются:

- квалификация преступления;
- место совершения преступления;
- время совершения преступления;
- предмет преступного посягательства;
- способ совершения преступления;
- использование орудия и средств для совершения преступления;
- результат осмотра места происшествия;
- характеристика потерпевших;
- характеристика подозреваемых;
- территориальная принадлежность;
- дополнительная характеристика преступления;

Выводы.

1. Создание и внедрение в повседневную деятельность ОВД РФ систем искусственного интеллекта с заложенными в них методами машинного обучения и семантического анализа данных позволит повысить эффективность предупредительной работы полиции, а также результативность раскрытия и расследования преступлений на основе выявления признаков их серийности.

2. Интеллектуальные системы выявления признаков серийности определённых категорий преступлений могут быть важным инструментом поддержки принятия решений, который расширяет интеллектуальные возможности человека, но не заменяет сотрудников правоохранительных органов, осуществляющих следственные действия и оперативно-розыскные мероприятия по установлению личности серийного преступника.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Национальная стратегия развития искусственного интеллекта на период до 2030 года, утвержденная Указом Президента Российской Федерации от 10.10.2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации». – Текст: электронный // Cremlin.ru : [сайт] – 2025 / – URL: <https://www.cremlin.ru/acts/bank/44731/> (дата обращения: 10.09.2025).
2. Применение технологий анализа больших данных и информационного подхода в целях выявления признаков серийности преступлений/ П.С. Величко, В.В. Конюшев, А.И. Лёвин, А.В. Сухов – Текст: непосредственный // Международная научно-практическая конференция «Развитие учения о противодействии расследованию преступлений в условиях цифровой трансформации» – Москва : Академия управления МВД России. - 2021.
3. Дуглас, Д. Сексуальные маньяки. Психологические портреты и мотивы / Д. Дуглас, Р. Ресслер, Э. Берджесс – Москва: Эксмо, 2021. - 368 с. - ISBN 978-5-04-116455-3 / – Текст: непосредственный.
4. Оперативно-розыскная и следственная деятельность по уголовным делам о серийных преступлениях – Текст: электронный // Crimlib.info: [сайт]. – 2025 / – URL: [https:// crimlib.info](https://crimlib.info) (дата обращения: 18.09.2025).
5. Степаненко, Д.А. Использование систем искусственного интеллекта в правоохранительной деятельности / Д.А. Степаненко, Ю.А. Бахтеев – Текст: непосредственный // Всероссийский криминологический журнал – 2020 – Т. 14. – № 2 – С. 206-214.
6. Бахтеев, Д.В. Компьютеризация криминалистических учетов и возможности использования искусственного интеллекта в криминалистической регистрации / Д.В. Бахтеев, А.А. Беляков – Текст: непосредственный // Вестник Санкт-Петербургского военного института войск национальной гвардии – 2020 – № 2(11) – С. 89-92.
7. Исследование применимости методов машинного обучения и анализа данных для выявления признаков серийности (сходства) определенных категорий преступлений / Отчет о НИР // Акционерное общество «РАМЭК-ВС» – Санкт-Петербург : 2022 – Текст: непосредственный.
8. Бессонов, А.А. Перспективы использования искусственного интеллекта в раскрытии серийных преступлений / А.А. Бессонов – Текст: непосредственный // Развитие учения о противодействии расследованию преступлений и мерах по его преодолению в условиях цифровой трансформации / Сборник научных статей по материалам международной научно-практической конференции, Москва, 21 мая 2021 года / Под редакцией Ю.В. Гаврилина, Ю.В. Шпагиной. – Москва: Академия управления Министерства внутренних дел Российской Федерации, 2021 – С. 97-105.
9. Стоянов, Д.Д. Разработка и исследование алгоритмов обнаружения сигналов в когнитивных радиосетях / Д.Д. Стоянов – Текст: электронный // ya.ru: [сайт] – 2025 / – URL: [https : // diss.vlsu.ru/uploads/media/Dissertacija – Stojanov.pdf](https://diss.vlsu.ru/uploads/media/Dissertacija-Stojanov.pdf) (дата обращения: 11.09.2025).

УДК 654.16
ББК 32.843

ЛЯЛЕВИЧ ВИТАЛИЙ ГЕННАДЬЕВИЧ, НАУЧНЫЙ СОТРУДНИК ФКУ «НИЦ
«ОХРАНА» РОСГВАРДИИ

МИХАЙЛОВ АЛЕКСАНДР АЛЕКСЕЕВИЧ, НАУЧНЫЙ СОТРУДНИК ФКУ «НИЦ
«ОХРАНА» РОСГВАРДИИ

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ИОНИСТОРОВ ДЛЯ ОБЕСПЕЧЕНИЯ АВТОНОМНОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ

Аннотация. В статье рассмотрены вопросы применения ионисторов в качестве источников электрической энергии, в том числе в тревожных кнопках.

Ключевые слова: ионистор, тревожные кнопки, саморазряд, удельная мощность, источник электропитания.

LYALEVICH VITALY GENNADIEVICH, RESEARCHER AT THE FSI «SRC «OKHRANA»
OF THE FEDERAL SERVICE OF THE NATIONAL GUARD OF THE RUSSIA

MIKHAILOV ALEXANDER ALEKSEEVICH, RESEARCHER AT THE FSI «SRC «OKHRANA»
OF THE FEDERAL SERVICE OF THE NATIONAL GUARD OF THE RUSSIA

PROSPECTS FOR USING IONISTORS TO ENSURE THE AUTONOMY AND RELIABILITY
OF TECHNICAL SECURITY MEANS

Annotation. The article discusses the use of ionistors as sources of electrical energy, including in panic buttons.

Keywords: ionistor, panic button, self-discharge, specific power, power supply.

В современных условиях бесперебойная работа систем охранной сигнализации играет ключевую роль в обеспечении безопасности объектов, охраняемых подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации.

Среди таких систем особое значение имеют автономные комплексы охранной и тревожной сигнализации. В их число входят кнопки тревожной сигнализации (далее – КТС), позволяющие вручную передать сигнал тревоги при возникновении экстренной ситуации.

Наибольшую популярность приобрели беспроводные КТС. Их главное достоинство – лёгкость монтажа и отсутствие потребности в прокладке кабельных коммуникаций. Тем не менее у этих устройств есть существенный недостаток: они работают от батарей, срок службы которых ограничен. Это создаёт две проблемы: необходимость периодической замены элементов питания, что увеличивает эксплуатационные затраты, риск внезапного разряда батареи в критический момент.

В настоящее время ФКУ «НИЦ «Охрана» Росгвардии изучает возможность использования ионисторов как альтернативного источника электропитания для автономных технических средств охраны, оценивая целесообразность такого решения.

Чаще всего для электропитания КТС используются аккумуляторные батареи и химические источники электропитания. Использование ионисторов в качестве источников электропитания для КТС один из вариантов создания автономных средств охраны с улучшенными тактико-техническими характеристиками.

Ионисторы благодаря своим уникальным электрохимическим свойствам выступают идеальным накопителем для систем сбора электроэнергии

за короткие промежутки времени, решая задачи быстрого накопления заряда.

Ионисторы при применении в КТС в качестве источника электропитания являются идеальным решением и альтернативой применения традиционных источников электропитания.

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

Физические основы и преимущества ионисторов.

В отличие от батарей (химические реакции) и обычных конденсаторов (электростатическое поле), ионисторы накапливают энергию преимущественно за счет формирования диэлектрического слоя на границе электрод/электролит. Некоторые типы ионисторов дополнительно используют быстрые обратимые окислительно-восстановительные реакции на поверхности электродов.

В электролитическом конденсаторе в качестве диэлектрического слоя используют пленку оксида алюминия. В танталовом конденсаторе диэлектрический слой – оксид титана.

Ионистор не имеет диэлектрического слоя в привычном понимании. Принцип работы ионистора основан на механизме образования диэлектрического слоя в момент заряда, аналогично заряженному диэлектрику.

Процесс накопления заряда происходит в слое ионов, сформированных на поверхности положительных и отрицательных обкладок ионистора (рис.1).

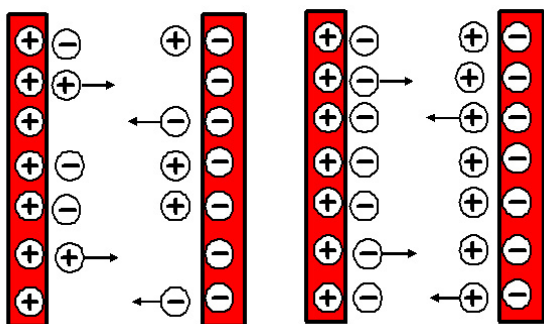


Рисунок 1 – Образование диэлектрического слоя в ионисторах

В ионисторах применяются два типа электролита: водные и органические.

Ионисторы на органическом электролите позволяют прикладывать к ячейке ионистора напряжение 3 В, а водные только 1,5 В. В настоящее время наиболее распространены ионисторы на органическом электролите. Эти напряжения обусловлены «напряжением разложения» электролитов. Дальнейшее увеличение напряжения заставит электролит разлагаться, что приведет к появлению паразитных токов и пробую ионистора. Напряжение, которое можно приложить к ионистору ограничивается напряжением разложения электролита. Положительные и отрицательные заряды формируются на поверхности обкладок ионистора и образуют диэлектрический слой.

Толщина двойного диэлектрического слоя равна молекулам электролита и составляет порядка 5 – 10 нм. Часто в качестве электродов ионистора используют активированный уголь, имеющий хорошую пористость, а в качестве электролита водные растворы сульфата натрия, гидроксида лития, гидроксида калия и др. Активируемый уголь пропитывается электролитом, что позволяет рассматривать ионистор как множество микроскопических конденсаторов.

Площадь частиц активированного угля составляет порядка

500 – 1300 м²/г, что позволяет создавать ионисторы емкостью до 100 фарад.

Значительная емкость ионистора позволяет активно использовать ионисторы в качестве элементов питания КТС.

При прикладывании напряжения (U) к ионистору, зарядный ток ионистора (I) можно описать следующей формулой [5]:

$$I = \frac{U}{R} \cdot \exp\left(\frac{-1}{CR}\right) \quad (1)$$

Экспериментальная зависимость зарядного тока величиной 0,1 А,

от времени заряда ионистора емкостью 1,0 Ф показан на (рис. 2). Что хорошо согласуется с приведенной формулой (1)

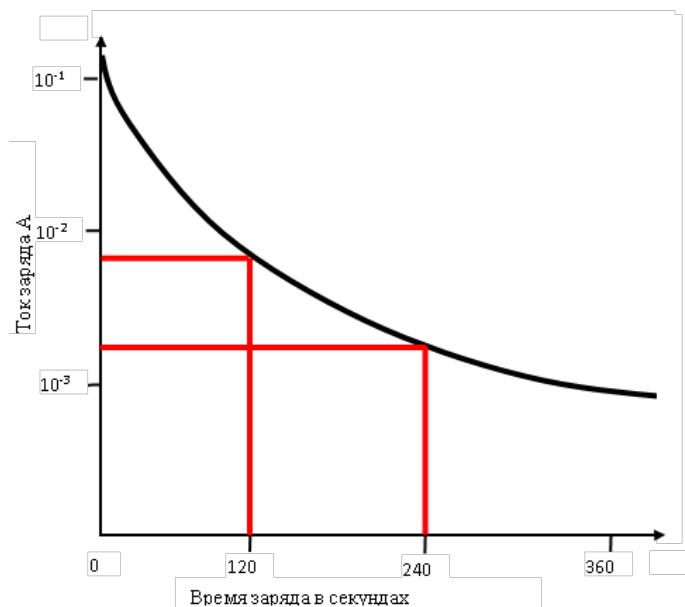


Рисунок 2 - Зависимость зарядного тока от времени заряда ионистора емкостью 1,0 Ф

Ток зарядного источника ограничен величиной 0,1 А, что обеспечивает «щадящий» режим заряда и не допускает перегрев ионистора. Из графика мы видим, что за первые 120 секунд зарядный

ток ионистора уменьшается более чем в 10 раз. При стабильном напряжении энергия, поступающая в ионистор уменьшается также в 10 раз. За вторые 120 секунд ионистор заряжается практически полностью и ток заряда уменьшается приблизительно

до 0,001,25 А. Что говорит о том, что ионистор зарядился практически полностью. Это одно из главных достоинств ионисторов – малое время заряда. Если аккумулятору до полного заряда требуется время около нескольких часов, то ионистору достаточно несколько минут.

Емкость ионистора может быть оценена следующим образом [5]:

$$C = \frac{I \cdot t}{(U1 - U2)} \quad (2)$$

где:

C – емкость ионистора;

I – зарядный ток;

t – время заряда;

U1 – конечное напряжение ионистора;

U2 – первоначальное напряжение ионистора.

Используя формулу (2), всегда можно рассчитать зарядный ток, время заряда, и емкость ионистора. Эти данные необходимы для использования ионистора при создании принципиальных электрических схем.

По количеству запасенной энергии ионисторы занимают промежуточное положение между конденсаторами и аккумуляторами, но имеют массу преимуществ.

Ключевые преимущества ионисторов в контексте их использования как элементов электропитания КТС.

Сверхбыстрый заряд. Ионистор способен принять кратковременный импульс напряжения практически мгновенно, без потерь, характерных для медленно заряжающихся аккумуляторов.

Высокая удельная мощность (кВт/кг): для радиопередачи (особенно на старте) необходим кратковременный всплеск тока (десятки мА). Ионистор легко обеспечивает этот пиковый ток, необходимый для работы передатчика (BLE, Sub-GHz, LoRa).

Большое количество циклов заряда/разряда (более 500 000 циклов). Литиевые батарейки (CR2032) выдерживают лишь сотни либо тысячи циклов разряда. Ионистор же практически «не стареет» от частых неглубоких (10-20%) циклов заряда/разряда при каждом нажатии. Это гарантирует продолжительный срок службы кнопки годами без замены элементов питания.

Широкий температурный диапазон применения (от -40 °С до +70 °С). КТС может использоваться в неотапливаемых помещениях, на улице, в промышленных цехах. Ионистор сохраняет работоспособность в условиях, где батареи теряют емкость или выходят из строя.

Относительная безопасность. Отсутствие легковоспламеняющихся компонентов (в отличие от Li-ion) и низкое рабочее напряжение (от 2.5 до 3.3 В) упрощают конструкцию и сертификацию.

Ионистор обладает большим сроком службы. Срок службы ионистора равен сроку службы технической аппаратуры.

Отсутствует необходимость в контроле токов заряда/разряда. Ионистор работает в большом диапазоне разрядных/зарядных токов. Отсутствует нагрев ионистора при заряде/разряде.

Экологическая чистота ионисторов. В ионисторах нет токсичных материалов типа свинца, ртути, кадмия и т.д. Ионисторы не надо утилизировать особым способом после вывода его из эксплуатации.

Ионистор допустимо разряжать до нуля и снова заряжать.

Высокий коэффициент полезного действия цикла заряда/разряда, который достигает 95% и выше.

Невысокая стоимость устройства накопления энергии в расчете на единицу запасенной мощности.

Небольшой вес.

Перспективы развития ионисторов.

Одна из новинок последних лет – графеновые ионисторы. У графена площадь поверхности больше, чем у активированного угля (3000 м²/г), они лучше сохраняют электростатический заряд. Высокие гибкость, механическая прочность и электропроводность (до ~ 20 000 С/см) делают графен перспективным материалом. С графеновыми ионисторами мечты о смартфоне с большой емкостью аккумулятора, который заряжается в течение минуты, становятся реальностью.

Уже выпущены графеновые ионисторы с удельной емкостью 140 Ф/г.

Плотность мощности графеновых ионисторов составляет 200 Вт/см³. Графен активно внедряют в новые разработки ионисторов.

Ультраконденсатор SkelCap SCX5000 имеет напряжение 3,0 В и плотность энергии 83 Вт х ч/кг.

Разработан графеновый ионистор с напряжением 3 В/12 000 Ф способный обеспечить

энергией трамвай на 6 км всего за 30 секунд зарядки, и еще одну модель с напряжением 2,8 В/30 000 Ф для автобуса (дает возможность ехать 10 км после минутной зарядки).

Выводы. Проведённый анализ показывает, что ионисторы представляют собой технологически обоснованную альтернативу традиционным химическим источникам тока при обеспечении автономного электропитания КТС. Благодаря таким свойствам, как высокая удельная мощность, устойчивость к большому количеству циклов зарядки (свыше 500 000 циклов заряда/разряда), способность работать в широком температурном диапазоне (от $-40\text{ }^{\circ}\text{C}$ до $+70\text{ }^{\circ}\text{C}$), сверхбыстрая зарядка и отсутствие необходимости в сложных схемах управления питанием, ионисторы обеспечивают значительное повышение надёжности и долговечности автономных технических средств охраны.

Современный уровень развития материаловедения – в частности, применение графена и других наноструктурированных электродов – позволяет снижать уровень саморазряда и повышать удельную энергоёмкость

ионисторов, что расширяет их применимость в устройствах с низким энергопотреблением, таких как КТС с радиоканалом на базе BLE, LoRa или Sub-GHz. В сочетании с микроэлектроникой наноамперного класса ионисторы открывают перспективы создания полностью автономных систем, не требующих технического обслуживания на протяжении всего срока эксплуатации.

Реализация КТС на базе ионисторов в соответствии с «Едиными требованиями к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнальным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации» позволяет удовлетворить нормативные требования к надёжности, автономности и эксплуатационной устойчивости, что делает данное решение целесообразным для практического внедрения в системах обеспечения безопасности, эксплуатируемых подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 3 июля 2016 г. N 226-ФЗ «О войсках национальной гвардии Российской Федерации» опубликован в «Российской газете» от 6 июля 2016 г. N 146, в Собрании законодательства Российской Федерации от 4 июля 2016 г. N 27 (часть I) ст. 4159.
2. ГОСТ Р 58593-2019. Национальный стандарт Российской Федерации Источники тока химические. Термины и определения (утв. и введен в действие приказом Росстандарта от 7 октября 2019 г. № 964-ст) – М.: Стандартинформ, 2019.
3. [сайт] //URL: <https://nicohrana.ru/> Единые требованиями к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнальным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации. Утверждены решением расширенного заседания Технического совета ГУВО Росгвардии (Протокол №2 от 13 – 16 октября 2025 г.), (дата обращения: 23.07.2025).
4. Об утверждении требований при обращении с группами однородных отходов I – V классов опасности: приказ Минприроды России от 11 июня 2021 г. № 399 (ред. от 04.04.2023).
5. Т.А. Писарева, Е.М. Борисова, С.М. Решетников Учебное пособие Создание и изучение эффективных суперконденсаторов на основе двойного электрического слоя – 2021. ФГБОУ ВО «Удмуртский государственный университет». – С. 41-42.

УДК 623.9
ББК 68.80

**МИХАЙЛОВ АЛЕКСЕЙ АЛЕКСЕЕВИЧ, НАУЧНЫЙ СОТРУДНИК ФКУ «НИЦ «ОХРАНА»
РОСГВАРДИИ**

**ЛАЗЕРНЫЕ КОМПЛЕКСЫ ПОРАЖЕНИЯ ЦЕЛЕЙ, ОГРАНИЧЕНИЯ
ПО ИХ ПРИМЕНЕНИЮ ПРИ ЭКСПЛУАТАЦИИ В ПРИЗЕМНОЙ ПОВЕРХНОСТИ
АТМОСФЕРЫ**

Аннотация. В статье рассмотрены особенности применения лазерных комплексов в системах противодействия беспилотным воздушным судам при охране критически важных объектов Росгвардии. Проанализированы принципы работы лазерных комплексов поражения БВС и ограничения по их применению, связанные с физикой данного процесса.

Ключевые слова: беспилотные воздушные суда, лазерный комплекс, коллиматор, объектив.

**MIKHAILOV ALEKSEY ALEKSEEVICH, RESEARCHER AT THE FSI «SRC «OKHRANA»
OF THE FEDERAL SERVICE OF THE NATIONAL GUARD OF THE RUSSIA**

**LASER TARGET DESTROYING SYSTEMS, RESTRICTIONS ON THEIR USE DURING
OPERATION IN THE ATMOSPHERIC GROUND SURFACE**

Annotation. The article discusses the features of using laser systems in countering unmanned aerial vehicles systems while protecting critical facilities of the Russian National Guard. The principles of operation of laser systems for destroying UAVs and the limitations on their use related to the physics of this process are analyzed.

Keywords: unmanned aerial vehicles, laser system, collimator, and lens.

Согласно положению о Федеральной службе войск национальной гвардии Российской Федерации, утвержденного Указом Президента Российской Федерации от 30 сентября 2016 г. № 510 [1], одной из основных задач Росгвардии Российской Федерации является обеспечение безопасности объектов топливно-энергетического комплекса (далее – ТЭК).

Федеральный закон "О безопасности объектов топливно-энергетического комплекса" от 21.07.2011 № 256-ФЗ [2] в статье 3 указывает на необходимость разработки и реализации мер по созданию системы физической защиты объектов ТЭК.

Одной из основной угроз для объектов ТЭК являются беспилотные воздушные суда (далее – БВС), используемые в противоправных и террористических целях. Одним из средств поражения БВС является лазер. По ГОСТР 58373 – 2019 "Лазеры и лазерное оборудование. Термины и определения" [3], лазер (laser), это устройство с усиливающей средой в пределах оптического резонатора, способное генерировать когерентное электромагнитное излучение длиной волны не более 1 мм посредством усиленного

вынужденного излучения (стимулированной эмиссии).

В дальнейшем под этим термином будем понимать лазерный комплекс, поскольку в него кроме самого лазера входят устройства обнаружения и сопровождения целей, вместе с системой автофокусировки луча на цели.

В настоящее время наблюдается бурное развитие лазерных комплексов. Первые попытки использовать лазеры для поражения летательных аппаратов предпринимались более 40 лет назад, они не дали реальных образцов, готовых к широкому внедрению в силовые структуры [4].

Почему же данная тема то уходит на второй план, то возрождается вновь? Дело в том, что меняются технологии, но не исчезают фундаментальные ограничения, основанные на физических процессах, которые протекают при работе этих комплексов. Попробуем разобраться в них.

Физические принципы, лежащие в основе работы лазеров. Все лазеры работают по одинаковой схеме: энергетическая накачка среды (накачку можно осуществлять оптическим, электрическим, химическим, газодинамическим, электронным пучком, рентгеновским излучением

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

и другими способами), переход электрона на верхний энергетический уровень, возврат электрона на нижние энергетические уровни с испусканием кванта определенной длины волны, определяемой средой накачки.

Основные типы лазеров (по среде накачки). Лазеры бывают газовые, жидкостные (лазеры на красителях), твердотельные, на свободных электронах, рентгеновские лазеры.

Основные типы лазеров и длины волн их излучения. Лазеры различаются по длине волны излучения. Диапазон длин волн лежит от 0,193 мкм до 10,6 мкм. Для целей поражения БВС представляет интерес лазеры с длиной излучения от 0,337 мкм до 10,6 мкм, поскольку более коротковолновые диапазоны излучения имеют значительное затухание в атмосфере. Окна прозрачности атмосферы наблюдаются [5] в диапазоне видимого света и ближайшего к нему ИК- излучения (ИК- излучения 3,5- 4,2 мкм и ИК-излучения 8,5- 12 мкм).

Факторы, влияющие на эффективность работы лазера. Эффективность передачи энергии лазерного излучения определяется следующими факторами: поглощением и рассеянием, молекулярным составом атмосферы, дифракционной расходимостью, воздействием турбулентности, характеристиками и концентрацией атмосферного аэрозоля, динамической ошибкой наведения, тепловым самовоздействием пучка.

Минимально возможный диаметр лазерного пятна на цели. Минимально возможный диаметр лазерного пятна на цели определяется дифракционным пределом, который можно оценить по следующей формуле [6]

$$d = 2,44 \cdot \lambda \cdot \frac{L}{D} \quad (1)$$

где:

λ - длина волны лазерного излучения;

D - диаметр выходной апертуры лазера;

L - расстояние до цели.

Вычислим дифракционный предел для длины волны $\lambda_1 = 1$ мкм,

$\lambda_2 = 10$ мкм, при $D = 0,4$ м и $L = 1000$ м.

$d_1 = 2,44 \cdot 10^{-6} \cdot 1000 / 0,4 = 2,5 \cdot 10^{-3} \text{ м} = 2,5 \text{ мм}$

$d_2 = 2,44 \cdot 10^{-5} \cdot 1000 / 0,4 = 61 \text{ мм}$

Таким образом, увеличение длины волны лазера в 10 раз (с 1 мкм до 10 мкм) дает приемлемое значение дифракционного предела.

Воздействие турбулентности на распространение лазерного луча. Воздействие турбулентности на распространение лазерного луча может проявляться в двух случаях, когда неоднородность

атмосферы много больше диаметра луча лазера, см. рисунок 1, и когда диаметр луча соизмерим с неоднородностью в атмосфере и они действуют как линзы, см. рисунки 2, 3. [3]

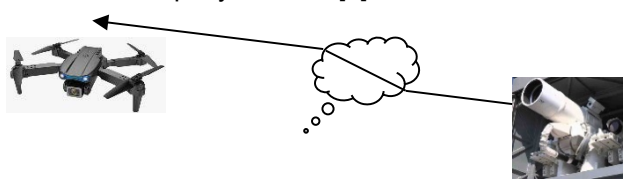


Рисунок 1 – Образование диэлектрического слоя в ионисторах

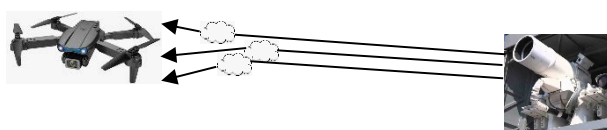


Рисунок 2 – Отклонение лазерного луча после прохождения через множества мелких неоднородностей атмосфер

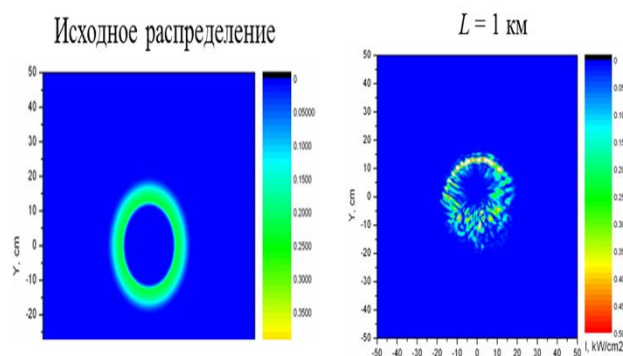


Рисунок 3 – Моделирование прохождения через атмосферу излучения 100 кВт кислородно-йодного лазера (длина волны 1,315 мкм) при воздействии атмосферной турбулентности [4]

Данные неоднородности могут возникать при контакте воздуха с грунтом с различными температурами, например при пересечении лесного массива полем, оврагом, при протекании реки в данной местности или быть техногенного характера т.д.

Влияние аэрозолей на прохождения луча. Влияние аэрозолей на прохождения луча. Аэрозоли в воздухе могут быть как техногенного, так и природного характера, к аэрозолям следует отнести и утренний туман, и атмосферную дымку,

Аэрозоли, туманы, дымки характеризуются затуханием излучения, выраженного в дБ/км. В зависимости от этого параметра они могут резко снизить эффективность работы лазерного комплекса вплоть до его полной неработоспособности.

Для тумана категории 1 (с дальностью видимости 1220 м), потери, как в средневолновом ИК диапазоне, так и в длинноволновом

ИК диапазоне значительно меньше, чем в видимом диапазоне наблюдения (примерно в 6-8 раз).

Для тумана категории 2 (с дальностью видимости 610 м) выигрыш в потери полезного сигнала будет меньше (примерно в 3-4 раза) и то только для длинноволнового ИК диапазона наблюдения (8-14 мкм). Потери в средневолновом ИК диапазоне наблюдения (3-5 мкм) даже больше, чем в видимом диапазоне наблюдения.

Для тумана категории 3 (с дальностью видимости 305 м) потеря полезного сигнала примерно одинаковы как в видимом диапазоне, так и в ИК диапазонах.

Однако, в большинстве случаев длинноволновый диапазон излучения лазера (10-12 мкм) предпочтителен.

Поглощение лазерного излучения при осадках. Любые осадки приводят к значительному поглощению лазерного излучения, см. рисунок 4. [7]

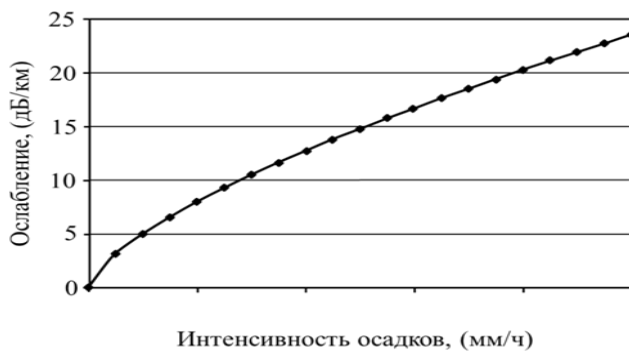


Рисунок 4 – Ослабление лазерного излучения в зависимости от интенсивности осадков (мм/ч)

Тепловое самовоздействие лазерного излучения. При прохождении мощного лазерного луча через атмосферу наблюдаются различные процессы, связанные с локальным разогревом воздуха, появлением структурных неоднородностей, ионизаций молекул газа, взрывным испарением частичек воды в воздухе, что приводит к расфокусировке и поглощению излучения в среде, данный физический процесс накладывает ограничения на плотность энергии в луче лазера.

Говоря о лазерных комплексах, нельзя не сказать о объективах лазеров. В основном они делятся на два типа: коллиматорные объективы и объективы с подфокусировкой на цель. [8]

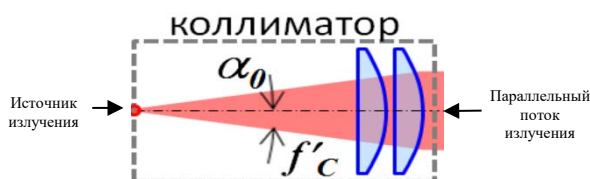


Рисунок 5 – Коллиматорный объектив даёт параллельный поток излучения

Рассчитаем плотность потока энергии в луче при использовании коллиматорного объектива.

Исходные данные:

- мощность излучения лазера -10 кВт;
- диаметр выходной линзы коллиматора - 6 см (площадь линзы $S = \pi \cdot 3^2 / 4 \approx 28 \text{ см}^2$);

Тогда удельная мощность излучения $P_{уд} = 10 \text{ кВт} / 28 \text{ см}^2 = 357 \text{ Вт/см}^2$

В реальных условиях такой поток не позволит поразить большинство целей.

Лазерные комплексы при достаточно большом времени экспозиции излучения способны резать практически любые материалы, но реальное время экспозиции на БВС находится в диапазоне 5-7 с, за это время при скорости движения БВС в 100 м/с он сможет преодолеть 500-700 м дистанции, что для многих охраняемых объектов является критическим параметром.

В общем случае плотность энергии лазерного излучения g [Дж/м²] вычисляется по следующей формуле (2) [6]

$$g \approx \frac{(1 - K_o) \cdot P \cdot t}{L^2 \cdot \theta^2} \quad (2)$$

где:

- P - средняя мощность источника излучения (Вт);
- t - длительность излучения (с);
- L - расстояние до цели (м);
- θ - угол расходимости луча (рад);
- K_o - коэффициент отражения.

В этой формуле стоит обратить внимание на такие параметры, как:

- угол расходимости луча. В предыдущих рассуждениях мы принимали, что угол расходимости коллиматорного объектива равен нулю, на самом деле это не так. Во многом качество объектива лазера определяется этим углом расходимости;

- коэффициент отражения. Разумеется, что при 100% отражении лазер не оказывает воздействие на цель. Из-за ограниченного объема публикаций не будем углубляться в эту тему.

Поэтому в реальных комплексах используется объектив с подфокусировкой излучения на цель, см. рисунок 6.

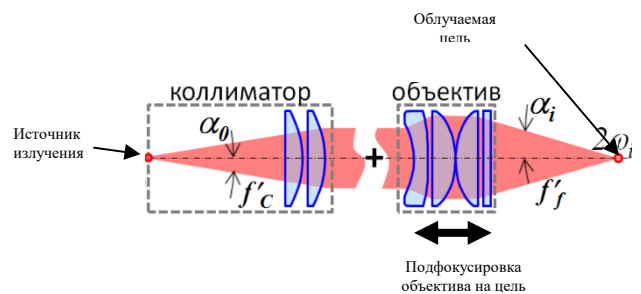


Рисунок 6 – Схема объектива с возможностью подфокусировки на цель [5]

В такой конструкции устройство подфокусировки в большой мере определяет реальную эффективность лазерного комплекса. Обычно

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

первоначально для определения расстояния до цели используется лазерный дальномер, далее быстродействующая (необходимо как можно быстрее произвести подфокусировку объектива лазера на цель) телевизионная камера с высоким разрешением оценивает размер пятна на цели и в автоматическом режиме стремится к получению минимального его размера.

Оценим необходимое быстродействие такой системы.

Исходные данные:

- скорость движения БВС - 100 м/с;

- точность фокусировки (L) - 1 см (10-2 м).

$L = V \cdot T$ быс, (3)

отсюда следует, что T быс = $L/V = 10^{-2}$ м/100 м/с = 10⁻⁴ с.

Таким образом, при скорости движения БВС в 100 м/с для получения ошибки подфокусировки в 1 см требуется быстродействие в 10⁻⁴ с, что является непростой технической задачей.

Влияние вибрации корпуса лазерного излучателя на точность фокусировки. Оценим влияние вибрации на точность фокусировки лазерного излучателя на цель. Если длина консоли, на которой закреплен объектив лазерного излучателя равен 1 м, и вибрация приводит к его колебанию в 1 мм., то на дистанции в 1 км, амплитуда такого колебания будет уже 1 м, что делает невозможным поражение таких целей, как БВС.

Лазерные комплексы из-за возникающих вибраций неспособны поражать цели при движении. Поэтому мобильные лазерные установки используют выдвижные опоры для фиксации своего положения, однако, при этом дизель/бензогенераторы, питающие лазерный комплекс, приходится располагать отдельно от передвижного лазерного модуля.

Использование лазерных комплексов в ночное время. Использование лазерных комплексов в ночное время является проблемным вопросом, поскольку для подфокусировки лазера используется высококачественная телевизионная камера. К сожалению, ни дальность действия, ни разрешение матрицы тепловизора не позволяют их использовать для подфокусировки. Значит в ночное время необходимо использовать внешнюю подсветку цели со всеми вытекающими отсюда ограничениями (см. потери при прохождении излучения через туман и аэрозоли).

Примечание. Если в телевизионной телекамере возможно использование длиннофокусного объектива с разрешением матрицы до

50 Мп, то разрешение тепловизоров на базе микроболометра не превышает 1024×768 пикселей (менее 0,8 Мп), а время обновления информации не более 30 кадр/с (3,3 · 10⁻³ с), тогда как необходимое время подфокусировки составляет T быс = 10⁻⁴ с.

Ограничение по углам и скорости наведения лазера на цель. Поскольку объектив лазера механически связан (оптоволоком или иной

оптической схемой) с основным модулем лазерного комплекса, то всегда существуют ограничения по углам наведения и скорости наведения объектива лазера на цель. Имеют ограничения и пределы фокусировки объектива по дальности. При проведении натурных и приемочных испытаний таких комплексов надо эти параметры тщательно проверять, уделяя особое внимание при наведении объектива на цель на близких дистанциях, когда угловые скорости наведения и предельные углы становятся максимально большими, а дистанция поражения - минимальной.

Попадание загрязнений на объектив лазерного излучателя. Обычно этому вопросу уделяется крайне мало времени, однако этот вопрос важен. В мощных лазерах плотность энергии лазерного излучения может достигать до 2 кВт/см², что при потере локальной прозрачности линзы объектива приведет к взрывному её разрушению. Поэтому попадания осадков в виде грязи, снега, дождя на объектив лазерного излучателя недопустимы. Защитить выходную линзу лазерного излучателя можно установкой защитных бленд (насадок) и созданием с помощью вентилятора противотока воздуха, а также проведением профилактических очисток линзы с помощью спиртовых растворов в ручном или автоматическом режимах.

Примечание. При проведении натурных испытаний, почти всегда работа лазерных комплексов демонстрируется на полигоне, где отсутствует турбулентность атмосферы, при хороших погодных условиях в дневное время суток. При этом поражение БВС самолетного типа производится на оптимальном удалении от лазерного комплекса в боковую проекцию, что позволяет выбрать уязвимую часть БВС и обеспечить необходимое для поражения время экспозиции (удержание на цели) луча. Хотя наибольший интерес представляют результаты поражения БВС: при высокой турбулентности воздуха днем, поражение БВС в ночное время, при наличии атмосферных осадков, в лобовую проекцию БВС самолетного типа, совершающих маневр уклонения с предельными перегрузками.

Положительные качества лазерных комплексов поражения. Кажется, что при таком объеме ограничений и спорных технических решений лазерные комплексы поражения не должны представлять большого практического интереса, однако, в России и во всем мире проводятся интенсивные работы в этих областях. Причем в последнее время наблюдается всплеск интереса к таким комплексам.

Такое положение объясняется появлением доступных лазерных комплексов, созданных на базе иттербиевого оптоволокна. Они характеризуются высоким КПД (25-30%), относительно большой мощностью (до 50 кВт), и по своей структуре относятся к твердотельным лазерам.

Несмотря на первоначальную высокую стоимость лазерных комплексов, стоимость

выстрела по цели определяется стоимостью электроэнергии на работу комплекса.

Отсутствие при поражении БВС сопутствующих поражающих элементов в виде осколков и пуль, прошедших мимо цели, позволяет их применять в городской черте.

Имеется потенциал для дальнейшего их совершенствования.

Вывод. Все лазеры работают по одинаковой схеме.

Лазерное излучение всегда монохромное и когерентное, что в свою очередь позволяет создавать поток света с очень малой расходимостью.

Атмосферные осадки, турбулентность атмосферы, наличие в ней различных аэрозолей существенно влияют на эффективность работы лазерного комплекса.

Использование длинноволнового лазерного ИК-излучения (10 мкм) уменьшает затухание излучения в легком тумане и слабых осадках.

При прохождении мощного лазерного излучения возможно получить локальный разогрев атмосферы, который окажет негативное воздействие на излучение, исходя из этого существует ограничение на мощность лазерного излучения.

Большинство лазерных комплексов имеют объективы с функцией автоматической подфокусировки на цель, что требует применение высококачественных телекамер с высоким разрешением и быстродействием. В свою очередь это требует решение дополнительных вопросов при работе лазерного комплекса в ночное время.

Существуют ограничения по углам наведения и скорости наведения объектива лазера на цель. Имеют ограничения и пределы фокусировки объектива по дальности.

В настоящее время поражение БВС, при установке лазера на движущуюся наземную платформу (поражение в движении по грунту), практически невозможно.

Попадание загрязнений на объектив лазерного излучателя недопустимо, причем этот вопрос должен решаться техническими средствами, а не организационно-профилактическими методами.

Появление доступных лазерных комплексов, созданных на базе иттербиевого оптоволокна, породило дополнительный интерес к ним.

Наиболее рационально использовать лазерные комплексы на стационарных объектах, где недопустимо применение зенитных или стрелковых комплексов поражения БВС.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Указ Президента РФ от 30 сентября 2016 г. N 510 "О Федеральной службе войск национальной гвардии Российской Федерации".
2. Федеральный закон "О безопасности объектов топливно-энергетического комплекса" от 21.07.2011 N 256-ФЗ.
3. ГОСТР 58373— 2019 "Лазеры и лазерное оборудование. Термины и определения".
4. Борейшо В.А., Клочков Д.В., Коняев М.А., Никулин Е.Н. Военные применения лазеров: учебное пособие гос. тех. ун-т. – СПб., 2015 – 103 с.
5. [сайт] // URL: https://wiki2.org/ru/Файл:Atmosfaerisk_spredning-ru_svg (дата обращения: 20.07.2025).
6. [сайт] // URL: <https://ppt-online.org/156370> (дата обращения: 20.07.2025).
7. [сайт] // URL: <https://ppt-online.org/156371> (дата обращения: 20.07.2025).
8. [сайт] // URL: https://ritm-magazine.com/sites/default/files/Public/RHYRHM_of_machinery_3_2019/statia_optika_lazer_prom_ystanovok_ris1_rhythm_of_machinery_3_2019.png (дата обращения: 20.07.2025).

УДК 621.039.57+654.9

ББК 342.9:68.69

**МОРОЗ ИГОРЬ ВЛАДИМИРОВИЧ, СТАРШИЙ НАУЧНЫЙ СОТРУДНИК ФКУ «НИЦ
«ОХРАНА» РОСГВАРДИИ**

ТРЕБОВАНИЯ ПОСТАНОВЛЕНИЙ ПРАВИТЕЛЬСТВА РФ К ОБОРУДОВАНИЮ ИТСО ОБЪЕКТОВ (ТЕРРИТОРИЙ)

Аннотация. В статье указаны особенности Требований постановлений Правительства РФ к ИТСО для разных объектов (территорий).

Ключевые слова: инженерно-технические средства охраны (ИТСО), технические средства охраны (ТСО), антитеррористическая защищенность, собственные объекты, приказ, Федеральная служба войск национальной гвардии Российской Федерации.

MOROZ IGOR VLADIMIROVICH, **SENIOR RESEARCHER OF THE DEPARTMENT OF DEVELOPMENT OF NORMATIVE AND METHODOLOGICAL DOCUMENTS FSI «SRC «OKHRANA» OF THE FEDERAL SERVICE OF NATIONAL GUARD OF RUSSIA**

REQUIREMENTS OF THE GOVERNMENT OF THE RUSSIAN FEDERATION REGULATIONS FOR THE EQUIPMENT OF IT FACILITIES (TERRITORIES)

Annotation. The article highlights the specifics of the Requirements of the RF Government regulations for ITSO for different facilities (territories).

Keywords: engineering and technical means of protection (ITSO), technical means of protection (TSO), antiterrorist security, own facilities, order, Federal Service of the National Guard of the Russian Federation.

Антитеррористическая защищенность объектов – это не просто формальность, а динамичная система, чутко реагирующая на меняющиеся угрозы и оперативную обстановку. Ее цель – максимально эффективное и рациональное использование имеющихся сил и средств, подобно надежному щиту, возведенному с умом и точным расчетом.

Напомню выбор конкретных моделей средств охраны – это тонкая, кропотливая работа, требующая пристального внимания к деталям. Это определяется на начальном этапе разработки проектной документации. На этом этапе определяется направление организации системы безопасности при проведении строительно-монтажных работ, реконструкции или ремонте.

Ответственность за безопасность, организацию оборудования объекта системами безопасности лежит на руководителе. Он направляет действия сотрудников, добиваясь слаженной работы всего коллектива для достижения общей цели.

В современном мире, где цифровые технологии пронизывают все сферы жизни, создание комплексов инженерно-технических средств охраны (ИТСО) невозможно без применения передовых решений. Они обеспечивают своевременное обнаружение злоумышленников,

подобно зоркому глазу, неусыпно следящему за горизонтом.

ИТСО вновь оборудуемых, реконструируемых и технически перевооружаемых объектов (помещений) должны соответствовать следующим принципам:

Гармоничное соответствие: Состав, структура и размещение ИТСО должны быть согласованы с особенностями объекта, его техническим процессом, степенью важности и секретности, наиболее вероятными угрозами и предполагаемой моделью нарушителя. Это похоже на создание индивидуального плана обороны, учитывающего все уязвимости и сильные стороны.

Проектной документацией должно быть определено необходимый достаточный минимум ИТСО для защиты объекта. Решения в проектной должны быть взаимно согласованными и идеально сбалансированной системой, где каждый элемент выполняет свою функцию без излишеств и пробелов.

В соответствии со статьей 2 Федерального закона от 03.07.2016 № 226-ФЗ [2], войска национальной гвардии Российской Федерации несут ответственность за охрану особо важных и режимных объектов, объектов, подлежащих обязательной охране (согласно перечню,

утвержденному Правительством РФ), а также за охрану имущества по договорам и обеспечение безопасности объектов первостепенной важности.

Оборудование ИТСО собственных объектов должно осуществляться в соответствии с:

Приказом Федеральной службы войск национальной гвардии Российской Федерации от 21 октября 2024 г. № 385дсп [8];

Приказом Федеральной службы войск национальной гвардии Российской Федерации № 177дсп [9].

Для достижения наилучшей защиты применяется категорирование объектов (территорий), которое можно сравнить с разделением на классы защиты. Этот процесс включает оценку текущего состояния защищенности, значимости объекта для инфраструктуры и жизнеобеспечения, а также степени потенциальной опасности и возможных последствий теракта.

Мероприятия и меры необходимые для организации безопасности объектов должны учитывать возможные последствия при преступных посягательствах, защищенность, значимость инфраструктуры, жизнеобеспечение, управления и определяются при проведении обследования объектов.

По результатам обследования оформляется акт состояния защищенности.

Категория присваивается по результатам обследования, учитывающего состояние защищенности, инфраструктурные особенности, потенциальные опасности и вероятные угрозы террористических актов, а также их возможные последствия. Критерии категорирования регламентированы постановлением Правительства РФ № 304 от 21 мая 2007 года.

В акте состояния защищенности объекта указывается его группа значимости, определяемая как В (высокая), С (средняя) или Н (низкая).

Выбор требуемого минимального состава средств защиты (комплекса безопасности), а также требований к инфраструктуре физической охраны для объектов, осуществляется в зависимости от установленной группы значимости.

Требования к оборудованию объектов ИТСО указаны в приказе Федеральной службы войск национальной гвардии Российской Федерации № 177дсп [9] (п. 30.1 приказа Федеральной службы войск национальной гвардии Российской Федерации от 21 октября 2024 г. № 385дсп [8]).

Также следует учитывать группу значимости объекта (приложение № 2 к приказу Федеральной

службы войск национальной гвардии Российской Федерации от 21 октября 2024 г. № 385дсп [8]).

Информация, содержащаяся в акте обследования, относится к служебной информации ограниченного распространения и подлежит маркировке грифом «Для служебного пользования».

Режимные помещения собственных объектов оснащаются ИТСО в соответствии с требованиями пункта 173 приказа Росгвардии от 20 февраля 2024 г. № 015 [10].

Объекты, подлежащих обязательной охране войсками национальной гвардии Российской Федерации, оборудуются в соответствии с требованиями Постановления Правительства РФ от 25 марта 2015 г. N 272 [6].

Инженерная защита, охватывает все этапы жизненного цикла объекта, от проектирования до утилизации.

Тип и состав ИТСО определяется техническим заданием на проектирование. При необходимости усиления защиты объект может быть оснащен оборудованием более высокого класса.

Наиболее мощная защита создается в зонах расположения наиболее важных мест, на не видимых или изогнутых участках ограждения и в труднодоступных местах.

К ИТСО предъявляются требования, зависящие от категории объекта, которые детально описаны в специальном приложении к постановлению правительства.

Контроль за соблюдением этих требований осуществляет Росгвардия посредством плановых и внеплановых проверок.

Плановые проверки проводятся ежегодно и включают проверку документации и выезд на объект. Внеплановые проверки могут быть инициированы в случае не устранения нарушений, поступления жалоб или информации о проблемах с антитеррористической защищенностью, а также по поручению руководства.

Перечень должностных лиц, уполномоченных на проведение проверок, утверждается руководителем территориального управления Росгвардии.

При оборудовании системами охраны объектов Росгвардии работы выполняются при строительстве или в процессе эксплуатации собственными силами или подрядными организациями. Порядок приемки таких объектов регламентирован приказом Росгвардии.

Условия охраны имущества вневедомственной охраной определяются договором, в котором

согласовываются правила прохода и поведения на объекте. Разрабатываются схема объекта с указанием границ, постов охраны и уязвимых мест, перечень технических средств охраны, схема блокировки с указанием уровней защиты и типов оборудования, расчет необходимого количества охранников и маршруты патрулирования.

При технической или комбинированной охране вневедомственная охрана проверяет работоспособность оборудования при подключении

к пульту (если договор заключен по результатам торгов) и контролирует его исправность. Контроль может быть оперативным и периодическим. Любые изменения в схемах или замена оборудования должны быть согласованы.

Все решения должны обеспечивать надежную защиту объекта. Важно учитывать требования, регулирующие оборудование объектов системами охраны.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Градостроительный кодекс Российской Федерации: Федеральный закон от 29 декабря 2004 г. № 190-ФЗ // Собрание законодательства Российской Федерации – 03.01.2005 – № 1 (часть I)– Ст. 16.
2. О войсках национальной гвардии Российской Федерации: федеральный закон от 3 июля 2016 г. № 226-ФЗ // Собрание законодательства Российской Федерации – 04.07.2016 – № 27 (часть I) – Ст. 4159.
3. О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд: Федеральный закон от 5 апреля 2013 г. N 44-ФЗ // Собрание законодательства Российской Федерации – 12.04.2013 – № 14 – Ст. 1652.
4. О закупках товаров, работ, услуг отдельными видами юридических лиц: Федеральный закон от 18 июля 2011 г. N 223-ФЗ // Собрание законодательства Российской Федерации – 25.07.2011 – № 30 (часть I) – Ст. 4541.
5. О классификации чрезвычайных ситуаций природного и техногенного характера: постановление Правительства Российской Федерации от 21 мая 2007 г. N 304 // Собрание законодательства Российской Федерации – 28.05.2007 № 22 - Ст. 2640.
6. Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии Российской Федерации, и форм паспортов безопасности таких мест и объектов (территорий): постановление правительства РФ от 25 марта 2015 г. N 272 // Собрание законодательства Российской Федерации – 6.04.2015 № 14 - Ст. 2119.
7. Об утверждении Инструкции о порядке сдачи, приемки и передачи в эксплуатацию законченных строительством объектов войск национальной гвардии Российской Федерации: приказ Федеральной службы войск национальной гвардии Российской Федерации от 27.12.2017 № 556 [сайт] // URL: <https://hq-isnpa-01.rosgvard.ru/cons/cgi/online.cgi?req=doc&base=SVB207&n=872&cacheid=4167E7914481D94CC9DD08179F2C6778&mode=splus&rnd=0.011259729839668275#v611aUUz6fl2QC7A/> (дата обращения – 07.10.2024).
8. Об утверждении инструкции по организации охраны собственных объектов войск национальной гвардии Российской Федерации от преступных посягательств: приказ Федеральной службы войск национальной гвардии Российской Федерации от 21 октября 2024 г. № 385дсп;
9. Об утверждении требований к оборудованию инженерно-техническими средствами охраны собственных объектов войск национальной гвардии Российской Федерации и Руководства по организации оборудования инженерно-техническими средствами охраны собственных объектов войск национальной гвардии Российской Федерации: приказ Федеральной службы войск национальной гвардии Российской Федерации от 27 мая 2019 г. № 177 дсп.
10. Об утверждении Инструкции по защите гостайны и ведению секретного делопроизводства в ВНГ РФ и форм учетных документов по защите гостайны и ведению секретного делопроизводства в ВНГ РФ: приказ Росгвардии от 20 февраля 2024 г. № 015.
11. Режимные помещения собственных объектов оборудуются ИТСО в соответствии с требованиями п. 173 приказа Росгвардии от 20 февраля 2024 г. № 015 «Об утверждении Инструкции по защите гостайны и ведению секретного делопроизводства в ВНГ РФ и форм учетных документов по защите гостайны и ведению секретного делопроизводства в ВНГ РФ».

УДК 654.09
ББК 32.972

ПАРХАЕВ АЛЕКСЕЙ ВЛАДИМИРОВИЧ, НАУЧНЫЙ СОТРУДНИК ФКУ «НИЦ «ОХРАНА»
РОСГВАРДИИ

МИХАЙЛОВ АЛЕКСЕЙ АЛЕКСЕЕВИЧ, НАУЧНЫЙ СОТРУДНИК ФКУ «НИЦ «ОХРАНА»
РОСГВАРДИИ

ПРОБЛЕМЫ ОЦЕНКИ И ТЕСТИРОВАНИЯ СОВРЕМЕННОЙ ВИДЕОАНАЛИТИКИ

Аннотация. В статье анализируются ключевые вызовы в оценке эффективности систем видеоаналитики, основанных на работе искусственного интеллекта и компьютерного зрения, рассматриваются проблемы отсутствия стандартизированных метрик и протоколов, что затрудняет сравнение технических решений и приводит к переоценке их точности. Проанализированы технические аспекты, такие как ложные срабатывания и необходимость интеграции с реальными сценариями. Предлагаются решения, включая разработку универсальных стандартов и использование гибридных методов тестирования. Обосновывается необходимость внедрения инноваций для повышения надежности видеоаналитики в областях противокриминальной безопасности.

Ключевые слова: ситуационная видеоаналитика, видеоаналитика, метрики, видеоаналитики, эффективность видеоаналитики.

Annotation. The article "Problems of evaluation and testing of modern video analytics" analyzes the key challenges in evaluating the effectiveness of video analytics systems based on artificial intelligence and computer vision. It examines the lack of standardized metrics and protocols, which makes it difficult to compare solutions and leads to an overestimation of their accuracy. Ethical and technical aspects such as false positives and the need to integrate with real-world scenarios are discussed. Solutions are proposed, including the development of universal standards and the use of hybrid testing methods. The article highlights the need for innovation to improve the reliability of video analytics in the fields of security, transportation, and retail.

Keywords: situational video analytics, video analytics, metrics, video analytics, effectiveness of video analytics.

Проблемы оценки и тестирования современной видеоаналитики.

Современная видеоаналитика — это технология, использующая искусственный интеллект (далее ИИ) и компьютерное зрение для анализа видеопотоков в реальном времени. Она применяется в различных отраслях, в том числе на производстве и в системах безопасности (распознавание лиц, обнаружение вторжений и т. д.). Но определить степень необходимости применения таких систем можно только после оценки их эффективности, результативности и возможности принимать решения на основе полученных видеоданных. Такая оценка сводится к точности распознавания объектов в сложных условиях и отсеву возможных ложных срабатываний [1].

Рассмотрим ключевые проблемы оценки эффективности систем видеоаналитики, которые условно можно разделить на три группы, это технические, методические и организационные.

К техническим можно отнести:

– отсутствие универсальных методов обработки видеоматериалов и изображений, способных гарантировать удовлетворительное качество выполнения задач на разнообразных сценах и при отличных условиях наблюдения;

– неспособность системы корректно приспособиться к изменениям условий наблюдения после начальной настройки;

– излишне высокая вычислительная нагрузка большинства современных алгоритмов обработки видео и изображений приводит к тому, что в практике предпочитают менее сложные, но менее результативные методы;

– недостаток эвристического анализа заключается в фиксированных характеристиках или параметрах обнаружения, установленных вручную. Если объект не соответствует заданным критериям, система способна допустить ошибку;

– отрицательное воздействие низкого качества видеоданных, то есть низкое разрешение видео, слабое освещение или неудачные углы обзора камер [2].

К организационным проблемам можно отнести: Трудности с монтажом и конфигурацией оборудования.

Специфические условия по размещению камеры, переделываемые разработчиками аналитических решений по: дистанции до цели, числу и видам объектов, условиям внутри и снаружи помещений, освещению и прочим аспектам.

Неполная оптимизация рабочих процессов систем видеоаналитики — к примеру, активация системы занимает много времени, и часто недостаточно лишь разместить и подключить камеру.

К методологическим проблемам относятся:

Неверное определение задач — решения в видеоаналитике требуют детализации, к примеру, интеграция распознавания лиц в систему контроля доступа отличается от аналитики посетителей в торговом центре;

Недостаток документированной процедуры тестирования, которая включает цели, условия, последовательность и способы испытаний, а также критерии оценки.

Некорректное проведение тестирования системы, например, проверка на камерах, не предназначенных для финального решения, может вызвать плохие результаты функционирования системы [2, 3].

Саму видеоаналитику, в общем виде можно разделить по целям и задачам на промышленную, бытовую и охранную.

Под промышленной видеоаналитикой понимают в первую очередь видеоаналитику основанную на машинном зрении и затрагивающей вопросы касающейся техники безопасности человека на производстве и контроля качества выпускаемой продукции. К основным элементам промышленной видеоаналитики относятся:

- контроль качества выпускаемой продукции;
- контроль положения детали в технологическом оборудовании;
- проведение различных замеров при проведении технологических операций;
- контроль действий персонала;
- контроль проникновения в запретные зоны;
- контроль средств индивидуальной защиты;
- учёт изготовленной продукции;
- контроль промышленных инцидентов и аварий и т.д.

Отличительной чертой промышленной видеоаналитики является простота получения обширных баз данных событий (датасетов), поскольку технологический процесс уже

существует и получение событий не представляет сложности. Данное обстоятельство позволяет произвести обучение нейронную сеть на основе большого количества событий, что обеспечивает сравнительно высокие показатели работы системы. Аналогично гораздо проще контролировать качество такой видеоаналитики, создавая набор данных для проведения контрольного тестирования. Пожалуй, исключение из этого правила составляет видеоаналитика контроля крупных аварий, поскольку база таких событий всегда ограничена или полностью отсутствует.

К охранной видеоаналитике можно отнести следующие направления:

- автоматическое распознавание номеров;
- измерение скорости движения транспортных средств, и прочие нарушения ПДД;
- проверка автомашин по различным базам розыска контроля;
- фиксация всех транспортных средств в зоне контроля, данные о направлении, траектории движения, средней плотности потока;
- обнаружения на проезжей части предметов, не являющихся частью дорожного полотна или участником движения;
- детектор оставленных предметов;
- детектор передвижения физических лиц;
- детектор движения в запрещенном направлении;
- детектор движения и нахождения в запрещенной зоне;
- детектор нетипичных изменений в сцене (саботаж);
- детектор образования толпы;
- детектор счетчик пассажиропотока;
- детектор агрессивного поведения;
- детектор дыма и огня;
- детектор падения на рельсы и прочие опасные зоны;
- трекинг объектов;
- идентификация объектов;
- детектор запрещенной символики;
- детектор времени обслуживания;
- детектор остановки или парковки в неполюженном месте;
- детектор фотографирования экрана монитора или документов;
- модуль контроля регламентов при доступе к хранилищу материальных ценностей;
- модуль биометрического распознавания по лицу;
- модуль кассовой безопасности;
- контроль работы с банковскими кассетами;

- детектор громкого звука, выстрела, криков;
- модуль определение эмоций;
- модуль выявления муляжа лица.

Уже на данном этапе мы сталкиваемся с проблемой создания объемных датасетов как для обучения нейросети, так и её контроля. Например, крайне сложно реализовать датасеты в объеме 10-100 тыс. событий для таких типов видеоаналитики как: детектор оставленных предметов, детектор агрессивного поведения, детектор дыма и огня, детектор падения на рельсы, детектор оставленных предметов, детектор агрессивного поведения, определение эмоций, определение муляжа лица и т. д.

Даже такая простейшая сцена как выстрел из огнестрельного оружия крайне сложен для создания датасетов, т. к. выстрелы из пистолета, автомата, охотничьего оружия, как и само оружие различны форме, положению, цвету и способу удержания. Причем следует учесть, что базы данных, на которых обучалась нейросеть и базы по которым производится оценка качества работы нейросет (её видеоаналитики) должны быть различны.

В настоящее время видеоаналитика проходит аналогичные этапы становления, что в своё время проходила биометрия. Поэтому опыт в развитии биометрии следует использовать в развитии видеоаналитики. Так вскоре после зарождения биометрии были созданы независимые биометрические сообщества, которые, в частности, осуществляли и её тестирование. Как пример таких обществ можно назвать «Некоммерческое партнерство «Русское биометрическое общество» и программу FRVT (Face Recognition Vendor Test), разработанную национальным институтом стандартов и технологий (NIST) США по тестированию систем биометрии.

К сожалению, в области видеоланалитики в России этого пока не случилось.

Если говорить про тестирование в Европе, то можно назвать библиотеку «i-LIDS», (Imagery library for intelligent detection systems), дословно - «Библиотека изображений для интеллектуальных систем обнаружения». Департамент научных разработок МВД Великобритании совместно с Центром защиты национальной инфраструктуры разработали данную методику. Сертификат «i-LIDS» является общепризнанным стандартом качества видеоаналитики в Великобритании.

В России при этом отсутствуют общепринятые и утвержденные метрики тестирования видеоаналитики.

Очевидно, что как минимум, видеоаналитику надо проверять на «матрицу ошибок», которая показана на рисунке 1. [4]



Рисунок 1 — Матрица ошибок

Примечание:

Модель — (в упрощенном понимании) это математическая структура нейронной сети с выработанными весовыми коэффициентами в нейронных связях, полученными в процессе обучения нейронной сети;

Класс — это шаблон, по которому объекты классифицируются по определенным свойствам или поведению, например, человек, собака, лошадь, или стоящий человек, идущий человек, бегущий человек и т.д.

«True Positive» (TP, истинно-положительный) — количество случаев, когда модель правильно предсказала положительный класс-результат.

«False Positive» (FP, ложноположительный) — количество случаев, когда модель неправильно предсказала класс-положительный.

«False Negative» (FN, ложноотрицательный) — количество случаев, когда модель неправильно предсказала класс-отрицательный.

«True Negative» (TN, истинно-отрицательный) — количество случаев, когда модель правильно предсказала класс-отрицательный.

В видеоаналитике все эти параметры тесно взаимосвязаны, а соответственно проверять их необходимо в совокупности. Как пример можно привести следующие метрики бинарной классификации:

«Accuracy» - данная метрика (1) характеризует качество модели, агрегированное по всем классам. Это полезно, когда классы для нас имеют

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

одинаковое значение. В случае, если это не так, «ассигуру», может быть обманчивой.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

«Precision» (точность) - Отношение правильно предсказанных положительных наблюдений к общему количеству предсказанных положительных результатов (2).

$$\text{Precision} = \frac{TP}{TP + FP} \quad (2)$$

«Recall» (полнота, чувствительность) - Отношение правильно предсказанных положительных наблюдений ко всем наблюдениям в классе.

$$\text{Recall} = \frac{TP}{TP + FN} \quad (3)$$

«F(мера)» - среднегармоническое между Precision и Recall.

$$F_\beta = (\beta^2 + 1) \frac{\text{Recall} \cdot \text{Precision}}{\text{Recall} + \beta^2 \text{Precision}} \quad (4)$$

«ROC»-кривая и «ROC-AUC»

Для построения кривых «ROC» и «ROC-AUC» используют параметр «TPR» и «FPR».

$$\text{TPR} = \frac{TP}{P} = \frac{TP}{TP + FN} \quad (5)$$

Примечание. Параметр «TPR» дублирует «Recall». Данный параметр используется для построения кривой «ROC».

«True Positive Rate» (TPR) — это полнота, доля положительных объектов, правильно предсказанных положительными.

False Positive Rate (FPR) - это доля отрицательных объектов, неправильно предсказанных положительными.

$$\text{FPR} = \frac{FP}{N} = \frac{FP}{FP + TN} \quad (6)$$

Кривая «ROC» представляет собой графическое представление компромисса между чувствительностью и специфичностью при различных порогах классификации. Идеальная модель классификации будет стремиться к точке в верхнем левом углу графика, где TPR равно 1, а FPR равно 0.

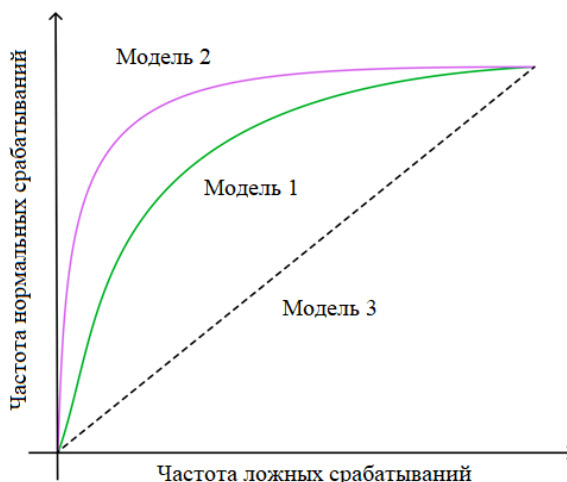


Рисунок 2 —Кривая «ROC» [4]

Примечание. На этом рисунке модель 2 имеет лучшие характеристики чем модель 1, а модель 3 по своей сути выполняет случайное угадывание ситуации. Кривая ниже диагональной линии указывает на производительность хуже, чем при случайном угадывании.

По данным ROC-кривой можно рассчитать метрику ROC-AUC (англ. ROC — receiver operating characteristic, AUC — area under the curve, «площадь под кривой»).

Её значение равно площади под графиком.

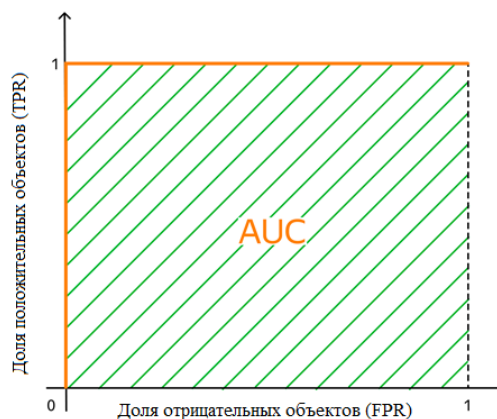


Рисунок 3 —метрика «ROC-AUC» [4]

Максимальное значение площади равно 1, это значение ROC-AUC идеальной модели, которая совсем не ошибается, при значении 0,5 модель соответствует работе системы со случайным угадыванием.

Примечание. Кроме того, существуют следующие кривые

Кривая FAR (False Acceptance Rate) – ошибка первого рода.

Кривая FRR (False Rejection Rate) – ошибка второго рода.

КОО – кривая компромиссного определения ошибки (англ. DET detection error tradeoff curve; DET curve).

Следующей проблемой является выбор допустимых значений метрик. При общих равных подходах приемлемые значения метрик видеоаналитики по обнаружению номеров автомобиля могут на порядок отличаться от приемлемых значений метрик видеоаналитики, допустим по обнаружению огнестрельного оружия в руках человека.

Обращаю внимание, что значение метрик полученных при проведении испытаний в лаборатории путём проверки готовых датасетов может отличаться от результатов полученных проведении испытаний в реальных условиях, поскольку на его качество будут влиять характеристики используемой видеокамеры, уровень освещенности, используемый спектральный диапазон осветителя сцены наблюдения, применяемый алгоритм компрессии и степень компрессии видеосигнала, а также такие факторы, как блики от различных источников, свет фар проезжающих автомобилей, качание веток деревьев, встречная засветка от солнца, время года, реальный ракурс наблюдения сцены видеокамерой.

Анализируя указанные проблемы можно сделать следующие выводы:

– сообществу необходимо объединить усилия для выработки единого подхода и методик тестирования видеоаналитики;

– назрела необходимость в создании органа (государственного, коммерческого или некоммерческой структуры) который будет иметь возможность проводить независимую экспертизу видео;

– должны быть определены значения метрик для возможности ранжирования видеоаналитики по критерию уровня качества видеоаналитики;

– любая методика проведения лабораторных испытаний при использовании и одинаковых подходов тестирования даст оценку критерию лучше или хуже видеоаналитики по сравнению с той, которая уже прошла тестирование;

– наиболее объективные показатели смогут дать только натурные испытания;

– общая тенденция развития систем видеоаналитики движется в сторону решения описанных проблем, но на данный момент существует необходимость, специалистам, занимающимся существующей проблематикой, проводить совместные испытания, вырабатывать методики проведения испытания, делиться полученными результатами на страницах открытой печати. Поскольку в результатах получения честных и объективных исследований заинтересованы все, и потребители, и производители. Причем в наибольшей степени в этом заинтересованы производители, т. к. себя можно обмануть, но вот ещё никому не удавалось обмануть действительность.

ТЕРМИНЫ И АББРЕВИАТУРЫ

СОТ - система охранная телевизионная;

И.И. - искусственный интеллект;

ПДД - правила дорожного движения;

Датасет - структурированный набор данных, предназначенный для обучения И.И.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. [Электронный ресурс]. - Режим доступа: <https://rzddigital.ru/glossary/726/>
2. [Электронный ресурс]. - Режим доступа: <https://macroscop.com/o-kompanii/blog/videoanalytyka>
3. [Электронный ресурс]. - Режим доступа: https://hk-russia.ru/index.php?route=tmdblog/blog&blog_id=26
4. [Электронный ресурс]. - Режим доступа: <https://education.yandex.ru/handbook/ml/article/metriki-lassifikacii-i-regressii>

УДК 004.8
ББК 32.813

ПРОСКУРИН РОМАН АНАТОЛЬЕВИЧ, ГЛАВНЫЙ НАУЧНЫЙ СОТРУДНИК ОТДЕЛА РАЗВИТИЯ ИННОВАЦИОННЫХ РЕШЕНИЙ, ЦИФРОВЫХ ТЕХНОЛОГИЙ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ФЕДЕРАЛЬНОГО КАЗЕННОГО УЧРЕЖДЕНИЯ «НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР «ОХРАНА» РОСГВАРДИИ, КАНДИДАТ ТЕХНИЧЕСКИХ НАУК, СТАРШИЙ НАУЧНЫЙ СОТРУДНИК

**ИННОВАЦИОННЫЕ ПОДХОДЫ К ПОВЫШЕНИЮ ЭФФЕКТИВНОСТИ
УПРАВЛЕНИЯ ВО ВНЕВЕДОМСТВЕННОЙ ОХРАНЕ НА ОСНОВЕ ТЕХНОЛОГИЙ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА**

Аннотация. В статье рассмотрены проблемные вопросы эффективности организационного управления во вневедомственной охране войск национальной гвардии Российской Федерации. Предложены подходы повышения эффективности управления за счет внедрения инновационных решений на основе технологий искусственного интеллекта, а именно, систем поддержки принятия решений, реализованных в виде экспертных систем, построенных на базе нейронных сетей.

Ключевые слова: вневедомственная охрана, управление, принятие решений, экспертные системы, нейронные сети, оптимизация.

PROSKURIN, ROMAN ANATOLYEVICH, CHIEF RESEARCHER OF THE DEPARTMENT OF INNOVATIVE SOLUTIONS, DIGITAL TECHNOLOGIES, AND SOFTWARE DEVELOPMENT OF THE FEDERAL STATE INSTITUTION SCIENTIFIC RESEARCH CENTER "OKHRANA" OF THE RUSSIAN GUARD, CANDIDATE OF TECHNICAL SCIENCES, SENIOR RESEARCHER

INNOVATIVE APPROACHES TO IMPROVING MANAGEMENT EFFICIENCY IN NON-GOVERNMENT PROTECTION BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Annotation. The article discusses the problematic issues of reducing the efficiency of organizational management in the private security services of the National Guard Troops of the Russian Federation. The authors propose approaches to improving management efficiency through the implementation of innovative solutions based on artificial intelligence technologies, namely, decision support systems implemented as expert systems based on neural networks.

Keywords: private security, management, decision-making, expert systems, neural networks, and optimization.

Главными исполнительными элементами системы вневедомственной охраны (ВО) войск национальной гвардии Российской Федерации (ВНГ РФ - Росгвардии) являются строевые подразделения (СПВО). К СПВО относятся линейные (объектовые) отделения Центра специального назначения вневедомственной охраны (ЦСН ВО), полки (батальоны, роты, взводы и отделения (строевые) управлений (отделов) вневедомственной охраны войск национальной гвардии по субъектам Российской Федерации (УВО) и филиалов УВО, выполняющие задачи, возложенные законодательством Российской Федерации на войска национальной гвардии, по охране имущества и (или) объектов, а также участие в охране общественного порядка,

обеспечении общественной безопасности. Согласно Приказу Росгвардии от 28.12.2024 г. №505 [1] служба СПВО осуществляется нарядами различных видов: группа задержания (ГЗ), патруль по охране объекта (патруль), наряд на посту охраны объекта (ПОО или пост), наряд по охране имущества при транспортировке (ИТ), наряд по охране мест стоянок и (или) обслуживания судов и иных плавсредств с ядерными энергетическими установками в морских портах, в которые разрешен их заход (НМЛ).

Наряды СПВО при несении службы находятся под оперативным руководством дежурных служб ЦСН ВО Росгвардии, центра оперативного управления УВО, филиала, группы обеспечения служебной деятельности нарядов (ЦОУ (ГОСДН))

или иных должностных лиц, осуществляющих руководство службой, уполномоченных начальником УВО или филиала.

Непосредственному несению службы нарядами ВО и дежурными ЦОУ предшествует значительный объем предварительной работы, результатом которой является большой информационный массив, который предстоит в оперативном режиме анализировать и на основе этого анализа принимать управляющие решения дежурному – человеку-оператору т.е. лицу, принимающему решения (ЛПР), с точки зрения теории автоматизированных систем. Даже если исходить из теоретического предположения, что вся достаточно объемная и сложная работа по информационному обеспечению деятельности ЦОУ организована и реализована в строгом соответствии с регламентирующими документами, штаты всех подразделений ВО полностью укомплектованы высококвалифицированными и опытными профильными сотрудниками и работниками, а также весь личный состав СПВО мотивирован, дисциплинирован, оснащен в достаточном количестве качественным материально-техническим обеспечением исполнения служебных обязанностей, то и при этом организационное управление большим числом нарядов, в общем случае разных видов, не является тривиальной задачей. Практика службы СПВО показывает, что данное предположение не всегда реализуется в полной мере, а значит дополнительно усложняется задача эффективного анализа информации и принятия решений. Приказ Росгвардии №35 от 06.02.2019 г. [2] утверждает и содержит текст Руководства по организации службы ЦОУ подразделений ВО ВНГ РФ (далее Руководство). В тексте Руководства часто встречается словосочетание «принимает решение», но не дается разъяснений, как принять правильное, т.е. оптимальное или хотя бы рациональное решение, когда разнородной информации очень много, а времени на ее обработку крайне мало. Общеизвестно, что принятие решения человеком в значительной степени зависит от полноты и достоверности анализируемой информации. Кроме того, существуют физиологические ограничения возможностей человека по восприятию и эффективной обработке информации, необходимой для принятия решения. В случае использования неполной, неточной, искаженной или косвенной информации, в условиях жестких временных ограничений, часто в стрессовой

ситуации сложность задачи принятия хотя бы рационального решения человеком возрастает на порядки. Такие ситуации в практике служебной деятельности ВО ВНГ РФ нередки, и частота их проявления будет увеличиваться по мере роста информационной энтропии.

Несмотря на очевидную потребность в средствах интеллектуального содействия дежурным ЦОУ и другим сотрудникам в принятии управленческих решений, по результатам анализа открытых источников и опроса экспертов-практиков данной предметной области отсутствует информация о разработке и реальном применении подобных автоматизированных систем во вневедомственной охране ВНГ РФ.

Из открытых источников известны научные разработки моделей, методов и алгоритмов поддержки принятия решений дежурными ЦОУ и операторами укрупненных пунктов централизованной охраны (УПЦО) [3,4]. Они, в основном, направлены на повышение эффективности решения транспортной задачи, в широком смысле, т.е. поиск оптимального плана перемещения нарядов ВО с маршрутов или мест дислокации в пункты, с которых поступили сигналы тревоги или сработки технических средств охраны (ТСО), с минимальными общими временными затратами. При всей важности подобных работ можно говорить о том, что они относятся, либо сводятся путем введения определенных допущений, к классу задач линейного программирования, а значит могут быть достаточно эффективно решены путем наращивания производительности вспомогательных вычислительных средств. Однако, этот путь повышения эффективности решения задач управления имеет принципиальные ограничения, обусловленные последовательной архитектурой традиционных вычислительных средств, экономической целесообразностью, а также слабой приспособленностью к решению именно интеллектуальных задач принятия решений.

Как уже отмечалось, в ближайшей перспективе спектр и сложность задач, а, следовательно, объем обрабатываемой информации сотрудниками вневедомственной охраны будет только возрастать. Это обусловлено, в частности, тем, что помимо значительного числа стационарных объектов охраны, растет число мобильных охраняемых объектов (транспорта), все более широкое распространение получают мобильные кнопки тревожной сигнализации, установленные на смартфоны, весьма вероятно в ближайшее время

использование в охране беспилотных летательных аппаратов, активно внедряются средства видеоаналитики и т.д. Все это увеличивает разнородный информационный поток, зачастую слабоструктурированный, а иногда вовсе неформализованный, который нужно анализировать, как правило, в условиях лимита времени. Поэтому создание систем помощи человеку-оператору лишь путем прямого наращивания производительности вычислительных средств нельзя считать удовлетворительным решением проблемы.

Учитывая ограниченные ресурсы материального мотивирования личного состава ВО ВНГ РФ, неизбежно возникает проблема нехватки и большой текучести опытных кадров, а, как следствие этого, возникает потребность в сохранении и использовании в эргатических системах не только и не столько данных, сколько интеллектуальных знаний. Это позволит накапливать и использовать предыдущий практический опыт решения сложных задач управления для сокращения времени и облегчения процесса принятия решений ЛПР в дальнейшем.

Таким образом, существуют объективные предпосылки для внедрения в сферу деятельности вневедомственной охраны инновационных решений, в том числе из области технологий искусственного интеллекта, об этом же свидетельствуют и нормативные документы. Так, в проекте Концепции развития и совершенствования правового регулирования и организации охранной деятельности в Российской Федерации в рамках реализации государственной политики, осуществляемой Федеральной службой войск национальной гвардии РФ (далее – Концепция), разработанном ФКУ «НИЦ «Охрана» в 2025 г. [5], отмечается, что современные вызовы в сфере безопасности требуют трансформации подходов к организации и осуществлению охранной деятельности. Внедрение инновационных технологий позволит не только повысить эффективность защиты жизни и здоровья человека и гражданина, охраны объектов и имущества всех форм собственности от противоправных посягательств, но и интегрировать охранные системы в цифровую экосистему государства, обеспечивая синергию безопасности и социально-экономического развития.

При этом к перспективным технологиям, используемым при организации и осуществлении охранной деятельности, можно отнести:

1. Применение искусственного интеллекта и роботизированных комплексов при организации

охраны объектов:

- применение технологий искусственного интеллекта для распознавания угроз, анализа поведения и прогнозирования инцидентов;

- развертывание беспилотных воздушных, подводных и надводных судов и аппаратов, беспилотных транспортных средств и иных автоматизированных беспилотных комплексов для охраны периметров и труднодоступных зон;

- развитие систем безопасности, включая защиту от взлома и противодействие беспилотным воздушным, подводным и надводным судам и аппаратам, беспилотным транспортным средствам и иным автоматизированным беспилотным комплексам.

2. Технологии Больших данных и системы поддержки принятия решений:

- агрегация и анализ данных из множества источников (камеры, датчики, социальные сети, криминальная статистика) для выявления скрытых угроз;

- создание «адаптивных алгоритмов», способных обучаться на новых типах атак и оперативно корректировать меры защиты;

- внедрение «когнитивных помощников» для операторов, сокращающих время реакции и минимизирующих человеческие ошибки.

3. Использование Цифровых двойников для моделирования систем безопасности:

- разработка виртуальных копий охраняемых объектов для моделирования и тестирования сценариев атак, а также разработки оптимальных методов защиты;

- использование симуляций для оценки уязвимостей и расчета наиболее эффективных конфигураций охраны;

- прогнозирование последствий чрезвычайных ситуаций и отработка координации между уполномоченными подразделениями и ведомствами в виртуальной среде.

4. Переход к интеллектуальным системам охраны на основе технологий искусственного интеллекта, робототехники и цифровых двойников позволит не только усилить безопасность, но и создать основу для «умной» превентивной защиты.

Одним из наиболее перспективных направлений развития вневедомственной охраны в технической сфере в Концепции определено повышение уровня оперативности и мобильности действий дежурных сил за счет применения для их управления технологий поддержки принятия решений на основе искусственного интеллекта.

Среди технологий искусственного интеллекта

для повышения эффективности управления предлагается использовать технологию систем поддержки принятия решений, реализуемых в виде экспертных систем, которые могут быть построены на основе нейронных сетей, обучаемых с помощью различных, в том числе, генетических алгоритмов. Обоснование выбора конкретных топологий нейронных сетей и алгоритмов их обучения (оптимизации) для решения задач поддержки принятия решений выходит за рамки данной статьи.

В контексте Росгвардии, термин экспертные системы пока не является общепринятым в отношении вневедомственной охраны. Однако, можно говорить о применении автоматизированных систем управления, которые должны помочь в обеспечении безопасности и повышения эффективности работы подразделений вневедомственной охраны. Такие системы позволяют в режиме реального (или близком к реальному) времени отслеживать состояние охраняемых объектов, получать информацию о тревожных сигналах, координировать действия сотрудников, а также обеспечивать связь с дежурными частями. Следовательно, можно говорить о применении методов искусственного интеллекта и машинного обучения для анализа данных, полученных от вышеуказанных систем.

Экспертные системы используют знания специалистов предметных областей для консультации (содействия) при решении задач, математическая формулировка которых затруднена. Конструктивно экспертные системы могут строиться из различных компонент, однако, обязательными в их составе являются: база знаний, блок логического вывода, блок объяснения и диалоговые средства связи с пользователем. С экспертной системой обычно работают три категории пользователей:

Эксперт – специалист в предметной области, обладающий набором эвристических приемов для решения прикладных задач. Именно его знания составляют основной информационный фонд экспертной системы;

Инженер по знаниям – посредник между экспертом и экспертной системой, знакомый с формализмами, позволяющими перевести человеческие знания в «машинную» форму. Такие формализмы получили название моделей знаний;

Конечный пользователь – специалист, эксплуатирующий при решении своих задач экспертную систему, база знаний которой

наполнена знаниями эксперта.

В отечественной науке доктором технических наук, профессором Бондаревым П.А. и учениками возглавляемой им научной школы была разработана информационная технология построения систем искусственного интеллекта [6]. Главная отличительная особенность этой технологии – поддержка основного методологического положения, отличающего системы искусственного интеллекта от традиционных интерактивных систем. Имеется ввиду разделение в системе механизма вывода и средств описания предметных областей. Такой подход позволяет сделать тождественными операционную семантику системы и денотационную семантику средств описания предметных областей, а значит в полной мере реализовать все преимущества систем искусственного интеллекта. Ученикам профессора Бондарева П.А. удалось развить технологию построения интеллектуальных систем и, в частности, разработать методы использования нейронных сетей для создания систем поддержки принятия решений в виде экспертных систем, сочетающих преимущества и нивелирующие недостатки тех и других [7]. Данные методы на практике доказали свою валидность при решении сложных с точки зрения теории распознавания образов (в широком смысле, т.е. классов, сцен, ситуаций) задач специального вида (траекторных измерений, контроля космического пространства и др.). По методу аналогии нет оснований сомневаться, что данная технология может быть успешно применена в области деятельности вневедомственной охраны ВНГ РФ и позволит перейти от обработки данных к обработке знаний.

В целом, построение СППР в значительной степени базируется на теории распознавания образов. Известные методы распознавания достаточно эффективны в условиях традиционных ограничений и допущений относительно представления и анализа входной информации и вида решающих функций. Анализ публикаций по распознаванию образов показывает, что несмотря на очевидные достижения в теории и практике, проблема высокоэффективного, инвариантного по отношению к объекту (сцене, образу) распознавания не решена, за исключением частных случаев нормально распределенных классов с общей известной ковариационной матрицей. Для случаев же непараметрической априорной неопределенности относительно

многомерного признакового пространства обычно применяются те же статистические методы, основанные на сведениях указанной неопределенности к параметрической путем нормализации распределения признаков и использования выборочных моментов. Для классов, различающихся только средним, эффективность (достоверность) распознавания выражается через табулированные функции, что позволяет свести задачу к минимизации функции одной или двух переменных. Для классов, различающихся не только средним, но и дисперсиями или ковариационными матрицами, число переменных пропорционально возрастает, что увеличивает вычислительную сложность задач, традиционно решаемых, тем не менее, стандартными методами оптимизации. Еще одним ограничением традиционных подходов к решению сложных задач распознавания образов, а значит принятия решений, является использование вычислительных систем традиционной фон Неймановской архитектуры, которая делает компьютер гибким и универсальным относительно вычислительных функций, но обладает существенным недостатком, а именно, – машина может выполнить в каждый момент времени только одну базовую операцию. Задачи искусственного интеллекта слишком

сложны, чтобы их решение подобным способом было эффективным и в настоящее время главным препятствием для моделирования параллельных процессов, характеризующих нейросетевые вычисления, на ЭВМ последовательного типа является их низкое (относительно нейроморфных компьютеров) результирующее быстродействие. Однако, это не отменяет необходимости разработки моделей функционирования нейронных сетей, априори предполагающих параллельную обработку информации на вычислительных средствах последовательного типа.

Таким образом, сложились теоретические предпосылки и практическая необходимость разработки и создания систем поддержки управленческих решений во вневедомственной охране ВНГ РФ, которые предлагается реализовать на основе инновационных решений, путем разработки методического аппарата и программного обеспечения в виде экспертных систем, реализующих функции систем поддержки принятия решений, построенных на основе нейронных сетей различной топологии. Подобный подход к повышению эффективности управления во вневедомственной охране ВНГ РФ, насколько известно автору, ранее не применялся, поэтому может быть отнесен к новым научным разработкам.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Об утверждении Наставления по организации службы строевых подразделений вневедомственной охраны войск национальной гвардии Российской Федерации: Приказ Федеральной службы войск национальной гвардии РФ от 28 декабря 2024 г. № 505// «Консультант Плюс»: справочно-правовая система: [сайт]. - URL: <https://www.minjust.consultant.ru> (дата обращения 21.07.2025).
2. Об утверждении Руководства по организации службы центров оперативного управления (групп обеспечения служебной деятельности нарядов) подразделений вневедомственной охраны войск национальной гвардии Российской Федерации: Приказ Федеральной службы войск национальной гвардии Российской Федерации от 6 февраля 2019 г. № 35// «Консультант Плюс»: справочно-правовая система: [сайт]. - URL: <https://www.minjust.consultant.ru> (дата обращения 21.07.2025).
3. Щербакова И.В. Оптимизация процессов обработки информации в деятельности укрупненных пунктов централизованной охраны. Вестник Воронежского института МВД России. - 2016. - №1. – с. 96- 102.
4. Меньших В.В., Калков Д.Ю., Кузнецов А.В. Алгоритм оптимизации маршрутов патрулирования с использованием сервиса онлайн-карт. Вестник Воронежского института МВД России. - 2018. - №4.
5. Правовое регулирование и организация охранной деятельности в Российской Федерации. Стратегические приоритеты и перспективные направления осуществляемых Росгвардией функций по выработке и реализации государственной политики в рассматриваемой области правоотношений: отчет о НИР/ ФКУ «НИЦ «Охрана» Росгвардии. - М., 2025.
6. Бондарев П.А. Основы искусственного интеллекта/П.А. Бондарев, С.К. Колганов. — М.: Радио и связь, 1998. – 123 с.
7. Проскурин Р.А. «Методы использования нейронных сетей для решения задач распознавания образов». Диссертация на соискание ученой степени кандидата технических наук. — М., 1998. - 147 с.

УДК 654.924.32

ПРОШУТИНСКИЙ ДМИТРИЙ АНДРЕЕВИЧ, СТАРШИЙ НАУЧНЫЙ СОТРУДНИК
ФЕДЕРАЛЬНОГО КАЗЕННОГО УЧРЕЖДЕНИЯ «НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
«ОХРАНА» РОСГВАРДИИ

УГРОЗЫ ПРОТИВОПРАВНОГО ПРИМЕНЕНИЯ БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ИМ НА ОБЪЕКТАХ (ТЕРРИТОРИЯХ)

Аннотация. В статье рассмотрены основные угрозы противоправного использования беспилотных воздушных судов, рассматриваются правовые аспекты применения беспилотных воздушных судов, проводится обзор и анализ различных методов обнаружения и противодействия беспилотным воздушным судам.

Ключевые слова: беспилотные воздушные суда, техническое средство противодействия, воздушное пространство, технологии обнаружения и отслеживания беспилотных воздушных судов.

Annotation. The article examines the main threats of the illegal use of unmanned aircraft, examines the legal aspects of the use of unmanned aircraft, reviews and analyzes various technologies for detecting and countering unmanned aircraft.

Keywords: unmanned aircraft, technical means of counteraction, airspace, technologies for detecting and tracking unmanned aircraft.

В современных условиях использование беспилотных воздушных судов (далее – БВС) становится одним из ключевых факторов угрозы безопасности объектов. Развитие беспилотных технологий и доступность БВС в свободной коммерческой продаже обуславливают необходимость комплексного подхода к защите критических важных государственных объектов.

Современные БВС представляют собой многофакторную угрозу для безопасности объектов. К основным рискам относятся, ведение разведки, завоз или вывоз предметов с территории объекта, сброс взрывчатых веществ, взрывных устройств химических, бактериологических, радиоактивных веществ, которые могут привести к масштабным разрушениям и жертвам, полеты БВС вблизи аэродромов могут создавать угрозы для авиационной безопасности.

Также возможная опасность связана с промышленным и военным шпионажем, когда дроны используются фото- и видеокамерами для сбора информации.

Нарушение воздушного пространства вокруг охраняемых объектов большой площади и с протяженным периметром создает риски для безопасности граждан, а психологический фактор от постоянного воздействия отрицательно влияет на работоспособность персонала.

Кроме того, беспилотники могут усложнить перемещение в воздушном пространстве, создав опасность для других воздушных судов, а также

привести к авариям или сбоям в работе аэропортов. В некоторых случаях БВС даже используются для намеренного вмешательства в работу авиационных систем [1].

Перечень основных возможных угроз о применения БВС представлен в таблице 1. Кроме того, БВС могут применяться для наблюдения за отдельными людьми и их поражения.

В современных условиях рост использования БВС в целях совершения противоправных действий требует разработки комплексных мер по их обнаружению и противодействию. Способы противоправного применения БВС определяются рядом факторов: возложенными задачами, особенностями местности применения, тактико-техническими характеристиками БВС, а также уровнем защиты объекта и эффективностью применяемых мер по отражению и противодействию атаке БВС.

Первым и ключевым этапом в борьбе с угрозой со стороны БВС является обнаружение. В зависимости от условий и требуемого уровня безопасности, на каждом объекте возможны различные схемы несанкционированного использования дронов – от простого наблюдения за объектом до заброса взрывчатых веществ или электронных средств, препятствующих функционированию объекта. Сценарии противоправного применения БВС могут включать в себя различные тактические приемы,

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

своевременное противодействие которым требует построения многоуровневой системы защиты, включающей как технические средства

обнаружения, идентификации и сопровождения цели, так и ее нейтрализации.

Таблица 1 – Основные угрозы применения БВС

Вид объекта	Угрозы с применением БВС
Объекты ТЭК	<ul style="list-style-type: none"> – разведка сил охраны; – механическое повреждение опор и других несущих конструкций ЛЭП, распределительных подстанций и другого оборудования электрических сетей, в первую очередь трансформаторов открытого типа; – сброс ВВ и ВУ или применения БВС-камикадзе с ВВ или ВУ во взрыво- и пожароопасных зонах; – распыление (разбрасывание) токопроводящих материалов с целью создания короткого замыкания; – кибератаки через БВС
Объекты транспортной инфраструктуры	<ul style="list-style-type: none"> – разведка сил охраны; – размещение ВВ и ВУ на критических элементах объекта транспортной инфраструктуры; – препятствие деятельности воздушного транспорта, работе навигации, создание аварийных ситуаций, слежение за воздушным движением – кибератаки через БВС
Места массового скопления людей	<ul style="list-style-type: none"> – подрыв боеприпасов с целью поражения людей; – создание шумовых и световых эффектов с целью провоцирования давки; – наведение основных групп террористов на цель; – отвлечение внимания представителей служб безопасности
Сети связи и вещания	<ul style="list-style-type: none"> – механическое повреждение антенно-фидерных устройств и опор (мачты, столбы связи); – распыление электропроводящих материалов для создания пассивных помех средствам связи и вещания; – распыление электропроводящих материалов для создания пассивных помех средствам связи и вещания; – кибератаки через БВС
Объекты большой площади и с протяженным периметром	<ul style="list-style-type: none"> – разведка сил охраны, промышленный, военный шпионаж; – механическое повреждение критических элементов другого оборудования; – сброс ВВ и ВУ или применения БВС-камикадзе с ВВ или ВУ во взрыво- и пожароопасных зонах; – незаконные ввоз или вывоз предметов с территории; – для аграрных комплексов, порча урожая на полях или в местах складирования; – кибератаки через БВС

Для контроля воздушного пространства над охраняемыми объектом используются технические средства, основанные на нескольких принципах:

радиотехнические средства обнаружения, позволяет обнаруживать БВС по радиообмену между дурном и оператором, при передаче сигналов управления, телеметрии бортового оборудования;

оптические и тепловизионные системы позволяют фиксировать визуальные и инфракрасные следы БВС;

акустические датчики фиксируют характерные звуковые волны, издаваемые пропеллерами и двигателями БВС;

системы радиолокационного обнаружения способны обнаруживать дроны на расстоянии до нескольких километров [2].

Особое значение имеет использование интегрированных платформ, объединяющих

данные с различных источников — радаров, видеокамер, тепловизоров и акустических датчиков. Применение многосенсорного обнаружения позволит значительно повысить точность и надежность обнаружения, а также более точно идентифицировать цель.

Кроме того, применение алгоритмов искусственного интеллекта и машинного обучения позволяет проанализировать поведение БВС в момент обнаружения, спрогнозировать траекторию его полета и оценить уровень угрозы. Это позволяет автоматизировать процесс принятия решений и минимизировать время реакции.

После обнаружения и идентификации выявления БВС, применяются меры противодействия. К ним относятся:

нарушение каналов связи — блокировка радиосигналов между БВС и оператором, что приводит к потере управления;

подавление спутниковых навигационных систем (GPS/ГЛОНАСС и т.д.), что затрудняет автономный полет и может вызвать аварийную посадку;

физическая нейтрализация – перехват дронов с помощью сетей, лазерных или микроволновых установок, огнестрельного оружия, управляемых ракетных систем или БВС-перехватчиков [2].

Таким образом, эффективная защита от БВС строится на последовательной и логически выстроенной цепочке: от обнаружения с использованием многофункциональных датчиков

и интеллектуального системного анализа, идентификации типа цели и степени угрозы к ней, до нейтрализации с применением соответствующих контрмер. Только такой комплексный подход позволяет обеспечить надежную защиту объектов от БВС в условиях постоянно меняющихся угроз.

Основные преимущества и недостатки физических методов обнаружения БВС приведены в таблице 2.

Таблица 2 – Преимущества и недостатки методов обнаружения БВС

Физический метод обнаружения	Преимущества	Недостатки
Радиолокационный	Дальность действия может достигать нескольких километров. Настройки позволяют отфильтровывать помехи: птиц, других ЛА	На территориях со сложным рельефом могут возникать участки радиотени, препятствующие обнаружению БВС, особенно в городских условиях и на местности со сложным рельефом, сложность обнаружения БВС, двигающихся на предельно малой высоте, в определенных скоростных режимах
Оптический и ИК	Невосприимчивость к шуму, обнаружение небольших БВС, летящих на малой высоте	Сравнительно небольшой радиус действия, снижение эффективности ночью и в плохих метеоусловиях Примечание. В наименьшей степени подвержен атмосферным воздействиям ИК-канал наблюдения с длиной волны 8-12 мк
Акустический	Низкая стоимость отдельных датчиков, невосприимчивость к препятствиям (деревьям, проводам и т. д.), низкая заметность	Чувствительность к уровню фонового шума, низкая дальность действия, в связи с этим потребность в насыщении большим количеством сенсоров, необходимость значительных вычислительных мощностей
Радиотехнический	Невосприимчивость к уровню фонового шума, условиям ограниченной видимости	Не эффективен против БВС, совершающих полет в автономном режиме по заранее запрограммированному заданию

Для нейтрализации управления БВС применяются стационарные радиоэлектронные комплексы, которые глушат радиосигналы в круговом направлении и прерывают каналы обмена информацией между оператором и БВС. Одновременно используются кинетические методы воздействия, а также активно разрабатываются лазерные и микроволновые системы противодействия.

К кинетическим методам относятся как поражение БВС специальными боеприпасами, ракетами, так и выстрелы сетью для физического захвата БВС.

Кроме того, в последнее время получило развитие направление по разработке специальных БВС, которые атакуют аппараты нарушители в воздушном пространстве, с целью сбить или повредить БВС-нарушитель.

Еще одним методом борьбы с БВС является GPS-спуфинг, который работает путем отправки

ложных координат для принудительного посадки или возврата дрона.

Лазерные системы путем фокусировки на БВС высокомоощных лазеров повреждают его электронику или силовую установку.

При этом наблюдаются следующие тенденции, лазерные системы применяются для точечного воздействия на БВС, особенно на автономные и FPV-модели, микроволновые системы показывают свою эффективность против групп (роя) БВС.

Для противодействия БВС применяются также кибератаки осуществляющиеся путем взлома управления дроном через уязвимости в протоколах связи (например, перехват и подмена командных сигналов).

На основании данных, приведенных в таблице 3 можно провести анализ эффективности и возможности комбинирования различных методов противодействия БВС.

Таблица 3 – Анализ различных методов по противодействию БАС

Возможности	Дальность действия	Возможность противодействия групповой атаке	Возможность противодействия БВС, осуществляющим полет в режиме автопилота	Устойчивость к климатическим воздействиям	Эффективность вне зоны прямой видимости	Возможность применения по низколетящим целям в условиях урбанистической застройки
Физический принцип						
Акустический	Низкая	+	+	-	-	-
Лазерный	Высокая	-	+	-	-	-
Микроволновой	Низкая	-	+	+	-	-
Радиоэлектронный	Высокая	+	+/-	+	+/-	+
Перехват управления	Высокая	+/-	-	+	+/-	+
Кинетический	Средняя	+	+	+	+/-	+

В тоже время нельзя пренебрегать организационными и правовыми мерами, как-то создание запретных зон вокруг критически важных объектов (аэропорты, энергетические комплексы) строго ограничивающие полеты БВС. Персонал объектов должен регулярно обучаться и тренироваться порядку действий при

обнаружении БВС, включая протоколы эвакуации и уведомления спецслужб.

Современные технические решения позволяют объединять все этапы от раннего обнаружения и идентификации БВС до нейтрализации угроз, что позволяет создавать единую «цепочку» защиты.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. <https://k-radio.ru/blog/ugrozy-i-sredstva-zashchity-ot-ispolzovaniya-dronov/> Угрозы и средства защиты от дронов.
2. Макаренко С. И. Анализ средств и способов противодействия беспилотным летательным аппаратам // Systems of Control, Communication and Security №3. 2020.

УДК 654.9
ББК 30ц

РЯБЦЕВ НИКОЛАЙ АЛЕКСЕЕВИЧ, НАЧАЛЬНИК ОТДЕЛА РАЗВИТИЯ СРЕДСТВ ОБНАРУЖЕНИЯ ФЕДЕРАЛЬНОГО КАЗЕННОГО УЧРЕЖДЕНИЯ «НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР «ОХРАНА» РОСГВАРДИИ, КАНДИДАТ ТЕХНИЧЕСКИХ НАУК

О НЕКОТОРЫХ ВОПРОСАХ СОЗДАНИЯ И ПРИМЕНЕНИЯ ЗВУКОВЫХ ИЗВЕЩАТЕЛЕЙ СИСТЕМЫ ОХРАННОЙ СИГНАЛИЗАЦИИ

Аннотация. В докладе рассмотрены вопросы создания и применения звуковых извещателей системы охранной сигнализации. Рассмотрены возможные механизмы нивелирования особенностей распространения акустических волн в процессе разработки извещателей и основные факторы, влияющие на работу извещателей при их применении на охраняемых объектах.

Ключевые слова: охранная сигнализация, средство обнаружения, извещатель, звук.

RYABTSEV NIKOLAY ALEKSEEVICH, HEAD OF THE DETECTION TOOLS DEVELOPMENT DEPARTMENT OF THE FEDERAL STATE INSTITUTION «SCIENTIFIC RESEARCH CENTER «OKHRANA» OF THE FEDERAL SERVICE OF NATIONAL GUARD OF THE RUSSIAN FEDERATION, CANDIDATE OF TECHNICAL SCIENCES

ON SOME ISSUES OF THE DEVELOPMENT AND USE OF SOUND DETECTORS FOR SECURITY ALARM SYSTEMS

Annotation. This report examines the development and use of sound detectors for security alarm systems. It examines possible mechanisms for mitigating the propagation of acoustic waves during detector development and the main factors influencing detector performance when used at protected facilities.

Keywords: security alarm, detection device, detector, sound.

Успешное применение звуковых извещателей зависит как от технических характеристик, заложенных в сами извещатели при их разработке, так и от их корректного применения на охраняемых объектах.

При создании звуковых извещателей, как и иных средств обнаружения, необходимо повышать степень достоверности обнаружения разрушающего воздействия на стеклянное полотно (минимизировать ложные сигналы тревог) [1], которые, в свою очередь напрямую зависят от ряда параметров.

Во-первых, набор информационных признаков, обрабатываемых извещателем, должен адекватно характеризовать тревожное событие.

Во-вторых, логическая схема обработки данных признаков должна учитывать особенности распространения акустических волн, возникающих при разрушении стеклянного полотна, и не допускать пропуска обнаружения нарушителя [2]. Рассмотрим подробнее наиболее значимые из них и возможные механизмы их минимизации.

Сигнал максимальной амплитуды, возникающий

при разрушении стекла – полезный сигнал, и помехи при неразрушающих случайных ударах по стеклу находятся в одной области средних частот [3].

В связи с чем целесообразно увеличивать количество анализируемых информационных признаков полезного сигнала, т.к. при этом (в случае их независимости) вероятность обнаружения извещателем разрушения стекла P_0 будет определяться произведением вероятностей их появления:

$$P_0 = \prod_{i=1}^n P_{i0}, \quad (1)$$

где, P_{i0} – вероятность появления в сигнале i -го признака;

n – количество анализируемых признаков.

К таким признакам следует отнести характер протекания полезного сигнала, особый вид возникающего энергетического спектра, порядок фаз разрушения стекла, наличие звука выпадения осколков и др.

Высокая вероятность девиации параметров

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

возникающего при разрушении стекла сигнала акустической эмиссии связанная с наличием множества таких факторов как марка стекла, его габаритные размеры и номинальная толщина, предельные отклонения по толщине и разнотолщинность, способы закрепления и разрушения, окружающая акустическая обстановка и многими другими.

С целью повышения обнаружительной способности P_0 и снижения вероятности ложного сигнала тревоги $P_{лст}$ анализ параметров сигнала необходимо проводить, следуя мажоритарной логике «N из M». Так, для двух анализируемых параметров в случае равенства вероятностей присутствия в каждом из них полезного признака k из общего количества анализируемых признаков n сигнала цепи 0,85 при использовании логического умножения по схеме «И» вероятность обнаружения P_0 составит $\approx 0,72$, а $P_{лст} \approx 0,28$. В тоже время при мажоритарной логике «2 из 3» ($k+1$) вероятность обнаружения составит $\approx 0,94$, а при логике «2 из 4» ($k+2$) – уже порядка 0,98 (рисунки 1 и 2).

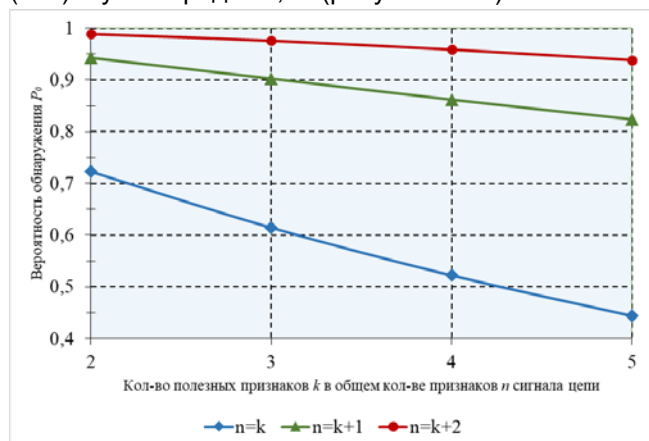


Рисунок 1 – Зависимость вероятности обнаружения от вида применяемой логической схемы и количества анализируемых полезных признаков

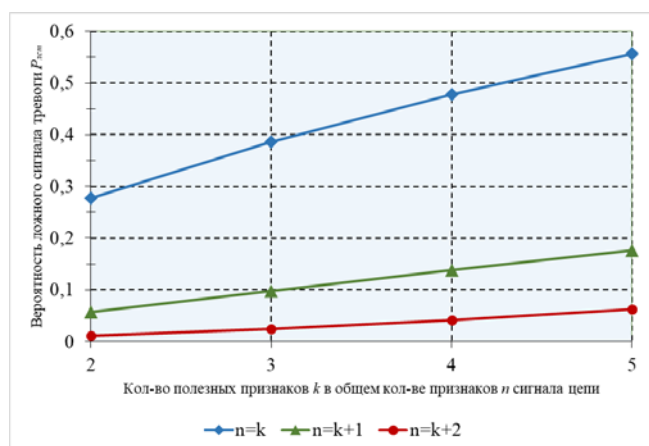


Рисунок 2 – Зависимость вероятности ложного сигнала тревоги от вида применяемой логической схемы и количества анализируемых полезных признаков

Для выполнения второго условия успешного функционирования извещателей – их корректного применения на охраняемых объектах, кроме вышеуказанных факторов, учитываемых при разработке, необходимо корректно осуществлять выбор места установки, монтаж и настройку при их применении. Рассмотрим основные требования по применению извещателей. Параметры обнаружения, помехозащищенности и устойчивости к воздействиям окружающей среды (диапазоны рабочих температур и относительной влажности окружающего воздуха) извещателей должны соответствовать условиям эксплуатации, представленным в эксплуатационной документации.

Место установки извещателя должно исключать воздействие на извещатели акустических, вибрационных и электромагнитных помех.

При этом при невозможности исключить потенциальные источники звуковых помех в помещении рекомендуется проверить их влияние на извещатели практическим путем и выбрать место установки таким образом, чтобы минимизировать их влияние.

Для исключения вибрационных помех, вызванных вибрацией строительной конструкции, на которой установлен извещатель, необходимо исключить установку извещателей на некапитальных строительных конструкциях, таких как гипсобетонные, фанерные или деревянные перегородки, а также на строительных конструкциях, в которые встроено или рядом с которыми установлено климатическое или промышленное оборудование, которое может создавать вибрацию.

Учет рекомендаций при создании и применении извещателей позволяет обеспечить высокую обнаружительную способность, высокие параметры помехозащищенности и обеспечить надежную охрану объектов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Рябцев Н. А. О вероятности обнаружения нарушителя системой тревожной сигнализации / Н.А. Рябцев, Т.А. Буцынская // Технологии техносферной безопасности. – 2017. – № 1(71). – С. 312-316.
2. Климов А.В. Противокриминальная защита остекленных конструкций / А.В. Климов, Н.А. Рябцев, В.А. Козлов // Алгоритм безопасности. – 2015. – № 4. – С. 6-8.
3. Никитин А.А., Членов А.Н., Климов А.В. Звуковые извещатели охранной сигнализации / Под ред. д-ра техн. наук проф. Членова А.Н. – М.: ФКУ НИЦ «Охрана» МВД России, 2015. – С. 5–9.

УДК 629.746

**АНДРЕЙ СЕРГЕЕВИЧ СБРОДОВ, КАНДИДАТ ТЕХНИЧЕСКИХ НАУК, ВОЕННАЯ ОРДЕНА
ЖУКОВА АКАДЕМИЯ ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ,
САНКТ-ПЕТЕРБУРГ, РОССИЯ**

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ В СИСТЕМЕ ОХРАНЫ ВАЖНЫХ ГОСУДАРСТВЕННЫХ ОБЪЕКТОВ

Аннотация. Статья посвящена актуальной проблеме совершенствования систем охраны важных государственных объектов охраняемых войсками национальной гвардии с применением беспилотных летательных аппаратов как перспективных средств ведения разведки и передачи информации. Исходя из специфики важных государственных объектов (протяженности периметров, наличия водоохраных зон, производства и хранения на их территориях вооружения, радиоактивных и химических веществ), применение беспилотных воздушных аппаратов позволит минимизировать «человеческий фактор» при принятии мер по недопущению на охраняемый объект нарушителей.

Ключевые слова: важный государственный объект, система охраны, беспилотный летательный аппарат, техническое средство охраны.

**ANDREY S. SBRODOV, CANDIDATE OF SCIENCES (TECHNOLOGY), MILITARY ORDER OF ZHUKOV
ACADEMY OF THE NATIONAL GUARD TROOPS OF THE RUSSIAN FEDERATION, SAINT-PETERSBURG,
RUSSIA**

PROSPECTS FOR THE USE OF UNMANNED AERIAL VEHICLES IN THE SYSTEM OF
PROTECTION OF IMPORTANT STATE FACILITIES

Annotation. The article is devoted to the actual problem of improving the systems of protection of important state facilities protected by the National Guard troops using unmanned aerial vehicles as promising means of reconnaissance and information transmission. Based on the specifics of important state facilities (the length of the perimeters, the presence of water protection zones, the production and storage of weapons, radioactive and chemical substances on their territories), the use of unmanned aerial vehicles will minimize the "human factor" when taking measures to prevent intruders from entering the protected facility.

Keywords: important state facility, security system, unmanned aerial vehicle, technical means of security.

Одной из задач, возложенных на войска национальной гвардии Российской Федерации, определенной Федеральным законом от 3 июля 2016 г. N 226-ФЗ "О войсках национальной гвардии Российской Федерации", является охрана важных государственных объектов, специальных грузов, сооружений на коммуникациях в соответствии с перечнями, утвержденными Правительством Российской Федерации [2, 9, 10].

Сложность решения стоящей перед войсками национальной гвардии Российской Федерации задачи по охране важных государственных объектов, специальных грузов, сооружений на коммуникациях определяется специфическими особенностями важных государственных объектов: обширной территорией с протяжённым периметром, относительно высокой плотностью зданий и сооружений, расположение в крупных городах, наличие регионов регулярных природных чрезвычайных ситуаций (землетрясений,

наводнений, тайфунов и ураганов, крупных лесных пожаров).

Важнейшими из них являются объекты атомной промышленности – атомные электростанции, в связи с тем, что аварии на них могут приводить к большим человеческим жертвам, крупномасштабному загрязнению окружающей среды и большим экономическим потерям, наличие водных акваторий затрудняет выполнение войсками задач.

В условиях сложной международной и непростой общественно-политической и социальной обстановки внутри страны в период проведения специальной военной операции [3, 11], постоянного противодействия силовых структур Российской Федерации проведению нарушителями (незаконными вооружёнными формированиями) террористических актов (в том числе в отношении охраняемых войсками национальной гвардии важных государственных объектов), постоянно

совершенствующейся тактики действий противника с связи с использованием современных технологий, возрастает необходимость постоянного мониторинга обстановки относительно ограниченной численностью личного состава выполняющего задачи по охране важных государственных объектов, обеспечивая сохранение их жизни и здоровье.

Решение задач по предупреждению, своевременному обнаружению, реагированию и нейтрализации несанкционированных действий нарушителей на важных государственных объектах, в соответствии с постановлением правительства Российской Федерации от 27 мая 2017 г.

№ 646дсп возложено на систему физической защиты, в которую входят система охраны, а также организационные мероприятия, направленные на её адаптацию в условиях постоянно меняющихся наиболее вероятных угроз безопасности (моделей нарушителя). Важнейшей составляющей системы охраны является комплекс инженерно-технических средств охраны.

С 1 января 2025 года вступили в силу пункты 19 и 23 постановления правительства РФ от 18.01.2023 № 45 «о внесении изменений и дополнений в постановление правительства № 646дсп», в них определено, что противодействие БПЛА является задачей комплекса инженерно-технических средств охраны, соответственно администрации объектов к этому сроку обязаны обеспечить необходимыми средствами.

Спецификой важных государственных объектов является охрана с привлечением значительного количества личного состава, располагающегося вблизи запретной зоны, в настоящее время требует поиска наиболее эффективных путей улучшения работы по заблаговременному предупреждению и выявлению действий нарушителей (вероятного противника) на ближних подступах, а в случае их проникновения – на территории объекта. В указанных условиях перспективным будет использование новейших технологий, комплексного применения сил и средств, а также методов, направленных на предупреждение, выявление и локализацию деятельности нарушителей. Известно, что выполнение данных задач связано с большим риском, требует высочайшей подготовки личного состава, совершенствования используемых технических средств, способов их применения. Для дистанционного мониторинга потенциально опасных территорий и зон охраняемых объектов,

контроля труднодоступных участков целесообразно использовать роботизированные системы, способные в реальном масштабе времени передавать соответствующим органам управления информацию об их состоянии для принятия оперативных и адекватных мер [5].

Использование беспилотных летательных аппаратов (БПЛА) в качестве вспомогательного элемента комплекса ИТСО важного государственного объекта минимизирует так называемый «человеческий фактор» [1]. Любой, даже самый опытный военнослужащий (сотрудник), находясь на дежурстве, может что-то пропустить или не заметить при несении службы, а высокотехнологичный «гаджет», оснащённый необходимым современным оборудованием, ничего не пропустит и не оставит без внимания, позволяет своевременно реагировать на различные угрозы и повысить эффективность профилактических мероприятий по предотвращению правонарушений, обеспечивая «управляемый» мониторинг в отдалённых зонах охраняемых объектов, в том числе использоваться для противодействия БПЛА нарушителей.

Расширение служебно-боевой деятельности войск национальной гвардии, изменение моделей угроз и возрастание сложности выполняемых задач ставят жёсткие требования по повышению эффективности охраны ВГО [3]. В связи с вышеизложенным, применение беспилотных летательных аппаратов в системах охраны важных государственных объектов является весьма актуальным.

Масштабное применение БПЛА самолетного, мультироторного и вертолетного типов, различных классов и тактико-технических характеристик [4], прежде всего, связано с быстрым развитием современных технологий в сфере производства оптического и акустического оборудования, систем дистанционного управления, навигации, приёма и передачи информации, позволит использовать БПЛА в целях:

- контроля периметра запретной зоны охраняемого объекта и прилегающей территории;
- контроля за территорией внутри охраняемого объекта и при природных и техногенных катастрофах;
- при попытке нарушителя проникнуть (покинуть) охраняемый объект;
- при срабатывании рубежей средств охранной сигнализации для установления причин.

Кроме того, по команде начальника караула под управлением оператора, перспективой применения БПЛА может быть контроль выявления

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

направления движения вероятных нарушителей, состояния.

Создание нового образца БПЛА или принятие на вооружение существующего для применения в составе систем охраны ВГО, ведёт к необходимости разработки чёткой формулировки выполняемых задач и требований, в которых должны быть всесторонне учтены современный уровень развития и пути совершенствования.

Перспективными задачами на БПЛА в системе охраны ВГО, например атомной электростанции, в применимых в интеграции с другими охранными системами, могут быть [4, 6]:

непрерывная разведка, в том числе и инженерная, передача цифровой информации, обнаружение подозрительных объектов, предметов и людей;

фото и видео съёмка, передача в режиме реального времени сигнала с регистрацией;

разведка объектов как в тёмное время суток, так и скрытых объектов, с применением с тепловизора;

решение задач инженерного обеспечения и тактических задач по охране периметра объекта, охране объектов, патрулирование периметра;

обследование отдельных зданий на охраняемом объекте;

доставка в указанное место различных малогабаритных грузов с возможностью их самостоятельного (без помощи человека) отцепа (сброса);

оценка результатов применения огневых (специальных) средств летального и нелетального действия;

мониторинг местности, формирования цифровых моделей местности, в целях контроля различных объектов, оборудуемых вероятным нарушителем на территории, граничащей с охраняемым объектом;

лазерная подсветка обнаруженного объекта и локальное освещение объекта (нарушителя) при его сопровождении;

контроль уровня радиации охраняемого объекта;

предварительная инженерная разведка больших участков местности на предмет обнаружения самодельных взрывных устройств (электронных систем управления СВУ) при проведении специальных мероприятий;

действие в составе наземных мобильных (роботизированных) комплексов обнаружения самодельных взрывных устройств, возможность координатной и визуальной привязки обнаруженного места установки самодельного взрывного устройства, возможность предметного осмотра требуемого участка местности (путём зависания), передача данных с борта беспилотного

летательного аппарата на пункт управления в реальном масштабе времени;

наблюдение за выбранным объектом в непосредственной близости от него, в том числе и скрытное;

осмотр объектов, которые представляют повышенную опасность для человека, включая ядерные, взрывоопасные и токсичные;

противодействие БПЛА.

Кроме того, рассмотренные задачи, БПЛА должны быть способны выполнять и в автоматическом режиме.

Основные требования, предъявляемые к БПЛА, должны соответствовать каждому из «Общих требований», определяемых назначением образца и выполняемыми задачами, такими как: скорости и дальности полёта, взлётной массе, массе полезной нагрузки, продолжительности полёта, безопасности применения, малой радиолокационной, инфракрасной, оптической и акустической заметности, а также частным [7, 8]:

технические требованиями к конструкции БПЛА: прочность при всех возможных в полёте и при посадке нагрузках, жёсткость, малая масса изделия, простота и удобство технической эксплуатации, дешевизна изготовления и ремонта конструкции, применение недефицитных материалов, надёжность (вероятность безотказной работы, средняя наработка на отказ, технический (средний) ресурс и срок сохраняемости установленных характеристик;

требованиями к полезной нагрузке для БПЛА: взаимозаменяемость устройств и приборов полезной нагрузки, простота установки, использование унифицированных каналов связи и передачи данных, высокая точность, сохранение устойчивости функционирования, надёжное хранение и съём полученной информации на установленные виды носителей;

требования к комплектному применению: комплект БПЛА - совокупность функционально взаимосвязанных технических средств, обеспечивающих применение, подготовку БПЛА к применению и обслуживание.

Исходя из вышеизложенного следует, что выполнение задач охраны ВГО с применением в их системах охраны БПЛА позволит повысить безопасность применения сил охраны объектов, достичь максимального уровня скрытности, мобильности, точности и оперативности.

Учитывая актуальность защиты ВГО, охраняемых войсками национальной гвардии, современные тенденции развития робототехнических средств, предлагается определить некоторые перспективные направления, позволяющие внедрить БПЛА

в системы охраны объектов и повысить их эффективность применения, например:

внедрение искусственного интеллекта, позволяющего проводить анализ получаемой информации об обнаруженном объекте, распознать его и идентифицировать, а также производить мониторинг местности, формирования цифровых моделей;

создание автономных БПЛА, интегрированных в систему охраны, способных без участия человека прибывать в район срабатывания средств охранной сигнализации и определять причины, передавать информацию и оказывать помощь силам охраны в контроле перемещения нарушителей по территории охраняемого объекта;

повышение устойчивости применяемых на ВГО беспилотных летательных аппаратов к средствам радиоэлектронной борьбы;

техническое совершенствование применяемых полезных нагрузок;

развитие систем дистанционного управления, навигации, приёма и передачи информации.

Таким образом, учитывая сложность международной и общественно-политической и социальной обстановки, применение новых технологий нарушителями, современные тенденции развития робототехники и электроники в стране и в мире, применение беспилотных летательных аппаратов в системах охраны важных государственных объектов, является перспективным направлением совершенствования и разработки новых подходов к построению существующих систем охраны, позволит выполнить широкий спектр задач по предупреждению, своевременному обнаружению, реагированию и нейтрализации несанкционированных действий нарушителей на важных государственных объектах, а также других задач охраны связанных с риском для жизни и здоровья военнослужащих (сотрудников), минимизировать «человеческий фактор» при принятии решения во взаимосвязи с возможностями технической реализации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Курилов А.В., Сбродов А.С., Яшин М.Г. Беспилотные летательные аппараты в составе комплекса инженерно-технических средств охраны охраняемых объектов: Сборник статей V-ой международной научно-практической конференции инновационная железная дорога. Новейшие и перспективные системы обеспечения движения поездов. Проблемы и решения. Санкт-Петербург, Петергоф, 2022. С. 257-265.
2. Постановление Правительства РФ от 7 марта 1997 г. N 264 «Об утверждении правил физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов».
3. Применение беспилотных летательных аппаратов в современных военных конфликтах / Р. А. Павлов, К. П. Савельев. — Текст: непосредственный // Молодой учёный. — 2022. — № 51 (446). — С. 48-50. — URL: <https://moluch.ru/archive/446/98257/> (дата обращения 05.08.2025).
4. Ростопчин В.В. ООО «Техкомтех» Современная классификация беспилотных авиационных систем военного назначения [Электронный ресурс] – режим доступа: <http://www.uav.ru/articles/bas.pdf.html> (дата обращения: 05.08.2025).
5. Сбродов А.С., Перспективы применения мультисредних робототехнических комплексов на охраняемых объектах. Сборник: Применение робототехнических средств и комплексов в боевом обеспечении войск национальной гвардии Российской Федерации. Круглый стол в рамках региональной выставки: сборник научных статей. Санкт-Петербург, СПВИ войск национальной гвардии, 2024. С. 6-13.
6. Сбродов А.С., Архипов В.Л., Применение беспилотных воздушных судов для повышения уровня защищённости охраняемых объектов: Сборник научных статей. Применение беспилотных воздушных судов при выполнении служебно-боевых задач войсками национальной гвардии. Санкт-Петербург, СПВИ войск национальной гвардии, 2023. С. 7-13.
7. Сбродов А.С., Курилов А.В., Применение радиолокационных средств для обнаружения малых беспилотных воздушных судов: Сборник научных статей II Межведомственной научно-практической конференции с международным участием. В 2-х частях. Под общей редакцией В.В. Косу-хина. Новосибирск, 2023. С. 238-242.
8. Сбродов А.С. Основные требования, предъявляемые к беспилотным летательным аппаратам, применяемым в составе комплекса инженерно-технических средств охраны важных государственных объектов: Сборник Проблемы технического обеспечения войск в современных условиях. Труды V межвузовской научно-практической конференции. 2020. С. 488-492.
9. Федеральный закон Российской Федерации от 21 ноября 1995 г. № 170-ФЗ «Об использовании атомной энергии»;
10. Федеральный закон от 03.07.2016 № 226-ФЗ (ред. от 31.07.2025) «О войсках национальной гвардии Российской Федерации».
11. Яцук К.В., Стафеев М.С., Казаринов С.В. Применение беспилотных летательных аппаратов в локальных конфликтах и войнах // Молодой ученый. - 2016. - № 25.

УДК 355.233

**СЕМЕНОВ КОНСТАНТИН ПЕТРОВИЧ, КАНДИДАТ ТЕХНИЧЕСКИХ НАУК, ДОЦЕНТ,
НАЧАЛЬНИК КАФЕДРЫ МАТЕМАТИКИ И ИНФОРМАТИКИ САРАТОВСКОГО ВОЕННОГО
ОРДЕНА ЖУКОВА КРАСНОЗНАМЕННОГО ИНСТИТУТА ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ В СИСТЕМЕ ОХРАНЫ ВАЖНЫХ ГОСУДАРСТВЕННЫХ ОБЪЕКТОВ

Аннотация. В статье рассматривается современное состояние и перспективы развития цифровизации образования и цифровой трансформации образовательной деятельности военных образовательных организаций высшего образования войск национальной гвардии Российской Федерации.

Ключевые слова: цифровизация, цифровая трансформация, образовательная деятельность, цифровые технологии, военные образовательные организации высшего образования.

Образованность в современном социуме является важным маркером успеха и конкурентоспособности человека в профессиональной и социальной сферах. Поэтому значительную роль играет не только доступность образования для граждан, но и его качество, на которое напрямую влияют используемые в образовательном процессе инновации и передовые технологии.

Одной из таких инноваций является цифровизация образования, которая активно развивается в Российской Федерации через государственные и национальные программы и проекты. Так, например, государственная программа Российской Федерации «Развитие образования» [1], которая одной из задач определяет внедрение принципов цифровизации в деятельность системы образования, предполагающее развитие различных цифровых инструментов и сервисов и создание условий для их использования в образовательных организациях, повышение квалификации педагогических работников в области цифровых технологий, искусственного интеллекта. Согласно данной программе, безопасная цифровая образовательная среда с проверенным контентом будет дополнять традиционную систему образования, обеспечивая равные возможности для получения качественного образования на всей территории Российской Федерации.

Согласно мнению современных ученых, основными достижениями цифровизации образования являются:

- 1) электронное обучение в режиме онлайн;
- 2) интерактивные образовательные платформы;
- 3) компьютерное тестирование и оценка знаний;
- 4) персонализированное обучение;
- 5) применение элементов виртуальной реальности (VR) и дополненной реальности (AR).

Более подробно содержание вышеуказанных достижений и их влияние на образовательный процесс расписано в [2].

Смежным, но несколько отличающимся

от цифровизации, является понятие цифровой трансформации. Цифровая трансформация - совокупность действий, осуществляемых государственным органом, направленных на изменение (трансформацию) государственного управления и деятельности государственного органа по предоставлению им государственных услуг и исполнению государственных функций за счет использования данных в электронном виде и внедрения информационных технологий в свою деятельность.

В рамках организации проекта цифровой трансформации Росгвардии, на основании решения заместителя директора Федеральной службы войск национальной гвардии Российской Федерации – главнокомандующего войсками национальной гвардии Российской Федерации от 30.11.2023 г. по служебной записке от 23.11.2023 г. № 1/8152-дз «Об инициировании создания информационной системы», в войсках национальной гвардии с 2024 года создается информационная система автоматизации процессов образовательной деятельности ведомственных образовательных организаций.

Согласно проектной документации, указанная система предназначена для автоматизации процессов образовательной деятельности образовательных организаций Росгвардии, планируется к использованию должностными лицами Росгвардии — участниками образовательной деятельности, и создается в целях:

1) повышения эффективности информационной поддержки образовательной деятельности ведомственных образовательных организаций на всех уровнях за счет реализации непосредственного доступа к хранимой и обрабатываемой информации, создания единого порядка работы и средств обмена информацией;

2) обеспечения аналитической поддержки образовательной деятельности ведомственных образовательных организаций с использованием

современных методов обработки информации, в том числе сокращения времени принимаемых решений с одновременным повышением их качества и результативности;

3) унифицирования данных, сокращения их избыточности и дублирования первичного ввода информации, уменьшения объема бумажного документооборота;

4) усовершенствования организации и планирования образовательной деятельности за счет внедрения специализированного для работы программного продукта;

5) обеспечения требуемого качества процессов, автоматизируемых в рамках функционирования информационной системы.

Предметами автоматизации должны являться:

- 1) организация образовательной деятельности;
- 2) планирование образовательной деятельности;
- 3) динамическое ведение списков должностных лиц — участников образовательной деятельности;
- 4) составление расчета нагрузки и распределение ее по педагогическим работникам;
- 5) проведение мероприятий приемной компании;
- 6) отображение, управление и внесение информации, необходимой для участников образовательной деятельности;
- 7) отображение, управление и внесение информации о личных достижениях участников образовательной деятельности;
- 8) составление расписания учебных занятий;
- 9) ведение и учет данных обучающихся;
- 10) ведение динамической информации об образовательной деятельности и разграничение зоны ответственности участников образовательной деятельности;
- 11) создание и хранение систематизированных учебно-методических материалов и инструментов контроля;

12) применение в образовательной деятельности электронного обучения, дистанционных образовательных технологий при реализации образовательных программ;

13) осуществление систематической проверки уровня знаний обучающихся;

14) отслеживание динамики и оперативный контроль ключевых показателей образовательной деятельности за образовательные организации.

23 сентября 2024 года между ФГКУ «ГЦИТ войск национальной гвардии» и ООО «МТ - ГРУПП» был заключен Государственный контракт № 0373100001324000021-01, в рамках которого ООО «МТ-ГРУПП» обязалась создать информационную систему автоматизации

процессов образовательной деятельности ведомственных образовательных организаций Росгвардии, получившую сокращенное обозначение ИС «Образование».

Этапы реализации Государственного контракта:

1. Разработка специального программного обеспечения и установка его на серверное оборудование заказчика (сентябрь-ноябрь 2024 г.)

2. Автономные предварительные испытания ИС «Образование» силами разработчика (13 ноября 2024 г.)

3. Доработка специального программного обеспечения по результатам автономных предварительных испытаний (14 ноября - 8 декабря 2024 г.)

4. Опытная эксплуатация ИС «Образование» должностными лицам Росгвардии (9 -27 декабря 2024 г.)

5. Доработка специального программного обеспечения по результатам опытной эксплуатации (28 декабря 2024 г. - 16 марта 2025 г.)

6. Ведомственные испытания ИС «Образование» комиссией Росгвардии (17 марта - 11 апреля 2025 г.)

7. Доработка специального программного обеспечения по результатам ведомственных испытаний (12 апреля 2025 г. - н.в.)

ИС «Образование» реализована как web-приложение и запускается как вкладка в браузере. Рекомендуется использовать браузеры «Mozilla Firefox» и «Яндекс.Браузер» актуальной версии из состава официального репозитория ОС СН «Astra Linux», разрешенные для использования в Росгвардии. В настоящее время система развернута на серверном оборудовании ГЦИТ Росгвардии (г. Москва, ул. Красноказарменная 9) в составе 4-х автономных серверов (по одному для каждой военной образовательной организации высшего образования Росгвардии). Доступ к соответствующему серверу ИС «Образование» предоставляется должностным лицам военных образовательных организаций по учетным данным (логину и паролю) доступа в ЕИП Росгвардии (рис. 1, показано зеленым). Специальной авторизации система не требует.

При нажатии на ссылку соответствующей военной образовательной организации (рис. 1, показано красным) происходит автоматическое подключение пользователя к соответствующему серверу, авторизация пользователя в соответствии с его учетными данными ЕИП Росгвардии и отображается главная страница подсистемы Алекс-ВУЗ (рис. 2).

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

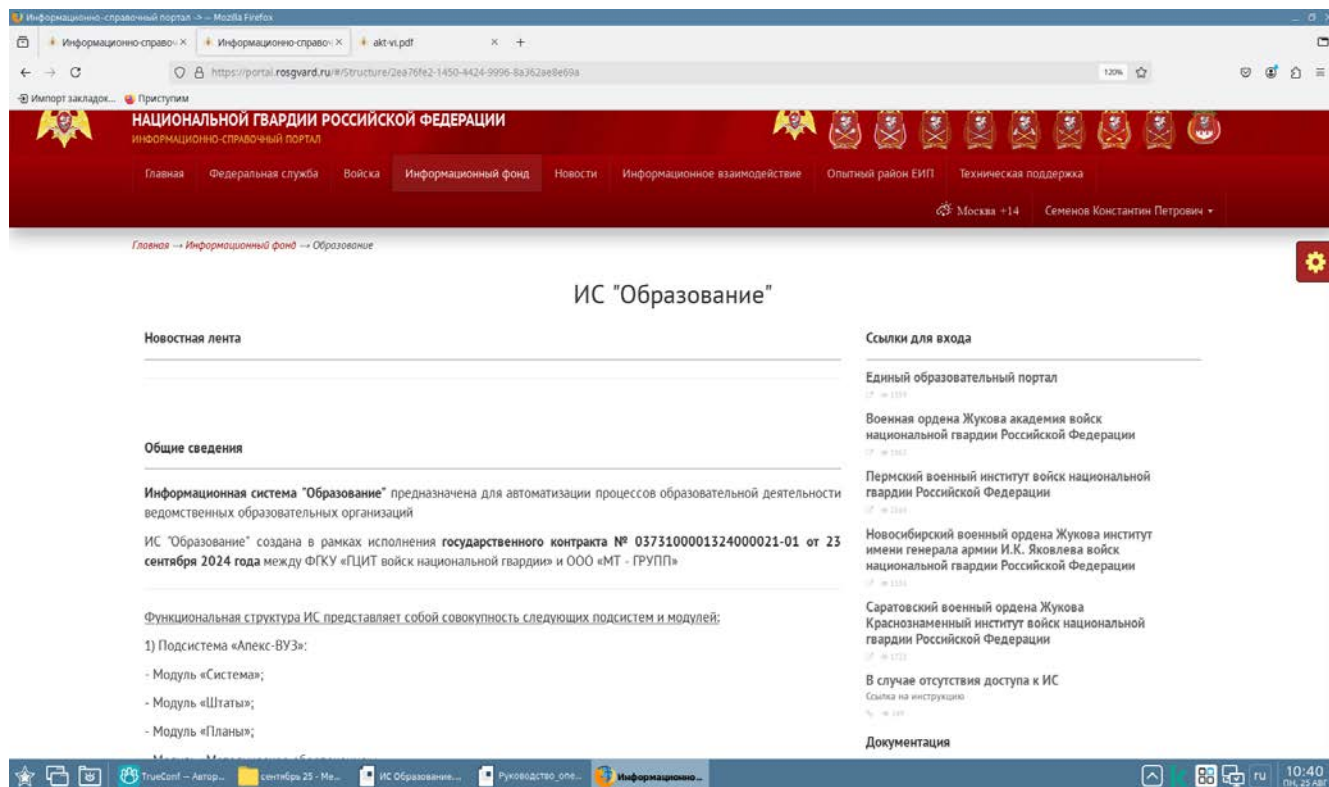


Рисунок 1. Вход в ИС «Образование» через портал ЕИП Росгвардии.

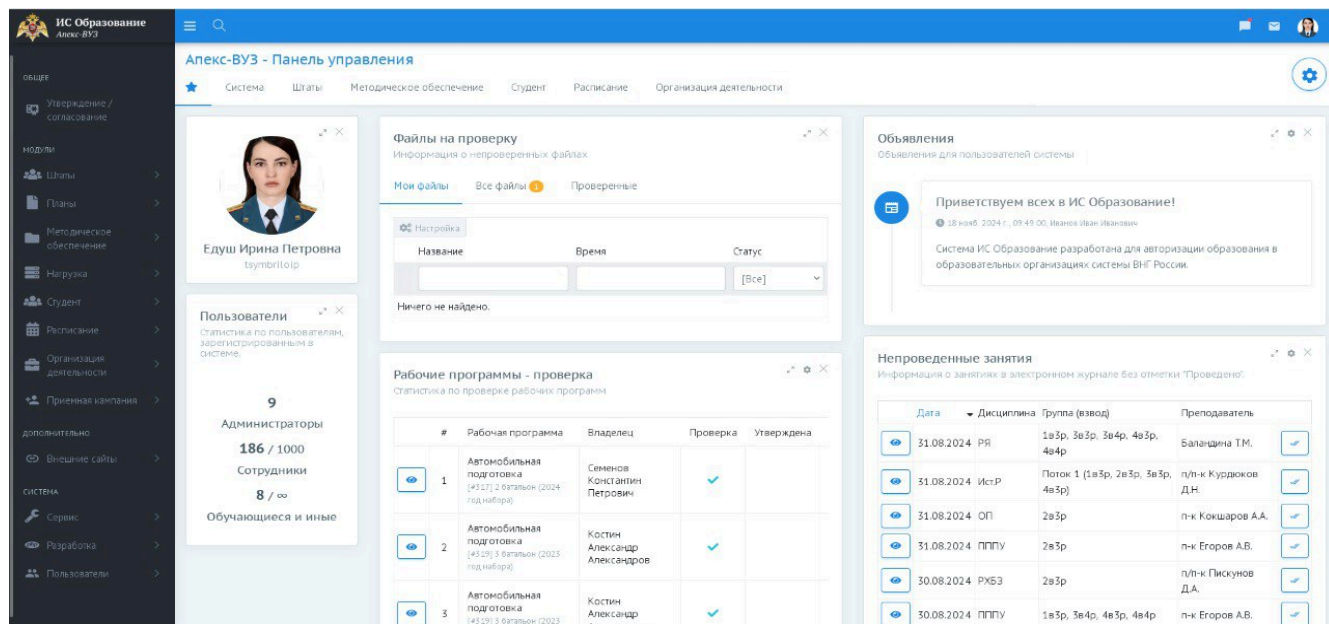


Рисунок 2. Главная страница подсистемы «Алекс-ВУЗ»

ИС «Образование» состоит из трех подсистем:

- подсистема «Алекс-ВУЗ», предназначенная для автоматизации организации образовательной деятельности конкретной образовательной организации;
- подсистема «Единый образовательный портал», предназначенная для просмотра, анализа, координации и управления данными по всем образовательным организациям;
- подсистема «Электронное обучение», предназначенная для использования в учебном

процессе учебных и контролирующих материалов, данная подсистема реализована на базе свободно распространяемого программного кода Moodle.

Подсистема «Алекс-ВУЗ», в свою очередь, обладает модульной структурой и для каждой образовательной организации состоит из 9 модулей:

- модуль «Система»;
- модуль «Штаты»;
- модуль «Планы»;
- модуль «Методическое обеспечение»;

- модуль «Нагрузка»;
- модуль «Расписание»;
- модуль «Студент»;
- модуль «Организация деятельности»;
- модуль «Приемная кампания».

Наиболее важными с точки зрения функционирования системы являются модули «Штаты», «Планы», «Методическое обеспечение» и «Нагрузка», назначение и возможности которых рассмотрены далее.

1. Модуль «Штаты» предназначен для структурирования образовательной организации и управления ее сотрудниками: в основном – педагогическими работниками, но возможно внесение информации о вспомогательном составе, руководстве образовательной организации. Он включает в себя следующие разделы:

- «Сотрудники»;
- «Штатный приказ»;
- «Справочники»;
- «Отчеты».

Подготовка модуля «Штаты» к работе включает в себя:

- 1) заполнение справочников;
- 2) формирование структуры подразделений образовательной организации;
- 3) заполнение штатного приказа (если необходимо анализировать наличие вакантных должностей в подразделении);
- 4) добавление сотрудников образовательной организации.

Повседневная работа с модулем «Штаты» предусматривает:

- 1) редактирование личных данных сотрудников, в том числе ведение их портфолио;
- 2) перевод сотрудников на новые должности внутри одного или разных подразделений, назначение на несколько должностей одновременно (совмещение);
- 3) увольнение и восстановление сотрудников.

Отметим, что в модуле реализована возможность строить иерархию подразделений, которые могут быть как самостоятельными, так и иметь древовидную архитектуру с определенной «подчиненностью», т.е. могут быть созданы родительские и дочерние подразделения (например, факультету могут принадлежать кафедры).

В модуле «Штаты» реализована такая полезная функция, как ведение портфолио сотрудников. Портфолио позволяет сотруднику добавлять личные достижения, относящиеся к любому виду работы (виды достижений формируются и настраиваются в справочнике). К достижениям прикрепляется описание, допускается загрузка файлов, фотографий или сканированных копий

грамот или иных подтверждающих документов. Реализована возможность подтверждения достижений сотрудниками образовательной организации, у которых есть специальные права. С помощью портфолио создается рейтинг сотрудников по средству добавления достижений. Важно отметить, что достижения могут, как повышать рейтинг, так и понижать в зависимости от их характера (например, дисциплинарные взыскания, нарушение сроков выполнения задач и пр.). При добавлении различных достижений создается рейтинг. Чем выше суммарный балл достижений, тем выше сотрудник в рейтинге. ИС «Образование» предоставляет возможность выводить отчеты как по рейтингу подразделений, так и по достижениям выбранного сотрудника.

2. Модуль «Планы» предназначен для создания (импорта) учебных планов, проверки их на соответствие образовательным стандартам.

Модуль «Планы» включает в себя разделы:

- «Шаблоны планов»;
- «Планы»;
- «Календарный график»;
- «Справочники»;
- «Отчеты».

Подготовка модуля «Планы» к работе включает в себя:

- 1) заполнение справочников;
- 2) создание и заполнение шаблонов планов.

Повседневная работа с модулем «Планы» заключается в создании, заполнении и проверке учебных планов по всем реализуемым образовательной организацией образовательным программам.

Отметим, что в ИС «Образование» реализован чрезвычайно интересный и полезный инструмент работы с планами - шаблоны планов.

Шаблон плана – это фактически образовательный стандарт. Шаблон плана включает в себя набор параметров, которые определяют, как учебный план должен выглядеть и как будет проверяться на соответствие образовательным стандартам. Работающие с шаблонами пользователи имеют возможность настраивать множество параметров, которые могут варьироваться в зависимости от требований образовательной организации и стандартов. Один шаблон может быть создан на несколько форм обучения одновременно. Если план создается по шаблону, то в него уже закладываются все прописанные в шаблоне параметры, что существенно экономит время на подготовку учебных планов и исключает возможность технических ошибок при их составлении.

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

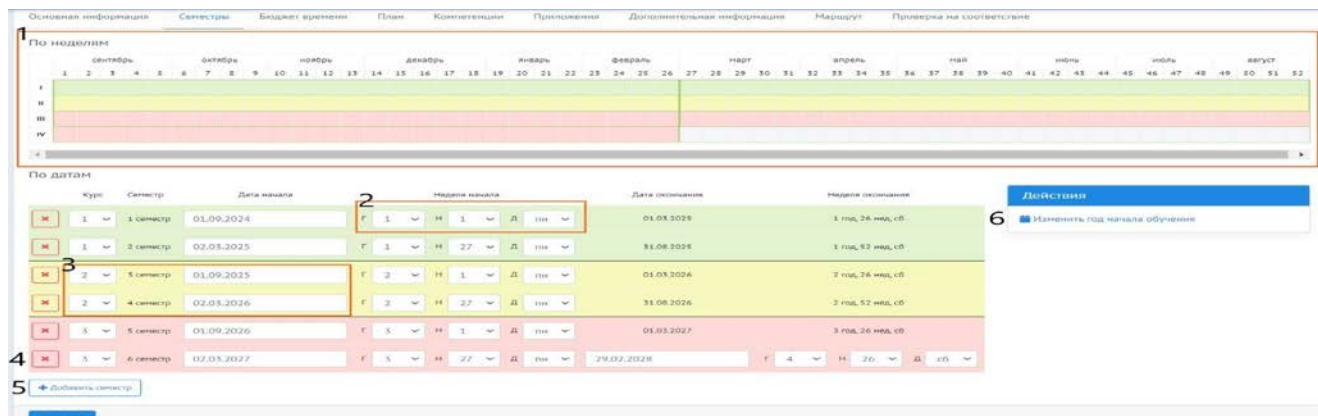


Рисунок 3. Календарный график учебного процесса.

Особенностью ИС «Образование» являются разные, удобные для визуального восприятия, формы представления различных элементов учебного плана: календарный график учебного процесса с визуальным представлением

распределения времени по семестрам и курсам (рис. 3), бюджет времени с информацией о распределении учебного времени по видам учебного процесса (рис 4), перечень учебных дисциплин с отведенными на их изучение часами по каждому виду занятий (рис. 5).

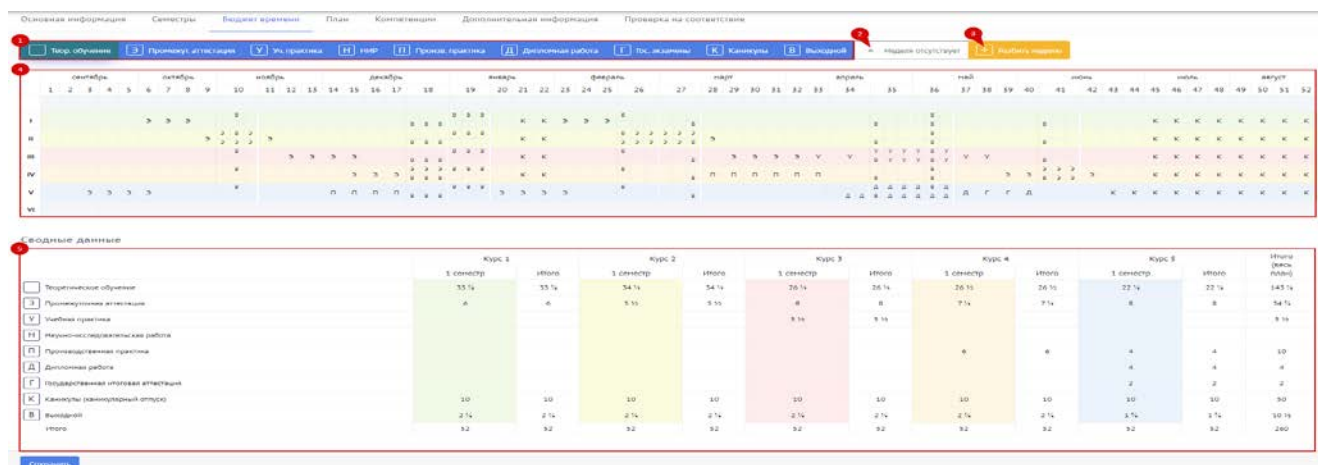


Рисунок 4. Распределение бюджета времени.

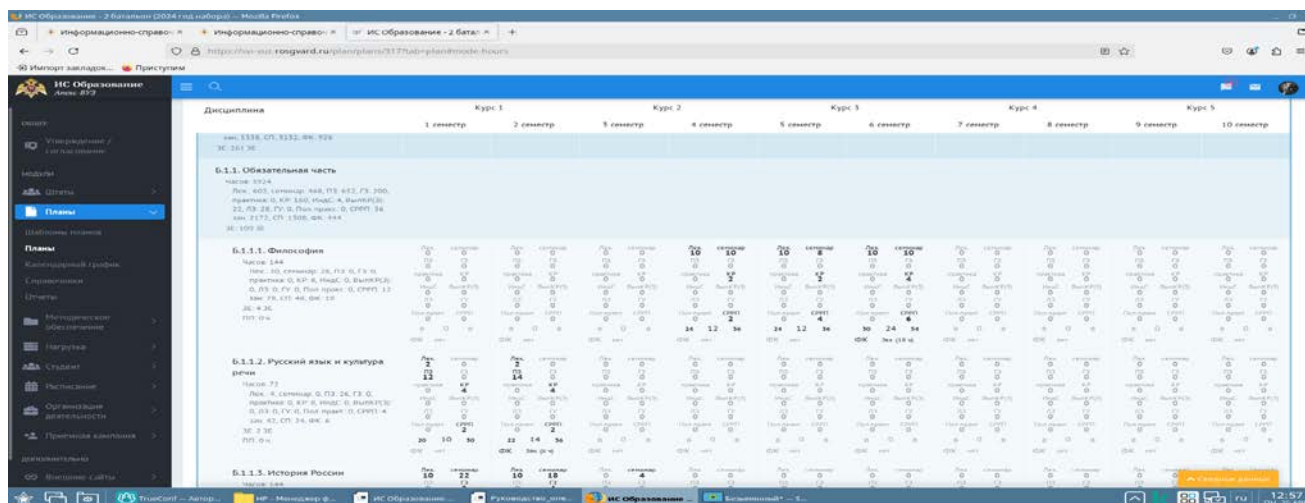


Рисунок 5. Представление дисциплин в учебном плане.

3. Модуль «Методическое обеспечение» предназначен для работы с методическими материалами, ведение которых регламентировано внутри образовательной организации и включает следующие разделы:

- «Материалы»;
- «Контроль»;
- «Электронная библиотека»;
- «Справочники»;
- «Отчеты».

Отметим, что ИС «Образование» предусматривает две категории методических материалов:

1) материалы, которые формируются непосредственно в программе, заполняются и выводятся в печатную форму (например, рабочая программа, тематический план);

2) материалы, которые можно прикрепить в виде готового документа и хранить на сервере, предоставляя доступ заинтересованным пользователям (виды таких материалов формируются в справочнике образовательной организацией самостоятельно).

Очень важными и удобными функциональными возможностями модуля является контроль обеспеченности методическими материалами дисциплин, преподаваемых в определенном учебном году: программа сама найдет дисциплины, не обеспеченные каким-либо материалом, проверит срок действия каждого методического материала, качество его подготовки, соответствия актуальным данным из учебных планов, выдаст рекомендации и замечания для любой дисциплины.

Данные модуля «Методическое обеспечение» используются в модулях «Нагрузка», «Студент» и «Расписание» для упрощения внесения исходных данных.

Для подготовки модуля к работе необходимо заполнить справочники, дальнейшая работа в модуле сводится к созданию, заполнению и редактированию рабочих программ и иных методических материалов, а также к периодическому анализу обеспеченности дисциплин методическими материалами.

4. Модуль «Нагрузка» предназначен для составления расчета учебной нагрузки по подразделениям (кафедрам/батальонам) и педагогическим работникам, а также учета фактического выполнения ими нагрузки.

Модуль «Нагрузка» включает в себя следующие разделы:

- «Учебные группы (взводы»);
- «Параметры расчета»;
- «Составление нагрузки»;
- «Распределение нагрузки»;
- «Учет нагрузки»;
- «Проверка выполнения»;
- «Индивидуальный план»;
- «Справочники»;
- «Отчеты».

Для составления расчета нагрузки применяется метод поручений: то есть расчет составляется не кафедрами, а теми, кто имеет доступ к учебным планам (сотрудниками факультетов или учебно-методического управления). На кафедрах же происходит распределение составленного по подразделению расчета нагрузки по педагогическим работникам.

Данные модуля «Нагрузка» используются в модулях «Студент» и «Расписание» для упрощения внесения исходных данных.

Для подготовки модуля «нагрузка» к работе необходимо:

- 1) заполнить справочники;
- 2) сформировать учебных групп для расчета нагрузки;
- 3) заполнить необходимых параметры (нормы) расчета нагрузки.

Далее в начале каждого учебного года проводится составление расчета нагрузки на основании утвержденных учебных планов по подразделениям (кафедрам), составленная нагрузка распределяется по подразделениям (кафедрам) и по педагогическим работникам.

В течение учебного года ИС «Образование» ведет учет фактического выполнения нагрузки, а уполномоченные на то должностные лица осуществляют контроль фактического выполнения нагрузки.

В декабре 2024 года ИС «Образование» прошла опытную эксплуатацию, а в марте 2025 года вышла на ведомственные испытания, которые в целом успешно завершились в апреле 2025 года. По итогам ведомственных испытаний разработчику информационной системы необходимо выполнить ряд доработок в части, касающейся модуля работы с расписанием учебных занятий, после чего ИС «Образование» начнет использоваться военными образовательными организациями высшего образования Росгвардии.

В заключение необходимо отметить, что цифровизация образования и цифровая трансформация деятельности образовательных организаций представляют собой неразрывно связанные поступательные процессы, предоставляющие огромные потенциальные возможности участникам образовательной деятельности, а именно расширение доступа к информации, улучшение качества обучения и контроля знаний обучающихся, повышение эффективности учебного процесса в целом.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Постановление Правительства РФ от 26.12.2017 № 1642 «Об утверждении государственной программы Российской Федерации «Развитие образования»/ Официальный интернет-портал правовой информации <http://pravo.gov.ru>, 29.12.2017

2. Фролова Г.С. Актуальные проблемы цифровизации образовательной деятельности военных образовательных организаций высшего образования войск национальной гвардии Российской Федерации // Известия Саратовского военного института войск национальной гвардии. Сетевой научный журнал. 2023. № 4. С. 76-80.

УДК 658.71+ 351.853.1

ББК 65.412+28пр1,88

**СОРОЧИНСКИЙ ЯРОСЛАВ ЛЕОНИДОВИЧ, МЛАДШИЙ НАУЧНЫЙ СОТРУДНИК
ОТДЕЛА РАЗРАБОТКИ НОРМАТИВНО-МЕТОДИЧЕСКИХ ДОКУМЕНТОВ ФКУ «НИЦ
«ОХРАНА» РОСГВАРДИИ**

**УЧАСТИЕ ПОДРАЗДЕЛЕНИЙ ВНЕВЕДОМСТВЕННОЙ ОХРАНЫ РОСГВАРДИИ
В ЭЛЕКТРОННЫХ ТОРГАХ: СТРАТЕГИЯ РОСТА НА КОНКУРЕНТНОМ РЫНКЕ
ОХРАННЫХ УСЛУГ**

Аннотация. Статья посвящена актуальной проблеме эффективного участия подразделений вневедомственной охраны Росгвардии в электронных торгах на конкурентном рынке охранных услуг. Автор анализирует сложное и динамично изменяющееся нормативно-правовое поле, регулирующее данную деятельность. В работе предложена практическая стратегия, состоящая из трех фундаментальных направлений: определение административного фундамента (распределение ответственности), обеспечение цифрового суверенитета (техническое оснащение и ЭЦП) и открытие доступа ко всем электронным торговым площадкам. Далее процесс участия в закупках систематизирован в виде пошагового алгоритма: от поиска закупок и анализа документации до непосредственного участия в торгах и надежного завершения сделки. Особое внимание уделяется критической роли человеческого фактора, необходимости дублирования полномочий и постоянного обучения специалистов.

Ключевые слова: вневедомственная охрана, электронные торги, закупки, конкурентный рынок, электронная торговая площадка (ЭТП), Единая информационная система (ЕИС), электронная подпись (ЭЦП).

YAROSLAV LEONIDOVICH SOROCHINSKY, **LEONIDOVICH SOROCHINSKY, JUNIOR RESEARCHER
OF THE DEPARTMENT OF DEVELOPMENT OF NORMATIVE AND METHODOLOGICAL DOCUMENTS FSI
«SRC «OKHRANA» OF THE FEDERAL SERVICE OF NATIONAL GUARD OF RUSSIA**

PARTICIPATION OF ROSGVARDAIA UNITS IN ELECTRONIC BIDDING: GROWTH STRATEGY
IN THE COMPETITIVE MARKET OF SECURITY SERVICES.

Annotation. The article is devoted to the actual problem of effective participation of the Rosgvardia's non-departmental security units in electronic tenders in the competitive market of security services. The author analyzes the complex and dynamically changing legal framework regulating this activity. The paper proposes a practical strategy consisting of three fundamental areas: defining the administrative foundation (distribution of responsibilities), ensuring digital sovereignty (technical equipment and digital signatures), and opening access to all electronic trading platforms. Further, the process of participation in procurement is systematized in the form of a step-by-step algorithm: from the search for procurement and the analysis of documentation to the direct participation in the bidding and the reliable completion of the transaction. Special attention is paid to the critical role of the human factor, the need for duplication of authority and continuous training of specialists.

Keywords: private security, electronic tenders, procurement, competitive market, electronic trading platform (ETP), Unified Information System (EIS), electronic signature (ES).

Российский рынок охранных услуг характеризуется высокой степенью конкуренции. Наряду с частными охранными предприятиями, подразделениями ведомственной охраны федеральных органов исполнительной власти, определяемых Правительством Российской Федерации, федеральных государственных органов и организаций в соответствии с федеральными законами, высшего исполнительного органа субъекта Российской

Федерации – города федерального значения Москвы и юридическими лицами с особыми уставными задачами (далее – подразделения охраны) активное участие в оказании услуг по защите объектов и имущества принимают подразделения вневедомственной охраны войск национальной гвардии Российской Федерации (далее – вневедомственная охрана, УВО (ОВО)), в том числе путем централизованной охраны и реагирование на сигналы «тревога». Ключевым

каналом привлечения новых клиентов для всех участников рынка стало участие в электронных торгах на закупку услуг централизованной охраны. Это конкурентная среда, где победа зависит не только от репутации и надежности, но и от строгого соблюдения сложного законодательства, оперативности и технологической грамотности. В этих условиях УВО (ОВО) необходима четкая, регламентированная система действий, позволяющая эффективно конкурировать и наращивать объем оказываемых услуг.

Участие подразделений вневедомственной охраны в закупках строго регламентировано. Основу правового поля составляют два федеральных закона:

- Федеральный закон от 5 апреля 2013 г. № 44-ФЗ регулирует закупки для государственных и муниципальных нужд [1];

- Федеральный закон от 18 июля 2011 г. 223-ФЗ применяется для закупок отдельными видами юридических лиц [2].

Федеральный закон от 5 апреля 2013 г. № 44-ФЗ устанавливает обязательность конкурентных процедур (аукционы, конкурсы, запросы котировок), определяет требования к участникам, срокам, обеспечению заявок и исполнения контрактов.

Также положения закона направлены на закрепление принципов открытости, прозрачности и равноправия участников закупок.

Федеральный закон от 18 июля 2011 г. № 223-ФЗ предоставляет заказчикам большую свободу в выборе процедур закупок, согласно разрабатываемых Положений о закупках.

Указанные законодательные акты о закупках задают общие правила игры. В них прописано, как проводить конкурсы и аукционы, как должны взаимодействовать между собой заказчики и поставщики. Эти же законы делегируют Правительству Российской Федерации и министерствам право разрабатывать более детальные инструкции.

Главным инструментом, который перевел все эти процедуры в современную цифровую реальность, стали электронные торговые площадки (ЭТП). Они позволяют проводить закупки онлайн, что выгодно всем: бизнес получает простой и равный доступ к тендерам, а госзаказчики экономят время и деньги, что особенно важно, такая система работает на принципах прозрачности и честной конкуренции, создавая надежный барьер для коррупции.

Важную роль в рассматриваемом аспекте играют подзаконные акты, такие как постановления

Правительства Российской Федерации, к которым в контексте деятельности вневедомственной охраны прежде всего можно отнести:

- постановление от 8 мая 2020 г. № 645 – наделяет Росгвардию полномочиями по установлению порядка определения цен контрактов на охранные услуги [3];

- постановление от 6 декабря 2016 г. № 1303 – определяет порядок установления тарифов на услуги войск национальной гвардии [4];

- постановление от 31 декабря 2021 г. № 2604 – устанавливает единые критерии оценки заявок (цена, качество, квалификация участника) [5].

В развитие законодательных и правительственных документов подготовлены и введены ведомственные акты Росгвардии:

- приказ от 1 июня 2020 г. № 149 – содержит типовой контракт на оказание охранных услуг [6];

- приказ от 6 июня 2017 г. № 158 – утверждает методику расчета тарифов на охрану [7];

- приказ от 15 февраля 2021 г. № 45 – определяет порядок расчета начальной цены контракта [8].

Приведенная выше нормативная база, регулирующая закупки, не является исчерпывающей. Законодательство в сфере закупок динамично изменяется, требует постоянного отслеживания и глубокого понимания. Кроме того, нарушение установленных процедур влекут риски признания закупки недействительной, а контракта – незаключенным.

Чтобы вывести работу подразделений вневедомственной охраны на новый уровень и уверенно действовать в сфере госзакупок, необходим целый комплекс продуманных шагов. Для этого целесообразно сосредоточиться на трех ключевых направлениях, которые позволят систематизировать работу и гарантировать ее результат.

1. Заложить административный фундамент. Всё начинается с четкого распределения ролей и ответственности. Руководителю УВО (ОВО) важно издать распорядительный документ, который станет основой всей дальнейшей работы. В нем назначаются ответственные должностные лица – юристы, экономисты, техники, – каждый из которых отвечает за свой участок. Отдельно определяется ответственное должностное лицо, которое будет координировать весь процесс: от мониторинга торговых площадок в поиске выгодных контрактов до подготовки заявок, непосредственного участия в электронных аукционах и подписания итоговых документов.

Это позволяет избежать неразберихи и гарантирует, что каждое действие выполняется профессионально.

2. Обеспечить цифровой суверенитет. Без современной техники и надежных электронных инструментов работа в цифровом поле невозможна. На этом этапе необходимо оборудовать и настроить автоматизированные рабочие места (АРМ) так, чтобы они бесперебойно взаимодействовали с Единой информационной системой (ЕИС) – главной витриной государственных закупок. Но главный «ключ доступа» к торгам – это усиленная квалифицированная электронная подпись (ЭЦП). Именно она придает документам юридическую силу, заменяя собственноручную подпись и печать. Получить ее надежнее всего в Удостоверяющем центре Казначейства России.

3. Открыть двери на все торговые площадки. Чтобы начать реальную борьбу за контракты, УВО (ОВО) должно пройти два обязательных этапа. Сначала – регистрация в ЕИС (zakupki.gov.ru), что равносильно получению пропуска в мир госзаказа. Затем – аккредитация на всех без исключения государственных электронных торговых площадках (ЭТП), а также на выбранных коммерческих платформах. Только после этого УВО (ОВО) получает право подавать заявки и участвовать в аукционах наравне с другими поставщиками.

Таким образом, последовательное выполнение этих шагов превращает разрозненные действия в отлаженный механизм, позволяя вневедомственной охране эффективно работать в конкурентной среде госзакупок. Участие в госзакупках напоминает слаженную работу механизма, где каждый шаг выверен и подчинен единой цели – обеспечить победу и заключить выгодный контракт. Этот путь состоит из нескольких ключевых этапов.

Первый шаг – стратегический поиск. Специалисты ежедневно «прочесывают» электронные торговые площадки и госзакупки, используя точные фильтры: от региона до конкретных услуг, таких как «охрана» или «экстренное реагирование». Но найти – полдела. Каждую заявку подвергают строгой проверке: подходит ли объект по расположению? Не завышена ли начальная цена? Соответствует ли она нашим тарифам? Это помогает сразу отсеять неподходящие варианты.

Второй шаг – подготовка и анализ. Обнаружив перспективный тендер, команда юристов и экономистов внимательно изучает все требования заказчика. Если в документах встречаются двусмысленные формулировки или

спорные технические условия – например, о совместимости оборудования – поставщик имеет право запросить официальные разъяснения. Только полностью оценив все «за» и «против», принимается окончательное решение – вступать в борьбу или нет.

Третий шаг – аукцион, сердце борьбы. Здесь важны не только скорость, но и точный расчет. Еще до начала торгов определяется «коридор цен» – от максимальной, заявленной заказчиком, до минимально возможной. В назначенный час ответственный сотрудник в режиме онлайн включается в аукцион, оперативно снижая цену и борясь за наиболее выгодную позицию.

Финальный шаг – надежное завершение сделки. После победы работа не заканчивается: проект контракта тщательно сверяется с изначальной документацией. При обнаружении несоответствий можно направить протокол разногласий. Итоговый документ подписывается электронной подписью и отправляется заказчику через оператора площадки, работа которого, конечно, тоже оплачивается.

Однако даже самый совершенный алгоритм бессилён без грамотных специалистов. В условиях, когда законодательство меняется быстро, а сроки проведения торгов строго ограничены, решающую роль играет человеческий фактор.

Критически важно, чтобы доступ к торгам и полномочия для работы были как минимум у двух сотрудников. Это простое правило страхует от любых неожиданностей – будь то болезнь, отпуск или увольнение ключевого сотрудника.

Постоянное обучение – не формальность, а необходимость. Регулярное повышение квалификации (рекомендуется не реже раза в три года) позволяет специалистам быть в курсе последних изменений в законах, а также судебной и антимонопольной практики. В динамичном мире госзакупок тот, кто владеет информацией, владеет ситуацией.

В заключении следует отметить, что участие подразделений вневедомственной охраны в электронных торгах должно осуществляться на плановой и системной основе и как показывают данные за 2023-2024 годы, уже демонстрирует положительные результаты, наблюдается рост количества участия в торгах, увеличение числа принятых под охрану объектов и значительный прирост суммы заключенных контрактов.

Опыт вневедомственной охраны – это пример того, как государственная структура может успешно адаптироваться к новым реалиям, внедряя цифровые технологии, четкие регламенты и развивая профессиональные навыки своих сотрудников. В современной борьбе

за безопасность побеждает не тот, кто сильнее, а тот, кто умнее, организованнее и быстрее осваивает правила игры на цифровом поле.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 5 апреля 2013 г. № 44-ФЗ (ред. от 26 декабря 2024 г.) «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».
2. Федеральный закон от 18 июля 2011 г. № 223-ФЗ (ред. от 8 августа 2024 г.) «О закупках товаров, работ, услуг отдельными видами юридических лиц».
3. Постановление Правительства Российской Федерации от 8 мая 2020 г. № 645 «О федеральном органе исполнительной власти, уполномоченном на установление порядка определения начальной (максимальной) цены контракта, цены контракта, заключаемого с единственным поставщиком (подрядчиком, исполнителем), начальной цены единицы товара, работы, услуги при осуществлении закупок охранных услуг».
4. Постановление Правительства Российской Федерации от 6 декабря 2016 г. № 1303 «О порядке определения тарифов на оказываемые войсками национальной гвардии Российской Федерации услуги по охране имущества и объектов граждан и организаций, а также на иные услуги, связанные с обеспечением охраны имущества, и признании утратившими силу некоторых актов Правительства Российской Федерации».
5. Постановление Правительства Российской Федерации от 31 декабря 2021 г. № 2604 «Об оценке заявок на участие в закупке товаров, работ, услуг для обеспечения государственных и муниципальных нужд, внесении изменений в пункт 4 постановления Правительства Российской Федерации от 20 декабря 2021 г. № 2369 и признании утратившими силу некоторых актов и отдельных положений некоторых актов Правительства Российской Федерации».
6. Приказ Росгвардии от 1 июня 2020 г. № 149 «Об утверждении типового контракта на оказание охранных услуг и информационной карты типового контракта на оказание охранных услуг».
7. Приказ Росгвардии от 6 июня 2017 г. № 158 «Об утверждении методики установления тарифов на оказываемые войсками национальной гвардии Российской Федерации услуги по охране имущества и объектов граждан и организаций, а также на иные услуги, связанные с обеспечением охраны имущества на договорной основе».
8. Приказ Росгвардии от 15 февраля 2021 г. № 45 «Об утверждении порядка определения начальной (максимальной) цены контракта, цены контракта, заключаемого с единственным поставщиком (подрядчиком, исполнителем), начальной цены единицы товара, работы, услуги при осуществлении закупок охранных услуг».
9. <http://zakupki.gov.ru> – официальный сайт ЕИС.
10. «Информационно-справочный портал Федеральной службы войск национальной гвардии Российской Федерации».

УДК 323.28т+ 669.8

ББК 67.408.131.11

**СОРОЧИНСКИЙ ЯРОСЛАВ ЛЕОНИДОВИЧ, МЛАДШИЙ НАУЧНЫЙ СОТРУДНИК
ОТДЕЛА РАЗРАБОТКИ НОРМАТИВНО-МЕТОДИЧЕСКИХ ДОКУМЕНТОВ ФКУ «НИЦ
«ОХРАНА» РОСГВАРДИИ**

**ПРОБЛЕМЫ ОСУЩЕСТВЛЕНИЯ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ ПО
АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ (ТЕРРИТОРИЙ)
РАЗЛИЧНОЙ ВЕДОМСТВЕННОЙ ПРИНАДЛЕЖНОСТИ**

Аннотация. В статье рассматриваются актуальные проблемы организации и проведения контрольных мероприятий по обеспечению антитеррористической защищённости объектов (территорий) различной ведомственной принадлежности. Особое внимание уделяется объектам топливно-энергетического комплекса (ТЭК), образования, спорта и гостиниц. Анализируется существующая нормативно-правовая база, выявляются пробелы и противоречия в системе контроля, включая дублирование полномочий, недостаточную эффективность межведомственного взаимодействия и устаревшие требования, не учитывающие современные угрозы (кибератаки, БПЛА и др.). На основе проведённого анализа предлагаются конкретные меры по совершенствованию системы контроля, включая разграничение полномочий, цифровизацию процессов и усиление ответственности должностных лиц.

Ключевые слова: антитеррористическая защищённость (АТЗ), контрольные мероприятия, объекты, межведомственное взаимодействие, инженерно-технические средства охраны (ИТСО), угрозы безопасности, административные нарушения, цифровизация контроля

YAROSLAV LEONIDOVICH SOROCHINSKY, LEONIDOVICH SOROCHINSKY, JUNIOR RESEARCHER
OF THE DEPARTMENT OF DEVELOPMENT OF NORMATIVE AND METHODOLOGICAL DOCUMENTS FSI
«SRC «OKHRANA» OF THE FEDERAL SERVICE OF NATIONAL GUARD OF RUSSIA

PROBLEMS OF IMPLEMENTING CONTROL MEASURES FOR ANTI-TERRORIST PROTECTION
OF OBJECTS (TERRITORIES) OF DIFFERENT BODIES

Annotation. The article discusses the current problems of organizing and conducting control measures to ensure the anti-terrorist security of facilities (territories) of various departments. Special attention is paid to facilities in the fuel and energy complex (FEC), education, sports, and hotels. The existing regulatory framework is analyzed, and gaps and contradictions in the control system are identified, including duplication of authority, insufficient efficiency of interagency cooperation, and outdated requirements that do not take into account modern threats (cyberattacks, UAVs, etc.). Based on the analysis, specific measures are proposed to improve the control system, including clear delineation of responsibilities, digitalization of processes, and increased accountability of officials.

Keywords: Anti-terrorism security (ATS), control measures, facilities, interdepartmental cooperation, engineering and technical security measures (ITS), security threats, administrative violations, and digitalization of control.

Представьте: утро, но мир уже не тот. Электричества нет – ни в розетках, ни на улицах. Телефоны разряжены, интернет исчез, карты не работают. На заправках – очереди, но бензин скоро закончится.

В больницах – резервные генераторы, но топлива хватит лишь на сутки. Метро и поезда стоят, продукты в магазинах портятся без холодильников. Через день люди начнут волноваться, через три – искать еду, а что дальше зависит от того, как быстро вернётся свет.

Это не сценарий апокалипсиса. Это реальный риск, если террористы или диверсанты ударят по энергосистеме. Одна хорошо спланированная атака – и страна может погрузиться в хаос.

Почему энергетика – цель №1?

- каскадный эффект: выход из строя одной ключевой подстанции может обесточить целые регионы;

- долгое восстановление: даже если диверсанты просто повредят трансформаторы – новые придется ждать месяцами;

- социальный взрыв: без электричества нет воды, тепла, связи. Города превращаются в ловушки.

С начала специальной военной операции угрозы энергетической безопасности России перешли из разряда гипотетических в категорию ежедневных рисков. Удары по подстанциям, поджоги электросетей, кибератаки на системы управления – все это уже не сценарии учений, а реальность последних лет. И если раньше мы говорили о потенциальных угрозах, то сегодня счет идет на часы: одна успешная диверсия может

оставить без света и тепла миллионы граждан, парализовать оборонные предприятия и поставить крест на экономической устойчивости страны.

С начала конфликта противник перешел к тактике ударов по гражданской инфраструктуре. И если раньше террористические атаки на энергообъекты рассматривались, как локальные инциденты, то теперь:

- ливерсионные группы целенаправленно атакуют нефтеперерабатывающую инфраструктуру, терминалы, подстанции и ЛЭП (поджоги, обстрелы, минирование);

- кибератаки стали сложнее: хакеры пытаются внедряться в автоматические системы управления технологическими процессами, чтобы вызвать аварии;

- разведсообщества западных стран НАТО собирают данные о ключевых энергоузлах, готовя почву для точечных ударов.

Необходимо отметить, что обеспечение безопасности объектов топливно-энергетического комплекса (ТЭК) всегда являлась приоритетом и, как следствие, вопросы касающиеся их защиты от актов незаконного вмешательства были урегулированы путем принятия соответствующего профильного Федерального закона от 21 июля 2011 г. № 256-ФЗ, а также иных базовых нормативных правовых актов, устанавливающих требования по обеспечению безопасности и антитеррористической защищенности объектов ТЭК в которых подробно, в зависимости от присвоенной категории опасности, определены мероприятия по их оборудованию инженерно-техническими средствами охраны и обеспечения функционирования подразделений охраны, а также обеспечения физической защиты таких объектов [1].

Одновременно с этим законодательством предусмотрены нормы по осуществлению федерального государственного контроля (надзора) за обеспечением безопасности объектов ТЭК, который проводится специально созданными и сформированными подразделениями государственного контроля территориальных органов Росгвардии в соответствии с утвержденными Правилами [2]. Общее руководство их деятельностью осуществляется ГУЛРРИГК Росгвардии.

В рамках осуществления своей деятельности сотрудники подразделений государственного контроля территориальных органов Росгвардии наделены полномочиями по предупреждению, выявлению и пресечению нарушений требований обеспечения безопасности и антитеррористической защищенности объектов ТЭК, а также по вынесению предписаний об устранении выявленных нарушений и составлению в отношении субъектов и должностных лиц объектов ТЭК административных протоколов за такие нарушения [3].

Таким образом, в целом можно констатировать, что безопасность и антитеррористическая защищенность объектов ТЭК в целом

урегулирована на всех этапах от оборудования ИТСО и построения физической защиты до осуществления контрольных мероприятий за выполнением соответствующих требований.

А что представляет комплекс мероприятий в сфере обеспечения антитеррористической защищенности объектов образования, спорта и гостиниц?

Давайте представим риски, которые могут последовать в случае террористических атак в отношении таких объектов.

- паника и социальная дестабилизация;
- значительные человеческие жертвы;
- большие финансовые затраты на покрытие последствий;
- репутационные потери как на внутригосударственном уровне, так и на международной арене.

Это только тот минимум, который «лежит на поверхности».

Предлагаю рассмотреть максимальные угрозы, например, в отношении крупного образовательного объекта, на котором помимо осуществления образовательной деятельности проводятся исследования, связанные с использованием наркотических веществ, или в области культивирования наркосодержащих культур.

Так какими требованиями к антитеррористической защищенности должны руководствоваться правообладатели или руководители такого объекта?

Наверное, прежде всего, требованиями антитеррористической защищенности объектов (территорий) Министерства науки и высшего образования Российской Федерации, его территориальных органов и подведомственных ему организаций, объектов (территорий), относящихся к сфере деятельности Министерства науки и высшего образования Российской Федерации [4].

Таким образом даже в случае присвоения такому образовательному учреждению первой категории опасности на объекте должны обеспечиваться:

- пропускной и внутриобъектовый режим (ЧОП или ведомственная (вневедомственная) охрана);
- оснащение ИТСО (в том числе КТС);
- оборудование системой оповещения и управления эвакуацией;
- КПП, въезды и критические элементы оборудуются системой видеонаблюдения.

При этом, в части противокриминальной защиты таких объектов необходимые требования к оборудованию ИТСО), на которых осуществляется оборот наркотических средств конкретизированы в приказе Росгвардии и МВД России от 15 сентября 2021 г. № 335/677 [5].

Казалось-бы предусмотрен необходимый комплекс организации охранных и антитеррористических мероприятий (в том числе и критических элементов), но на практике при проведении обследований объектов

представителями правообладателя или должностными лицами объекта, несмотря на рекомендации специалистов Росгвардии, необходимые меры по оборудованию ИТСО стараются свести к минимуму.

И здесь, в очередной раз, встает вопрос об осуществлении контроля за выполнением требований к АТЗ.

Плановая проверка осуществляется в соответствии с план-графиком, утверждаемым руководителем организации – правообладателя. Для объектов первой категории, таких как образовательные учреждения, установлена периодичность проверок – не реже 1 раза в 3 года. Однако в постановлении № 1421 также указано, что ежегодные плановые проверки проводятся в рамках подготовки к учебному году, причем не только по основному план-графику, но и в соответствии с планами региональных и муниципальных органов власти. Это создает правовую неопределенность: может ли один объект проверяться дважды в течение года – например, федеральным ведомством (Минобрнауки России) и региональным органом управления? Подобная ситуация приводит к дублированию контрольных мероприятий, что противоречит принципам эффективного и разумного надзора, заложенным в законодательстве. Требуется четкое разграничение полномочий во избежание двойной нагрузки.

И второй вопрос возникает об обязательности участия в таких проверках представителей ФСБ, МЧС России и Росгвардии? В требованиях указано, что в состав межведомственной комиссии «могут включаться» данные представители [4].

И как следствие, «вишенка на торте», а какие полномочия комиссии при выявлении нарушений требований к АТЗ, если в нее не входят представители ФСБ России и Росгвардии?

Полномочия, следующие:

- составить акт проверки и направить в Минобрнауки России;
- инициировать проведение внеплановой проверки.

А в случаях контроля АТЗ объектов спорта ситуация, следующая:

На сегодняшний день обеспечение безопасности спортивных объектов полностью возложено на их собственников и владельцев. При этом отсутствует система обязательной отчетности и внешнего контроля принимаемых мер [6].

Особую озабоченность вызывает организация охраны во время местных соревнований. Фактически, комплекс мер безопасности применяется только в день проведения мероприятия. В предшествующий период охрана объектов либо осуществляется бессистемно, либо отсутствует вовсе.

Такое положение дел создает серьезные риски, так как отсутствие постоянного контроля позволяет злоумышленникам:

- беспрепятственно изучать объект;
- выявлять уязвимые места;
- осуществлять подготовку к возможным противоправным и террористическим действиям.

Необходимо отметить, что данная ситуация характерна не только для объектов местного значения, но и в ряде случаев крупных спортивных сооружений, где уровень защищенности зачастую остается минимальным.

Требуется пересмотр существующего подхода к организации АТЗ спортивных объектов с внедрением системы постоянного контроля и четких стандартов безопасности.

Кроме того, возникает закономерный вопрос о наличии соответствующих знаний и компетенций у проверяющих такие объекты, без привлечения соответствующих специалистов, по определению правильности монтажа, эксплуатационному обслуживанию и проверке работоспособности установленных ТСО.

По аналогии можно отметить и состояние АТЗ в части оснащения ИТСО гостиниц.

В постановлении Правительства РФ от 14 апреля 2017 г. № 447 по АТЗ гостиниц установлено, что в состав комиссий по обследованию и категорированию таких объектов могут включаться представители Росгвардии. Закономерный вопрос – в подавляющем большинстве случаев гостиницы находятся в управлении юридических и физических лиц и являются частной собственностью, что ставит под сомнение желание привлечения к обследованиям представителей правоохранительных органов, поскольку основная цель владельцев гостиницы – это извлечение прибыли при возможных минимальных затратах [7].

При этом организация и осуществление контроля АТЗ гостиницы осуществляется ответственными лицами, уполномоченными правообладателями. И здесь интересно следующее, а каким образом такие ответственные лица будут контролировать выполнение ими же необходимых требований по АТЗ?

Следующим, по моему мнению, спорным моментом является применение понятий видов проводимых проверок гостиниц – комплексные и экстренные. На данный момент это является нововведением, не встречающимся в действующей нормативной правовой базе.

На объектах спорта ситуация, в принципе, схожая по инициированию проверок, а вот понятий видов проверок еще больше – комплексные, контрольные и целевые.

Подводя итог можно отметить следующее:

- по ряду объектов проверки идут по принципу «каждый тянет одеяло на себя», а уполномоченный орган с возможностью осуществления административного воздействия не определен;
- для различных объектов установлены свои правила обеспечения их АТЗ, при этом последствия совершения на них террористических актов могут, при определенных условиях, носить одинаковый трагический характер;

- отсутствие властных и административных полномочий контролирующих органов обеспечения АТЗ объектов, находящихся в их ведении или сфере их деятельности;

- требования к АТЗ устарели – появились новые виды и модели угроз (БПЛА, кибератаки, новые виды оружия и взрывчаток и т.д.).

Какой выход из сложившейся ситуации?

По моему мнению:

1. Планомерный пересмотр нормативных правовых актов по совершенствованию механизма разграничения и осуществления контроля за их выполнением между соответствующими органами государственной власти.

2. Одна проверка АТЗ объекта в установленный промежуток времени специально определенными государственными органами, наделенными правами принятия административных мер реагирования, вместо нескольких в составе межведомственной комиссии и исключая бесконечные визиты разных структур.

3. Цифровизация контроля за выполнением требований к АТЗ – единая база нарушений, чтобы не пришлось каждый раз собирать одни и те же справки и отчеты об устранении недостатков.

4. Реальные санкции за отписки – если чиновник подписал паспорт безопасности, не проверив объект, – отвечать по закону.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» (ред. от 07 июля 2025 г.) // Собрание законодательства Российской Федерации – 25.07.2011 – № 30 (ч. 1) – ст. 4604.
2. Постановление Правительства РФ от 12 мая 2023 г. № 740 «Об утверждении Правил осуществления федерального государственного контроля (надзора) за обеспечением безопасности объектов топливно-энергетического комплекса, которым присвоена категория опасности, и о признании утратившими силу некоторых актов Правительства Российской Федерации» // Официальный интернет-портал правовой информации <http://pravo.gov.ru> // Собрание законодательства Российской Федерации – 15.05.2023 – № 20 – ст. 3568.
3. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. 3 195-ФЗ (ред. от 31 июля 2025 г.) (с изм. и доп., вступ. в силу с 06.09.2025) // Собрание законодательства Российской Федерации – 07.01.2002 – № 1 (ч. 1) – ст. 1.
4. Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства науки и высшего образования Российской Федерации, его территориальных органов и подведомственных ему организаций, объектов (территорий), относящихся к сфере деятельности Министерства науки и высшего образования Российской Федерации, формы паспорта безопасности этих объектов (территорий) и признании утратившими силу некоторых актов Правительства Российской Федерации: постановление Правительства Российской Федерации от 7 ноября 2019 г. № 1421 // Собрание законодательства Российской Федерации. – 18.11.2019 – № 46 – С.6491.
5. Об утверждении Требований к оснащению инженерно-техническими средствами охраны объектов и помещений, в которых осуществляются деятельность, связанная с оборотом наркотических средств, психотропных веществ и внесенных в список I перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации, прекурсоров, и (или) культивирование наркосодержащих растений для использования в научных, учебных целях и в экспертной деятельности, для производства используемых в медицинских целях и (или) в ветеринарии наркотических средств и психотропных веществ: приказ Федеральной службы войск национальной гвардии Российской Федерации и МВД России от 15 сентября 2021 г. № 335/677 // Официальный интернет-портал правовой информации [сайт]. – URL: <http://www.pravo.gov.ru>, 15.11.2021 г. № 000120211115009 (дата обращения – 03.08.2025).
6. Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства спорта Российской Федерации и подведомственных ему организаций, а также формы паспорта безопасности объектов (территорий) Министерства спорта Российской Федерации и подведомственных ему организаций: постановление Правительства Российской Федерации от 28 января 2019 г. № 52 // Собрание законодательства Российской Федерации – 04.02.2019 – № 5 – С. 397.
7. Об утверждении требований к антитеррористической защищенности гостиниц и иных средств размещения и формы паспорта безопасности этих объектов: постановление Правительства Российской Федерации от 14 апреля 2017 г. № 447 (ред. от 03.09.2025) // Официальный интернет-портал правовой информации <http://www.pravo.gov.ru> 18.04.2017 // Собрание законодательства Российской Федерации – 24.04.2017 – № 17 – ст. 2570.

УДК 614.84.31

ББК 30н6

ФИРСОВ АЛЕКСАНДР ГЕОРГИЕВИЧ, ВЕДУЩИЙ НАУЧНЫЙ СОТРУДНИК ОТДЕЛА
ПОЖАРНОЙ СТАТИСТИКИ ФГБУ ВНИИПО МЧС РОССИИ

СИБИРКО ВИТАЛИЙ ИВАНОВИЧ, НАЧАЛЬНИК СЕКТОРА ОТДЕЛА ПОЖАРНОЙ
СТАТИСТИКИ ФГБУ ВНИИПО МЧС РОССИИ

МАЛЁМИНА ЕКАТЕРИНА НИКОЛАЕВНА, СТАРШИЙ НАУЧНЫЙ СОТРУДНИК ОТДЕЛА
ПОЖАРНОЙ СТАТИСТИКИ ФГБУ ВНИИПО МЧС РОССИИ

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ СИСТЕМ ОХРАННО-ПОЖАРНОЙ СИГНАЛИЗАЦИИ ПО ОБЕСПЕЧЕНИЮ ПОЖАРНОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ ЗАЩИТЫ В 2024 Г.

Аннотация. Авторами статьи рассмотрены основные функции и классификация систем охранно-пожарной сигнализации. Приведены существующие виды технического обслуживания систем охранно-пожарной сигнализации. Осуществлен статистический анализ результатов работы охранно-пожарной сигнализации на пожарах. Определены ведущие причины возникновения и объекты пожаров, на которых были установлены системы охранно-пожарной сигнализации. Осуществлен расчет социальных и материальных последствий пожаров на объектах защиты, оборудованных охранно-пожарной сигнализацией. Рассмотрены статистические данные, характеризующие соответствие установок охранно-пожарной сигнализации действующим нормативным правовым актам и нормативным документам.

Ключевые слова: охранно-пожарная сигнализация, пожар, социальные последствия пожара, материальные последствия пожара, причина возникновения пожара, объект пожара.

ALEXANDER GEORGIYEVICH FIRSOV, LEADING RESEARCHER OF DEPARTMENT
OF FIRE STATISTICS OF THE FGBU VNIPO EMERCOM OF RUSSIA

VITALIY IVANOVICH SIBIRKO, HEAD OF SECTOR OF DEPARTMENT OF FIRE STATISTICS
OF THE FGBU VNIPO EMERCOM OF RUSSIA

EKATERINA NIKOLAEVNA MALYOMINA, SENIOR RESEARCHER OF THE FIRE STATISTICS
DEPARTMENT OF THE ALL-RUSSIAN RESEARCH INSTITUTE OF FIRE PROTECTION OF THE EMERCOM
OF RUSSIA

MAIN RESULTS OF FIRE ALARM SYSTEMS IN 2024

Annotation. The authors of the article consider the main functions and classification of security and fire alarm systems. The article describes the existing types of maintenance for security and fire alarm systems. A statistical analysis of the results of fire alarm systems in fires has been carried out. The leading causes and objects of fires where fire alarm systems were installed have been identified. The social and material consequences of fires at protected facilities equipped with fire and security alarms have been calculated. The article examines statistical data characterizing the compliance of security and fire alarm systems with current legal acts and regulatory documents.

Keywords: fire alarm system, fire, social consequences of fire, material consequences of fire, cause of fire, object of fire.

Эффективное развитие современного общества невозможно без использования средств защиты от различных негативных факторов, воздействующих на него. Одним из видов защиты является защита от нанесения вреда имуществу, а также жизни и здоровью людей при пожаре и осуществлении противоправных действий. Это достигается в т.ч. за счет использования определенных технических средств защиты. Одним из наиболее распространенных технических средств является автоматическая сигнализация. Историческая справка: первая автоматическая

пожарная сигнализация появилась в 1851 г. в Германии, а первая электрическая охранная сигнализация была запатентована в США в 1853 г.

Любая современная автоматическая сигнализация – это сложный технический комплекс, объединяющий в себе не только различные электронные элементы обнаружения и передачи информации, но и сложнейшие программно-технические решения и алгоритмы, специальное компьютерное оборудование и соответствующее программное обеспечение [4]. Совершенствование систем автоматической сигнализации

и использование новейших достижений научно-технического прогресса, с одной стороны, ведет к повышению уровня защиты объекта, а с другой стороны – к существенному удорожанию систем безопасности. С целью повышения уровня безопасности на объекте защиты должно находиться одновременно несколько средств автоматической защиты, выполняющих, в свою очередь, различные функции, в том числе обнаружение пожара, иногда с возможностью его дальнейшего тушения и предотвращением возможности несанкционированного проникновения в защищаемое помещение. Подобная коллизия иногда приводит к тому, что заказчиками используются менее современные и менее функциональные, но более дешевые технические решения. С этой точки зрения идеальным решением оказывается охранно-пожарная сигнализация (далее – ОПС), которая объединяет в себе одновременно несколько функций.

ОПС сегодня – это сложная интегрированная система, объединяющая в себе функции пожарной сигнализации и охранной системы. Она подходит для обеспечения безопасности как крупных промышленно-производственных комплексов, так и совсем небольших объектов защиты. Например, для защиты жилого помещения одновременно от пожара и несанкционированного проникновения. ОПС может быть как самостоятельной системой, так и являться неотъемлемой частью автоматической системы пожарной защиты и одновременно частью комплексной системы безопасности объекта. При этом она может быть также задействована в работе системы контроля управления доступом на защищаемый объект [3].

Основные функции ОПС:

- обнаружение пожара,
- оповещение о возникновении пожара,
- тушение пожара в начальной стадии развития (если это предусмотрено),
- обнаружение и предотвращение несанкционированного доступа.

Обнаружение пожара достигается за счет использования специальных пожарных датчиков, реагирующих на пороговые значения опасных факторов пожара (дым, температура, пламя и др.) (далее – ОФП). Нередко ОПС могут быть объединены с системами автоматического пожаротушения, что дает возможность осуществлять тушение пожара еще в начальной стадии его развития. Оповещение о пожаре или иной угрозе осуществляется через соответствующую систему оповещения персонала, позволяющую своевременно начать эвакуацию людей из помещения. Ну и, конечно, охранная функция по обнаружению и предотвращению несанкционированного доступа осуществляется с помощью специальных охранных датчиков, реагирующих на движение, инфракрасное

излучение, изменение объема в помещении, открытие дверных и оконных проемов и т.п. [7, 2].

Основные требования к ОПС изложены в ряде нормативных документов [6, 1], которые устанавливают следующую классификацию ОПС: адресная, неадресная (пороговая) и адресно-аналоговая. Неадресная ОПС чаще используется для защиты мелких объектов и имеет определенные технические ограничения, существенно сужающие ее функции в плане определения точного места возникновения угрозы. Адресные ОПС используются на средних и крупных объектах защиты, позволяют более точно определить место возникновения пожара и несанкционированного проникновения на защищаемый объект. Адресно-аналоговые ОПС представляют собой более совершенные в техническом плане системы обеспечения контроля. Они в непрерывном режиме анализируют поступающую информацию от пожарных и охранных датчиков. Данная система может самостоятельно принимать решение о включении сигнала пожарной или охранной тревоги, эвакуации людей из помещений и начале тушения возникшего пожара.

Для эффективной и стабильной работы ОПС необходимо систематически осуществлять установленные законодательством следующие виды технического обслуживания ОПС:

- периодическое,
- профилактическое,
- ремонтно-восстановительное.

Периодическое обслуживание направлено на поддержание в целом работоспособности технического оборудования. Профилактическое обслуживание ОПС подразумевает под собой комплекс мер, нацеленных на предотвращение выхода из строя технических элементов ОПС. В свою очередь, ремонтно-восстановительное обслуживание осуществляется в случае выявления серьезных неисправностей в работе ОПС (замена неисправных технических элементов и узлов, настройка оборудования и т.п.). Своевременное техническое обслуживание ОПС и правильно выбранный вид обслуживания позволяет содержать элементы ОПС в работоспособном состоянии и снижать возможные риски от пожаров и противоправных действий на объекте защиты. Таким образом, правильно подобранная, спроектированная и регулярно обслуживаемая система ОПС является залогом обеспечения безопасности любого объекта защиты. Далее на примере 2024 г. рассмотрим основные результаты работы систем ОПС, осуществляющих функцию по защите объектов от пожаров и их последствий.

За рассматриваемый период было зарегистрировано порядка 1 535 пожаров на объектах, на которых была установлена система ОПС (см. табл. 1) [5]. При данных пожарах погибло 24 чел. и травмировано 57 чел., зарегистрирован

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

прямой материальный ущерб в размере 1 064 млн руб. В доленом отношении от общего количества пожаров с использованием различных установок и систем пожарной автоматики это составило: количество пожаров – 19 %, количество погибших людей при пожарах – 11 %, количество травмированных людей при пожарах – 12%, прямой материальный ущерб от пожаров – почти 19%. Как видно из приведенной статистики, количество пожаров и их последствия, связанные с ОПС, характеризуются весьма внушительным объемом.

Таблица 1– Основные результаты работы систем ОПС на пожарах на объектах защиты в 2024 г.

Результаты работы систем ОПС	Количество пожаров, ед.	Консолидированное количество погибших и травмированных людей, чел.	Зарегистрированный ущерб от пожара, млн руб.
ОФП воздействовали в зоне, защищаемой пожарной автоматикой			
Не включена	23	0	65,8
Неисправна	48	5	39,1
Сработала и подала сигнал о пожаре, став первоначальным источником сведений о пожаре	934	51	384,7
Исправна, но не сработала вследствие не достижения порога срабатывания	250	13	8,2
Сработала и подала сигнал о пожаре после получения информации о пожаре из других источников	186	6	477,5
Всего	1 441	75	975,3
ОФП воздействовали вне зоны, защищаемой пожарной автоматикой			
Пожарная автоматика исправна и не включена	2	0	0,0
Пожарная автоматика неисправна	6	3	53,0
Пожарная автоматика исправна и включена	86	3	36,0
Всего	94	6	89,0
Итого по ОПС	1 535	81	1 064,3

В данной таблице содержатся сведения о работе ОПС в зоне воздействия ОФП и состоянии ОПС, если она находилась вне зоны воздействия ОФП. Надо отметить, что количество пожаров и, соответственно, их последствий значительно больше в зоне воздействия ОФП. В общей сложности за 2024 г. на 1 456 пожарах ОПС была исправна и включена. И только на 79 пожарах система ОПС была неисправна или выключена. Этот статистический факт говорит о том, что изначально были допущены ошибки в проектировании или выборе системы защиты, либо о некачественном техническом обслуживании систем ОПС.

На рисунках 1-3 приведено распределение количества пожаров и их последствий по различным видам объектов пожаров, на которых использовалась система ОПС в 2024 г. Наибольшее количество пожаров отмечается на следующих группах объектов: объекты торговли – 426 ед., здания жилого назначения – 227 ед., объекты производственного назначения – 184 ед., объекты административного назначения - 151 ед., объекты общественного питания – 131 ед., объекты складского назначения – 105 ед. На остальных объектах защиты отмечается менее 100 пожаров. Наименьшее количество пожаров соответствует объектам сельскохозяйственного назначения – 4 ед. - и строящимся, реконструируемым объектам – 4 ед. (см. рисунок 1).

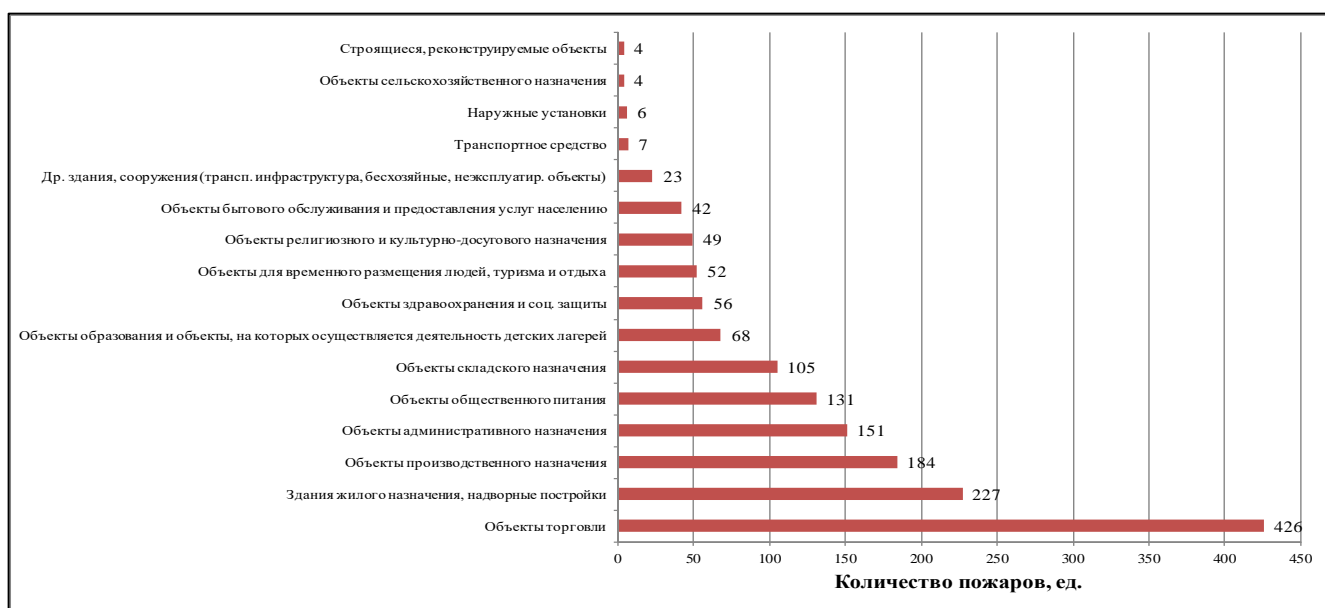


Рисунок 1 – Распределение количества пожаров по объектам возникновения пожаров, на которых была установлена система ОПС, в 2024 г.

Наибольшее количество погибших в зданиях жилого назначения – 24 чел. - и объектах травмированных людей отмечается на пожарах производственного назначения – 15 чел.

Отсутствуют социальные последствия на пожарах на транспортных средствах, наружных производственных установках, объектах

сельскохозяйственного назначения, строящихся и реконструируемых объектах (см. рисунок 2).

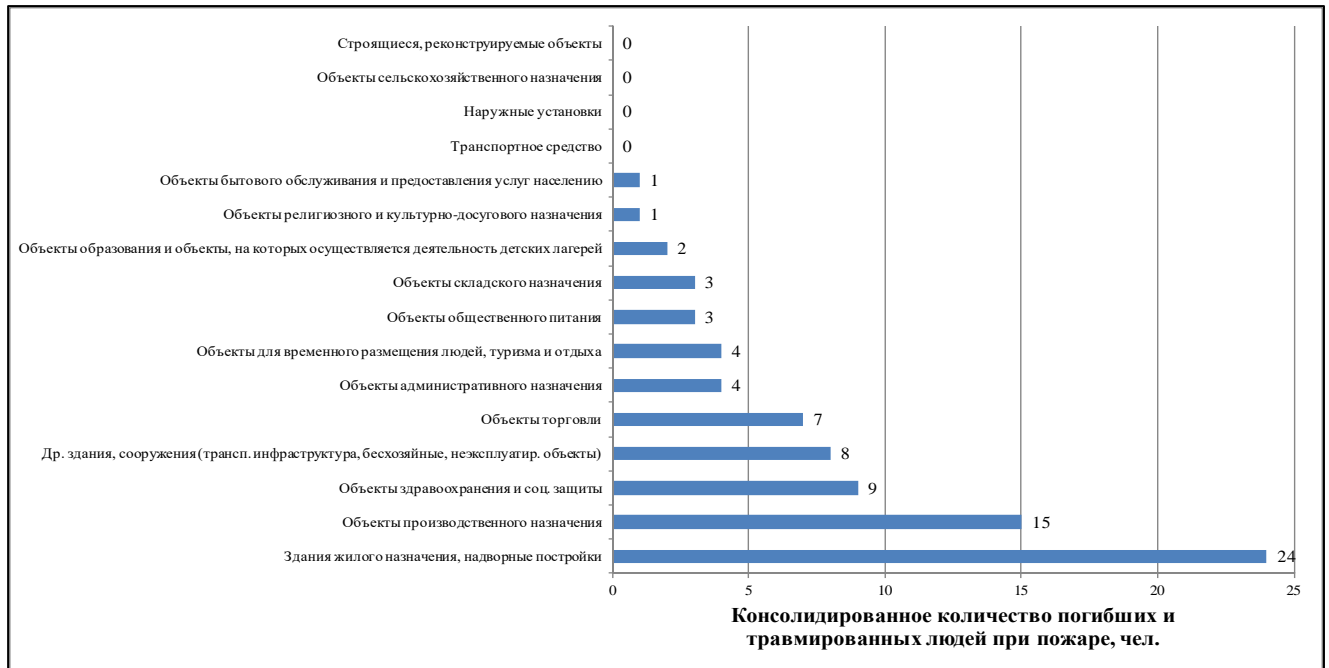


Рисунок 2 – Распределение социальных последствий пожаров по объектам возникновения пожаров, на которых была установлена ОПС, в 2024 г.

Что касается материальных последствий (см. рисунок 3), то наибольший прямой ущерб зарегистрирован на объектах производственного назначения – 426 млн руб., объектах складского назначения – 103 млн руб. Минимальные значения

материальных последствий соответствуют объектам сельскохозяйственного назначения – 0,2 млн руб., строящимся и реконструируемым объектам – 0,04 млн руб., наружным технологическим установкам – 0 руб.



Рисунок 3 – Распределение материальных последствий пожаров по объектам возникновения пожаров, на которых была установлена ОПС, в 2024 г.

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА

Рассмотренная выше структура распределений пожаров и их последствий по объектам пожаров с большой долей вероятности сохранится в ближайшие 3-5 лет.

На основе полученных данных по пожарам и их последствиям, характеризующих работу ОПС в 2024 г., осуществлен расчет социальных и материальных последствий пожаров в расчете на 1 пожар (см. таблица 2).

Таблица 2 – Расчетные значения последствий пожаров в расчете на 1 пожар на объектах, защищаемых системами ОПС

Результаты работы ОПС	Социальные последствия пожаров, чел./пожар	Материальные последствия пожаров, млн руб./пожар
Воздействие ОФП в зоне, защищаемой пожарной автоматикой		
Не включена	0,00	2,9
Неисправна	0,10	0,8
Сработала и подала сигнал о пожаре, став первоначальным источником сведений о пожаре	0,05	0,4
Исправна, но не сработала вследствие не достижения порога срабатывания	0,05	0,03
Сработала и подала сигнал о пожаре после получения информации о пожаре из других источников	0,03	2,6
Всего	0,05	0,7
Воздействие ОФП вне зоны, защищаемой пожарной автоматикой		
Пожарная автоматика исправна и не включена	0,00	0,0
Пожарная автоматика неисправна	0,50	8,8
Пожарная автоматика исправна и включена	0,03	0,4
Всего	0,06	0,9
Итого по ОПС	0,05	0,7

Анализ полученной информации показал, что в зоне воздействия ОФП наибольшие социальные последствия в расчете на 1 пожар отмечаются в случае неисправности средств автоматики (0,1 чел./пожар), а материальные последствия – при не включенной ОПС (2,9 млн руб./пожар) и в случае срабатывания и подачи сигнала о пожаре после получения информации о пожаре из других источников (2,6 млн руб./пожар). Что касается случаев воздействия ОФП вне зоны, защищаемой пожарной автоматикой, то наибольшие социальные последствия в расчете на 1 пожар наблюдаются в случае, когда пожарная автоматика неисправна: социальные последствия – 0,5 чел./пожар, материальные последствия – 8,8 млн руб./пожар). Таким образом, расчетные последствия от пожаров на объектах с ОПС выше в тех случаях, если пожарная автоматика неисправна.

Основными причинами пожаров на объектах, оборудованных ОПС, являются: нарушение правил устройства и эксплуатации (далее – НПУиЭ) электрооборудования – 64,4 % - и неосторожное обращение с огнем – 13,1 % (рисунок 4). Количество пожаров по причине поджога

составляет 5,2 %. Доля пожаров по остальным причинам возникновения пожара составляет от 0,4 % (НПУиЭ газового оборудования) до 4,4 % (НПУиЭ печного оборудования). Что касается последствий пожаров, то их высокие абсолютные значения соответствуют указанным выше ведущим причинам пожаров. На пожарах по причине НПУиЭ электрооборудования социальные последствия составили 46 чел., материальные – 671,6 млн руб. На пожарах по причине неосторожного обращения с огнем социальные последствия – 17 чел., а материальные – 290,3 млн руб.

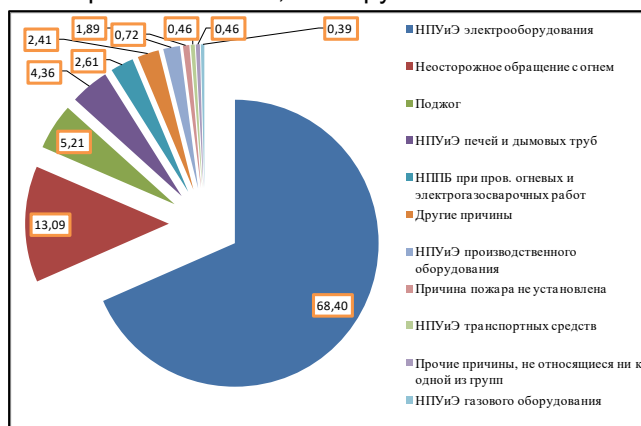


Рисунок 4 – Долевое распределение количества пожаров (%) по причинам их возникновения на объектах защиты, на которых были установлены ОПС, в 2024 г.

В заключение необходимо отметить, что на более чем 90 % пожаров, зарегистрированных в 2024 г., установки ОПС соответствовали требованиям существующих нормативных правовых актов, нормативных документов (далее – НПА). При данных пожарах погибло 79 % чел., травмировано 89 % чел. и зарегистрированный ущерб от пожаров составляет более 56 %. Количество пожаров, на объектах на которых не установлено соответствие ОПС требованиям НПА, составляет 6 %, количество газово погибших и травмированных людей соответственно 13 % и 2 %, а материальные потери – 32 %. Несоблюдение ОПС требованиям НПА установлено на 2,5 % объектов пожаров, на которых доля погибших людей составила 8 %, травмированных людей – 9 % и материальный ущерб – 6 % от общей величины зарегистрированных последствий пожаров. Количество объектов пожаров, на которых система ОПС должна быть установлена, но отсутствует, составляет всего 0,6 %. При этом на данных пожарах не зарегистрированы социальные потери от пожаров, а доля материального ущерба не превысила 6 %.

Проведенные статистические исследования показали, что доля систем ОПС в обеспечении

пожарной защиты объектов составляет не менее 20 %. Дальнейшее развитие систем ОПС, несомненно, будет связано с искусственным интеллектом. Исследования, проводимые в этом направлении, позволят, с одной стороны, значительно расширить существующую функциональность охранно-пожарных систем и увеличить уровень защищенности охраняемого объекта, а с другой стороны, снизить число ложных срабатываний ОПС и временные задержки

в принятии необходимых решений по обеспечению безопасности, в том числе и пожарной. В целом, такой подход позволит снизить возможные риски, связанные с защитой объекта, жизни и здоровья людей. А внедрение отечественных комплектующих и программного обеспечения еще дополнительно снизит затраты на оборудование объектов системами ОПС и их техническое обслуживание.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ 26342-84 Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры (с Изменениями № 1, 2) URL: <https://docs.cntd.ru/document/1200031059?ysclid=mdxfva71ll41586397> (дата обращения: 15.07.2025).
2. Гражданская защита. Энциклопедия. Т. III / Под общ.ред. С.К. Шойгу; МЧС России. – М.: ЗАО ФИД «Деловой экспресс», 2007. – 512 с. илл.
3. Обзор системы охранно-пожарной сигнализации / Блог Видеоглаз URL: <https://videoglaz.ru/blog/sistemy-ohranno-pozharnoy-signalizacii-1> (дата обращения: 01.07.2025).
4. Пожарная безопасность. Энциклопедия. 3-е изд. и доп. М.: ФГБУ ВНИИПО МЧС России, 2013, 564 с.
5. Пожары и пожарная безопасность в 2024 году: информационно-аналитический сборник / В.С. Гончаренко, Т.А. Четчина, В.И. Сибирко [и др.]. – Балашиха: ФГБУ ВНИИПО МЧС России, 2024. – 112 с. URL: <https://vniipo.ru/institut/informatsionnye-sistemy-reestry-bazy-i-banki-danny/federalnyy-bank-dannykh-rozhary/> (дата обращения: 17.07.2025).
6. Федеральный закон «Технический регламент о требованиях пожарной безопасности» от 22.07.2008 № 123-ФЗ (последняя редакция) / КонсультантПлюс URL: https://www.consultant.ru/document/cons_doc_LAW_78699/ (дата обращения: 20.07.2025).
7. Что такое ОПС: правила и особенности монтажа охранно-пожарной сигнализации URL: <https://admaer.ru/blog/articles/chto-takoe-ops/> (дата обращения: 01.07.2025).

УДК 351.74/75
ББК 67.7/67.51

ШИПУЛИН АНДРЕЙ ВЛАДИМИРОВИЧ, НАЧАЛЬНИК ОТДЕЛА АНАЛИЗА,
ПЛАНИРОВАНИЯ И КОНТРОЛЯ ГЛАВНОГО УПРАВЛЕНИЯ ВНЕВЕДОМСТВЕННОЙ
ОХРАНЫ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ
ФЕДЕРАЦИИ, ПОЛКОВНИК ПОЛИЦИИ

ПРОБЛЕМЫ И РЕШЕНИЯ ПРИ ИСПОЛЬЗОВАНИИ БИОМЕТРИЧЕСКИХ ДАННЫХ В СИСТЕМАХ БЕЗОПАСНОСТИ И ОХРАНЕ ОБЩЕСТВЕННОГО ПОРЯДКА.

Аннотация. В данной статье рассмотрены некоторые проблемные вопросы использования биометрических данных в системах контроля и управления доступом и системах охранных телевизионных в целях обеспечения безопасности при осуществлении охраны общественного порядка и обеспечении общественной безопасности. Рассмотрены особенности реализации требований законодательства Российской Федерации в области использования и защиты биометрических данных в данной сфере. Предложены варианты решения имеющихся проблем.

Ключевые слова: охрана общественного порядка, обеспечение общественной безопасности, вневедомственная охрана, цифровизация, системы безопасности, система контроля и управления доступом, система видеонаблюдения, биометрические данные, «изображение лица человека», единая биометрическая система.

Безопасность человека в нашем быстроменяющемся мире, в том числе в его цифровой части одна из актуальных задач правоохранительных органов. С учетом большого объема реализуемых государственных проектов цифровизации [5] законодательство Российской Федерации не успевает полноценно урегулировать все проблемы и вопросы, возникающие при внедрении новых технологий в деятельность человека. В данной статье будут рассмотрены некоторые из них, связанные с использованием биометрических данных граждан в целях обеспечения безопасности, к которым в соответствии с законодательством относится в том числе «изображение лица человека», полученное с помощью технических устройств и использование которого регламентируется федеральным законом Российской Федерации от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» [6]. При этом еще до принятия обозначенного федерального закона системы безопасности, использующие «изображение лица человека», уже получили широкое применение:

- в системах контроля и управления доступом в целях предотвращения несанкционированного проникновения на территорию охраняемого объекта,

- в системах видеонаблюдения - в целях идентификации и аутентификации отдельных лиц, в том числе и при осуществлении оперативно-розыскной деятельности, обеспечении общественной безопасности и охраны общественного порядка (системах охранных телевизионных, аппаратно-программных комплексах «Безопасный город» и в иных средствах получения видеoinформации (автомобильных и носимых видеорегистраторах, сотовых телефонах).

Однако, в связи с принятием федерального закона [6] возникла сложность использования биометрических данных, связанная с ужесточением требований к их получению, защите, хранению, обработке и передаче. Так, на сегодняшний день, биометрические данные («изображение лица человека») должны храниться только в Единой биометрической системе (далее – ЕБС) или иных, предусмотренных законом системах, аккредитованных в соответствии с законодательством. Нормативно определен оператор ЕБС – АО «Центр биометрических технологий». При этом по данным на август 2025 года, размещенным на сайте оператора ЕБС Российской Федерации в сети Интернет [4]

аккредитацию прошли всего пять разработчиков, два оператора связи, восемь организаций банковского сектора и Министерство Цифрового развития Российской Федерации. Необходимо отметить, что любая организация, которая планирует осуществлять обработку биометрических данных в системах контроля и управления доступом, столкнется с:

- необходимостью подключения системы к сети Интернет (или иным каналам) для доступа к Единой биометрической системе;
- проблемами увеличения времени прохождения через точки доступа (из-за высоких требований по защите информации и возможно недостаточной пропускной способностью каналов связи);
- оплатой оператору за каждый проход и необходимостью сдачи пользователями своих биометрических данных;
- увеличением затрат на систему в целом (оплата разработчикам за используемый программный продукт - биометрический процессор).

Поэтому в настоящий момент «изображение лица человека» в системах контроля и управления доступом практически не применяется. Исключение составляет региональный сегмент ЕБС, созданный в г. Москве, который позволяет осуществлять проход через системы контроля доступа с использованием «изображения лица» на территорию государственных органов (за исключением федеральных) и организаций г. Москвы [7].

В целом для государственных организаций видится целесообразным создание и использование собственных аккредитованных информационных систем, так как для ряда государственных организаций (ФСБ, МВД, УФСИН, ФСО России, Росгвардия) федеральным законом предусмотрено требование по запрету отождествления в единой биометрической системе принадлежности сотрудников и работников к силовым ведомствам. Для чего даже предусмотрено удаление такой информации по заявкам соответствующих государственных органов.

При использовании биометрии в системах контроля и управления доступом также необходимо учитывать, что пунктом 1 статьи 13 федерального закона [6] определено, что при проходе на территорию организаций оборонного, атомного, ядерного, химического, топливно-энергетического комплексов, ряда объектов транспортной инфраструктуры, режимных и некоторых иных

организаций, предусмотрена обязательная работа информационных систем только через оператора ЕБС.

Как уже ранее было обозначено использование «изображения лица человека» в системах видеонаблюдения широко используется сотрудниками МВД России для раскрытия совершенных преступлений [1], Тогда как

в соответствии со статьей 2 федерального закона [6] его положения не применяются при использовании биометрии в оперативно-розыскной деятельности. Также действие данного закона не распространяется на правоотношения, возникающие при осуществлении идентификации лиц с помощью биометрии в целях «обороны страны, обеспечения безопасности государства и охраны правопорядка» [6]. Вместе с тем не определено, в каких конкретно случаях возможно использование данного положения федерального законодательства. При этом федеральным законом предусмотрена обязанность операторов ЕБС (в том числе региональных сегментов) предоставлять по мотивированному запросу МВД или ФСБ России данные из системы. Порядок такого взаимодействия определен постановлением Правительства Российской Федерации [8]. Обмен информацией осуществляется посредством систем межведомственного электронного взаимодействия, срок предоставления сведений не более одного дня.

Вместе с тем, с учетом того, что задачи, решаемые правоохранительными органами в рамках охраны общественного порядка

и обеспечения общественной безопасности, часто требуют оперативной необходимости определения возможного нарушителя с использованием биометрических данных (в том числе и в автоматическом режиме, посредством различных программных продуктов), и не всегда это связано с оперативно-розыскной деятельностью, следует полагать, что данный порядок взаимодействия не в полной мере отвечает требованиям общественной безопасности.

Отдельно хочется отметить, что, несмотря на то, что участие в обеспечении охраны общественного порядка принимают также подразделения Росгвардии, на них подобные полномочия не возложены и при этом также отсутствует порядок их взаимодействия по данному вопросу с МВД и ФСБ России. Необходимо учитывать, что подразделения вневедомственной

охраны войск национальной гвардии также осуществляют охрану особо важных и режимных объектов, объектов подлежащих обязательной охране войсками национальной гвардии, а войсковые подразделения осуществляют охрану важных государственных объектов, специальных грузов и сооружений на коммуникациях и практически все выше обозначенные объекты оборудованы системами видеонаблюдения, управления контроля доступа, техническими средствами охраны. При этом весь это большой массив образующейся в сфере безопасности информации, несомненно представляющей интерес, никаким образом не используется.

В рамках этого видится целесообразным для его анализа использовать технологии искусственного интеллекта, в том числе обработки Больших данных.

Подобная ситуация складывается для всех правоохранительных органов и реализовать в рамках осуществления охраны общественного порядка потенциальную возможность оперативной проверки подозрительных граждан невозможно.

В дополнение к вышесказанному видится недостаточным, что федеральным законодательством [6] предусмотрена только добровольная сдача биометрических данных, кроме случаев обязательной сдачи иностранными гражданами и лицами без гражданства. При этом также только для данных лиц предусмотрено размещение биометрических данных без их согласия.

В заключении хочется отметить, что в условиях цифровизации деятельности правоохранительных органов внедрение технологий обработки Больших данных позволит при анализе информации, имеющейся в системах безопасности (на основе данных систем охранной сигнализации, управления контролем доступом, видеонаблюдения и иных), сформировать прогноз оперативной обстановки и окажет помощь в принятии управленческих решений (в том числе и с использованием технологий искусственного интеллекта). С учетом вышеизложенного, видится целесообразным пересмотреть установленный постановлением Правительства Российской Федерации [8] порядок и установить конкретные случаи получения правоохранительными органами (в том числе и Росгвардией) информации

в автоматизированном режиме (посредством сопряжения информационных систем) из ЕБС в целях охраны общественного порядка и обеспечения общественной безопасности.

Несомненно, имеющиеся возможности современных технологий в сфере безопасности должны использоваться в полном объеме правоохранительными органами. Вместе с тем их применение требует постоянного совершенствования правового, организационного и информационного взаимодействия при защите законных прав граждан

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Роль видеонаблюдения в качестве информационно-поисковой системы в раскрытии и расследовании преступлений по «горячим следам». / Эндреев М.М., Золотарев Д.В., Мехмет Б.// Актуальные вопросы борьбы с преступлениями, №2, 2024 г. с.63-67.
2. Использование достижений науки в розыскной и идентификационной деятельности. / Буряков Е.В.//Уголовно-правовые науки, №3, 2023 г., с.53-59.
3. Цифровая трансформация и государственное управление: научно-практическое пособие. / Емельянов А.С., Ефремов А.А., Калмыкова А.В. и др.// СПС «Гарант» (дата обращения 28 марта 2025 г.).
4. [www.https://ebs.ru](https://ebs.ru). Интернет-сайт оператора единой биометрической системы Российской Федерации.
5. Указ Президента Российской Федерации от 9 мая 2017 г. №203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «Консультант Плюс» (дата обращения 28 марта 2025 г.).
6. Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // СПС «Консультант Плюс» (дата обращения 28 марта 2025 г.).
7. Постановление Правительства Российской Федерации от 26 августа 2024 г. № 1151 «Об образовании регионального сегмента единой биометрической системы в г. Москве» // СПС «Консультант Плюс» (дата обращения 28 марта 2025 г.).

8. Постановление Правительства Российской Федерации от 28 декабря 2018 г. № 1703 «О предоставлении оператором единой биометрической системы и оператором регионального сегмента единой биометрической системы в Министерство внутренних дел Российской Федерации и Федеральную службу безопасности Российской Федерации сведений, содержащихся в единой биометрической системе и региональном сегменте единой биометрической системы» // СПС «Консультант Плюс» (дата обращения 28 марта 2025 г.).

УДК 343.984:351.74:347.7
67.9(2Рос=Рус)+66.9/10

**ЮДИНА СВЕТЛАНА МИХАЙЛОВНА, СТАРШИЙ НАУЧНЫЙ СОТРУДНИК ОТДЕЛА
РАЗРАБОТКИ НОРМАТИВНО-МЕТОДИЧЕСКИХ ДОКУМЕНТОВ ФКУ «НИЦ «ОХРАНА»
РОСГВАРДИИ**

**СПОРНЫЕ ВОПРОСЫ ОПРЕДЕЛЕНИЯ ОБЪЕКТОВ (ТЕРРИТОРИЙ),
ПОДЛЕЖАЩИХ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИТЕ**

Аннотация. Статья посвящена анализу правового регулирования и правоприменительной практики в сфере обеспечения антитеррористической защищенности объектов и территорий Российской Федерации. Рассмотрены проблемы точного отнесения объектов к конкретным постановлениям Правительства РФ, выявлены пробелы и коллизии в законодательстве, влияющие на эффективность реализации мер безопасности. Особое внимание уделено организациям образовательной, социальной и медицинской сфер, а также местам массового пребывания людей и объектам общественного питания. Обоснована необходимость межведомственного взаимодействия, уточнения понятийного аппарата и унификации требований по антитеррористической защищенности для формирования согласованной и устойчивой системы защиты граждан.

Ключевые слова: антитеррористическая защищенность, объекты и территории, правовое регулирование, правоприменительная практика, образовательные организации, социальные учреждения, медицинские организации, места массового пребывания людей.

YUDINA SVETLANA MIKHAILOVNA, SENIOR RESEARCHER, DEPARTMENT FOR THE DEVELOPMENT OF REGULATORY AND METHODOLOGICAL DOCUMENTS, FEDERAL STATE INSTITUTION «SCIENTIFIC AND RESEARCH CENTER «SECURITY» OF THE NATIONAL GUARD OF THE RUSSIAN FEDERATION

CONTROVERSIAL ISSUES IN THE CLASSIFICATION OF OBJECTS (TERRITORIES) SUBJECT TO ANTI-TERRORISM PROTECTION

Annotation. The article is devoted to the analysis of legal regulation and law enforcement practice in the field of ensuring anti-terrorism security of objects and territories in the Russian Federation. It examines issues related to the precise classification of objects under specific Government resolutions, identifies gaps and conflicts in the legislation affecting the effectiveness of security measures. Particular attention is paid to educational, social, and medical organizations, as well as places of mass gatherings and food service establishments. The study substantiates the necessity of interagency cooperation, clarification of terminology, and unification of anti-terrorism security requirements to establish a coherent and sustainable system for protecting citizens.

Keywords: anti-terrorism security, objects and territories, legal regulation, law enforcement practice, educational organizations, social institutions, medical organizations, places of mass gatherings.

В современной правоприменительной практике особую актуальность приобретает проблема корректного определения правового статуса объектов и территорий в контексте их отнесения к сферам действия нормативных правовых актов Правительства Российской Федерации, устанавливающих требования к обеспечению антитеррористической защищенности. Указанный аспект представляет собой не только вопрос формального соответствия объекта определенному постановлению, но и существенный элемент реализации политики

государства в области противодействия терроризму.

Неверная квалификация объектов с точки зрения применимости конкретного правового режима способна повлечь системные нарушения при организации мер антитеррористической защищенности. В результате правообладатели, исходя из ошибочных предпосылок, нередко реализуют комплекс мероприятий, не соответствующий реальному уровню террористической угрозы, а также противоречащий установленным нормативным требованиям, что, в конечном счете, снижает эффективность

профилактических мер и создает риски правовой неопределенности.

Существенным фактором, осложняющим процесс правоприменения, являются пробелы и коллизии в действующем законодательстве, регулирующем рассматриваемую сферу. Эти недостатки проявляются,

в частности, в следующих формах:

— отсутствие законодательных требований к обеспечению антитеррористической защищенности отдельных категорий объектов (например, предприятий общественного питания, объектов жилищного фонда, многоквартирных домов);

— неопределенность понятийно-категориального аппарата, препятствующая однозначной идентификации объекта в системе нормативного регулирования;

— неурегулированность критериев разграничения объектов по сферам нормативного воздействия в случаях, когда их ведомственная принадлежность и функциональное назначение подпадают под действие нескольких постановлений Правительства Российской Федерации.

Наибольшее количество правоприменительных ошибок, связанных

с некорректным определением категории объектов, подлежащих антитеррористической защите, наблюдается при интерпретации и реализации положений постановления Правительства Российской Федерации, предусматривающего обязательные мероприятия к антитеррористической защите мест массового пребывания людей (далее - ММПЛ) [1]. Данное постановление, являясь основным в части регулирования обеспечения безопасности в публично-доступных пространствах, требует от субъектов правоотношений не только формального соблюдения предписаний,

но и комплексного правового анализа характера объекта, интенсивности человеческого потока и уровня потенциальной террористической уязвимости.

Законодатель, установив понятие ММПЛ, определил в качестве таких мест:

территории общего пользования поселений, муниципальных или городских округов;

специально выделенные территории за пределами поселений, муниципальных или городских округов;

места общего пользования в зданиях, строениях, сооружениях или иных объектов.

При этом вышеуказанные объекты должны предусматривать при определенных условиях

одновременное нахождение на них более пятидесяти человек [2].

Тем не менее, анализ правоприменительной практики региональных органов исполнительной власти и органов местного самоуправления позволяет выявить устойчивую тенденцию к более широкому толкованию указанного понятия. Формируя перечни ММПЛ на соответствующих территориях, данные органы зачастую включают в них объекты, которые по своей правовой природе и функциональному назначению не отвечают критериям, установленным законом. К числу таких объектов, как правило, относятся здания органов государственной власти и местного самоуправления, иные административные сооружения, а также деловые, офисные и бизнес-центры, МФЦ.

Следует подчеркнуть, что само по себе отдельное здание, строение либо сооружение не охватывается нормативно закрепленным определением ММПЛ, поскольку законодатель прямо указывает на территории общего пользования за пределами зданий и места общего пользования внутри зданий, не распространяя действие нормы непосредственно на сам объект. Более того, нормативно закрепленное определение понятия места общего пользования в нежилом здании, строении, сооружении в действующем законодательстве отсутствует.

Исходя из анализа судебной практики, под указанной категорией, как правило, понимаются помещения, предназначенные для совместного использования несколькими субъектами, то есть обслуживающие более одного отдельного помещения в здании: лестничные клетки, холлы, лифтовые узлы, коридоры, подвальные и чердачные помещения. Так, Арбитражный суд Московского округа, рассматривая дело № А40-21524/2024, при разрешении вопроса о правомерности включения административного здания в перечень ММПЛ, пришел к выводу о несоответствии данного объекта критериям, закрепленным в Федеральном законе № 35-ФЗ, и признал включение здания в перечень неправомерным [3].

Указанное свидетельствует о необходимости законодательного уточнения и систематизации понятийного аппарата в сфере обеспечения антитеррористической защищенности. Целесообразным представляется корректировка легального определения ММПЛ, закрепленного в Федеральном законе № 35-ФЗ, с тем чтобы предусмотреть возможность отнесения к данной

категории отдельных зданий, строений и сооружений. Также необходимо конкретизировать антитеррористические меры к таким объектам и установить специальные положения в отношении административных зданий органов государственной власти субъектов Российской Федерации и органов местного самоуправления, а также дополнительные инженерно-технические меры охраны с учетом конструктивных и функциональных особенностей соответствующих объектов.

Особого анализа заслуживает и практика включения организаций общественного питания (кафе, ресторанов и иных аналогичных заведений) в перечни ММПЛ, которая представляется необоснованной. Правовыми нормами установлено, что в соответствующие перечни включаются только те ММПЛ, собственниками или пользователями которых не являются ФОИВ либо объекты, не относящиеся к сфере их деятельности [1]. Между тем деятельность по организации общественного питания нормативно отнесена к сфере ведения Роспотребнадзора, в том числе в части нормативно-правового обеспечения организации питания населения [4].

Исходя из этого, представляется обоснованным предложение о разработке Роспотребнадзором постановления Правительства Российской Федерации, регламентирующего требования к антитеррористической защищенности объектов общественного питания, либо в качестве альтернативного варианта – внесение соответствующих изменений в постановление Правительства Российской Федерации от 3 декабря 2014 г.

№ 1309, предусматривающее распространение установленных требований на объекты, относящиеся к сфере деятельности Роспотребнадзора, с одновременным уточнением состава и содержания мероприятий по обеспечению антитеррористической защищенности применительно к специфике функционирования предприятий общественного питания [5].

Следующим аспектом, заслуживающим внимание, является то обстоятельство, что в действующей системе нормативного регулирования организации, осуществляющие дополнительное образование, в настоящее время не включены в перечень объектов, подлежащих обязательной антитеррористической защите. Такая правовая лакуна порождает состояние неопределенности в вопросах обеспечения безопасности данной категории образовательных

учреждений, что объективно снижает уровень защищенности обучающихся и персонала.

Дополнительное образование направлено на всестороннее удовлетворение образовательных потребностей личности в ее духовно-нравственном, физическом, интеллектуальном, профессиональном развитии и не влечет за собой повышения уровня образования [6]. Соответствующие образовательные организации, осуществляющие такую деятельность, вправе реализовывать дополнительные общеобразовательные программы — как общеразвивающие, так и предпрофессиональные. Общеразвивающие – предназначены для детей и взрослых, предпрофессиональные — преимущественно для детей. Реализующие предпрофессиональные программы образовательные организации функционируют в специализированных формах — детские школы искусств, музыкальные, художественные и спортивные школы, школы художественных ремесел и иные учреждения аналогичного профиля.

С учетом изложенного представляется обоснованным отнесение организаций дополнительного образования к объектам, находящимся в сфере деятельности Минпросвещения России как ФОИВ, уполномоченному на нормативно-правовое обеспечение в сфере дополнительного образования детей и взрослых [7].

Планируемые изменения в постановление Правительства Российской Федерации от 2 августа 2019 г. № 1006 [8] предусматривают возможность включения организаций, осуществляющих образовательную деятельность по реализации дополнительных образовательных программ в региональные перечни объектов (территорий), подлежащих антитеррористической защите и находящихся в сфере ведения Министерства просвещения Российской Федерации. Однако включение объектов в указанные перечни будет осуществляться на основании представлений уполномоченных органов, их формирующих, и оформляться решениями высших должностных лиц субъектов Российской Федерации.

Однако следует учитывать, что, например, учреждения дополнительного образования в сфере культуры и искусства, уже подпадают под действие специальных норм антитеррористического регулирования. Так, детские школы искусств, учрежденные органами государственной власти субъектов Российской Федерации либо органами

местного самоуправления в области культуры отнесены к данному виду объектов [9].

Таким образом, устранение пробелов в нормативном определении статуса организаций дополнительного образования в контексте антитеррористической защищенности представляется необходимым направлением совершенствования правового регулирования. Это позволит обеспечить единообразие правоприменения, повысить уровень безопасности образовательной среды и обеспечить реализацию принципа дифференцированного подхода к защите объектов с учетом особенностей их образовательной и социокультурной деятельности.

Существенные сложности в правоприменительной практике вызывает вопрос отнесения к объектам, подлежащим обязательной антитеррористической защите, организаций, предназначенных для детей-сирот и детей, оставшихся без попечения родителей. Указанная категория учреждений характеризуется сложной межотраслевой правовой природой, что обуславливает неоднозначность их нормативной квалификации и, как следствие, вызывает затруднения при определении компетентных органов, ответственных за обеспечение их антитеррористической защищенности.

Следует учитывать, что в зависимости от основного вида деятельности конкретная организация может быть отнесена как к образовательным учреждениям, так и к медицинским или организациям, оказывающим социальные услуги. Такое разграничение имеет принципиально важное значение, поскольку именно от этого зависит выбор нормативного правового акта, регулирующего обеспечения антитеррористической защищенности объекта.

Дети в возрасте от рождения и до достижения трехлетнего возраста находятся на содержании в учреждениях, представляющих социальные услуги, либо в образовательных организациях, в структуре которых созданы необходимые условия для их содержания, воспитания и развития в соответствии с возрастными потребностями [10]. Несовершеннолетние в возрасте от трех лет и до достижения ими совершеннолетия (либо признания полностью дееспособными в порядке, установленном гражданским законодательством) размещаются в организациях, оказывающих социальные услуги, при этом получают образование в расположенных поблизости дошкольных и общеобразовательных

учреждениях, либо направляются непосредственно в образовательные организации, если иное не представляется возможным.

Оказание стационарных социальных услуг детям-сиротам и детям, оставшимся без попечения родителей, осуществляется в детских домах-интернатах, в том числе специализированных, например, психоневрологических, и иных аналогичных учреждениях [11]. Полустанционарная форма социального обслуживания несовершеннолетних, нуждающихся в социальную поддержку и реабилитации, реализуется в специализированных центрах, приютах и центрах помощи детям, оставшимся без попечения родителей [12].

Следовательно, данные учреждения относятся к сфере деятельности Министерства труда и социальной защиты Российской Федерации, и реализуют мероприятия по антитеррористической защищенности в соответствии с положениями постановления Правительства Российской Федерации от 13 мая 2016 г. № 410 [13].

Отдельную группу составляют организации, ведущие деятельность по образовательным программам для детей-сирот и детей, оставшихся без попечения родителей. Указанные учреждения имеют статус некоммерческих организаций и осуществляют образовательную деятельность в качестве основного вида деятельности на основании лицензий, выдаваемых в установленном порядке [6]. К этой категории относятся детские дома, школы-интернаты, детские дома-школы, а также специальные (коррекционные) образовательные учреждения для детей с ограниченными возможностями здоровья и отклонениями в развитии. Их деятельность находится в сфере ведения Минпросвещения России, а обеспечение антитеррористической защищенности регламентируется постановлением Правительства Российской Федерации от 2 августа 2019 г. № 1006 [8].

К особой категории относятся дома ребенка, являющиеся самостоятельными юридическими лицами, осуществляющими медицинскую деятельность в качестве основного вида деятельности в соответствии с лицензиями, выданными в установленном порядке [14]. Дома ребенка создаются для круглосуточного содержания и воспитания детей в возрасте от рождения до четырех лет, оставшихся без попечения родителей либо временно помещенных в них по медицинским или

социальным показаниям. В рамках своей деятельности дома ребенка обеспечивают комплекс медицинских, социальных и психолого-педагогических мер, направленных на восстановление здоровья и развитие детей [15]. Антитеррористическая защищенность домов ребенка, как объектов здравоохранения регулируется положениями постановления Правительства Российской Федерации от 13 января 2017 г. № 8 [16].

Таким образом, нормативное разграничение организаций для детей-сирот и детей, оставшихся без попечения родителей, по ведомственному принципу обуславливает необходимость системного подхода к их правовому регулированию в сфере антитеррористической защищенности. В целях исключения коллизий правоприменения и обеспечения равного уровня защиты всех категорий данных учреждений представляется целесообразным разработать единые методические рекомендации по обеспечению антитеррористической защищенности организаций, функционирующих в системе образования, здравоохранения и социальной защиты, предусматривающие унифицированные критерии угроз и меры профилактического характера. Это будет способствовать формированию

целостного межведомственного механизма профилактики террористических рисков в отношении наиболее уязвимых социальных групп населения.

Анализ нормативно-правового регулирования и правоприменительной практики показывает, что эффективность обеспечения антитеррористической защищенности объектов и территорий напрямую зависит от точного отнесения объектов к конкретным постановлениям Правительства Российской Федерации. Выявленные пробелы, коллизии и отсутствие унифицированных критериев классификации создают риски несоответствия мер защиты реальной угрозе. Усиление межведомственного взаимодействия, уточнение понятийного аппарата и систематизация требований к объектам различных отраслей (образовательных, социальных, медицинских и иных) являются необходимыми условиями формирования согласованной и устойчивой системы антитеррористической защищенности.

Совершенствование правового регулирования в данной сфере должно обеспечить единообразное применение норм и адекватную защиту всех категорий объектов в интересах безопасности граждан Российской Федерации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии Российской Федерации, и форм паспортов безопасности таких мест и объектов (территорий): постановление Правительства Российской Федерации от 25 марта 2015 г. № 272 (ред. от 24.10.2023) // Собрание законодательства Российской Федерации — 06.04.2015 — № 14 — Ст. 2119.
2. О противодействии терроризму: федеральный закон от 6 марта 2006 г. № 35-ФЗ (ред. от 28.02.2025) // Собрание законодательства Российской Федерации — 13.03.2006 — № 11 — Ст. 1146.
3. Постановление Арбитражного суда Московского округа от 28 ноября 2024 г. № Ф05-26228/2024 по делу № А40-21524/2024.
4. Об утверждении Положения о Федеральной службе по надзору в сфере защиты прав потребителей и благополучия человека: постановление Правительства Российской Федерации от 30 июня 2004 г. № 322 (ред. от 02.04.2025) // Собрание законодательства Российской Федерации — 12.07.2004 — № 28 — Ст. 2899.
5. Об утверждении требований к антитеррористической защищенности объектов (территорий) Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека и формы паспорта безопасности этих объектов (территорий): постановление Правительства Российской Федерации от 3 декабря 2014 г. № 1309 (ред. от 07.03.2025) // Собрание законодательства Российской Федерации — 15.12.2014 — № 50 — Ст. 7098.
6. "Об образовании в Российской Федерации: федеральный закон от 29 декабря 2012 г. № 273-ФЗ (ред. от 29.09.2025) // Собрание законодательства Российской Федерации — 31.12.2012 — № 53 (ч. 1) — Ст. 7598.
7. Об утверждении Положения о Министерстве просвещения Российской Федерации и признании утратившими силу некоторых актов Правительства Российской Федерации: постановление Правительства Российской Федерации от 28 июля 2018 г. № 884 (ред. от 21.02.2025) // Собрание законодательства Российской Федерации — 06.08.2018 — № 32 (Часть II) — Ст. 5343.

8. Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий): постановление Правительства Российской Федерации от 2 августа 2019 г. № 1006 (ред. от 05.03.2022) // Собрание законодательства Российской Федерации — 12.08.2019 — № 32 — Ст. 4716.
9. Об утверждении требований к антитеррористической защищенности объектов (территорий) в сфере культуры и формы паспорта безопасности этих объектов (территорий): постановление Правительства Российской Федерации от 11 февраля 2017 г. № 176 (ред. от 08.05.2025) // Собрание законодательства Российской Федерации — 27.02.2017 — № 9 — Ст. 1358.
10. О деятельности организаций для детей-сирот и детей, оставшихся без попечения родителей, и об устройстве в них детей, оставшихся без попечения родителей: постановление Правительства Российской Федерации от 24 мая 2014 г. № 481 (ред. от 19.04.2022) // Собрание законодательства Российской Федерации — 02.06.2014 — № 22 — Ст. 2887.
11. Об утверждении примерной номенклатуры организаций социального обслуживания: приказ Минтруда России от 17 декабря 2020 г. № 918н // Официальный интернет-портал правовой информации: <http://pravo.gov.ru> — № 0001202102200036— 20.02.2021.
12. Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних: федеральный закон от 24 июня 1999 г. № 120-ФЗ (ред. от 01.04.2025) // Собрание законодательства Российской Федерации — 28.06.1999 — № 26 — Ст. 3177.
13. Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства труда и социальной защиты Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства труда и социальной защиты Российской Федерации, и формы паспорта безопасности этих объектов (территорий): постановление Правительства Российской Федерации от 13 мая 2016 г. № 410 (ред. от 24.03.2023) // Собрание законодательства Российской Федерации — 23.05.2016 — № 21 — Ст. 3006.
14. Об основах охраны здоровья граждан в Российской Федерации: федеральный закон от 21 ноября 2011 г. № 323-ФЗ (ред. от 23.07.2025) // Собрание законодательства Российской Федерации — 28.11.2011 — № 48 — Ст. 6724.
15. Об утверждении Типового положения о доме ребенка: приказ Минздравсоцразвития России от 12 апреля 2012 г. № 344н // Российская газета — № 141 — 22.06.2012.
16. Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства здравоохранения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства здравоохранения Российской Федерации, и формы паспорта безопасности этих объектов (территорий): постановление Правительства Российской Федерации от 13 января 2017 г. № 8 (ред. от 15.08.2025) // Собрание законодательства Российской Федерации — 23.01.2017 — № 4 — Ст. 654.

УДК 004.056

ББК 16.8

**ЯНГИРОВ АДиль ИЛДАРОВИЧ, КАПИТАН ПОЛИЦИИ, НАЧАЛЬНИК ОТДЕЛЕНИЯ
ЛАБОРАТОРНЫХ ИССЛЕДОВАНИЙ И ИСПЫТАНИЙ ФКУ «НИЦ «ОХРАНА» РОСГВАРДИИ**

**ПОДХОД К РАСПРЕДЕЛЕНИЮ РЕСУРСОВ БЕЗОПАСНОСТИ
ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

Аннотация. Обеспечение эффективности системы безопасности автоматизированных систем обуславливает необходимость рационального распределения ресурсов. В статье предложен подход к распределению приоритетности реализации мер защиты автоматизированных систем, основанный на анализе банка данных угроз ФСТЭК России.

Ключевые слова: автоматизированная система, распределение ресурсов, меры защиты.

**YANGIROV ADIL ILDAROVICH, HEAD OF THE LABORATORY RESEARCH AND TESTING
DEPARTMENT FSI «SRC «OKHRANA» OF THE FEDERAL SERVICE OF NATIONAL GUARD OF RUSSIA**

**APPROACH TO DISTRIBUTION OF SECURITY RESOURCES
TO ENSURING SECURITY OF AUTOMATED SYSTEMS**

Annotation. Ensuring the effectiveness of the security system of automated systems requires rational distribution of resources. The article proposes an approach to the distribution of the priority of implementing measures to protect automated systems, based on the analysis of the FSTEC of Russia threat database.

Keywords: automated system, prioritization, resource allocation, security measures.

Современные автоматизированные системы (далее – АС) представляют собой сложные комплексы, обрабатывающие значительные объемы информации и данных, зачастую конфиденциального характера.

Особую важность подобные системы имеют в государственных структурах, в частности, в войсках национальной гвардии Российской Федерации, МВД России, МЧС России и других аналогичных ведомствах. Функционирование АС в таких государственных структурах напрямую связано с обеспечением национальной безопасности, правопорядка и защиты населения.

Воздействие злоумышленников на обрабатываемые АС данные способно вызвать катастрофические последствия, включая полный паралич работы организационных, технических, финансовых и других значимых систем. Подобные инциденты приводят к коллапсу функционирования государственных и коммерческих организаций, нарушая общественную стабильность и нанося непоправимый экономический ущерб.

Потенциальные последствия недостаточного внимания к вопросам информационной безопасности были наглядно продемонстрированы инцидентом, произошедшим 28 июля 2025 года в компании «Аэрофлот», где сбой в работе ключевых АС привел к масштабным нарушениям

в деятельности компании [1]. Данный случай еще раз подчеркивает, что уязвимости в критической информационной структуре способны парализовать работу организации и нанести значительный репутационный и экономический ущерб. Таким образом, обеспечение защищенности АС является стратегической и актуальной задачей национальной и экономической безопасности, а не просто технической необходимостью.

На практике выделяемые на безопасность ресурсы обычно ограничены, что делает невозможным реализацию всех потенциально возможных защитных мер в равной степени. В связи с этим возникает проблема оптимального распределения ресурсов безопасности и принятия соответствующих мер для достижения требуемого уровня защищенности АС с учётом ограничений. Научная новизна настоящего исследования заключается в разработке нового формализованного подхода к распределению ресурсов безопасности АС, основанного а статистическом анализе угроз.

В 2015 году Федеральной службой по техническому и экспортному контролю (ФСТЭК России) в целях информационной и методической поддержки при работах по определению и оценке угроз безопасности информации

в информационных системах был создан Банк данных угроз безопасности информации (далее – БДУ) [2] (рисунок 1).

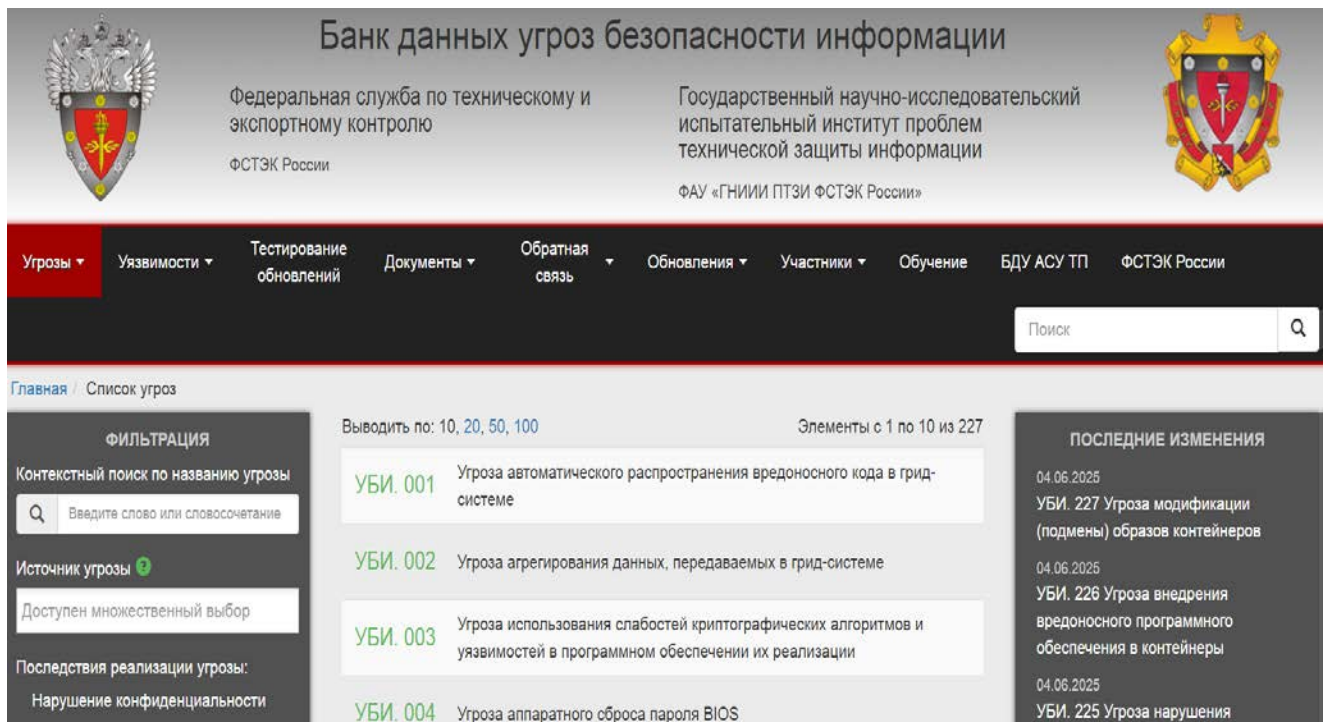


Рисунок 1 – Банк данных угроз ФСТЭК России

БДУ регулярно обновляется, последние изменения были внесены буквально недавно: 10 сентября 2025 года. На основе БДУ возможно определение оптимального соотношения мер защиты, по состоянию на 10 сентября 2025 года в БДУ включено 227 угроз. Для каждой из 227 угроз приводится описание, включающее информацию об источнике их происхождения: внешние нарушители, внутренние нарушители либо обе категории одновременно. Визуальное представление структуры указанных угроз отражено на рисунках 1, 2.

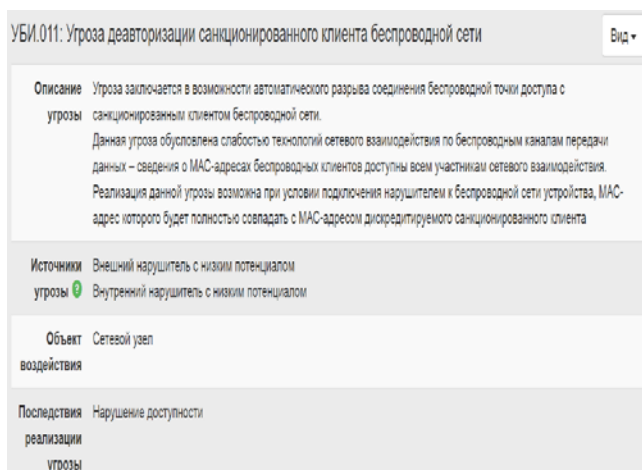


Рисунок 2 – Вариант представления угроз с разными последствиями

Помимо этого, существует категория угроз, источником которых не являются нарушители (рисунок 3). Такие угрозы возникают вследствие технических сбоев, ошибок, обусловленных человеческим фактором и тому подобного.

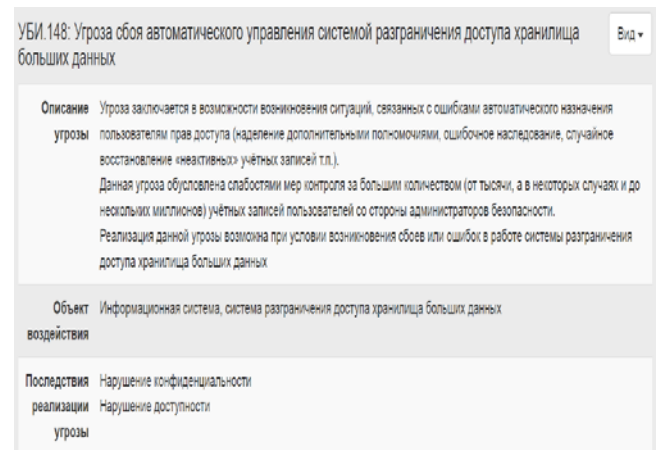


Рисунок 3 – Вариант представления угроз, источником которых не являются нарушители

Таким образом, атаки на АС можно разделить на три основные категории:

- 1) внешние угрозы;
- 2) внутренние угрозы;
- 3) угрозы, вызванные сбоями и ошибками.

С учетом классификации по источникам происхождения общее количество угроз достигает

332, из которых: 172 относятся к внешним угрозам, 158 – к внутренним и 2 угрозы обусловлены техническими сбоями, ошибками и прочими недостатками.

Полученные статистические данные применимы для решения задачи распределения ресурсов безопасности в целях обеспечения защищенности автоматизированных систем. Для наглядности и удобства практического использования представим указанные значения в процентном виде:

- 1) внешние угрозы ($\approx 51,8\%$);
- 2) внутренние угрозы ($\approx 47,6\%$);
- 3) угрозы, вызванные сбоями и ошибками ($\approx 0,6\%$).

В условиях воздействия 332 угроз, исходя из полученных значений, можно сделать вывод, что 51,8% мер должно быть направлено на противодействие внешним угрозам, 47,6% – на противодействие внутренним угрозам, а 0,6% – на предотвращение сбоев и ошибок.

Следует подчеркнуть, что использование данного подхода требует индивидуального анализа в каждой конкретной ситуации. Не во всех случаях полный перечень угроз, представленных в БДУ, будет актуален, так как функционал защищаемой АС может не включать операции, на которые эти угрозы направлены.

Кроме представленного варианта возможно распределение ресурсов безопасности в зависимости от последствий реализации угроз.

В сборнике передового опыта «Защита критически важных объектов инфраструктуры от террористических атак», подготовленном Контртеррористическим управлением ООН (КТУ ООН) и Исполнительным директором Контртеррористического комитета Совета Безопасности ООН (ИДКТК) при участии Интерпола в 2018 году, обобщен международный опыт и аргументируется необходимость сосредоточения ресурсов на противодействии наиболее опасным угрозам для обеспечения требуемого уровня защиты от террористических рисков. Особое внимание в документе уделяется киберугрозам, которые, несмотря на иную природу по сравнению с физическими угрозами, способны приводить к сопоставимым последствиям [3].

В Российской Федерации одним из ключевых нормативных актов в этой сфере выступают Правила категорирования объектов критической информационной инфраструктуры, утвержденные постановлением Правительства РФ от 8 февраля 2018 г. № 127. Согласно пункту 14.1 указанных Правил при формировании моделей нарушителей и угроз приоритет должен отдаваться наихудшим

сценариям, предполагающим целенаправленные компьютерные атаки на объекты критической информационной инфраструктуры с максимальным ущербом [4].

В БДУ также для каждой угрозы представлено описание возможных потенциальных последствий при реализации угрозы, выделены следующие типы последствий: «нарушение конфиденциальности», «нарушение целостности» и «нарушение доступности». Количество потенциальных последствий реализации угрозы варьируется от одного до трёх

в зависимости от её потенциала, что позволяет осуществлять категоризацию угроз на основе данного критерия.

В соответствии с БДУ [2] от общего количества угроз с учётом источника (332 шт.):

- а) имеющие 1 возможное последствие – 127 шт ($\approx 38,25\%$);
- б) имеющие 2 возможных последствия – 73 шт ($\approx 22\%$);
- в) имеющие 3 возможных последствия – 132 шт ($\approx 39,75\%$).

Таким образом, в первую очередь 39,75 % мер должно быть направлено на противодействие угрозам, имеющим 3 последствия (наиболее опасным и имеющим наивысший приоритет по противодействию), далее 22% мер угрозам, имеющим 2 последствия, и в конечном итоге 38,25 % мер должно быть направлено против угроз, имеющих 1 последствие.

Представленный подход, основанный на анализе статистических данных об угрозах и их распределении по источникам происхождения, может быть применен при планировании мер и распределении ресурсов защиты АС специалистами по информационной безопасности.

В отличие от качественных и зачастую субъективных методов оценки рисков, предлагаемый подход позволяет перейти к количественному

и статистически обоснованному распределению мер защиты, задавая четкие приоритеты на основе объективных статистических данных об источниках и потенциальной тяжести угроз.

Вместе с тем, применение данного подхода невозможно без тщательного учета индивидуальных особенностей АС, ее архитектуры, функционального назначения и специфики обрабатываемой информации. Предлагаемый подход достаточно гибок и может быть модифицирован и масштабирован в зависимости от изменяющихся условий и конкретных задач обеспечения информационной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Хакеры взяли на себя ответственность за сбой «Аэрофлота»/ Анисимова Н., Шокурова Е., Костринский Г, Добрунов М.– [Электронный ресурс] – Режим доступа. – URL: https://www.rbc.ru/technology_and_media/28/07/2025/6887359f9a7947bac129a341 (Дата обращения: 11.09.2025).
2. Банк данных угроз безопасности информации – [Электронный ресурс] – Режим доступа. – URL: <https://bdu.fstec.ru/> (Дата обращения: 11.09.2025).
3. Защита критически важных объектов инфраструктуры от террористических атак: сборник передового опыта. – [Электронный ресурс] – Режим доступа. – URL: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_ru.pdf (Дата обращения: 11.09.2025).
4. Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127«Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // Собрание законодательства Российской Федерации – 19.02.2018 – № 8 (часть I) – Ст. 1204.