Воронежский институт МВД России

ОХРАНА, БЕЗОПАСНОСТЬ, СВЯЗЬ

Сборник статей

Выпуск 10

Часть 1

Воронеж – 2025

ББК 32.811
О-92

Охрана, безопасность, связь: сборник статей. Вып. 10. – Часть 1.
О-92 – Воронеж : Воронежский институт МВД России, 2025. – 183 с.

ISBN 978-5-00229-186-1
ISBN 978-5-00229-187-8

В журнале содержатся материалы Международной научно-практической конференции «Охрана, безопасность, связь – 2024», состоявшейся в Воронежском институте МВД России 28 ноября 2024 года. Издание представляет интерес для профессорско-преподавательского состава, адъюнктов, курсантов и слушателей образовательных организаций МВД России и сотрудников правоохранительных органов.

О-17-76(II)-25

ISBN 978-5-00229-186-1
ISBN 978-5-00229-187-8

ОГЛАВЛЕНИЕ

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ОХРАНЫ И БЕЗОПАСНОСТИ ОБЪЕКТОВ

ПРИМЕНЕНИЕ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ РОССИИ И ПЕРСПЕКТИВЫ ИХ РАЗВИТИЯ

Абросимова Евгения Михайловна,
кандидат технических наук

ИСПОЛЬЗОВАНИЕ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ И АНАЛИЗА ДАННЫХ ДЛЯ ПРОГНОЗИРОВАНИЯ УГРОЗ

USING VIDEO SURVEILLANCE AND DATA ANALYSIS SYSTEMS TO PREDICT THREATS

В статье рассмотрен вопрос применения систем видеонаблюдения и анализа данных для прогнозирования угроз общественной безопасности. Затронуты ключевые аспекты данного вопроса.

This article discusses the use of video surveillance systems and data analysis to predict threats to public safety. The key aspects of this issue are touched upon.

Использование систем видеонаблюдения и анализа данных для прогнозирования угроз стало важным направлением в сфере обеспечения безопасности. Эти технологии позволяют реализовать проактивные подходы к предотвращению преступлений и различным угрозам, что особенно актуально для государственных учреждений, бизнесов и общественных мест. Рассмотрим подробнее, как именно работают эти технологии и какие преимущества они дают.

1. Системы видеонаблюдения.

Современные системы видеонаблюдения оснащены высококачественными камерами, которые могут записывать в различных условиях освещения, а также с использованием технологий, таких как тепловое видение или ночное видение. Эти камеры могут устанавливаться в стратегических точках: на улицах, в общественном транспорте, на зданиях, в торговых центрах и т.д.

2. Умные алгоритмы и анализ данных.

Современные системы видеонаблюдения интегрируются с алгоритмами машинного обучения и искусственного интеллекта, позволяя осуществлять:

– распознавание лиц: системы могут идентифицировать известных правонарушителей на основе биометрических данных;

– анализ поведения: алгоритмы могут отслеживать поведение людей и выявлять подозрительные действия, такие как агрессивное поведение, группировки или длительное пребывание в определенном месте;

– событийный анализ: интеллектуальные системы способны выделять аномальные события, такие как падение человека, внезапное скопление людей или акты вандализма.

3. Прогнозирование угроз.

Использование больших данных и аналитических инструментов позволяет:

– собрать данные: системы записывают огромное количество информации, включая время, место, тип событий и даже метеорологические условия;

– моделирование угроз: на основании собранных данных формируются модели, которые помогают предсказать вероятность возникновения определенных угроз в будущем на основе исторического анализа;

– геопространственный анализ: оперативная информация может использована для построения карт угроз, что позволяет определить «горячие точки» (районы с высокой вероятностью преступлений). Это позволяет правоохранительным органам и службам безопасности заранее направлять ресурсы в зоны повышенного риска.

4. Реализация системы оповещения.

На основе анализа данных системы могут автоматически генерировать уведомления для операторов безопасности, что позволяет своевременно реагировать на потенциальные угрозы. Это может включать в себя:

– различные уровни сигнализации для различных типов угроз (например, низкий, средний и высокий уровень риска);

– синхронизация с другими системами безопасности, такими как контроль доступа или системы охраны.

5. Этические и правовые аспекты.

Несмотря на многочисленные преимущества, использование систем видеонаблюдения вызывает ряд этических и правовых вопросов:

– конфиденциальность: необходимо гарантировать, что сбор и обработка данных не нарушает права граждан на личную жизнь;

– законодательство: разработка четких регуляторных норм, которые будут учитывать использование лицензионных систем и защиту данных;

– ошибки алгоритмов: несмотря на высокую эффективность, машины могут ошибаться. Это требует наличия человека, который будет проверять действия системы.

Системы видеонаблюдения могут интегрироваться с другими механизмами, такими как системы оповещения, ЧП, службы экстренной

помощи и т.д. Это позволяет оперативно реагировать на возможные угрозы, получая полное представление о ситуации.

6. Преимущества.

6.1. Повышение безопасности. Системы видеонаблюдения способствуют созданию безопасной городской среды, останавливая потенциальных преступников, которые осознают, что их действия будут зафиксированы.

6.2. Данные для анализа. Собранные данные могут использоваться для более глубокого анализа общественной безопасности. Например, можно получать данные о времени и частоте преступлений в определенных зонах, что позволит целенаправленно усиливать патрулирование.

6.3. Эффективность реагирования. При помощи предсказательной аналитики, правоохранительные органы могут более эффективно использовать свои ресурсы, управляя ими на основе реальных данных о возможных угрозах.

В краткосрочной перспективе ожидается дальнейшее совершенствование технологий. Искусственный интеллект будет продолжать эволюционировать, что сделает системы видеонаблюдения еще более умными и способными к самообучению. В долгосрочной перспективе возможно развитие широких сетей различных подключенных устройств, в том числе дронов и мобильных камер, которые смогут дополнить системы стационарного видеонаблюдения.

Кроме того, важно будет наладить международное сотрудничество в сфере безопасности, чтобы делиться опытом, лучшими практиками и технологическими новинками, что поможет оптимизировать процессы диагностики угроз и минимизировать риски.

Использование систем видеонаблюдения и анализа данных для прогнозирования угроз представляет собой мощный инструмент для повышения уровня безопасности. Современные технологии позволяют не только реагировать на угрозы в режиме реального времени, но и предсказывать их, что делает возможным проактивное предотвращение преступлений. Однако необходимо учитывать этические нормы и правовые аспекты, чтобы гарантировать баланс между безопасностью и личной свободой.

Технологии видеонаблюдения и анализа данных являются мощным инструментом для предотвращения угроз и повышения безопасности общественных пространств. Правильное применение этих технологий, с учетом этических и правовых аспектов, открывает новые горизонты в области общественной безопасности, превращая проактивный подход к управлению угрозами в реальность.

ЛИТЕРАТУРА

1. ГОСТ Р 56875-2016. Информационные технологии. Системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий : национальный стандарт Российской Федерации / разработан ЗАО «Интегра-С» с участием ЗАО «Волгаспецремстрой», ООО «Интегра-Т», ООО «Интегра-М», ФГУП «НИЦ охрана» МВД России. – Москва : Стандартинформ, 2019 год. – 40 с. – URL: https://docs.cntd.ru/document/1200132478 (дата обращения: 10.10.2024). – Режим доступа: электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс». – Текст : электронный.

2. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : Приказ ФСТЭК России от 18 февраля 2013 г. № 21. – URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 10.10.2024). – Режим доступа: официальный сайт ФСТЭК России. – Текст : электронный.

3. ООО «Спецстрой-связь» телекоммуникационное оборудование и системы безопасности : [сайт] / ООО ГК «Спецстрой-связь». – Таганрог, 2024. – URL: https://www.proton-sss.com/ (дата обращения: 10.10.2024). – Текст : электронный.

4. Производство охранных систем : [сайт] / ООО «НПП Риэлта». – Санкт-Петербург, 2024. – URL: https://rielta.ru/ (дата обращения: 10.10.2024). – Текст : электронный.

5. НИКИРЭТ - комплексное обеспечение безопасности объектов : [сайт] / АО «НИКИРЭТ» государственной корпорации по атомной энергии «Росатом». – ЗАТО г. Заречный, 2024. – URL: https://nikiret.ru/ (дата обращения : 10.10.2024). – Текст : электронный

СВЕДЕНИЯ ОБ АВТОРЕ

Абросимова Евгения Михайловна. Старший преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: chip_ik@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Abrosimova Evgeniya Mikhailovna. Senior Lecturer in electronic systems and complexes of security monitoring. Candidate of technical Sciences.

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

Ключевые слова: видеонаблюдение; аналитика данных; повышение безопасности; прогнозирование угроз.

Key words: video surveillance; data analytics; security improvement; threat forecasting.

УДК 681.772.7

Багринцева Оксана Владимировна,
кандидат технических наук

РЕТРОСПЕКТИВНЫЙ АНАЛИЗ РАБОТЫ СИСТЕМЫ РАДИОМЕСТООПРЕДЕЛЕНИЯ ГЛОНАСС

RETROSPECTIVE ANALYSIS OF THE OPERATION OF THE GLONASS RADIO DETECTION SYSTEM

В статье рассматривается путь развития от простых навигационных систем начала 20-го века до современных спутниковых систем глобального позиционирования.

This article examines the path of development from simple navigation systems of the early 20th century to modern satellite global positioning systems.

Транспортировка имущества – это важный этап в цепи обеспечения безопасности и защиты ценных грузов. С ростом значимости логистики и расширением глобальных рынков, эффективная охрана имущества при его транспортировке становится критически важной задачей для компаний и организаций. В контексте обеспечения безопасности транспортировки ценных грузов с использованием глобальной навигационной спутниковой системы, неотъемлемой частью становится контроль и прослеживание перемещения объектов в режиме реального времени.

Глобальная навигационная спутниковая система (далее– Глонасс) предоставляет широкий спектр возможностей для обеспечения безопасности грузов во время транспортировки. Эта система включает в себя сеть спутников, позволяющих точно и надежно определять местоположение и скорость транспортного средства в реальном времени. На базе данной информации можно реализовать различные меры для обеспечения

безопасности грузового транспорта, включая следующие аспекты:

– мониторинг местоположения груза;

– реагирование на отклонения от маршрута;

– планирование оптимальных маршрутов;

– взаимодействие с охраной;

– управление доступом и аутентификация грузов.

Идея использования спутников для навигации впервые возникла у профессора В.С. Шебшаевича в 1957 году. Он пришел к этому открытию, изучая возможности применения радиоастрономии в аэронавтике. В дальнейшем, советские научные учреждения активно работали над улучшением точности и функциональности навигационных систем, стремясь к глобальному покрытию, круглосуточному функционированию и независимости от погоды. Результаты этих исследований легли в основу 3 создания первой отечественной низкоорбитальной системы «Цикада» в 1963 году. В 1967 году на орбиту был запущен первый отечественный навигационный спутник «Космос-192», который непрерывно передавал радионавигационные сигналы на частотах 150 и 400 МГц на протяжении всего периода своей активной работы.

Впоследствии спутники системы «Цикада» были модернизированы, получив приемные измерительные устройства для обнаружения терпящих бедствие объектов, оснащенных специальными маяками. Сигналы этих маяков принимались спутниками «Цикада» и передавались на наземную станцию, где рассчитывались точные координаты аварийных объектов, будь то суда, самолеты или другие средства передвижения.

В результате многолетних исследований отечественных специалистов была выбрана орбитальная группировка ГЛОНАСС, состоящая из 24 спутников, расположенных на средневысотных околокруговых орбитах. Спутники ГЛОНАСС расположены на высоте около 19 100 километров, с наклонением 64,8° и периодом обращения 11 часов 15 минут 44 секунды. Благодаря особому периоду обращения спутников ГЛОНАСС, в отличие от системы GPS, не требуется корректирующих импульсов для поддержания их орбиты на протяжении всего срока службы. Стабильный номинальный наклон орбиты обеспечивает 100% доступность навигации на территории России, даже в случае выхода из строя некоторых спутников.

К сожалению, в 1990-х годах орбитальная группировка ГЛОНАСС, как и система в целом, стала быстро деградировать из-за экономических проблем. К 2002 году в системе оставалось всего 7 спутников, что не позволяло обеспечить на территории России надежную навигацию сигналами ГЛОНАСС. Точность определения местоположения ГЛОНАСС отставала от системы GPS более чем в 10 раз, а срок службы спутников составлял всего 3-4 года.

В настоящее время система ГЛОНАСС требует дальнейшего развития, особенно в области потребительского навигационного оборудования. В первую очередь, это касается высокоточных применений, где требуется

точность определения местоположения на уровне дециметров и сантиметров в режиме реального времени. Также актуальны применения, связанные с обеспечением безопасности на воздушном, морском и наземном транспорте. Необходимо повысить эффективность навигационных решений и улучшить помехоустойчивость системы ГЛОНАСС. Существуют множество областей, где требуются более компактные и чувствительные навигационные приемники.

С 2012 года система ГЛОНАСС развивается в рамках федеральных целевых программ, которые предусматривают:

1. Поддержание системы ГЛОНАСС с гарантированными характеристиками навигационного поля на конкурентоспособном уровне.

2. Повышение тактико-технических характеристик системы ГЛОНАСС до уровня ведущих зарубежных навигационных систем и закрепление лидирующих позиций России в сфере спутниковой навигации.

3. Обеспечение доступа к системе ГЛОНАСС на территории Российской Федерации и за ее пределами.

Уровень совершенства тактико-технических характеристик системы определяется рядом направлений развития системы, основными из которых являются:

1. Развитие структуры орбитальной группировки ГЛОНАСС в части ее расширения и создания дополнений на других орбитах.

2. Переход к использованию нового поколения навигационных космических аппаратов с улучшенными тактико-техническими характеристиками.

3. Развитие наземного комплекса управления системы ГЛОНАСС, включая совершенствование эфемеридно-временного комплекса системы ГЛОНАСС.

4. Создание и развитие функциональных дополнений:

– широкозонной системы дифференциальной коррекции и мониторинга навигационных полей;

– глобальной дополняющей системы высокоточного определения навигационной и эфемеридно-временной информации в реальном времени для гражданских потребителей.

Система работает за счет приема сигналов, как минимум, с четырех спутников одновременно. Трекер, установленный на транспортном средстве, последовательно выполняет следующие действия:

– записывает в электронную память их текущие пространственные координаты;

– регистрирует время приема сигнала;

– на основании полученных данных рассчитывает расстояние от машины до каждого из спутников.

После вычисления координат автомобиля, трекер передает данные на GSM-модуль, встроенный в устройство ГЛОНАСС-мониторинга. SIM-карта, установленная в трекер, позволяет передать информацию через интернет на

телематический сервер. Данные, хранящиеся на сервере, обрабатываются программным обеспечением системы мониторинга и отображаются в графическом и цифровом виде на клиентском интерфейсе.

Анализируя историю систем радиопозиционирования, можно увидеть, что они прошли значительный путь развития от простых навигационных систем начала 20-го века до современных спутниковых систем глобального позиционирования.

ЛИТЕРАТУРА

1. Шуть В.Ю. Новые направления применения систем глобального позиционирования в дорожной отрасли / В. Ю. Шуть, А. В. Каменчуков // Проектирование развития региональной сети железных дорог. 2018. – № 6. – С. 99-104.

2. Шуть В. Ю. Перспективы применения систем GPS и ГЛОНАС в дорожно-транспортной инфраструктуре / В. Ю. Шуть, А. В. Каменчуков // Материалы секционных заседаний 57-й студенческой научно-практической конференции ТОГУ : в 2 т., Хабаровск, 17–27 апреля 2017 года / Тихоокеанский государственный университет. Том 1. – Хабаровск: Тихоокеанский государственный университет, 2017. – С. 253-258. – EDN YSSLXP.

3. Рысин А. В. Анализ многофункционального использования низкоорбитальных спутниковых систем связи (НССС) с оптимизацией радиотехнических параметров / А. В. Рысин, В. Н. Бойкачев, А. М. Наянов // Евразийский Союз Ученых. Серия: технические и физико-математические науки. – 2022. – № 7(100). – С. 22-61. – DOI 10.31618/ESU.2413-9335.2022.1.100.1.1676. – EDN RHWOZP.

СВЕДЕНИЯ ОБ АВТОРЕ

Багринцева Оксана Владимировна. Преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: bagrinceva-oksana@mail.ru

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

Bagrintceva Oksana Vladimirovna. Lecturer in electronic systems and complexes of security monitoring. Candidate of technical Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: bagrinceva-oksana@mail.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: транспортировка имущества; обеспечения

безопасности; глобальная навигационная система; спутниковая система.

Keywords: transportation of property, security, global navigation system, satellite system.

УДК 351.74; 614.8

Бондаренко Евгений Сергеевич

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СЕТЕЙ РАДИОСВЯЗИ ОТ НЕСАНКЦИОНИРОВАННОГО ПОЛУЧЕНИЯ ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ

FEATURES OF ENSURING THE SECURITY OF RADIO COMMUNICATION NETWORKS FROM UNAUTHORIZED RECEIPT OF TRANSMITTED INFORMATION

В статье рассматривается особенности безопасности сетей радиосвязи от несанкционированного получения передаваемой информации.

This article discusses the security features of radio communication networks against unauthorized receipt of transmitted information.

В современных условиях, когда развитие технологий беспроводной передачи данных стремительно набирает обороты, вопрос защиты радиосетей от неавторизованного доступа становится чрезвычайно актуальным. Чтобы предотвратить риски перехвата информации, применяются разнообразные методики, направленные на усиление безопасности каналов связи. Комплекс технических и программных решений служит основной преградой для стороннего вторжения, обеспечивая целостность и конфиденциальность данных.

Одним из ключевых аспектов безопасности является надежное шифрование передаваемой информации, что препятствует её расшифровке третьими лицами. Методики криптографической защиты непрерывно совершенствуются, следуя за возрастающей активностью злоумышленников, стремящихся найти уязвимые места в защите. Алгоритмы кодирования, оптимизированные для разных уровней передачи данных, являются основой создания неприступной цифровой границы.

Основными угрозами радиосвязи являются:

1. Угрозы непосредственного доступа. Внедрение в технические средства радиосвязи аппаратных закладок, что может привести к получению доступа к носителям данных, перехвату идентификаторов доступа и паролей на пользовательских устройствах.

2. Угрозы удалённого доступа. Прослушивание переговоров, перехват или подмена управляющей информации на базовых станциях, распространение вредоносного кода.

3. Угрозы целостности. Внедрение в оборудование ядра сети вредоносного программного обеспечения.

4. Угрозы утечки информации по техническим каналам. Например, утечка за счёт побочных электромагнитных излучений и наводок.

5. Влияние помех. Сети подвижной радиосвязи подвержены как случайным, так и преднамеренным помехам.

6. Блокирование какой-либо службы или услуги мобильной сети. Например, уничтожение сообщений, задержка сообщений, перегрузка сети ложными сообщениями, отключение узлов сети командами управления.

7. Несанкционированное использование ресурсов сети. Работа с запрещёнными к использованию ресурсами сети путём маскировки под другого пользователя или неправомерное использование разрешённых ресурсов сети.

8. Для защиты от угроз радиосвязи используются, например, криптографическая защита каналов радиосвязи, средства обнаружения вторжений в сетевую инфраструктуру ядра сети, постоянно обновляемые средства антивирусной защиты.

Эффективные методы защиты информации включают в себя многоуровневую структуру безопасности, охватывающую как аппаратные, так и программные средства, причем акцент должен быть сделан на проактивных мерах, гарантирующих своевременное реагирование на выявленные угрозы.

Для обеспечения безопасности связи применяются следующие методы:

– использование аппаратуры с функциями шифрования и соблюдение правил эксплуатации;

– предварительное шифрование и кодирование данных, использование скрытых документов и таблиц позывных;

– ограничение доступа к переговорным каналам, применение паролей и средств имитозащиты;

– проверка достоверности сообщений с помощью обратной передачи;

– правила установления связи и соблюдения режима секретности при обработке и хранении данных;

– защита от различных видов разведки, включая радио- и радиолокационную, лазерную и акустическую;

– поддержание высокого уровня подготовки и постоянной бдительности сотрудников, обслуживающих узлы связи.

Обеспечения безопасности сетей радиосвязи от попыток несанкционированного проникновения представляет собой важную задачу, подразумевающую комплексный подход к предотвращению доступа без разрешения. Сетевые системы должны быть оснащены современными средствами, которые могут успешно противостоять агрессивным действиям злоумышленников. Для поддержания безопасности необходимо внедрение

инновационных технологий, которые предусматривают детектирование и блокировку попыток вторжения с целью предотвращения потенциального ущерба.

Поток транспортных данных способен раскрыть структуру сети. Узлы, осуществляющие передачу и прием значительных объемов информации, представляют особый интерес для злоумышленников. Обнаружение узлов передачи гораздо легче, чем узлов приема, поскольку последние могут не отправлять квитанции о получении. Кроме того, сетевая топология может отражать географическое положение объектов, что упрощает для преступника задачу их нахождения и ликвидации.

Однако, кроме технических мер, важное значение имеют организационные меры, в частности развертывания систем контроля доступа, которые включают проверку подлинности пользователей и ограничение прав на использование сетевых ресурсов. Современные системы безопасности также предусматривают мониторинг активности и обнаружение аномалий в трафике, позволяя своевременно выявлять и нейтрализовать угрозы.

ЛИТЕРАТУРА

4. Требования по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации : приказ Министерства информационных технологий и связи Российской Федерации утвержденный от 9 января 2008 г. № 1 [Электронный ресурс]. – Режим доступа: http://www.garant.ru/doc/constitution.

5. Амочаева Г.П., Защита информации в телекоммуникационных системах. Учебное пособие / Амочаева Г.П., Алпысова Г.К., Роговая К.С. - Караганда: Изд-во «Полиграфист», 2018. – С. 79 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Бондаренко Евгений Сергеевич. Преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга.

Воронежский институт МВД России.

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

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

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

Voronezh Institute of the Ministry of the Interior of Russia.

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

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

Ключевые слова: безопасность сетей радиосвязи; обеспечение безопасности; угрозы; защита; несанкционированное проникновение.

Keywords: security of radio communication networks; security; threats; protection; security unauthorized entry.

УДК 621.39

Гречаный Сергей Анатольевич,
кандидат технических наук, доцент

ОСОБЕННОСТИ ПРИМЕНЕНИЯ СРЕДСТВ ФИЗИЧЕСКОГО ПРОТИВОДЕЙСТВИЯ НА ОБЪЕКТАХ ОХРАНЫ

FEATURES OF THE USE OF PHYSICAL COUNTERMEASURES AT SECURITY FACILITIES

В статье рассматривают способы и методы противодействия в системе борьбы с беспилотными летательными аппаратами (БПЛА). Рассмотрен пример работы перспективных технических средств, которые позволяют достаточно оперативно реализовывать проблему противодействия БПЛА на охраняемом объекте.

The article examines the principles of the operation of countermeasures in the system of combating unmanned aerial vehicles (UAVs). The considered principles of operation of promising means make it possible to quickly implement the problem of countering UAVs at a protected facility.

Современная социально-политическая ситуация отмечается значительным риском осуществления террористических действий и говорит о повышенной вероятности аварий и катастроф техногенного, эпидемиологического и экологического характера на охраняемых объектах.

Правила законодательства по нейтрализации активности беспилотных систем на охраняемых территориях активно формируются. Федеральный закон № 440-ФЗ, от 04.08.2023 года «О внесении изменений в отдельные законодательные акты Российской Федерации» увеличивает полномочия ряда федеральных исполнительных органов по вопросам пресечения работы беспилотных систем в воздушной, водной и наземной средах. Эти меры включают, среди прочего, изменение управляющих сигналов дронов и других беспилотников, а также непосредственное воздействие на их системы управления до их повреждения или уничтожения [1].

Лица, осуществляющие охранные функции в федеральных государственных органах и высших исполнительных структурах регионов, обладают возможностью остановки работы беспилотных систем. Данное право, предусмотренное законодательством РФ, распространяется также на

организации, участвующие в создании ведомственной охраны. Помимо этого, работники частных охранных предприятий, выполняющие деятельность по обеспечению безопасности объектов с установленными антитеррористическими мерами, наделены законодательной возможностью пресекать использование беспилотных летательных средств.

Для защиты безопасности населения и охраны здоровья граждан, а также предотвращения угроз на критически значимых государственных и потенциально опасных объектах, обязательно должен осуществляется контроль беспилотных летательных аппаратов [2].

Развитие различных технологий, прежде всего информационных, оказывает значимое влияние на современную действительность по противодействию БПЛА на объектах охраны. Применение современных автоматизированных систем противодействия позволяет производить не только обработку огромного количества информации в минимальные сроки, но и применять их в развитии перспективных средств противодействия БПЛА. На первый план выходит проблема по разработке и применению современных технологий в средствах противодействия БПЛА. Повышение надежности систем противодействия, помехозащищенности каналов связи, автономности и дальности действия требует максимально оперативного создания и развития перспективных средств по нейтрализации БПЛА.

Роль создания и внедрения средств противодействия позволяет способствовать следующим факторам: повышение эффективности выполнения задач правоохранительными органами в мирное время и в рамках специальной военной операции при охране объектов.

Сегодня нейтрализация беспилотников и предупреждение их несанкционированных действий производится за счёт следующих способов и методов:

– средства противодействия беспилотным летательным аппаратам включают радиоэлектронные методы, которые предназначены для нейтрализации каналов управления;

– измерение информационно-технических угроз, охватывающих такие аспекты, как несанкционированный доступ к системам путем взлома зашифрованных каналов связи или манипулирование данными авторизации. Также используются воздействия микроволны и лазерного воздействия, обеспечивая блокаду или сбой в работе системы управления;

– механическое воздействие, включающее в себя: кевларовые сети, огневое поражение, кинетическое воздействие.

Одно из эффективных устройств, которое может применяться при противодействии БПЛА – это изделие ПП, производитель ООО «ЭЛИАРС» [3].

Изделие ПП предназначено для направленного излучения радиопомех с целью противодействия управляемым БПЛА, находящимся над земной и водной поверхностью. В зависимости от времени воздействия на «дрон» и

модели БПЛА его можно принудительно посадить или отправить на место взлета, не причиняя материального вреда его владельцу.

Основным поражающим фактором, используемым в большинстве систем по борьбе с БПЛА, является электромагнитное излучение, создаваемое устройством, а также мощность этого излучения. Как правило – более мощное излучение позволяет более эффективно подавлять дроны, но может негативно сказаться на здоровье оператора. Конструкторские особенности, лежащие в основе изделий ПП, позволяют соблюсти баланс между мощностью устройства и безопасностью, избегая перегрева и избыточного излучения от работы ружей.

Таким образом, такой вид технических средств позволяет эффективно подавлять БПЛА в случае подлёта к объекту охраны.

Актуальное совершенствование технологий противодействия беспилотным летательным аппаратам необходимо для эффективного ответа на вызовы, с которыми сталкиваются правоохранительные структуры в условиях новых и непростых задач. Внедрение и усовершенствование физических методов защиты объектов охраны представляется многогранным вектором, который, без сомнения, способен значительно укрепить безопасность государства, обеспечивая защиту жизни и здоровья граждан в процессе выполнения ими профессиональных обязанностей.

ЛИТЕРАТУРА

1. Федеральный закон от 4 августа 2023 г. № 440-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации».

2. Приказ Росгвардии от 16 октября 2023 г. № 378 «Об утверждении Порядка принятия решения о пресечении функционирования беспилотных воздушных, подводных и надводных судов и аппаратов, беспилотных транспортных средств и иных автоматизированных беспилотных комплексов в целях отражения нападения либо угрозы нападения на объекты, охраняемые военизированными и сторожевыми подразделениями федерального государственного унитарного предприятия «Охрана» Федеральной службы войск национальной гвардии Российской Федерации, работников военизированных и сторожевых подразделений федерального государственного унитарного предприятия «Охрана» Федеральной службы войск национальной гвардии Российской Федерации или лиц, находящихся на этих объектах, а также Перечня должностных лиц федерального государственного унитарного предприятия «Охрана» Федеральной службы войск национальной гвардии Российской Федерации, уполномоченных на принятие такого решения».

3. ООО «ЭЛИАРС» специализируется на разработке и производстве высокоинтегрированной СВЧ-аппаратуры ELIARS. https://eliars.ru/security?ysclid=m65btrpmyk627975647.

СВЕДЕНИЯ ОБ АВТОРЕ

Гречаный Сергей Анатольевич. Начальник кафедры радиотехнических систем и комплексов охранного мониторинга. Кандидат технических наук.
Воронежский институт МВД России.
E-mail: grechan7777@mail.ru.
Россия, 394065, Воронеж, проспект Патриотов, 53.

Grechanyi Sergej Anatol'evich. Chief of department of radio engineering systems and complexes of security monitoring. Candidate of Engineering Sciences
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: grechan7777@mail.ru.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: охрана, безопасность; беспилотные летательные аппараты; физическая защита; объекты.

Key words: security; unmanned aerial vehicles; physical protection; facilities.

УДК 342; 623.746

Дуплякин Пётр Михайлович

ИСПОЛЬЗОВАНИЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

USING CLOUD TECHNOLOGIES TO ENSURE SECURITY

В статье исследуются основные подходы и инструменты, применяемые в облачных решениях, для защиты данных и инфраструктуры.

This article explores the main approaches and tools used in cloud solutions for data protection and infrastructure.

В современном мире облачные технологии стали неотъемлемой частью IT-инфраструктуры как для бизнеса, так и для индивидуальных пользователей. Одной из ключевых областей применения облачных решений является обеспечение безопасности данных и информационных систем. Этот подход предлагает множество преимуществ, включая масштабируемость, доступность и снижение затрат. В данной статье мы рассмотрим основные аспекты использования облачных технологий для обеспечения безопасности.

Одной из главных задач обеспечения безопасности является хранение данных. Облачные сервисы предоставляют высокозащищенные хранилища данных с функциями шифрования, резервного копирования и восстановления. Шифрование данных как при хранении, так и при передаче значительно снижает риск несанкционированного доступа [1].

Основными подходами к безопасности в облачных решениях являются:

- шифрование данных;
- управление доступом и аутентификация;
- мониторинг и аудит;
- резервное копирование и восстановление данных;
- защита сетевого трафика.

Шифрование является основным методом защиты данных как на уровне хранения, так и на уровне передачи. Данные шифруются при их передаче через сети и сохраняются в зашифрованном формате на серверах. Это обеспечивает конфиденциальность информации и защищает ее от несанкционированного доступа [2].

Использование многофакторной аутентификации (MFA) и принципа наименьших привилегий (PoLP) позволяет ограничить доступ к данным и приложениям в облаке. Это важно для предотвращения несанкционированного доступа пользователей и снижения рисков причинения вреда.

Постоянный мониторинг активности пользователей и событий безопасности в облачной среде позволяет быстро выявлять и реагировать на потенциальные угрозы. Интеграция средств аудита помогает соблюдать требования регулирования и отслеживать изменения в облачной инфраструктуре.

Регулярное создание резервных копий данных и разработка планов восстановления после сбоев критически важны. Облачные провайдеры часто предлагают встроенные решения для резервного копирования и восстановления, что упрощает этот процесс.

Использование VPN (виртуальных частных сетей), файрволов и IDS/IPS (систем обнаружения и предотвращения вторжений) помогает защитить сетевой трафик от атак и злоумышленников. Эти инструменты помогают защищать облачную инфраструктуру от внешних угроз.

Инструменты для обеспечения безопасности в облаке:

- облачные услуги безопасности (SECaaS);
- шифрование и управление ключами;
- системы DLP (предотвращение потери данных);
- управление идентификацией и доступом (IAM).

Провайдеры облачных сервисов предлагают специализированные решения для защиты, такие как облачные системы управления безопасностью (SIEM), SOC (центры операций безопасности) и другие инструменты, помогающие в обнаружении и реагировании на инциденты.

Многие облачные платформы предлагают встроенные инструменты для шифрования и управления криптографическими ключами, что позволяет организациям защитить свои данные и управлять доступом к ним.

Облачные технологии позволяют реализовывать многоуровневую систему управления доступом. Сервисы идентификации и управления доступом (IAM) предоставляют возможность тонкой настройки прав пользователя, а также многофакторной аутентификации. Эти инструменты позволяют предотвратить несанкционированный доступ и защищают критически важные данные.

Облачные платформы предлагают продвинутые средства мониторинга и анализа, которые могут выявлять подозрительную активность в режиме реального времени. Инструменты безопасности как сервис (SECaaS), такие как AWS GuardDuty и Azure Security Center, позволяют автоматизировать процессы аналитики угроз, минимизируя временные затраты на поиск уязвимостей.

Специализированные облачные решения помогают организациям соответствовать законодательным и нормативным требованиям, таким как GDPR и HIPAA. Облачные технологии предоставляют инструменты для реализации конфиденциальности и безопасности данных, позволяя организациям сосредоточиться на основном бизнесе, не отвлекаясь на юридические аспекты.

Системы безопасности, разрабатываемые на облачных платформах, легко масштабируются в зависимости от потребностей организации. Это особенно важно для организаций, которые растут или меняют свою структуру. Облачные технологии позволяют быстро адаптировать меры безопасности под изменяющиеся условия, уменьшив время реакции на инциденты.

Современные облачные технологии обеспечивают безопасный доступ к данным и системам из любой точки мира. Это ключевой фактор для бизнеса, который ориентирован на дистанционную работу и международные команды. При правильной настройке безопасности такие решения могут существенно повысить продуктивность сотрудников, обеспечивая при этом высокий уровень защиты.

Использование облачных технологий для обеспечения безопасности открывает новые горизонты для организаций. Современные инструменты и решения позволяют не только защитить данные, но и оптимизировать процессы управления безопасностью. Однако важно помнить, что облачные технологии — это не панацея, и необходимо комплексное понимание угроз и рисков, чтобы использовать их преимущества максимально эффективно. В конечном итоге, облачные технологии могут стать надежным защитником в эпоху цифровизации, обеспечивая безопасность данных в условиях постоянно меняющихся угроз.

ЛИТЕРАТУРА

1. Текущее состояние и перспективы внедрения облачных офисных решений в деятельности ОВД : учебно-практическое пособие / Л.Д. Матросова [и др.]. – Орел : ОрЮИ МВД России имени В.В. Лукьянова, 2021. – 45 с.

2. ГОСТ 34.12-2018 «Информационная технология. Криптографическая защита информации. Блочные шифры».

СВЕДЕНИЯ ОБ АВТОРЕ

Дуплякин Петр Михайлович. Преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга.

Воронежский институт МВД России.

E-mail: 00008540@mail. ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

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

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: 00008540@mail. ru

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

Ключевые слова: роботизированные комплексы; надводные дроны; подводные дроны; безопасность периметра ОВД.

Key words: robotic complexes; surface drones; underwater drones; security of the ATS perimeter.

УДК 004.056

Ивануха Иван Сергеевич;
Калков Дмитрий Юрьевич,
кандидат технических наук

ПРИМЕНЕНИЕ ЦИФРОВОЙ ТРАНКИНГОВОЙ СВЯЗИ АРСО-25 В ЦЕЛЯХ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ СЛУЖЕБНОЙ ДЕЯТЕЛЬНОСТИ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

APPLICATION OF DIGITAL TRUNKING COMMUNICATION ARSO-25 IN ORDER TO INCREASE THE EFFICIENCY OF OFFICIAL ACTIVITIES OF EMPLOYEES OF INTERNAL AFFAIRS BODIES

В статье рассказывается о преимуществах использования стандарта транкинговой связи АРСО 25 и о плюсах использования его служебной деятельности сотрудников органов внутренних дел.

The article describes the advantages of using the ARSO 25 trunking communication standard and the advantages of using it for the official activities of internal affairs officers.

В настоящее время процесс развертывания транкинговой связи в России характеризуется широкомасштабным внедрением цифровых систем. Практически все поставщики оборудования и услуг транкинговой связи перешли на цифровые системы. Основными потребителями являются представители органов внутренних дел и службы общественной безопасности Российской Федерации.

В настоящее время в Омской области развертываются радиосвязные системы, основанные на стандарте АРСО-25. Это связано в первую очередь с тем, что цифровые технологии стали более доступными для государственных учреждений и различных организаций, которые готовы внедрять цифровизацию в свои сетевые решения. Переход на цифровые системы транкинговой радиосвязи в России непосредственно связан с новыми цифровыми технологиями и имеет большие перспективы. Цифровые радиосистемы предлагают пользователям высокий уровень сервиса, множество режимов передачи информации, повышенную защищенность связи и возможности интеграции с фиксированными цифровыми сетями.

Интерес Управления МВД России по Омской области к цифровым системам радиосвязи стандарта АРСО-25 обоснован. После тщательного анализа различных цифровых стандартов радиосвязи Управление МВД России по Омской области приняло решение использовать систему АРСО-25. Это решение было зафиксировано в официальных документах и будет внедрено в работу правоохранительных органов. В качестве яркого примера можно выделить широкомасштабное использование системы

радиосвязи стандарта APCO-25 во время праздничных мероприятий, когда возможны сбои в работе системы сотовой связи из-за вышедших из строя базовых станций или перегрузках. Развернутая в интересах правоохранительных органов система цифровой радиосвязи в стандарте APCO-25 обеспечивает стабильную работу силовых подразделений в условиях сложной электромагнитной обстановки, когда применение обычных средств радиосвязи может быть затруднено.

Выбор органов внутренних дел МВД России в пользу стандарта APCO-25 обусловлен причинами, представленными ниже.

При создании транкинговой сети связи со стандартом APCO-25 нет необходимости затрачивать большое количество материальных, финансовых ресурсов для приобретения нового оборудования и полного перехода на него. Аналоговые средства радиосвязи, которые в настоящее время используются сотрудниками органов внутренних дел МВД России, беспрепятственно используются в сочетании с цифровыми средствами этой системы. Это связано с тем, что правоохранительные органы ограничены в финансировании и не могут за короткий интервал времени перейти на цифровой формат связи. Кроме того, оборудование других цифровых стандартов стоит достаточно дорого, а для развертывания транкинговых сетей требуется большое количество базовых станций. При внедрении стандарта APCO-25 требуется небольшое количество базовых станций, которые стоят значительно дешевле. Кроме того, оборудование APCO-25 совместимо с аналоговым оборудованием и имеет большую дальность действия по сравнению с другими стандартами, что очень важно для крупных регионов Российской Федерации.

В настоящее время в России используются транкинговые системы с каналом управления либо без канала управления.

Рассмотрим систему без канала управления. В такой системе свободный канал отмечается маркером (специальным сигналом). При осуществлении вызова радиостанция занимает свободный канал. Этот процесс занимает считанные секунды, поэтому незаметен для пользователя. Достоинствами данной системы является дешевизна оборудования, а также простота в установке и эксплуатации. Недостатками является увеличение времени поиска свободных каналов при большой загрузке системы, отсутствие возможности создания многозоновых систем, минимальный набор функций и сервиса.

Далее рассмотрим систему с каналом управления. Наличие канала управления уменьшает время ожидания соединения. Системы с каналом управления в свою очередь делится на:

- систему с выделенным контрольным каналом;
- систему без выделенного контрольного канала.

В системе с выделенным контрольным каналом микропроцессорный блок управления играет ключевую роль в координации работы базовых станций. Выделение отдельного канала для целей управления позволяет обеспечить надежное и эффективное взаимодействие между различными элементами сети, а также минимизировать риск помех и некорректной работы.

Функция установления соединения между двумя абонентами сети является основополагающей для обеспечения связи и передачи данных. Этот процесс может включать в себя несколько этапов, таких как:

1. Идентификация абонентов: определение, какие два абонента хотят установить связь.
2. Аутентификация: проверка прав доступа абонентов к сети.
3. Выбор канала: выделение подходящего канала для передачи данных между абонентами.
4. Установление соединения: обмен сигналами между абонентами для подтверждения готовности к общению.
5. Поддержка и управление соединением: обеспечение качества связи, управление пропускной способностью и возможное переключение между каналами в случае необходимости.

Использование специального управляемого канала также позволяет реализовать более сложные функции управления, такие как мониторинг состояния сети, обработка ошибок и оптимизация нагрузок, что в свою очередь способствует улучшению качества связи и снижению рисков сбоев.

Работа этой системы осуществляется следующим образом: микропроцессорный блок управления контролирует все базовые станции, а один из каналов «руководящее звено» устанавливает соединения между абонентами.

Работа системы без выделенного контрольного канала осуществляется следующим образом: вместо выделенного канала используется приемопередатчик центральной станции, при этом осуществляется жесткое закрепление канала, если он не занят. В противном случае контролер переключает пользователя на свободный канал связи. При занятости всех каналов контролер оповещает об этом пользователя.

Транкинговая система APCO-25 имеет различную архитектуру построения, а именно однозоновую или многозоновую.

Вся система строится на объединении центральных станций. Сердцем системы является центральный узел. В него входят центральный процессор и коммутатор.

Можно объединить несколько систем APCO-25 в межрегиональный процессор и через коммуникатор осуществлять коммуникацию каналов. Сам стандарт позволяет использовать оборудование разных фирм и объединяет разрозненные сети в одну [4].

Стандарт APCO-25 организует несколько видов связи:

1. Симплексная связь построена на использовании двух частот, одна для приема вторая для передачи. Возможна только передача голоса.

2. Полудуплексная связь также задействует две частоты, на одной частоте постоянно принимает, на другой транслирует то, что приняла.

3. Дуплексная связь построена на использовании двух частот, одна на приём, другая на передачу, в любое время аппаратура связи либо принимает, либо передаёт.

В настоящее время цифровые транкинговые системы находятся на вершине профессиональной связи. В них осуществляется защита от несанкционированного доступа, пакетная передача данных, а также передача больших потоков данных телеметрии и видео.

У стандарта открытая архитектура, переход к цифровой передаче речи осуществляется двумя способами. Для начала берется сетка частот с разделением на 12,5 кГц, а потом 6,25 кГц.

Разделение каналов осуществляется с использованием частотного метода FDMA, скорость передачи данных в канале составляет 9,6 Кбит/с. Речевой сигнал превращается в цифровой с помощью IMBE метода многополосного возбуждения, получается цифровой поток, скорость которого 4400 бит/с. Для помехоустойчивости кодирования добавляются символы, это увеличивает скорость до 7200 бит/сек, а после 9,6 кбит/сек [1].

Основным блоком системы является радиоподсистема RFSS (RFSS-радиочастотная подсистема), то есть сеть связи. RFSS обрабатывает системные вызовы и поддерживает множество интерфейсов. Радиоинтерфейс дает нам: частотное разделение, скорость потока, модуляцию, доступ к каналу, кодирование.

Архитектура бывает транкинговой и конвенциональной, состоит из радиоподсистемы, закрытого элемента и восьми интерфейсов. У каждого интерфейса свои физические и электрические параметры, протоколы обмена информацией, пропускная способность. Для проверки оборудования под интерфейсы существует программа о оценки на соответствие CAP – Compliance Assessment Program. Общий радиоинтерфейс (CAI) позволяет носимым или мобильным станциям от разных фирм работать в системе связи APCO-25. Стандарт APCO-25 одновременно использует два вида модуляции – четырехуровневую частотную C4FM и квадратурно-фазовую манипуляцию QPSK [2].

Основные особенности стандарта APCO-25: частотное разделение каналов (FDMA), работа с радиостанциями большой и малой мощности, конвенциональный режим, транкинговый режим, отдельный ретранслятор, системы с разнесенным приемом, симулкаст, мултикаст, DES-шифрация и т.д.

Как и в других цифровых системах связи, в APCO-25 речевой сигнал подвергается оцифровке и модуляции. В системе имеется единый радиоинтерфейс и наличие полного комплекта оборудования для управления работой над вызовами и для поддержки интерфейсов.

Организация единой ведомственной сети отдельно взятого региона базе стандарта APCO-25 строится по структуре интегрированной мультисервисной телекоммуникационной системы региона, которая d свою очередь состоит из главного коммутационного узла, опорных коммутационных узлов, ведомственных коммутационных узлов по субъекту Российской Федерации.

К радиооборудованию предъявляется ряд требований, в основном для совершенствования системы управления МВД России. Ряд требований носят следующий характер: например, необходимо современное радиооборудование

для покрытия большой территории, и в то же время необходимо иметь маломощный передатчик с небольшой массой и габаритами для скрытного использования радиостанций и высокой устойчивостью к помехам и избирательности.

Также предъявляются особые требования к надежности, к защите информации, связано это с тем, что ОВД арендуют цифровые каналы связи. В первую очередь, большим недостатком является нехватка частотного ресурса в городах более 500 тыс. человек. Все эти проблемы решает внедрение цифровых сетей в систему ОВД.

Созданные радиосистемы, решают следующие задачи: повышают эффективность работы радиосвязи, предоставляют передачу информации и открывать доступ ведомственным базам данных по радиоканалу.

Транкинговые системы радиосвязи представляют собой мощный инструмент для управления частотным спектром и эффективного использования радиочастотных ресурсов. Их преимущество заключается в том, что они способны обслуживать множество пользователей с помощью меньшего количества радиоканалов, что особенно важно в условиях неблагоприятной электромагнитной обстановки.

За счет динамического распределения каналов, транкинговые системы обеспечивают более эффективное использование радиочастот, что позволяет оптимизировать оперативное взаимодействие между службами или группами, особенно в ситуациях высокой нагрузки. Кроме того, благодаря возможностям цифровых радиостанций, такие системы становятся более гибкими и адаптируемыми к изменяющимся условиям, что делает их идеальными для использования в различных сферах, включая экстренные службы, транспорт, промышленность и беспроводные сети связи.

Транкинговая система также может обеспечить безопасную и защищенную передачу данных, что значительно повышает уровень информации и позволяет интегрировать передачу данных с голосовой связью. Возможность доступа к базам данных, передаваемым по радиоканалам, открывает новые горизонты для аналитической работы и мониторинга в реальном времени, что сказывается на повышении эффективности и скорости принятия решений.

Таким образом, использование транкинговых систем в цифровой радиосвязи дает значительные преимущества в гибкости, экономии ресурсов и улучшения оперативной работы.

В масштабах России структура организации единой ведомственной сети органов внутренних дел на базе стандарта APCO-25 выглядит как интегрированная мультисервисная телекоммуникационная система органов внутренних дел Российской Федерации, является частью единой информационно-телекоммуникационной системы органов внутренних дел и представляет собой совокупность коммутационных узлов и каналов (трактов), арендуемых у операторов связи. Все это позволяет обеспечить предоставление комплекса услуг связи подразделениям системы МВД России.

Системы с FDMA дают большую дальность связи происходит это за счет меньшей энергии сигнала на один бит информации. В реальных условиях стандарт APCO-25 способен покрыть большее пространство, чем другие стандарты за счет больших мощностей базовых и мобильных станций [3].

Таким образом, можно сделать выводы, что в настоящее время стандарт APCO-25 составляет большую конкуренцию другим стандартам цифровой связи. Развертывание систем связи различных стандартов на территории России может оказать положительное влияние на выполнение служебно-боевых задач органов внутренних дел (ОВД). Стандартизация процессов и процедур способствует повышению эффективности работы сотрудников, улучшает взаимодействие между различными подразделениями и позволяет унифицировать подходы к решению задач, связанных с обеспечением общественной безопасности.

Также стоит отметить, что стандарты могут предусматривать соответствующие меры по подготовке и обучению сотрудников ОВД, что ведет к повышению их квалификации и профессионализма. В результате, это благоприятно сказывается на способности сотрудников реагировать на современные вызовы и угрозы в сфере безопасности, что в конечном итоге обеспечивает защиту прав и свобод граждан.

ЛИТЕРАТУРА

1. Об утверждении структуры интегрированной мультисервисной телекоммуникационной системы органов внутренних дел : приказ МВД России № 763 от 26 сентября 2006 г. // Правовая система «Консультант Плюс»/ www.consultant.ru.

2. О связи : федеральный закон Российской Федерации от 16 февраля 1995 г. N 15-ФЗ в ред. Федерального закона Российской Федерации от № // Правовая система «Консультант Плюс»/ www.consultant.ru.

3. Галкин В.А. Цифровая мобильная радиосвязь : учебное пособие для вузов / В.А. Галкин. – М.: Горячая линия – Телеком, 2007. – 432 с.

4. Давыдов П.Б. Информация и сети связи. / П.Б. Давыдов. – М., 2000.

СВЕДЕНИЯ ОБ АВТОРАХ

Ивануха Иван Сергеевич. Преподаватель кафедры информационных технологий в деятельности ОВД.

Омская академия МВД России.

E-mail: scorpion-6588@mail.ru

Россия, 644092, г. Омск, ул. Проспект Комарова, 7.

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

Воронежский институт МВД России.

E-mail: DmitreyRUS@mail.ru
Россия, 394065, г. Воронеж, пр. Патриотов, 53.

Ivanukha Ivan Sergeyevich. Lecturer of the Department of Information Technology in the activities of the Department of Internal Affairs.
Omsk Academy of the Ministry of Internal Affairs of Russia.
E-mail: scorpion-6588@mail.ru
Russia, 644092, Omsk, Prospekt Komarova str., 7.

Kalkov Dmitry Yurievich. Associate Professor of the Department of Radio Engineering Systems and Security Monitoring Complexes. Candidate of Technical Sciences.
Voronezh Institute of the Ministry of internal Affairs of Russia.
E-mail: DmitreyRUS@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: АРСО-25, системы связи, стандарты связи, разделение каналов связи, обмен информацией.

Keywords: APCO-25, communication systems, communication standards, separation of communication channels, information exchange.

УДК 621.396.2

Калков Дмитрий Юрьевич,
кандидат технических наук;
Ивануха Иван Сергеевич

МОДЕЛЬ ОПТИМАЛЬНОГО РАСПРЕДЕЛЕНИЯ СИЛ И СРЕДСТВ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ПРИ ОХРАНЕ ОБЩЕСТВЕННОГО ПОРЯДКА И ОБЕСПЕЧЕНИИ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

THE MODEL OF OPTIMAL DISTRIBUTION OF FORCES AND MEANS OF LAW ENFORCEMENT AGENCIES IN THE PROTECTION OF PUBLIC ORDER AND ENSURING PUBLIC SAFETY

В данной статье рассматриваются вопросы обеспечения безопасности при проведении публичных массовых мероприятий. Представлен способ формализации задачи и математическая модель оптимального распределения сил и средств правоохранительных органов.

This article discusses the issues of ensuring security during public mass events. A method of formalizing the problem and a mathematical model of the optimal distribution of forces and means of law enforcement agencies are presented.

При решении задачи по охране общественного порядка (ООП) и обеспечении общественной безопасности (ООБ) во время проведения массовых мероприятий руководителю органа внутренних дел необходимо на подготовительном этапе провести тщательный анализ оперативной обстановки на подконтрольной территории, выявить уязвимые места, оценить риски и определить необходимый объем сил и средств, в том числе резерв. При этом важно не забывать про деятельность сотрудников, несущих службу согласно плану единой дислокации постов и маршрутов патрулирования в период проведения массовых мероприятий и на следующие сутки, которым, в свою очередь, также необходимо выделить время на отдых. Дополнительные трудности в решении поставленной задачи накладывает существенный некомплект личного состава, в частности младшего начальствующего состава, который наблюдается во многих подразделениях.

Охраной общественного порядка и обеспечением общественной безопасности в первую очередь занимаются подразделения МВД России. Однако существенную поддержку им оказывает на сегодняшний день и подразделения Росгвардии, в частности подразделения вневедомственной охраны.

Также с целью оказания помощи правоохранительным органам могут быть выделены дополнительные силы от частных охранных организаций и предприятий. Как правило, частные охранники обеспечивают пропускной режим через точки доступа в зону массового мероприятия. При этом один сотрудник полиции может быть закреплен за несколькими близко расположенными друг к другу точками доступа.

Для выполнения моделирования порядка расчета сил и средств подразделений правоохранительных органов необходимо предварительно выполнить формализацию поставленной задачи. Формализация задачи заключается в ее математическом описании и структурировании. Она позволяет провести систематический анализ и поиск наилучшего решения с учетом всех факторов и ограничений, является важным инструментом для принятия обоснованных решений и оптимизации использования ресурсов в различных сферах деятельности.

Введем следующие обозначения:

$M = \{m_1, m_2, \dots, m_n\}$ – множество мест массового пребывания людей;

$m = \langle S, P, k, l \rangle$ – место массового пребывания людей, характеризующееся следующими параметрами:

S – площадь места;

P – периметр места;

k – количество точек доступа к месту;

l – предполагаемое количество людей.

$S = \{s_1, s_2, \dots, s_n\}$ – количество сил, выделяемых для ООП и ООБ в n местах массового пребывания людей;

$C = \{c_1, c_2, \dots, c_n\}$ – количество средств, выделяемых для ООП и ООБ в n местах массового пребывания людей;

$\alpha = \{\alpha^1, \alpha^2, \dots, \alpha^k\}$ – количество выделенных сил подразделений МВД России для обеспечения *k* нарядов;

$\beta = \{\beta^1, \beta^2, \dots, \beta^k\}$ – количество выделенных сил подразделений Росгвардии для обеспечения *k* нарядов;

$\gamma = \{\gamma^1, \gamma^2, \dots, \gamma^k\}$ – количество выделенных сил частных охранных организаций и предприятий для обеспечения *k* нарядов;

$\sigma = \{\sigma^1, \sigma^2, \dots, \sigma^k\}$ – количество выделенных средств подразделений МВД России для обеспечения *k* нарядов;

$\varphi = \{\varphi^1, \varphi^2, \dots, \varphi^k\}$ – количество выделенных средств подразделений Росгвардии для обеспечения *k* нарядов;

$\theta = \{\theta^1, \theta^2, \dots, \theta^k\}$ – количество выделенных средств частных охранных организаций и предприятий для обеспечения *k* нарядов;

e^i – эффективность сил/средств правоохранительных органов *i* наряда.

В условиях финансовых ограничений, а также неполной укомплектованности подразделений правоохранительных органов задача сводится к нахождению такого оптимального количества сил *S* и средств *C* правоохранительных органов, при котором будет достигнут достаточный уровень безопасности в местах массового пребывания людей *M*.

Рассмотрим подробнее пример типичной задачи по расчету сил и средств правоохранительных органов для охраны общественного порядка и обеспечении общественной безопасности.

На территории условного населенного пункта запланировано проведение праздничных массовых мероприятий в нескольких местах $M = \{m_1, m_2, \dots, m_n\}$. Каждое место m_i обладает рядом характеристик, влияющих на количество требуемого объема сил и средств для обеспечения безопасности. Среди этих характеристик наибольший интерес вызывает площадь территории s_i, периметр территории p_i, предполагаемое количество людей l_i, пребывающих на территории m_i, а также количество точек доступа k_i, предназначенных для организации безопасного и контролируемого прохода лиц на территорию проведения праздничных мероприятий.

Руководитель территориального органа внутренних дел, опираясь на собственный опыт, опыт проведения подобных мероприятий в прошедшие периоды времени, должен принять решение о выделяемых силах и средствах.

Площадь территории s_i должна быть под контролем сотрудников правоохранительных органов, несущих службу, как правило, в виде пешего патруля в составе от одного до нескольких человек.

Периметр территории p_i должен быть защищён от проникновения посторонних лиц инженерными заграждениями, естественными препятствиями либо личным составом правоохранительных органов, несущих службу в виде полицейской цепочки. Исходя из оперативной обстановки и возможных рисков, руководитель может изменять количество привлекаемого личного состава в данный наряд путем сокращения либо увеличения расстояния между сотрудниками. Также по периметру территории p_i может нести службу группы задержания вневедомственной охраны Росгвардии.

Количество нарядов правоохранительных органов также зависит и от предполагаемого количества людей l_i, и связанного с ним количества вероятных правонарушений. Также этот показатель будет оказывать влияние на количество точек доступа k_i. Оптимальное количество точек доступа необходимо рассчитывать используя математические методы теории массового обслуживания [12].

Таким образом, на территории m_i необходимо выделить такое количество сил $s_i = \alpha_i + \beta_i + \gamma_i$, а также средств $c_i = \sigma_i + \varphi_i + \theta_i$ правоохранительных органов и организаций, чтобы обеспечить достаточный уровень безопасности.

Под эффективностью e^i сил и средств можно понимать их важность пребывания в том или ином месте несения службы. Данный показатель принимает значения $0 \leq e^i \leq 1$ и определяется руководителем территориального органа внутренних дел. Функция $e^i(k)$, где k – количество нарядов одного вида, может являться нелинейной, так как при достижении определенного k, дальнейшее увеличение нарядов этого вида не будет приносить существенного вклада.

При организации ООП и ООБ в местах массового пребывания людей, необходимо учитывать ряд условий и ограничений:

1) $S \leq S_{max}$, где S_{max} – максимально возможное количество выделяемых сотрудников правоохранительных органов, в том числе резерв. S_{max} определяется разностью фактической численности подразделений правоохранительных органов/организаций и численностью текущих и заступающих на службу нарядов, количеством лиц, находящихся в отпуске, командировке, на больничном и по иным уважительным причинам отсутствующих в подразделениях.

2) $C \leq C_{max}$, где C_{max} – максимально возможное количество выделяемых средств правоохранительных органов. В данной постановке задачи отсутствует разделение на конкретные виды средств, однако, необходимо это иметь в виду.

Таким образом, решение данной задачи можно описать следующим математическим выражением:

$$A = Argmax \sum_{i=1}^{n} \sum_{j=1}^{k} \left(\alpha_i^j e^{\alpha_i^j} + \beta_i^j e^{\beta_i^j} + \gamma_i^j e^{\gamma_i^j} + \sigma_i^j e^{\sigma_i^j} + \varphi_i^j e^{\varphi_i^j} + \theta_i^j e^{\theta_i^j} \right), \quad (1)$$

при следующих ограничениях:

$$S = \alpha_i^j + \beta_i^j + \gamma_i^j \leq S_{max}, \quad (2)$$

$$C = \sigma_i^j + \varphi_i^j + \theta_i^j \leq C_{max}, \quad (3)$$

Выражение (2) определяет предельное количество личного состава правоохранительных органов, включая подразделения МВД России, Росгвардии и частных охранных предприятий.

Выражение (3) определяет предельное количество средств правоохранительных органов, включая подразделения МВД России, Росгвардии и частных охранных предприятий.

Определение количества сил и средств Росгвардии и частных охранных организаций выполняется по согласованию с руководителями.

Для решения задачи, описанной математической моделью (1) при заданных ограничениях необходимо выбрать определенный алгоритм.

Для изучения задачи дискретной конечной математической структуры, как правило, можно найти комбинированный алгоритм ее решения, например, используя определенный итерационный процесс. Однако количество шагов быстро увеличивается по мере увеличения объема входных данных, и задача фактически становится неразрешимой.

Поиск эффективного алгоритма для решения дискретных математических задач привел к одной из его важнейших проблем - проблеме устранения возможности вариантной итерации в комбинаторных алгоритмах.

В самом широком смысле эффективность алгоритма связана со всеми вычислительными ресурсами, необходимыми для его работы. Однако обычно наиболее эффективный означает «самый быстрый» алгоритм.

Существует множество критериев для оценки алгоритмов. Но одним из самых важных критериев, можно сказать, является сложность его времени. Время выполнения алгоритма может быть выражено как функция размера входных данных, необходимых для описания задачи. Входные и выходные данные могут быть закодированы «разумным» способом в виде двоичной последовательности из «0» и «1». И наоборот, алгоритм можно рассматривать как последовательность двоичных операций, которые манипулируют памятью на основе двоичных символов.

Временная сложность алгоритма отражает время (количество шагов), необходимое для его работы. Это функция, которая сопоставляет каждую

входную длину n с минимальным временем, которое требуется алгоритму для решения всех одиночных задач одного типа этой длины.

На сегодняшний день проведено достаточно большое количество научных работ, посвященных решению задач оптимального распределения ресурсов, в основе которых наиболее часто лежат методы динамического программирования, линейного программирования и метод ветвей и границ [10, 11, 13-15].

Метод динамического программирования (Dynamic Programming) – это алгоритмический подход, который используется для решения оптимизационных задач с перекрывающимися подзадачами. Он основан на идее разбиения сложной задачи на более простые подзадачи, решение которых сохраняется и используется для решения более общей задачи.

Метод линейного программирования (Linear Programming, LP) – это математический метод для решения оптимизационных задач, где целевая функция и ограничения представлены линейными уравнениями или неравенствами.

Метод ветвей и границ (Branch and Bound) – это метод решения комбинаторных задач, который позволяет найти оптимальное решение путем систематического разбиения пространства поиска на подпространства и оценки их границ. Метод ветвей и границ эффективен для решения задач комбинаторной оптимизации, таких как задачи о раскраске графов, задачи о рюкзаке, задачи о покрытии множества и другие. Он позволяет систематически исследовать все возможные варианты решений и эффективно отсекать неперспективные подпространства, что приводит к сокращению времени выполнения задачи.

Обеспечение безопасности в местах массового пребывания людей является многогранной задачей, требующей комплексного подхода и совместных усилий различных структур. Как показывают международные практики, эффективно работать над минимизацией угроз можно только при условии тесного взаимодействия органов власти, правоохранительных структур, организаторов мероприятий и самих граждан. Внедрение современных технологий, таких как системы видеонаблюдения, анализ больших данных и автоматизированные процессы реагирования на чрезвычайные ситуации, значительно повышает уровень безопасности и помогает быстро реагировать на возникающие угрозы.

Однако важность профилактических мер нельзя недооценивать. Обучение персонала и информирование посетителей о правилах безопасности способствуют созданию культуры безопасности, где каждый чувствует свою ответственность за общее благополучие.

Задача обеспечения безопасности – это не только реакция на угрозы, но и создание спокойной, комфортной атмосферы, способствующей всеобъемлющему взаимодействию. Вовлекая общественность в диалог по вопросам безопасности, можно значительно повысить уровень доверия и взаимопонимания, что в конечном итоге принесет пользу всему обществу.

Важным аспектом в обеспечении безопасности является использование инновационных подходов к планированию мероприятий. К примеру, применение концепций риск-менеджмента позволяет заранее выявить потенциальные угрозы и разработать соответствующие стратегии реагирования. Это включает в себя не только технические меры, но и социальные инициативы, направленные на повышение осведомленности граждан о возможных рисках. Применение методов расчета оптимального количества сил и средств органов безопасности позволит максимально эффективно использовать имеющиеся ресурсы для охраны общественного порядка и обеспечению общественной безопасности

Помимо этого, создание партнерств между частным сектором и государственными органами может стать катализатором для внедрения новейших технологий и подходов. Частные компании, обладая экспертизой и ресурсами, могут внести значительный вклад в разработку эффективных решений, которые позволят улучшить уровень безопасности на массовых мероприятиях.

Таким образом, комплексный подход к безопасности на массовых мероприятиях строится на принципах вовлеченности, диалога и инноваций, что в итоге способствует созданию безопасной и комфортной общественной среды.

ЛИТЕРАТУРА

1. Плескунов, М.А. Теория массового обслуживания : учебное пособие / М.А. Плескунов ; М-во науки и высшего образования РФ, Урал. федер. ун-т. – Екатеринбург : Изд-во Урал. ун-та, 2022.– 264 с.

2. Костюк, А.В. Об оптимальном распределении временного ресурса по изучаемым темам – Текст : непосредственный / А.В. Костюк, А.К. Черных // В сборнике: Теоретические и прикладные вопросы образования и науки. сборник научных трудов по материалам Международной научно-практической конференции. – 2014. – С. 50-51.

3. Орлова, Е.В. Модель оперативного оптимального управления распределением финансовых ресурсов предприятия – Текст : непосредственный / Е.В. Орлова // Компьютерные исследования и моделирование. – 2019. – Т. 11. – № 2. – С. 343-358.

4. Струченков, В.И. Методы оптимизации в прикладных задачах. – Текст: непосредственный. – М. : СОЛОН-ПРЕСС, 2016. – 320 с.: ил. (Серия «Библиотека профессионала).

5. Струченков, В.И. Новые алгоритмы оптимального распределения ресурса – Текст : непосредственный / В.И. Струченков // Томск : Прикладная дискретная математика. – № 4(10). – 2010. – С. 73-78.

6. Топоров, Б.П. Игровая математическая модель оптимального распределения ресурсов в условиях дефицита информированности сторон – Текст : непосредственный / Б.П. Топоров, С.Л. Демидов // Труды ГосНИИАС.

Серия: Информационные технологии в разработках сложных систем. – 2004. – № 1 (12). – С. 3-11.

СВЕДЕНИЯ ОБ АВТОРАХ

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

Воронежский институт МВД России.

E-mail: DmitreyRUS@mail.ru

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

Ивануха Иван Сергеевич, преподаватель кафедры информационных технологий в деятельности ОВД.

Омская академия МВД России.

E-mail: scorpion-6588@mail.ru

Россия, 644092, г. Омск, ул. Проспект Комарова, 7.

Kalkov Dmitry Yurievich. Associate Professor of the Department of Radio Engineering Systems and Security Monitoring Complexes. Candidate of Technical Sciences.

Voronezh Institute of the Ministry of internal Affairs of Russia.

E-mail: DmitreyRUS@mail.ru

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

Ivanukha Ivan Sergeyevich, lecturer of the Department of Information Technology in the activities of the Department of Internal Affairs.

Omsk Academy of the Ministry of Internal Affairs of Russia.

E-mail: scorpion-6588@mail.ru

Russia, 644092, Omsk, Prospekt Komarova str., 7.

Ключевые слова: охрана общественного порядка; обеспечение общественной безопасности; публичные мероприятия; массовые мероприятия; безопасность; расчет сил и средств; математическое моделирование.

Keywords: protection of public order; ensuring public safety; public events; mass events; security; calculation of forces and means; mathematical modeling.

УДК 351.74

Меркулова Наталья Ивановна,
кандидат технических наук

ОСОБЕННОСТИ ОСНАЩЕНИЯ ОБЪЕКТОВ, УДАЛЕННЫХ ОТ ГОРОДСКОЙ ИНФРАСТРУКТУРЫ, И ОТКРЫТЫХ ЗЕМЕЛЬНЫХ УЧАСТКОВ ЗНАЧИТЕЛЬНОЙ ПЛОЩАДИ СРЕДСТВАМИ ОХРАНЫ ПЕРИМЕТРА

FEATURES OF EQUIPPING FACILITIES REMOTE FROM URBAN INFRASTRUCTURE AND OPEN LAND PLOTS OF SIGNIFICANT AREA WITH PERIMETER SECURITY FACILITIES

В статье приводятся аспекты организации систем охраны периметров открытых протяженных участков, удаленных от городской инфраструктуры.

This article presents aspects of the organization of perimeter security systems for open extended areas remote from urban infrastructure.

Охрана периметра – трудоемкий многогранный процесс, требующий комплексного подхода к соблюдению принципов многорубежности сигнализации при должном уровне инженерно-технической укрепленности (далее – ИТУ). Но когда речь заходит об открытых участках местности, удаленных от городской инфраструктуры, стоит учитывать и соотношение достаточности защиты объекта с эффективностью финансовых затрат. Тем не менее, должный уровень качества предоставляемых охранных услуг невозможен без минимального набора мер организационно-технического характера.

Например, для оптимизации условий патрулирования рекомендуется предусмотреть грунтовую дорогу по периметру охраняемого объекта, а для оперативного реагирования на нарушения границ, при отсутствии элементов ограждения, применять контрольно-следовую полосу.

С целью своевременной координации действий нарядов и дежурных служб сотрудники охраны обеспечиваются средствами связи.

Для противодействия несанкционированному проникновению на охраняемую территорию на время, необходимое для выявления и пресечения противоправного деяния, следует обеспечить установку механического препятствия, затрудняющего совершение противоправного действия и предоставляющего дополнительное время для реагирования подразделениям охраны. Учитывая, что периметр таких участков может измеряться десятками километров, его эффективная защита возможна при сочетании средств ИТУ и технических средств охраны (далее – ТСО), обеспечивающих наиболее раннее обнаружение попытки или факта преодоления периметра.

В случае отсутствия возможности применения ТСО на охраняемом объекте противодействие несанкционированному доступу на охраняемую территорию рекомендуется обеспечивать увеличением высоты ограждения путем использования дополнительного ограждения.

При установке основного ограждения целесообразно минимизировать количество изгибов и поворотов с целью наиболее благоприятных условий для функционирования периметровых средств обнаружения с линейными зонами обнаружения и создания оптимальных условий для визуального наблюдения посредством систем охранного телевидения. По решению руководителя охраняемого объекта основное ограждение объекта может быть дооборудовано дополнительным и/или предупредительным ограждениями.

Возможные к применению виды ограждения и порядок их применения отражены в ГОСТР 57278-2016 и методических рекомендациях Р 78.36.034-2013 «Мониторинг применения и сравнительный анализ испытаний различных видов периметрового ограждения (основного ограждения, дополнительного ограждения, предупредительного внешнего и внутреннего ограждения). Классификация».

В целях усиления защиты периметра охраняемого объекта рекомендуется использовать сочетание механического препятствия и ТСО, обеспечивающих в совокупности более раннее обнаружение попыток или фактов преодоления периметра. Для эффективной работы системы охранной сигнализации (далее – СОС) с выводом извещений на внутренний пост охраны или пункт централизованной охраны (далее – ПЦО) в ее состав целесообразно включение извещателей, обнаруживающих присутствие потенциального правонарушителя до механического воздействия с его стороны на ограждение, и позволяющих определять его место нахождения.

Одновременно, для исключения затрат времени на реагирование подразделений охраны при получении извещения о тревоге с целью визуального подтверждения совершения противоправных действий на охраняемом объекте и, в частности, при большой протяженности периметра контролируемого СОС, средства обнаружения целесообразно дополнять СОТ, обеспечивающей возможность визуального контроля наиболее уязвимых для несанкционированного преодоления мест периметра.

Оптимальным моментом обнаружения нарушителя периметровыми средствами обнаружения должна быть стадия преодоления ограждения, иначе, при более позднем обнаружении силы реагирования уже будут находиться в дефиците времени. Различные физические принципы обнаружения для такого класса ТСО определяют возможность их выбора при реализации функций охраны с учетом фактически имеющихся ограничений (рельеф местности, влажность и др.) и выбора наиболее эффективной тактики охраны для каждого конкретного случая. Применение извещателей с разными принципами обнаружения позволяет обеспечить охрану периметров различных конфигураций, из различных видов и материалов полотен ограждения, а также

с учетом наиболее вероятного предполагаемого варианта преодоления ограждения периметра.

Для любого вида извещателей характерен ряд технических характеристик и эксплуатационных особенностей, определяющих надежность работы и достоверность обнаружения проникновения. Так, при проектировании СОС на открытой местности, следует учитывать:

– физический принцип обнаружения воздействия;

– тип обнаруживаемого воздействия при проникновении;

– размеры зоны обнаружения проникновения (площадь, протяженность, высота);

– диапазон обнаруживаемых скоростей перемещения;

– точность локализации места проникновения;

– наличие функции автоматической корректировки или возможности дистанционного управления параметрами средства обнаружения (изменение чувствительности, изменение зон обнаружения и др.);

– помехозащищенность;

– климатическое исполнение;

– степень защиты внутренних элементов конструкции от воздействия внешних климатических и иных факторов (температура, влажность, атмосферные осадки, пыль и др.) обеспечиваемая оболочкой;

– степень защиты от внешних механических воздействий, обеспечиваемая корпусом;

– наличие защиты от доступа к элементам коммутации и управления, токоведущим элементам, от несанкционированного воздействия на конструктивные элементы, обеспечивающие обнаружение (маскирование), либо средств обнаружения указанных действий;

– наличие защиты от несанкционированного изменения режимов работы и положения в пространстве элементов извещателя;

– наличие, размер, геометрические характеристики и особенности формирования «мертвых» зон – участков пространства в зоне обнаружения, где вероятность обнаружения меньше заданной или обнаружение технически невозможно.

В зависимости от целевой задачи извещатели могут быть разделены на периметровые – обеспечивающие обнаружение проникновения через границу периметра вне помещений, и объектовые – обеспечивающие обнаружение нарушителя внутри помещений.

Следует учитывать ограничения технических средств обнаружения для периметра по устойчивости к помехам различного происхождения – порывам ветра, атмосферным осадкам, туману, росе, сейсмическим и виброакустическим помехам от транспортных средств и другим техногенным факторам.

Основной принцип классификации периметровых средств обнаружения ориентирован на физические принципы, положенные в основу

обнаруживаемого воздействия: электромеханические, вибрационные (трибоэлектрические, оптоволоконные), емкостные, индуктивные, радиолокационные, проводноволновые, магнитометрические, сейсмические, оптико-электронные (активные и пассивные), волоконно-оптические.

Использование технических средств, основанных на каком-либо одном физическом принципе обнаружения, имеют ограниченную помехоустойчивость, что приведет к низкой достоверности обнаружения на объектах со сложной помеховой обстановкой. Каждое сформированное по ложному срабатыванию тревожное извещение приведет к необоснованным затратам времени на реагирование групп задержания.

Более эффективная защита ограждений периметров объектов от наиболее вероятных способов преодоления может быть обеспечена преимущественно при использовании нескольких типов извещателей, работающих на разных принципах обнаружения, либо извещателями, объединяющими несколько модулей с различными принципами обнаружения в одном корпусе – совмещенные или комбинированные.

Принципы работы и технические характеристики некоторых типов извещателей требуют организации зоны отторжения, исключающей воздействие внешних помеховых факторов – наличия деревьев (кустарников), способных создать помехи для средств охранной сигнализации.

При проектировании СОС периметра объекта рекомендуется разделять основное ограждение, ворота и калитки на отдельные охраняемые участки (зоны) с подключением их раздельными шлейфами сигнализации к устройствам оконечным объектовым систем передачи извещений для более точного определения места срабатывания извещателя. Длина участков определяется исходя из тактики охраны, технических характеристик ТСО, конфигурации внешнего ограждения, условий прямой видимости и рельефа местности. Допускается использование адресных СОС с кольцевой структурой шлейфов сигнализации.

По решению руководителя объекта на открытых земельных участках значительной площади основное ограждение объекта может быть дооборудовано дополнительным и предупредительным ограждениями. Для обеспечения визуального контроля и видеодокументирования обстановки при охране объекта, проверки поступающих сигналов тревоги, анализа причин и развития нештатных ситуаций, получения дополнительной визуальной информации для принятия оперативных решений охраняемые объекты оборудуются СОТ, которая позволяет в реальном времени осуществлять оценку оперативной обстановки путем визуального наблюдения происходящих событий в поле зрения камер и обеспечивать передачу видеоинформации по имеющимся в наличии каналам связи [1].

Принимая во внимание удаленность охраняемого объекта и время, необходимое для прибытия сил охранной организации по сигналу «тревога», при организации охраны рекомендуется применять средства ИТУ, обеспечивающие противодействие несанкционированному проникновению на

охраняемый объект или иному механическому воздействию на его конструктивные элементы на период, необходимый для его выявления и пресечения.

При проведении обследования объекта, принимаемого под охрану, рекомендуется обращать особое внимание на его удаленность от мест дислокации подразделения вневедомственной охраны или организации, подведомственной Федеральной службе войск национальной гвардии Российской Федерации, возможность организации устойчивой передачи тревожных и служебных извещений с объекта, наличие автомобильных дорог и другие факторы, влияющие на своевременное реагирование нарядов охраны на сигналы «тревога», поступающие с данного объекта.

Принимая решение о приеме объекта под централизованную охрану, наиболее целесообразно учитывать время прибытия нарядов подразделений вневедомственной охраны по сигналу «тревога». В случае значительного времени прибытия нарядов подразделений вневедомственной охраны по сигналу «тревога» охрану рекомендуется организовать путем непосредственного выставления поста (патруля) охраны на объекте, что в соответствии с требованиями может быть реализовано по решению руководителя объекта. В данном случае СОС целесообразно выводить, помимо ПЦО, дополнительно на пост охраны на объекте в целях реагирования на сигналы «тревога» и оказания противодействия нарушителям до прибытия наряда подразделений вневедомственной охраны по сигналу «тревога».

Одновременно, в рамках организации охраны объектов, расположенных на значительном удалении от населенных пунктов, рекомендуется информировать заказчика о преимуществах оснащения объекта системой оповещения, включающей возможность оперативного информирования персонала объекта о совершении несанкционированных действий и исключении фактора проникновения нарушителя.

ЛИТЕРАТУРА

1. Особенности оснащения инженерно-техническими средствами охраны принимаемых под централизованную охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации объектов, на которых осуществляется культивирование наркосодержащих растений и представляющих собой открытые земельные участки значительной площади или строения, строительные конструкции которых сделаны из материалов, не позволяющих обеспечивать их взломостойкость (ударопрочность), а также объектов, расположенных в удаленных от населенных пунктов местностях, в которых осуществляются деятельность, связанная с оборотом наркотических средств, психотропных веществ и внесенных в список перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации :

методические рекомендации – М. : ФКУ «НИЦ «Охрана» Росгвардии, 2022. – 40 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Меркулова Наталья Ивановна. Доцент кафедры радиотехнических систем и комплексов охранного мониторинга. Кандидат технических наук.
Воронежский институт МВД России.
E-mail: gomova.nata2008@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Merkulova Natalia Ivanovna. Docent in department electronic systems and complexes of security monitoring. Candidate of Engineering Sciences.
Voronezh Institute of the Ministry of the Interior of Russia, Voronezh, Russia.
E-mail: gomova.nata2008@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: системы охраны периметра; охранная сигнализация; принципы обнаружения.

Key words: perimeter security systems; burglar alarms; detection principles.

УДК 654.16

Михайленко Евгений Владимирович

ПРАВОВЫЕ ОСНОВЫ СОТРУДНИЧЕСТВА МВД РОССИИ С КОМПЕТЕНТНЫМИ ОРГАНАМИ РЕСПУБЛИКИ БЕЛАРУСЬ

THE LEGAL BASIS OF COOPERATION BETWEEN THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA AND THE COMPETENT AUTHORITIES OF THE REPUBLIC OF BELARUS

В статье обосновывается тезис, что политика обеспечения общественной и национальной безопасности зависит не только от внутренних усилий государства, но и от качества заключаемых региональных соглашений, что позволят противодействовать преступности в эпоху роста трансграничных противоправных фактов. Приведен комплексный анализ сотрудничества МВД России и МВД Республики Беларусь по различным направлениям, принципиально значимым для упорядочивания общественных отношений и создания безопасных условий существования социума при взаимном соблюдении интересов.

The article substantiates the thesis that the policy of ensuring public and national security depends not only on the internal efforts of the state, but also on the quality of regional agreements concluded, which will make it possible to counter crime in an era of increasing cross-border illegal facts. The article provides a comprehensive analysis of cooperation between the Ministry of Internal Affairs of Russia and the Ministry of Internal Affairs of the Republic of Belarus in various areas that are fundamentally important for streamlining public relations and creating safe living conditions for society with mutual respect for interests.

Начало XXI века ознаменовано коренными политическими преобразованиями, вносящими существенные коррективы в содержание международных правоотношений и сотрудничество между государствами. Созданная модель однополярного мирового порядка с превалированием США изжила себя. Экономическое развитие и налаживание торгово-транспортных связей, образование союзов и усиление регионального взаимодействия повлекли за собой предпосылки для формирования многополярного мирового порядка, в развитие которого происходит перераспределение сфер влияния. Налаживание политических и экономических связей между Россией, Китаем, Индией, государствами Африки – существенное достижение последних лет. Построенные отношения минуют развитые страны Западного мира и США, в частности, создавая новые политические возможности.

Достигнутые результаты негативно воспринимаются странами коллективного Запада и США, что влечет за собой угрозы для национальной безопасности Российской Федерации, общественные и политические волнения, эскалацию напряженности, международные споры, в том числе по самым различным и, порой, абсурдным вопросам. Современная агрессивная политика западных государств проводит открытый курс по дестабилизации мировой безопасности, игнорируя решения важнейших международных институтов, нарушая нормативные положения международного уровня, порождая споры транснационального характера.

В созданных условиях международная арена претерпевает существенные изменения, а создание угроз и вызовов для государств происходит повсеместно. Одним из принципиальных направлений обеспечения безопасности является взаимодействие национальных правоохранительных органов, что возможно как в рамках сотрудничества с Международной организацией уголовной полиции – Интерпол, так и на основании региональных соглашений.

Политическая модель России во многом ориентирована на рядом расположенные государства и страны Ближнего Востока, а также Африки. Однако достаточно крепкие и устойчивые дипломатические связи сложились с Республикой Беларусь и взаимодействие происходит по всем возможным направлениям, включая правоохранительные органы.

Основным источником сотрудничества является «Соглашение о сотрудничестве между Министерством внутренних дел Российской

Федерации и Министерством внутренних дел Республики Беларусь», заключенное 30.09.1997 в г. Москва [4]. Двусторонний правовой акт предписывает множество сфер взаимодействия в сфере различных преступлений, таким как: преступления против жизни, здоровья, свободы и достоинства личности, а также против собственности; террористических актов; коррупции и организованной преступности; незаконного оборота оружия, боеприпасов, взрывчатых и ядовитых веществ, а также радиоактивных материалов; незаконных производства и оборота наркотических средств и псих тройных веществ, а также веществ, используемых в процессе их изготовления; преступлений в сфере экономики, в том числе незаконных операций валютными ценностями, незаконных международных финансовых и экспортных операций, легализации доходов, полученных от преступной деятельности изготовления и сбыта поддельных денежных знаков и финансовых документов ценных бумаг и средств безналичных платежей; преступных посягательств на культурные и исторические ценности; преступлений на транспорте.

Одновременно с этим стороны берут на себя обязательства содействовать в сфере охраны общественного порядка; обеспечения безопасности дорожного движения; розыска лиц, скрывающихся от уголовного преследования или исполнения приговора, а также без вести пропавших лиц; идентификация (установление) неопознанных трупов, личности неизвестных больных и детей, а также лиц, не могущих сообщить о себе; розыск и передача предметов (вещей), имеющих номера или специфические (индивидуальные) отличительные признаки, в том числе автотранспорта и огнестрельного оружия, а также номерных ценных бумаг и паспортов (удостоверений личности) и т.д.

С течением времени и преображении преступности, возникли объективные потребности в доработке действующего соглашения, ввиду чего 15.09.2014 в г. Брест принимается «Соглашение между Российской Федерацией и Республикой Беларусь о повышении эффективности взаимодействия в борьбе с преступностью» [6], основным направлением которого стало расширение сфер сотрудничества, усиление координационных мер, систематический обмен опытом, в совокупности с проведением научных исследований и повышению квалификации правоохранительных органов.

Заключение подобных договоров позволяет наглядно реализовывать принцип неотвратимости правосудия на территории двух государств, причем весьма плодотворно. Наглядным примером можно обозначить события в июне 2023 года, когда в Воронежской области МВД России, при тесном сотрудничестве с МВД Республики Беларусь провели задержание лица, который в 1996 году, находясь в г. Минск 1996 года изнасиловал женщину, затем убил её и сжег. В последующем, установлена его причастность к двум аналогичным фактам. Предъявлено обвинение в совершении преступлений, предусмотренных ст.ст. 105, 131, 158, 159, 162, 167 и 325 УК РФ [9].

Кроме того, существуют различные профильные соглашения между МВД России и МВД Республики Беларусь, которые регламентируют определенную сферу правоотношений. К таким можно отнести заключенное «Соглашение о сотрудничестве между Министерством Внутренних Дел Российской Федерации и Министерством Внутренних Дел Республики Беларусь о сотрудничестве органов внутренних дел приграничных регионов» от 30.09.1997 в г. Москве [5]. Предметом сотрудничества является обмен оперативно-розыскной, криминалистической и иной информацией, значимой для обеспечения общественной безопасности и правопорядка, в том числе практическое содействие в оперативно-розыскных мероприятиях по противодействию различным уголовно наказуемым деянием (обороту оружия, наркотических средств, психотропных веществ и их прекурсоров, их контрабанде, и т.д.).

Обособленно стоит указать о сотрудничество МВД России и МВД Республики Беларусь по вопросам противодействия незаконной миграции, что крайне актуально в настоящее время. Действуя во исполнение Договора «О создании Союзного государства» от 08.12.1999 заключенного в г. Москве [2]. Закладывая основу в сфере российско-белорусских отношений особенно акцентировано внимание на создание упорядоченной миграции, как одного из сегмента обеспечения общественной и национальной безопасности. В развитие указанных положений 04.11.2021 утвержден стратегический документ – Концепция миграционной политики Союзного государства [7]. Региональные подразделения МВД принимают активное участие в формировании единого миграционного пространства. Кроме того, 09.12.2022 Постановлением Совета Министров Союзного государства № 40 утвержден «План мероприятий по реализации в 2022-2026 годах Концепции» [8], предусматривающий разработку и реализацию общих подходов по вопросам государственного регулирования в сфере миграции, обеспечение безопасности, информационное и кадровое взаимодействие. Не смотря на тот факт, что данные акты не являются прямым соглашениями между правоохранительными органами, таковые активно вовлечены в правотворческий процесс и правоприменение.

Существуют также соглашения между высшими органами государственной власти по вопросам противодействия обособленным сегментам преступности. Для примера можно обозначить Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь от 22.11.1999 года «О сотрудничестве в борьбе с незаконным оборотом наркотических средств и психотропных веществ и злоупотреблением ими» [3]. В основе принятия данного правового источника лежит концепция того, что стороны осознают опасность незаконного оборота наркотических средств и психотропных веществ, их не медицинское потребление, социальный характер данного вопроса и прямое влияние на благосостояние населения. Основной взаимодействия считается сотрудничество государств (осуществляемого в различных формах), в основе

которого лежит обеспокоенность о нарастающий тенденциях в сфере наркотрафика. В соглашении установлен перечень органов государственной власти, участвующих в оказании межгосударственного содействия, а для обмена информацией предусмотрено не только установление каналов связи, но и создание единых баз данных. Цель же заключенного Соглашения в полной мере выражается в ст.ст. 11,12,13 – профилактике наркомании и реабилитации больных, осуществлении контроля за легальным оборотом наркотиков и прекурсоров, унификации законодательства в данной сфере правоотношений. МВД Российской Федерации и МВД Республики Беларусь назначены главными субъектам в сфере реализации данного регионального соглашения, так как обязаны обмениваться информацией, оказывать содействие в реализации запросов, а также проводить совместные оперативно-розыскные мероприятия.

Резюмируя вышесказанное, сотрудничество МВД Российской Федерации и МВД Республики Беларусь – результат многолетней работы и тесных дипломатических связей, обусловленные совместной заинтересованностью в создании должного уровня общественной и национальной безопасности. На современном этапе взаимодействие не ограничивается лишь обменом информацией, так как включает в себя оперативно-розыскные, следственные, уголовные меры, а также совместное правотворчество и правоприменение в различных сферах общественных отношений.

ЛИТЕРАТУРА

1. Конституция Российской Федерации // СП «Гарант.ру» [Электронный ресурс] Режим доступа: URL: http://www.garant.ru/doc/constitution/
2. О создании Союзного государства: Договор от 08.12.1999 г. Москва [Электронный ресурс] Режим доступа URL: https://docs.cntd.ru/document/901756243
3. О сотрудничестве в борьбе с незаконным оборотом наркотических средств и психотропных веществ и злоупотреблением ими: Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь от 22.11.1999 [Электронный ресурс] Режим доступа URL: https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/47010/
4. О сотрудничестве между Министерством Внутренних Дел Российской Федерации и Министерством Внутренних Дел Республики Беларусь: Соглашение 30.09.1997 г. Москва [Электронный ресурс] Режим доступа URL: https://mvd.ru/userfiles/30_09_1998_rbelarus.doc
5. О сотрудничестве между Министерством Внутренних Дел Российской Федерации и Министерством Внутренних Дел Республики Беларусь о сотрудничестве органов внутренних дел приграничных регионов: Соглашение от 30.09.1997 г. Москва [Электронный ресурс] Режим доступа

URL: https://mvd.ru/userfiles/30_09_1998_rbelarus.doc

6. О повышении эффективности взаимодействия в борьбе с преступностью: Соглашение между Российской Федерацией и Республикой Беларусь от 15.09.2014 г. Брест [Электронный ресурс] Режим доступа URL: https://docs.cntd.ru/document/420229309

7. Концепция миграционной политики Союзного государства: Концепция от 04.11.2021 [Электронный ресурс] Режим доступа URL: https://belarus.mid.ru/ru/countries/bilateral-relations/migratsionnaya_politika/

8. План мероприятий по реализации в 2022-2026 годах Концепции: Постановление Совета Министров Союзного государства № 40 от 09.12.2022 [Электронный ресурс] Режим доступа URL: https://soyuz.by/projects/resheniya-zasedaniy-gruppy-vysokogo-urovnya/postanovlenie-soveta-ministrov-soyuznogo-gosudarstva-ot-8-dekabrya-2023-g-40

9. МВД Медиа - Сотрудничество МВД России и Беларуси помогло раскрыть преступления, совершенные в 1996 году [Электронный ресурс] Режим доступа URL: https://mvdmedia.ru/news/operativnye-novosti/sotrudnichestvo-mvd-rossii-i-belarusi-pomoglo-raskryt-prestupleniya-sovershennye-v-1996-godu/

СВЕДЕНИЯ ОБ АВТОРЕ

Михайленко Евгений Владимирович. Начальник отдела полиции № 2 УМВД России по г. Воронежу ГУ МВД России по Воронежской области.

Магистрант Академии управления МВД России.

E-mail: mihaylenko1976@inbox.ru

Россия, 394000, г. Воронеж, Московский проспект, 13.

Mikhailenko Evgeny Vladimirovich. Head of the Police Department № 2 of the Ministry of Internal Affairs of Russia in Voronezh, the Ministry of Internal Affairs of Russia in the Voronezh Region. Master's student at the Academy of

Master's student at the Academy of Management of the Ministry of Internal Affairs of Russia.

E-mail: mihaylenko1976@inbox.ru

Work address: Russia, 394000, Voronezh, Moskovsky Prospekt, 13

Ключевые слова: преступность; региональное взаимодействие; МВД России; МВД Республики Беларусь; противодействие преступности; международное взаимодействие; общественная безопасность и правопорядок.

Keywords: crime; regional cooperation; the Ministry of Internal Affairs of Russia; the Ministry of Internal Affairs of the Republic of Belarus; crime prevention; international cooperation; public safety and law and order.

УДК 341.23

Сидоров Александр Викторович,
кандидат технических наук

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТОВ ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА ОТ АКТОВ НЕЗАКОННОГО ВМЕШАТЕЛЬСТВА, СОВЕРШАЕМЫХ С ПРИМЕНЕНИЕМ БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ

ENSURING THE SECURITY OF FUEL AND ENERGY COMPLEX FACILITIES FROM ACTS OF ILLEGAL INTERFERENCE COMMITTED WITH THE USING UNMANNED AIRCRAFT

В данной статье проведен анализ защищенности объектов топливно-энергетического комплекса от угроз, связанных с применением беспилотных воздушных судов. Рассмотрены особенности обеспечения безопасности объектов топливно-энергетического комплекса, даны концептуальные рекомендации по созданию системы физической защиты этих объектов, предложены инженерно-технические решения по защите объекта в целом и его критических элементов от актов незаконного вмешательства, совершаемых с применением беспилотных воздушных судов.

This article analyzes the security of fuel and energy complex facilities from threats associated with the use of unmanned aircraft. The features of ensuring the safety of fuel and energy complex facilities are considered, conceptual recommendations are given for creating a system of physical protection of these facilities, engineering and technical solutions are proposed to protect the facility as a whole and its critical elements from acts of illegal interference committed using unmanned aircraft.

В связи с проведением специальной военной операции, беспилотные воздушные суда (БВС) стали основной угрозой безопасности объектам различного функционального назначения. В настоящее время, объекты топливно-энергетического комплекса (ТЭК) все чаще подвергаются атакам БВС. Это серьезный вызов, который связан с прямой военной угрозой, совершением террористических актов с использованием БВС, поэтому актуальность обеспечения безопасности объектов ТЭК только возрастает.

Сбор, обработку оперативной информации о всех отраслях ТЭК, подготовку статистических и аналитических информационных материалов в России осуществляет Центральное диспетчерское управление топливно-энергетического комплекса, которое является филиалом ФГБУ «РЭА» Минэнерго России (далее – ЦДУ ТЭК) [1]. По данным ЦДУ ТЭК, на основе мониторинга средств массовой информации, в период с января по май 2024 года атакам украинских БВС крупные российские объекты нефтепереработки подвергались 17 раз, а именно [1]: 18 января –

Петербургский нефтяной терминал, расположенный на территории четвертого района Большого порта Санкт-Петербурга; 19 января – Клинцовская нефтебаза (г. Клинцы, Брянской области); 3 февраля –«ЛУКОЙЛ-Волгограднефтепереработка» (г. Волгоград); 12 марта – «ЛУКОЙЛ-Нижегороднефтеоргсинтез» (г. Кстово, Нижегородской области; 13 марта – Рязанская нефтеперерабатывающая компания (г. Рязань); 13 марта – Новошахтинский нефтеперерабатывающий завод (Ростовская область); 17 марта – Славянский нефтеперерабатывающий завод (г. Славянск-на-Кубани, Краснодарский край) и другие объекты.

В своей статье Наталия Котляр, заместитель директора по развитию бизнеса НИИ «Вектор» пишет: «По состоянию на конец января 2024 года, по данным из открытых источников, власти регионов сообщали об атаках БПЛА на различные объекты России (без учета территорий, на которых проходит специальная военная операция) более 600 раз. Целями дронов становились, в том числе, предприятия топливно-энергетического комплекса (ТЭК). Так в конце января этого года была предотвращена атака беспилотника на нефтеперерабатывающий завод в Ярославской области». Также 1 сентября 2024 года одной из целей атаки украинских БВС стал Московский нефтеперерабатывающий завод. В результате данных террористических актов с применением БВС объекты получили различного рода повреждения, возникли пожары [2].

Можно сделать вывод, что угроза атаки на объекты ТЭК, юридически можно назвать актом незаконного вмешательства (далее – АНВ), с использованием БВС, стала реальна, что требует соответствующих мер противодействия.

Несомненно, БВС являются одним из самых современных достижений в военной технике. Они представляют собой автономные устройства, управляемые дистанционно, что позволяет значительно снизить риск для лица, его применяющего и увеличить их возможности в боевых условиях.

В соответствии с федеральным законом от 4 августа 2023 г. № 440-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» определен перечень органов и организаций, наделенных правом пресекать функционирование не только беспилотных воздушных судов, но и подводных и надводных судов и аппаратов, беспилотных транспортных средств и иных автоматизированных беспилотных комплексов, в том числе посредством подавления или преобразования сигналов дистанционного управления беспилотными аппаратами, воздействия на их пульты управления, а также повреждения или уничтожения беспилотных аппаратов, в целях защиты собственных объектов, сил, средств и информации или охраняемых объектов по договорам [3]. К этим органам и организациям относятся: подразделения правоохранительных органов, органов безопасности, ведомственной охраны и частные охранные предприятия, которые осуществляют охрану объектов с высокими требованиями к антитеррористической защищенности. Однако, безопасность более 80% объектов ТЭК обеспечивали частные охранные организации, которые не

имели таких полномочий.

Федеральный закон от 25 декабря 2023 года № 666 «О внесении изменений в статью 12 Закона Российской Федерации «О частной детективной и охранной деятельности в Российской Федерации» и Федеральный закон «О безопасности объектов топливно-энергетического комплекса» наделил сотрудников частных охранных предприятий правом пресекать нахождение БВС вблизи объектов ТЭК путем их уничтожения, повреждения, подавления или преобразования сигналов дистанционного управления БВС [4-5]. Также с сентября 2024 года правом пресекать работу БВС в целях защиты объектов транспортной инфраструктуры наделяются подразделения транспортной безопасности. Таким образом сотрудники частных охранных организации с января 2024 года могут легитимно принимать меры к противодействию БВС на охраняемой территории, в том числе зонах безопасности объектов ТЭК.

Постановление Правительства РФ от 10 ноября 2020 года № 1809 (ред. от 20 июня 2024 года) «Об обеспечении особого режима защиты от актов незаконного вмешательства в зонах безопасности объектов топливно-энергетического комплекса, включенных в перечень отдельных объектов топливно-энергетического комплекса, вокруг которых устанавливаются зоны безопасности объектов топливно-энергетического комплекса с описанием местоположения границ таких зон» (вместе с «Правилами обеспечения особого режима защиты от актов незаконного вмешательства в зонах безопасности объектов топливно-энергетического комплекса, включенных в перечень отдельных объектов топливно-энергетического комплекса, вокруг которых устанавливаются зоны безопасности объектов топливно-энергетического комплекса с описанием местоположения границ таких зон») Этот документ определяет меры по обеспечению особого режима защиты от актов незаконного вмешательства в зонах безопасности объектов ТЭК, включенных в перечень отдельных, наиболее значимых, объектов топливно-энергетического комплекса. Однако, ряд положений применимо и к остальным объектам ТЭК.

Угрозы, связанные с применением БВС, объектам ТЭК, как объектам особо важным, повышенной опасности, условно можно разделить на 2 группы [6, 7]:

– угрозы безопасности зданий и сооружений, а также жизни и здоровья сотрудников, при применении БВС (ударных и FPV-дронов (First Person View);

– потеря сведений, составляющих государственную или иную охраняемую законом тайну, выявление постов и маршрутов патрулирования, выявление другой информации об охраняемом объекте с применением разведывательных БВС.

Для противодействия возможным АНВ с применением БВС не обходима разработка и внедрение комплексных систем защиты объектов ТЭК, с учетом особенностей конструкций и производственных процессов, расположения критических элементов объекта ТЭК. Данные системы обычно включают в себя как технические, так и организационные меры противодействия БВС. На

практике необходимо решить задачи обнаружения, сопровождения, перехвата управления и уничтожения (при необходимости).

Среди технических решений можно выделить внедрение радиолокационных систем и систем подавления сигналов управления БВС, а также создание специализированных средств физического уничтожения или захвата БВС [6, 7].

К таким решениям на рынке можно отнести: мобильную станцию технических средств охраны от беспилотных воздушных судов «ЭВЕНК», подавитель дронов «GroZZa», мобильную систему обнаружения БВС «Н1С», «1С» стационарное оборудование обнаружения и позиционирования БВС, радар-детектор «Skyeye» для обнаружения БВС, комплекс обнаружения БВС «РАДЕСКАН-АНТИДРОН», мобильный многофункциональный комплекс противодействия БВС «Сапсан-Бекас» и другие. Применение антидроновых ружий на объектах ТЭК, крайне неэффективно из-за сложности обнаружения (позднее время обнаружения), наведения, малой дальности и низкой селективности. Они могут применяться как дополнительное средство противодействия небольшим БВС (дронам).

Для наибольшей эффективности противодействия АНВ с использованием БВС целесообразно объединять эти системы в единый комплекс способный решать задачи обнаружения, сопровождения, перехвата управления и уничтожения БВС системно на основе одной интеграционной платформы.

Для обеспечения безопасности критических элементов объекта ТЭК помимо технических решений можно рекомендовать использовать инженерные средства защиты, показавших свою эффективность в зоне специальной военной операции. Например, использование защитных сетей реальных критических элементов объекта, а также, в некоторых случаях, сооружение муляжей этих элементов.

Новым вызовом для объектов ТЭК является групповое применение БВС, когда нападение осуществляется группой при четком распределении ролей в ней (разведчик, ударный БВС и другие). Однако, российские научно-исследовательские институты, научно-производственные объединения компаний разработчиков работают над решением задачи противодействия группе БВС в специальных условиях. К ним можно отнести: научно-технический центр радиоэлектронной борьбы, научно-исследовательский институт «Вектор», концерн ВКО «Алмаз-Антей», государственная корпорация «Ростех» и другие. На сегодняшний день есть разработки, они прошли апробацию, и применяются на многих объектах особой важности, повышенной опасности, в том числе объектах ТЭК, например, мобильный комплекс противодействия БПЛА «Защита» и «Серп-ВС6».

Защита объекта ТЭК должна строиться на основе взвешенной достаточности предполагающей оценку возможных последствий при успешной реализации АНВ, с применением БВС, и выбора конкретных адекватных мер защиты. При обеспечении безопасности стратегически важных для Российской Федерации объектов необходимо применять

эшелонированную защиту, которая предполагает создание многорубежной системы физической защиты объекта ТЭК.

В данной статье рассмотрены особенности обеспечения безопасности объектов ТЭК, даны концептуальные рекомендации по созданию системы физической защиты этих объектов, предложены инженерно-технические решения по защите объекта в целом и его критических элементов от АНВ, совершаемых с применением беспилотных воздушных судов.

ЛИТЕРАТУРА

1. Пимонов В. Безопасность НПЗ – задача комплексная / В. Пимонов // ТЭК России. – 2024. – № 8. [Электронный ресурс]. –URL: https://www.cdu.ru/tek_russia/issue/2024/8/1292.
2. Котляр Н. Как защитить российские НПЗ от атак беспилотников? [Электронный ресурс]. –URL: https://dzen.ru/a/ZcBypr-HhlP14gwa.
3. О внесении изменений в отдельные законодательные акты Российской Федерации : федеральный закон от 04.08.2023 № 440-ФЗ // СПС «КонсультантПлюс» (дата обращения: 28.10.2024).
4. О безопасности объектов топливно-энергетического комплекса : федеральный закон от 21.07.2011 № 256-ФЗ // СПС «КонсультантПлюс» (дата обращения: 28.10.2024).
5. О частной детективной и охранной деятельности в Российской Федерации : закон от 11.03.1992 № 2487-1 // СПС «КонсультантПлюс» (дата обращения: 28.10.2024).
6. Сидоров А. В. Обеспечение безопасности режимных объектов органов внутренних дел с использованием современных технических средств и технологий / А. В. Сидоров // Охрана, безопасность, связь. – 2024. – № 9-1. – С. 137-145.
7. Сидоров, А. В. К вопросу обеспечения безопасности режимных объектов / А. В. Сидоров // Охрана, безопасность, связь. – 2024. – № 9-1. – С. 145-150.

СВЕДЕНИЯ ОБ АВТОРЕ

Сидоров Александр Викторович. Заместитель начальника кафедры радиотехнических систем и комплексов охранного мониторинга. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: asidic@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Sidorov Aleksandr Viktorovich. Deputy Head of the Department of Radio Engineering Systems and Security Monitoring Complexes. Candidate of Engineering Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: asidic@mail.ru.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: безопасность; объект топливно-энергетического комплекса; беспилотное воздушное судно; акт незаконного вмешательства; меры противодействия; технический комплекс.

Key words: security, fuel and energy complex facility; unmanned aircraft; act of illegal interference; counteraction measures; technical complex.

УДК 699.81:654.924

Тараненко Дмитрий Анатольевич;
Гречаный Сергей Анатольевич,
кандидат технических наук, доцент;
Калков Дмитрий Юрьевич,
кандидат технических наук

ОХРАННАЯ СИГНАЛИЗАЦИЯ «АЛЬТОНИКА». ПРЕИМУЩЕСТВА, ФУНКЦИИ

SECURITY ALARM SYSTEM «ALTONICA». ADVANTAGES, FUNCTIONS

В статье представлены современные радиоканальные охранные системы, разрабатываемые компанией «Альтоника». Отражены их особенности эксплуатации, преимущества и недостатки.

This article presents modern radio channel security systems developed by Altonica. Their operational features, advantages and disadvantages are reflected.

Российская компания «Альтоника» – научно-производственное предприятие, специализирующееся на разработке и производстве радиоканальных комплексов безопасности. В активе имеет более пятисот изобретений. Система контроля качества соответствует мировым стандартам, что обеспечивает производство продукции высочайшего качества [1].

Охранная сигнализация «Альтоника» конфигурируется из сотни модулей, что позволяет решить весь спектр задач безопасности. Наличие

широкой номенклатуры изделий обеспечивает на их базе построение комплекса охранной сигнализации практически любой сложности.

Изготовляемое оборудование эффективно при охране объектов, распределенных на большой площади. Модели передатчиков обеспечивают трансляцию тревожной информации на расстояние до 50 км без ретрансляторов.

Центральная панель управления охранной сигнализации «Альтоника» дает возможность создать единый пульт централизованного контроля над большим количеством объектов. Допустимость перепрограммирования передатчиков и приемников позволяет работать с уже установленными системами охраны. Радиоканальная аппаратура адресная, точно определяет местонахождение тревожного события. Имеется возможность настройки приемо-передатчиков через эфир. Не требуется разрешение на использование радиоканалов.

По новым требованиям безопасности, сообщение о пожаре необходимо передавать непосредственно в пожарную службу, минуя посредников, с чем сигнализация «Альтоника» успешно справляется [2].

Набор модулей разработан на фиксированные радиусы действия: до 400 м, 800 м, 5, 10, 25 и 50 км. Такая дифференциация обеспечивает оптимальный выбор с точки зрения цены и технических характеристик.

К недостаткам комплекса можно отнести относительно высокую стоимость оборудования, сложность настройки для неподготовленного пользователя.

Системы охраны на базе оборудования «Альтоники» могут работать в различных условиях, но наилучшая эффективность от внедрения комплекса получается на удаленных и распределенных по большой территории объектах. Это могут быть гаражи, необслуживаемые узлы связи, дачи или коттеджный поселок, складские помещения, логистические центры, спортивные сооружения.

Установка радиоканального оборудования производится в тех местах, где невозможно или нецелесообразно подключить аналоговые телефонные линии связи. Получается значительная экономия средств по сравнению с проводными комплексами безопасности. Также существуют специальные модули, которые используются как противоугонное средство на автомобилях.

Компания производит тревожные кнопки и браслеты, обеспечивающие оповещение и охрану персонала, работающего на опасных производствах, используются правоохранительными органами и спецслужбами.

Основу комплекса охранной сигнализации «Альтоника» составляют приемники, передатчики, пульты-программаторы, радиокнопки и антенны.

Приемо-передатчики выполняют контрольную функцию, распространяют данные по радиоканалу, устанавливаются на всех охраняемых объектах. Самый простой вариант исполнения обеспечивает контроль состояния четырех шлейфов: пожар, дверь, вызов или периметр.

Для постановки под охрану нужно замкнуть вход «Взят/снят». Устройства, обслуживающие пять шлейфов, позволяют использовать ключи Touch Memory.

Имеются переносные принимающие устройства со звуковым оповещением, которые обеспечивают прием сигнала тревоги, если он находится в радиусе действия передатчика.

Для удаленной передачи данных необходима установка выносных антенн. Передатчики обеспечивают надежную передачу информации на расстояние до 2 км. Большой набор модулей позволяет создавать систему безопасности сложной конфигурации.

В зависимости от модели и применяемых антенн тревожный сигнал передается на расстояние от 400 метров до 50 километров. Некоторые модели имеют возможность передачи информации и команд управления через интерфейсы USB или RS-485, RS-232.

Приемо-передатчики «Альтоника» имеют стандартные разъемы для подключения питания или информационных кабелей для соединения с компьютером.

Специфика появляется при программировании отдельных блоков системы. Каждый модуль имеет свою инструкцию по монтажу и наладке, требует определенного уровня подготовки специалиста.

Настройка прибора может производиться без отключения питания. В режим настройки параметров можно войти только при снятии всех шлейфов с охраны. Программирование рабочих частот производится при снятом джампере на плате, который нужно поставить на место после выбора диапазона.

В процессе работы комплекс можно быстро перепрограммировать, добавляя или перемещая мобильные датчики и радиокнопки. В условиях плотной городской застройки рекомендуется использовать выносные антенны кругового или направленного действия.

Для создания сложных систем безопасности применяются модули расширения, обеспечивающие проводное соединение модулей системы. Расширители имеют выходы типа «сухой контакт», «открытый коллектор». Они имеют 10 выходов, с помощью которых осуществляется управление таким оборудованием, как ворота, видеокамеры, освещение и т.п. Релейные выходы способны управлять токами до 2 ампер.

Компанией «Альтоника» также разрабатывается мощная радиоканальная система «БазАльт», которая обеспечивает контроль и управление охранно-пожарными комплексами, расположенными на большом удалении на разнородных объектах.

Среди достоинств данного охранного комплекса можно выделить:

– дальность передачи тревожных сообщений без использования ретрансляторов до 50 км;
– большая информационная емкость комплекса;
– высокая помехозащищенность;
– двусторонний канал связи;
– возможность обслуживания 8192 каналов связи.

Комплекс «БазАльт» работает на лицензируемых частотах в диапазоне 420-475 МГц или 146-174 МГц, разрешенном на 433 МГц и мощности 10 мВт. Время прохождения сигнала тревоги 5 секунд.

Таким образом, можно сделать вывод, что радиоканальные системы безопасности представляют собой эффективное и удобное решение для обеспечения безопасности объектов различного назначения. Они позволяют организовать круглосуточное наблюдение и охрану территории, оперативно реагировать на чрезвычайные ситуации и предотвращать возможные угрозы.

ЛИТЕРАТУРА

1. Альтоника: системы безопасности [Электронный ресурс] / URL: http://www.altonika-sb.ru/ (дата обращения: 20.11.2024).
2. ГОСТ Р 52551-2016. Системы охраны и безопасности. Термины и определения : национальный стандарт Российской Федерации / Федеральное агентство по техническому регулированию. – Изд. Официальное. – Москва : Стандартинформ, 2016. – 28 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Тараненко Дмитрий Анатольевич. Коммерческий директор.
ООО «Альтоника СБ».
E-mail: taranenko@altonika.ru
Россия, 115230, г. Москва, Электролитный пр-д, 3, стр. 3.

Гречаный Сергей Анатольевич. Начальник кафедры радиотехнических систем и комплексов охранного мониторинга. Кандидат технических наук.
Воронежский институт МВД России.
E-mail: grechan7777@mail.ru.
Россия, 394065, Воронеж, проспект Патриотов, 53.

Калков Дмитрий Юрьевич. Доцент кафедры радиотехнических систем и комплексов охранного мониторинга. Кандидат технических наук.
Воронежский институт МВД России.
E-mail: DmitreyRUS@mail.ru
Россия, 394065, г. Воронеж, пр. Патриотов, 53.

Taranenko Dmitry Anatolyevich. Commercial Director.
Altonica SB LLC.
E-mail: taranenko@altonika.ru
Work address: Russia, 115230, Moscow, Electrolytny prospekt, 3, p. 3.

Grechanyi Sergej Anatol'evich. Chief of department of radio engineering systems and complexes of security monitoring. Candidate of Engineering Sciences
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: grechan7777@mail.ru.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Kalkov Dmitry Yurievich. Associate Professor of the Department of Radio Engineering Systems and Security Monitoring Complexes. Candidate of Technical Sciences.
Voronezh Institute of the Ministry of internal Affairs of Russia.
E-mail: DmitreyRUS@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: охрана; сигнализация; безопасность; радиоканал; Альтоника; Базальт.

Keywords: security; alarm; safe; radio channel; Altonics; Basalt.

УДК 654.94

Толстых Ольга Владимировна,
кандидат технических наук

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТА ОТ УГРОЗЫ БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ

ENSURING THE SAFETY OF THE FACILITY FROM THE THREAT OF UNMANNED AIRCRAFT

В статье представлены основные аспекты, которые могут быть использованы для защиты объекта от угроз, связанных с применением беспилотных воздушных судов.

The article presents the main aspects that can be used to protect an object from threats associated with the use of unmanned aircraft.

В современных условиях обеспечение безопасности объекта от угрозы беспилотных воздушных судов (БВС) является актуальной задачей, где использование дронов становится все более распространенным как в коммерческих, так и в криминальных целях. Это важное направление в сфере безопасности, которое требует комплексного подхода для предотвращения несанкционированного доступа и угроз, связанных с использованием дронов. Так как угроза может исходить как от злоумышленников, так и от случайных действий, необходимо учитывать различные аспекты при обеспечении безопасности объекта. Рассмотрим основные аспекты, которые могут быть использованы для защиты объектов от угроз, связанных с БВС:

1. Оценка угрозы: идентификация рисков (определение потенциальных угроз от БВС, таких как шпионство, прямая атака, доставка контрабанды и т.д.); анализ окружающей среды (оценка местности, особенностей объекта и возможных маршрутов полета БВС).

2. Технические меры безопасности: системы радиочастотного контроля (использование радиомониторинга для обнаружения сигналов управления БВС); применение средств, которые блокируют радиосигналы, используемые для управления дронами; механические барьеры (установка физической защиты, такой как сетки или заборы, которые могут предотвратить доступ дронов к определенной территории); использование технологических средств, таких как радары и инфракрасные датчики, для обнаружения и отслеживания дронов.

3. Специальные технологии и оборудование: системы активной защиты (использование направленных средств для нейтрализации дронов); дроны-перехватчики (разработка и использование специальных дронов, способных перехватывать и выводить из строя угрожающие БВС); системы визуального наблюдения (мониторинг объекта с помощью камер и других оптических систем, что может помочь в обнаружении дронов на ранней стадии).

4. Правовые аспекты: регулирование использования дронов (изучение и внедрение законодательных норм, касающихся использования БВС. Необходимость в создании зон, где БВС запрещены); сотрудничество с правоохранительными органами (установление эффективных каналов взаимодействия между организациями и правоохранительными органами для реагирования на инциденты).

5. Обучение и подготовка персонала: тренинг сотрудников (обучение сотрудников особенностям работы с системами безопасности и действиям в случае угрозы); симуляция инцидентов (проведение учений для отработки сценариев реагирования на атаки БВС).

6. Мониторинг и оценка эффективности: постоянный анализ угроз (регулярное обновление и переоценка системы безопасности, учитывая новые технологии и тактики использования дронов); отзывы и предложения от сотрудников (сбор информации от персонала для улучшения систем безопасности объектов).

Обеспечение безопасности объекта от угрозы БВС требует комплексного подхода, включающего технические решения, правовое регулирование и подготовку персонала. Соединение различных методов, технологий и сотрудничество с правоохранительными органами создают многоуровневую систему защиты, способную реагировать на быстро меняющиеся угрозы.

ЛИТЕРАТУРА

1. Ворона В.А. Концептуальные основы создания и применения системы защиты объектов: учебное пособие / В.А. Ворона, В.А. Тихонов. – М. : Горячая линия-Телеком, 2017. – 196 с.

2. Толстых О.В. Управление системой защиты объекта / О.В. Толстых, Д.С. Толстых // Сборник статей конференции «Охрана, безопасность, связь-2019». Воронежский институт МВД России, 2020. Т1.№5(1). – С. 146 – 149.

3. URL:http://www.consultant.ru – Официальный сайт компании «КонсультантПлюс».

4. URL:http://www.garant.ru/ – Информационно-правовое обеспечение Гарант.

5. URL:http://www.pravo.gov.ru – Официальный интернет-портал правовой информации.

СВЕДЕНИЯ ОБ АВТОРЕ

Толстых Ольга Владимировна. Доцент кафедры радиотехнических систем и комплексов охранного мониторинга Воронежского института МВД России, кандидат технических наук.

E-mail: tov48@mail.ru

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

Tolstykh Olga Vladimirovna. Associate Professor of the Department of Radio Engineering Systems and Security Monitoring Complexes of the Voronezh Institute of the Ministry of Internal Affairs of Russia, candidate of technical sciences.
E-mail: tov48@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: беспилотное воздушное судно; угроза безопасности; объект.

Key words: unmanned aircraft; security threat; object.

УДК 342; 623.746

Черкашин Ярослав Валериевич

ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА

LEGAL BASIS FOR ENSURING ANTI-TERRORIST PROTECTION OF FUEL AND ENERGY COMPLEX FACILITIES

В статье рассмотрен вопрос правовых основ обеспечения антитеррористической защищенности объектов топливно-энергетического комплекса. Приведены ключевые аспекты данного вопроса.

This article examines the issue of the legal basis for ensuring the anti-terrorist protection of fuel and energy complex facilities. The key aspects of this issue are presented.

Объекты топливно-энергетического комплекса (ТЭК) играют ключевую роль в экономике и обеспечении энергетической безопасности страны. В условиях растущих угроз, связанных с терроризмом и другими актами незаконного вмешательства, обеспечение антитеррористической защищенности этих объектов становится приоритетной задачей. Данная статья рассматривает правовые основы, регулирующие антитеррористическую защищенность объектов ТЭК в Российской Федерации. Рассмотрим ключевые аспекты данного вопроса.

Нормативно-правовая база:

1. Федеральный закон № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса».

Основным документом, регулирующим вопросы безопасности объектов ТЭК, является Федеральный закон от 21 июля 2011 года № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса». Этот закон устанавливает организационные и правовые основы для обеспечения безопасности объектов ТЭК, включая антитеррористическую защищенность. Основные положения закона включают:

- определение понятий «акт незаконного вмешательства» и «антитеррористическая защищенность объекта ТЭК».
- установление категорий опасности объектов ТЭК (высокая, средняя, низкая) и соответствующих требований к их защите.
- обязанности владельцев объектов по соблюдению установленных требований безопасности и составлению паспортов безопасности3.

2. Уголовный кодекс Российской Федерации.

Согласно изменениям, внесенным в Уголовный кодекс РФ, предусмотрены уголовные наказания за нарушение требований безопасности объектов ТЭК. Статья 217.1 УК РФ устанавливает ответственность за:

- нарушение требований, приведшее к причинению тяжкого вреда здоровью или ущерба в крупном размере.
- смерть человека или людей в результате таких нарушений.

3. Кодекс Российской Федерации об административных правонарушениях.

Статья 20.30 Кодекса Российской Федерации об административных правонарушениях (КоАП РФ) устанавливает ответственность за нарушение требований обеспечения безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса (ТЭК).

Статья 20.30 КоАП РФ охватывает следующие ключевые аспекты:

1. Объект правонарушения: Статья применяется к объектам ТЭК, включая электроэнергетику, нефтяную, газовую и угольную промышленности, а также объекты теплоснабжения и газоснабжения.

2. Категории опасности объектов: правонарушения классифицируются в зависимости от категории опасности объекта:

- низкая категория опасности: штрафы для граждан составляют от 3 до 5 тысяч рублей, для должностных лиц — от 30 до 50 тысяч рублей, для юридических лиц — от 50 до 100 тысяч рублей.
- средняя категория опасности: штрафы для граждан составляют от 5 до 10 тысяч рублей, для должностных лиц — от 50 до 70 тысяч рублей, для юридических лиц — от 100 до 300 тысяч рублей.
- высокая категория опасности: штрафы для граждан составляют от 10 до 15 тысяч рублей, для должностных лиц — от 70 до 100 тысяч рублей, для юридических лиц — от 150 до 450 тысяч рублей.

3. Объективная сторона правонарушения: правонарушение включает в себя как действия, так и бездействие, которые не содержат признаков уголовно наказуемого деяния.

4. Субъекты правонарушения: ответственность несут как граждане, так и должностные лица, включая руководителей субъектов ТЭК.

Законодательство выделяет несколько ключевых принципов, на которых основывается система антитеррористической защищенности объектов ТЭК:

- законность: все действия по обеспечению безопасности должны соответствовать действующему законодательству.

- комплексный подход: необходимость интеграции различных мер безопасности (физическая защита, информационная безопасность и т.д.) для создания эффективной системы защиты.

- ответственность: четкое распределение ответственности между государственными органами, владельцами объектов и другими заинтересованными сторонами.

Объекты ТЭК подлежат категорированию в зависимости от их потенциальной опасности. Это позволяет установить дифференцированные требования к их защите. Процесс категорирования осуществляется комиссией в соответствии с установленными правилами.

Каждый объект ТЭК должен иметь паспорт безопасности, который включает информацию о его характеристиках, категории опасности и мерах по обеспечению антитеррористической защищенности. Паспорт утверждается руководителем субъекта ТЭК после согласования с уполномоченными органами.

Правовые основы антитеррористической защищенности объектов топливно-энергетического комплекса в России формируются на основе комплексного подхода, включающего законодательные акты, организационные меры и принципы обеспечения безопасности. Эффективная реализация этих основ требует взаимодействия всех заинтересованных сторон и постоянного обновления механизмов защиты в ответ на новые вызовы и угрозы. Только при условии строгого соблюдения законодательства можно обеспечить надежную защиту критически важных объектов ТЭК от террористических актов и других форм незаконного вмешательства.

Обеспечение безопасности объектов топливно-энергетического комплекса (ТЭК) является одной из ключевых задач для поддержания стабильности и устойчивости экономики страны. В результате анализа можно выделить несколько основных выводов.

Стратегическая важность: Объекты ТЭК играют критическую роль в обеспечении энергетической безопасности государства, и их защита от угроз является приоритетной задачей.

Комплексный подход: Эффективная система безопасности должна включать в себя не только физическую защиту, но и правовое регулирование, информационную безопасность, а также подготовку и обучение персонала.

Категорирование объектов: Необходимость категорирования объектов по степени опасности позволяет адекватно оценивать риски и разрабатывать соответствующие меры защиты, что способствует более эффективному распределению ресурсов.

Адаптация к новым угрозам: в условиях быстро меняющейся геополитической ситуации и технологического прогресса необходимо постоянно обновлять методы и подходы к обеспечению безопасности, включая использование современных технологий и инновационных решений.

Сотрудничество с правоохранительными органами: Эффективное взаимодействие с правоохранительными структурами, а также обмен информацией о потенциальных угрозах являются важными аспектами в системе обеспечения безопасности ТЭК.

Общественное сознание: Повышение уровня осведомленности общества о важности безопасности объектов ТЭК может способствовать созданию более безопасной среды и вовлечению граждан в процессы обеспечения безопасности.

Инвестиции в безопасность: Необходимость инвестирования в современные технологии и инфраструктуру для повышения уровня защиты объектов ТЭК является важным условием для успешного функционирования сектора.

В целом обеспечение безопасности топливно-энергетического комплекса требует системного подхода, активного участия всех заинтересованных сторон и постоянного совершенствования существующих механизмов защиты. Это позволит минимизировать риски и обеспечить надежное функционирование энергетической инфраструктуры страны.

Обеспечение безопасности объектов топливно-энергетического комплекса России от угроз, связанных с использованием беспилотных летательных аппаратов (БПЛА), представляет собой актуальную задачу в условиях нарастающей вероятности атак на критически важные инфраструктурные объекты. В связи с увеличением числа инцидентов, связанных с использованием дронов, необходимо разработать и внедрить комплексные меры защиты, включая как технические, так и организационные аспекты.

Технические решения должны включать в себя системы радиолокационного контроля и радиоэлектронной борьбы, которые позволят своевременно обнаруживать и нейтрализовать угрозы БПЛА. Использование радиолокационных станций в сочетании с средствами РЭБ обеспечит создание сплошного радиолокационного поля вокруг объектов ТЭК, что позволит оперативно реагировать на приближающие дроны. Дополнительно, применение конструкций типа АНТиДРОН может значительно снизить риски, связанные с возможными атаками, создавая физические барьеры для дронов.

Организационные меры должны основываться на действующем законодательстве, в частности на Федеральном законе № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса». Этот закон определяет основные принципы обеспечения безопасности и устанавливает обязательства для владельцев объектов ТЭК по защите своих активов от актов незаконного вмешательства. Важно также учитывать необходимость

подготовки специалистов в области безопасности, что позволит обеспечить высокую степень готовности к реагированию на потенциальные угрозы.

Интеграция современных технологий защиты и строгое соблюдение законодательных норм являются ключевыми факторами для повышения уровня безопасности объектов ТЭК от угроз со стороны дронов. Эффективная защита этих объектов не только способствует сохранению их функциональности, но и защищает интересы общества и государства в целом.

Несмотря на наличие законодательной базы, существует ряд проблем, связанных с реализацией требований по антитеррористической защищенности. Некоторые эксперты указывают на избыточность некоторых требований и недостаточную адаптацию законодательства к современным угрозам. Важно также учитывать специфику каждого объекта ТЭК, что требует индивидуального подхода к обеспечению безопасности.

В заключение, правовые основы обеспечения антитеррористической защищенности объектов ТЭК в России представляют собой комплексный механизм, который требует постоянного обновления и адаптации к меняющимся условиям безопасности.

ЛИТЕРАТУРА

1. Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 09.11.2024);
2. Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ (ред. от 09.11.2024, с изм. от 12.11.2024);
3. Федеральный закон от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса»;
4. Постановление Правительства Российской Федерации от 22 декабря 2011 г. № 1107 «О порядке формирования и ведения реестра объектов топливно-энергетического комплекса»;
5. Постановление Правительства Российской Федерации от 5 мая 2012 г. № 459 «Об утверждении Положения об исходных данных для проведения категорирования объекта топливно-энергетического комплекса, порядке его проведения и критериях категорирования»;
6. Постановление Правительства Российской Федерации от 5 мая 2012 г. № 460 «Об утверждении Правил актуализации паспорта безопасности объекта топливно-энергетического комплекса»;
7. Постановление Правительства Российской Федерации от 2 октября 2013 г. № 861 «Об утверждении Правил информирования субъектами топливно-энергетического комплекса об угрозах совершения и о совершении актов незаконного вмешательства на объектах топливно-энергетического комплекса»;
8. Постановление Правительства Российской Федерации от 8 декабря 2022 г. № 2258 «Об утверждении специальных требований к частным охранным организациям, которые вправе осуществлять физическую защиту

объектов топливно-энергетического комплекса в соответствии с пунктами 2 и 3 части 4 статьи 9 Федерального закона»;

9. Приказ Росгвардии от 23 ноября 2023 № 420 «Об утверждении типовых форм документов, необходимых при осуществлении Федеральной службой войск национальной гвардии Российской Федерации и ее территориальными органами федерального государственного контроля (надзора) за обеспечением безопасности объектов топливно-энергетического комплекса, которым присвоена категория опасности»

10. Приказ Министерства энергетики РФ от 10 февраля 2012 г. № 48 «Об утверждении методических рекомендаций по включению объектов топливно-энергетического комплекса в перечень объектов, подлежащих категорированию».

СВЕДЕНИЯ ОБ АВТОРЕ

Черкашин Ярослав Валериевич. Начальник кабинета специальных дисциплин кафедры радиотехнических систем и комплексов охранного мониторинга.

Воронежский институт МВД России.

E-mail: yaroslav-cherkashin@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Cherkashin Yaroslav Valerievich. Head of the Cabinet of Special Disciplines of the Department of Radio Engineering Systems and Security Monitoring Complexes.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: yaroslav-cherkashin@mail.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: антитеррористическая защищенность; объекты топливно-энергетического комплекса; паспорт безопасности; правовые основы.

Key words: anti-terrorist security; facilities of the fuel and energy complex; safety data sheet, legal framework.

УДК 343.791

Янгиров Адиль Илдарович;
Янгиров Илдар Мухаматович;
Ахлюстин Сергей Борисович
кандидат технических наук;
Садчикова Наталия Александровна

СОВРЕМЕННЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ НАДЕЖНОЙ ОХРАНЫ ОБЪЕКТОВ В ОСОБЫХ КЛИМАТИЧЕСКИХ УСЛОВИЯХ

MODERN TECHNICAL SOLUTIONS TO ENSURE RELIABLE PROTECTION OF FACILITIES IN SPECIAL CLIMATIC CONDITIONS

В статье рассматриваются современные технические решения для обеспечения надежной охраны объектов в особых климатических условиях. Применение представленных в статье решений может повысить надежность работы технических средств в неблагоприятных условиях.

The article discusses modern technical solutions to ensure reliable protection of facilities in special climatic conditions. The use of the solutions presented in the article can increase the reliability of technical means in adverse conditions.

Для обеспечения бесперебойной работы многих видов технических средств, оборудования и поддержания оптимального электропитания требуются определенные температурные условия и защита от внешних климатических воздействий. Оборудование климатической защиты – это все, что защищает технические средства от атмосферной влаги и опасных температурных факторов: от монтажных коробок с определенной степенью защиты до магистральных термошкафов любых типов и размеров [1].

При рассмотрении вариантов защиты технических средств от внешних воздействующих факторов надо учитывать:

1) климатические условия эксплуатации и место (категорию) размещения в соответствии с 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» [2];

2) степень защиты, обеспечиваемой оболочками, от проникновения твердых предметов и воды – код IP по ГОСТ 14254–2015 «Степени защиты, обеспечиваемые оболочками (Код IP)» [3];

3) необходимость защиты от коррозии и выпадения конденсата и попадания влаги, запуска оборудования при отрицательных температурах – «холодный старт»;

4) механизмы или режимы, обеспечивающие удаленное обслуживание, таких как стеклоочиститель, омыватель, вентиляция;

5) требования безопасности к оборудованию, включая электробезопасность и техническое обслуживание.

Так, например, для щитов наружного исполнения предпочтительно применение порошковой полиэфирной краски как более устойчивой в сравнении с эпоксидно-полиэфирными составами. Для эксплуатации в прибрежных районах (морские порты, причалы) следует выбирать оболочки в климатическом исполнении М1 с повышенной до IP65 степенью пылевлагозащиты. Тропическое исполнение корпусов Т1 подходит для районов с влажным тропическим климатом (средний ежегодный абсолютный максимум температуры воздуха выше плюс 40 °С при высокой относительной влажности). В России подобное сочетание факторов встречается на побережье Черного моря. В различных условиях климатических зон Российской Федерации для обеспечения нормальных условий для функционирования технических средств возможно применение следующего специального климатического оборудования и устройств, предназначенных для минимизации негативных внешних воздействующих климатических факторов:

1) шкафы герметичные;

2) всепогодные термошкафы (термобоксы);

3) кабели в специальном климатическом исполнении;

4) специализированные электрические соединители;

5) другие виды климатического оборудования.

Шкаф герметичный используется для обеспечения защиты электрооборудования от проникновения твердых частиц и/или воды. Его климатическое исполнение предполагает устойчивость к ветру, водонепроницаемость, а также пылезащищенность. Корпуса любых шкафов герметичных – это преимущественно навесные конструкции с оборудованной герметичной дверью, герметичным замком, а также специальным козырьком, защищающим фасад конструкции от осадков (опционально). Антикоррозийные свойства и устойчивость к механическим повреждениям металлическому коробу обеспечивает плотное покрытие порошковой краской снаружи изделия.

Более функциональным дополнительным специальным оборудованием являются всепогодные термошкафы (термобоксы). Пример термошкафа (термобокса) представлен на рисунке 1.

Рис. 1. Внешний вид термошкафа (термобокса)

Их главное предназначение – обеспечить нормальные условия функционирования для размещенного внутри оборудования. Это достигается за счет встроенной системы контроля микроклимата, поддерживающей оптимальные значения влажности и температуры в течение года.

По функциональным характеристикам различают следующие виды термошкафов (термобоксов):

1) без подогрева и охлаждения. Такой термошкаф оберегает от пыли и осадков, снижает степень воздействия температуры воздуха на содержимое. Устройства данного типа применяются в качестве уличных боксов. В основном применяются в климатических зонах без резких температурных перепадов для оборудования, которому не требуется высокая степень защиты;

2) со встроенной системой обогрева. Термошкаф с обогревом и без кондиционирования рассчитан на эксплуатацию в холодном климате. Термодатчик, зафиксировав понижение температуры окружающего воздуха до заданной отметки, подает сигнал на включение нагревательного элемента. Таким образом, оборудование способно сохранять работоспособность при низких температурах;

3) оснащенные системой обогрева и вентиляцией. Термошкаф с вентиляцией и нагревательным элементом позволяет поддерживать температуру внутри камеры в заданных рамках. Вентиляция служит для охлаждения – теплый воздух выходит наружу, его замещает воздух с улицы. Такое охлаждение функционирует при условии, что температура снаружи ниже, чем внутри бокса;

4) оснащенные системами обогрева и кондиционирования. В таком термобоксе поддерживается оптимальный для оборудования микроклимат при любых внешних условиях. Термодатчик включает нагревательный элемент или встроенную систему кондиционирования по мере необходимости.

Этот вариант самый сложный в изготовлении и дорогой в эксплуатации из-за повышенного расхода электроэнергии. Всепогодные термошкафы могут применяться в регионах со сложными климатическими условиями. В зависимости от предназначения и габаритов, термоизолированные защитные

шкафы устанавливают на пол или землю с использованием специальных опор, навешивают на стены, столбы линий электропередачи или ограждений.

Широкая номенклатура типоразмеров термошкафов позволяет размещать в них практически любую современную аппаратуру. При изготовлении предусматривается защита от взлома для обеспечения сохранности установленного внутри оборудования. Для повышения безопасности целесообразно оборудовать термошкаф (термобокс) системой охранной сигнализации. Термошкафы (термобоксы) могут быть изготовлены из различных материалов. Корпус стального термошкафа представляет собой цельносварную конструкцию из листового металла. Стенки, как и навесная дверца, утепляются теплоизоляционными материалами. По периметру дверцы крепится уплотнитель, чтобы в термошкаф не проникла влага и пыль. Антикоррозийная обработка и внешнее защитно-декоративное покрытие, нанесенное по технологии порошкового окрашивания, защищают металл от атмосферных воздействий и продлевают срок службы изделия. Внутри термошкаф оснащается монтажной панелью для крепления устройств. Для некоторых типов оборудования могут быть установлены полки из стального листа с отверстиями для кабелей и циркуляции воздуха.

Полимерный корпус защитного утепленного шкафа представляет собой многослойную конструкцию. Пример термошкафа (термобокса) из полимерных материалов представлен на рисунке 2.

Рис. 2. Термошкаф (термобокс) из полимерных материалов

Внешний и внутренний слой выполнен из материала на основе пожаростойких ненасыщенных полиэфирных смол и армированного стекловолокна для повышения прочности. Средний слой представляет собой теплоизолятор из вспененного полимера – пенополиуретана. Поверхность боксов из стеклопластика антистатична. Материал устойчив ко всем видам внешних воздействий. В корпусе может быть предусмотрено смотровое окно для удобства контроля показаний измерительных устройств.

Если требуется защитить оборудование от несанкционированного доступа, целесообразно применение термошкафов (термобоксов) в антивандальном исполнении. Такой термошкаф изготавливается из более толстого листового металла, оборудуется усиленными петлями и замком наподобие сейфового. В зонах повышенной взрывоопасности используются шкафы во взрывозащищенном исполнении. За счет конструкции корпуса и толщины стенок такие боксы устойчивы к деформации, способны выдержать ударные нагрузки и нагрев до высоких температур.

Антивандальные и взрывозащищенные термобоксы могут относиться к любому типу, иметь или не иметь систему обогрева, охлаждения, кондиционирования. Из-за большей толщины металла такие боксы тяжелее стандартных аналогичного типа и размера, что влияет также на их стоимость.

Крупные производители выпускают термобоксы стандартных типоразмеров для размещения определенных видов оборудования. Этот вариант в основном применяется для решения типовых задач. Небольшие компании предлагают услуги по изготовлению боксов любого типа и размера. В частности, можно выбрать подходящий вариант подогрева термошкафа – электрический нагревательный элемент или подключение к водяной или паровой системе отопления. При выборе устройства или подготовке индивидуального проекта необходимо учитывать тип оборудования, условия эксплуатации, требования к прочности и взломостойкости корпуса. В тяжелых климатических условиях, характеризующимися резкими перепадами и экстремальными показателями температур, на устойчивость работы технических средств охраны и других технических средств может оказывать существенное влияние работоспособность линий передачи данных и электропитания. Анализ технических и эксплуатационных характеристик применяемых кабелей показывает, что в случае падения температуры до минус 50 °С и ниже оболочка и изоляция из поливинилхлоридного пластиката или хлорсульфированного полиэтилена становятся жесткими и хрупкими, так как в условиях низких температур происходит разрушение оболочки в результате растрескивания, что, в конечном итоге, влечет за собой выход кабеля из строя и последующий, зачастую, дорогостоящий ремонт кабельной линии. Это объясняется тем, что вода, находящаяся в порах материала оболочки, при замерзании увеличивается в объеме примерно на 10%, что вызывает давление льда (до 200 МПа) на стенки пор. Для решения этой проблемы специалистами кабельного завода НПП «Спецкабель» (г. Москва) разработаны и начато серийное производство большой группы специальных морозостойких универсальных кабелей категории «ХЛ» общепромышленного применения, изготовленных из материалов, позволяющих им оставаться гибкими даже при низких температурах.

Новая группа морозостойких кабелей, получивших товарный знак «СКАБ» (рисунок 3), позволяет решить проблему эксплуатации кабельно-проводниковой продукции при крайне низких температурах (до минус 70 °С), например, в арктических условиях.

Рис. 3. Внешний вид морозостойкого кабеля «СКАБ»

Кабели морозостойкие групповой прокладки для контрольно-измерительных приборов и аппаратуры исполнение «ХЛ» производятся в оболочке с защитным шлангом из безгалогенного термопластичного полиуретана (исполнение «Унг(А)-FRHF-ХЛ»), обеспечивающего высокую механическую прочность кабеля, стойкость к агрессивным средам и истиранию, эксплуатацию кабелей при температурах до минус 70°С в неподвижном состоянии.

Проведенные испытания показали, что кабели серии «СКАБ» производства НПП «Спецкабель» (г. Москва) могли бы использоваться в сложных арктических условиях для присоединения к стационарным электрическим приборам, аппаратам, сборкам электрических распределительных устройств [4].

Для волоконно-оптических линий связи также имеются готовые решения. Стандартные волоконно-оптические кабели должны допускать прокладку и монтаж при температуре от минус 10 °С до плюс 40 °С. При более низких температурах (но не ниже минус 30 °С) кабель необходимо выдержать в отапливаемом помещении, обеспечить прогрев его на барабане непосредственно перед прокладкой. Температура монтажа волоконно-оптических кабелей для внешней прокладки производства ЗАО «ОФС Связьстрой–1 ВОКК» (г. Самара) составляет от минус 30 до плюс 50 °С – ручным или механизированным способом без предварительного прогрева, а температура эксплуатации допускает диапазон температур от минус 60 до плюс 70 °С. Возможность работы при таких низких температурах определяется технологией изготовления, материалами и конструкцией волоконно-оптических кабелей [5]. Данные температурные значения подтверждаются испытаниями в соответствии с ГОСТ 17491–80 «Кабели, провода и шнуры с резиновой и пластмассовой изоляцией и оболочкой», а также положительной практикой применения. Так, зимой 2011–2012 годов велась прокладка 230 км самонесущего оптического кабеля на участке от города Горно-Алтайска до государственной границы с Монголией. Часть трассы строилась в феврале 2012 года при температуре минус 34 °С. Несмотря на то, что это уже выходит за допустимыми техническими условиями диапазон, все 230 км волоконно-оптических линий связи проложены в срок и успешно эксплуатируются.

Помимо кабелей, важнейшую роль в поддержании надежностных характеристик различных узлов электрооборудования играют электрические соединители, по оценкам специалистов, около 50 % всех отказов вызваны низким качеством разъемов. Как и кабели, соединители подвержены самым жестким и агрессивным внешним воздействиям, характерным для

эксплуатации на земле, на воде и в воздухе. В суровых арктических условиях к ним предъявляются повышенные требования по следующим параметрам:

1) степень защиты от воздействия влаги – уровень IP 67/68;

2) рабочая температура – от минус 65 до плюс 125 °С;

3) количество циклов соединения/размыкания – не менее 500;

4) возможность работы в разных агрессивных средах;

5) выдерживаемая разность давлений.

Кроме того, для обеспечения требований по массогабаритным характеристикам аппаратуры, соединители должны обеспечивать наличие максимального количества одновременно соединяемых (разъединяемых) цепей. Это требование предполагает наличие в одном соединителе большого количества электрических контактов, через которые могут проходить различные токи (от 10 до 50 А и более) при рабочих напряжениях от 1 мВ до 1 кВ. При этом рабочие частоты электрического тока, проходящего через контакты, могут достигать до 100 ГГц.

ЛИТЕРАТУРА

1. Аналитический обзор «Способы организации устойчивой работы систем передачи извещений, применяемых в практической деятельности подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации, в труднодоступных районах со сложными климатическими и географическими условиями», утвержденный начальником ГУВО Росгвардии генерал-лейтенантом полиции А.В. Грищенко 24.11.2022 г.

2. 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».

3. ГОСТ 14254–2015 «Степени защиты, обеспечиваемые оболочками (Код IP)».

4. Лобанов А.В. Кабельная продукция арктического исполнения от научно-производственного предприятия "Спецкабель" // Нефть. Газ. Новации. – 2022. – № 4(257). – С. 83-88.

5. Лопаткина С.В. Инновации для оптической связи // Инновационные технологии производства и хранения материальных ценностей для государственных нужд. – 2015. – № 4(4). – С. 149-153.

СВЕДЕНИЯ ОБ АВТОРАХ

Янгиров Адиль Илдарович. Начальник отделения лабораторных исследований и испытаний.

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

E-mail: Adil-Yan@yandex. ru

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

Янгиров Илдар Мухаматович. Научный сотрудник отдела развития средств обнаружений.

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

E-mail: YIMufa@yandex. ru

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

Ахлюстин Сергей Борисович. Начальник кафедры тактико-специальной подготовки, кандидат технических наук.

Воронежский институт МВД России.

E-mail: cerg7676@yandex.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

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

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

E-mail: nsadchikova6@mail.ru

Yangirov Adil Ildarovich. Head of the Laboratory Research and Testing Department.

Federal State Institution «Scientific Research Center «OKHRANA» of the Federal service of National Guard of the Russian Federation.

Work address: Russia, 111539, Moscow, Reutovskaya, 12B.

Yangirov Ildar Mukhamatovich. Researcher at the Department of Development of Detection Tools.

Federal State Institution «Scientific Research Center «OKHRANA» of the Federal service of National Guard of the Russian Federation.

Work address: Russia, 111539, Moscow, Reutovskaya, 12B.

Ahlyustin Sergey Borisovich. Head of the department of tactical and special training. Candidate of technical sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: cerg7676@yandex.ru

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

Sadchikova Natalia Alexandrovna. Investigator of the specialized department for the investigation of crimes of a general criminal orientation - «remote theft».

Investigative Department of the Department of Internal Affairs for the Southern Administrative District of the Ministry of Internal Affairs of Russia in Moscow.
E-mail: nsadchikova6@mail.ru

Ключевые слова: охрана объектов; особые климатические условия; технические решения.

Key words: protection of facilities; special climatic conditions; technical solutions.

УДК 654

ПРИМЕНЕНИЕ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ РОССИИ И ПЕРСПЕКТИВЫ ИХ РАЗВИТИЯ

Абдуллозода Неъматулло Рахматулло,
кандидат юридических наук

КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ И ИХ РОЛЬ В БОРЬБЕ С ЭКСТРЕМИЗМОМ НА ПРИМЕРЕ РЕСПУБЛИКИ ТАДЖИКИСТАН

COMPUTER TECHNOLOGIES AND THEIR ROLE IN THE FIGHT AGAINST EXTREMISM ON THE EXAMPLE OF THE REPUBLIC OF TAJIKISTAN

В статье исследуется проблема экстремизма в Республике Таджикистан, а также влияние современных информационных технологий на радикализацию общества. Автор аргументирует необходимость комплексного подхода к борьбе с экстремизмом, который включает в себя не только правовые меры и меры по устранению причин, способствующих росту радикальных настроений, но и активное использование информационно-коммуникационных технологий. Приведены примеры использования социальных сетей экстремистами для вербовки молодежи и распространения радикальных идей. Автор также обращает внимание на необходимость разработки современных методов защиты информационного пространства страны, чтобы предотвратить влияние экстремистов на общественное мнение и контекст формирования массовой культуры.

This article examines the problem of extremism in the Republic of Tajikistan, as well as the impact of modern information technologies on the radicalization of

society. The author argues for the need for a comprehensive approach to combating extremism, which includes not only legal measures and measures to eliminate the causes contributing to the growth of radical sentiments, but also the active use of information and communication technologies. Examples of the use of social networks by extremists to recruit young people and spread radical ideas are given. The author also draws attention to the need to develop modern methods of protecting the country's information space in order to prevent the influence of extremists on public opinion and the context of the formation of mass culture.

Как известно, Республика Таджикистан одним из первых государств в постсоветском пространстве столкнулась с проблемой экстремизма. Этот фактор особо выделяется в условиях гражданской войны 1992-1997 гг. Рассматривая эту проблему, сквозь сегодняшние процессы, можно с уверенностью утверждать, что проблема экстремизма тогда не была столь актуальной, как сейчас [5].

Современные геополитические трансформации евразийского пространства, обретение устойчивого характера основных вызовов и угроз безопасности всего центральноазиатского региона побуждает Таджикистан придавать первостепенное внимание вопросам обеспечения безопасности на национальном и региональном уровнях [3, С.573-583].

28 мая 2024 г., выступая на военном параде в честь 30-й годовщины образования Пограничных войск Лидер нации, Президент Республики Таджикистан, уважаемый Эмомали Рахмон заявил, что «…на протяжении более трёх десятилетий Таджикистан находится на переднем крае борьбы с современными глобальными угрозами, включая экстремизм и терроризм, играет ключевую роль в предотвращении распространения этих угроз в регионе и мире» [2].

Возрастающие риски центральноазиатской безопасности и меняющийся характер глобального радикального экстремизма и терроризма в сочетании с деятельностью международных террористических организаций в афганском приграничье, ростом экстремистских организаций, стремящихся дестабилизировать обстановку в центральноазиатских государствах, деятельностью частных военных формирований, распространением религиозного экстремизма, увеличением незаконного оборота наркотических средств и ростом влияния наркомафии, угрозой применения биооружия, деятельностью организованных преступных группировок, экологическими вызовами, с нерешенными этнополитическими проблемами; коррупцией на разных уровнях государственных структур, демографическими проблемами и повышением уровня бедности населения, снижением просвещения населения, сетевыми вызовами, а в конечном итоге с угрозами гибридных войн содействуют укреплению сотрудничества на глобальном и региональном уровнях и реализации политики противодействия на национальном уровне, исходя из понимания, что вышеперечисленные факторы будут снижать темпы реализации национальных стратегий развития и модернизации государств.

Следует отметить, что религиозный экстремизм и религиозные экстремистские группировки в регионе считаются серьезной угрозой безопасности и политической стабильности Таджикистана. По географическому и геополитическому положению Таджикистан находится в регионе, где действуют и всячески укрепляют свои идеологические аппараты особо опасные религиозные экстремистские и террористические группировки [1].

Таджикистан в борьбе с религиозным экстремизмом и международным терроризмом осуществляет комплексный подход: укрепляет правовую базу, принимает превентивные меры по устранению причин терроризма, а также предпринимает меры по защите основополагающих ценностей общества, учитывая государственные задачи по устранению локальных вызовов, способствующих росту экстремизма [3, С.573-583].

В период независимости Таджикистана была реализована «Национальня стратегия Республики Таджикистан по противодействию экстремизму и терроризму на 2016-2020 годы» и с учетом её реализации 1 июня 2021 года в Таджикистане принята новая «Стратегия противодействия экстремизму и терроризму в Республике Таджикистан на 2021–2025 годы и План действий по реализации Стратегии противодействия экстремизму и терроризму в Республике Таджикистан на 2021-2025 годы, в которых определены цели, задачи и основные направления государственной политики Республики Таджикистан по противодействию экстремизму и терроризму, а также коллективные усилия государства и гражданского общества [3, С.573-583].

При этом одной из внешних угроз считается воздействие на информационную среду с целью формирования и навязывания общественного мнения извне.

В век информационных технологий нам никак не пройти мимо них, именно они сейчас играют ключевую роль в каждой человеческой сфере жизни.

Компьютерные технологии (далее – КТ) включают в себя использование информационных технологий, сетей, программного обеспечения и других устройств для сбора, хранения, обработки, передачи и анализа данных. КТ охватывают широкий спектр технологий, включая разработку программного обеспечения, облачные вычисления, базы данных, сети, кибербезопасность, искусственный интеллект, интернет вещей и многое другое.

Ризоён Ш.Ш. отмечает, что анализ событий «арабской весны» показывает, что превосходство внешних информационных ресурсов над национальными информационными источниками приводит к пагубным последствиям, связанными с демотивацией и быстрыми темпами самоотчуждения населения, которое приводит к радикализации общества и активизации экстремистских течений. Другим немаловажным моментом можно назвать экспорт нетрадиционных религиозных учений из различных регионов исламского мира, которые с учетом переходного периода, а также религиозной неграмотности населения находят своих сторонников [5].

С усилением информационного общества, средства массовой информации (далее – СМИ) и информационно-коммуникационные технологии (далее – ИКТ) играют важную роль в процессе формирования общественного мнения и переориентации граждан к различным идеям. СМИ и ИКТ являются мощными инструментами «промывки мозгов», которые могут заметно повлиять и перенаправить потенциальных потребителей на нужное направление. Анализ показывает, что средства массовой информации и информационно-коммуникационные технологии, особенно социальные сети, широко используются со стороны экстремистских групп для распространения своих идей [5].

Рахими Ф.К. отмечает, что нынешнее поколение террористов и экстремистов, используя современные достижения ИКТ по заказу своих покровителей, продолжают совершать террор и убийство мирного населения планеты [4].

Так, экстремисты-вербовщики используют социальные сети и мессенджеры, такие как Facebook, Одноклассники, Телеграмм, Mail.ru, Twitter, YouTube и др. для вербовки молодежи в экстремистские группировки, а также для пропаганды таких групп [6, С. 57-58].

Результаты исследований показывают, что причины привлечения граждан (некоторые из них противоположны друг к другу) основываются на следующих факторах:

- отсутствие постоянной работы;
- отсутствие религиозного образования;
- проблемы с «социализацией»;
- жизнь в трудных условиях (отсутствие возможности для развития);
- «промывка мозгов» и попадание под влияние негативного (радикального) мировоззрения;
- люди из «проблемных» и «неполных» семей, и т.д.

Изучение отдельных примеров показывает, что молодежь, которая вступила в террористические группы, имела хорошие возможности для развития и социализации, например:

- люди из обеспеченных семей: эксперты их относят к «среднему классу», из семьи предпринимателей, представителей интеллигенции (учителей, врачей и т.д.);
- с религиозным образованием или с семьи местных религиозных деятелей;
- «успешные люди», которые занимались предпринимательством (бизнесом), т.е. имели свое дело, и воспитывали детей, отправляли родителей в хадж и т.д. [5].

Таким образом, подводя итог вышесказанному, следует отметить, что информационные технологии играют важную роль в руках экстремистов-вербовщиков. С целью минимизации возможности использования информационных технологий экстремистами, необходимо применять современные степени защиты, блокирование IP-адресов, сервера сайтов

с которых происходит вещание в глобальной сети интернет запрещенной информации, а также улучшать степень защиты сайтов, которые используются в качестве информационной подложки социальных сетей.

Лишив экстремистов информационного пространства, можно уменьшить их влияние на общество и население Республики Таджикистан в целом.

ЛИТЕРАТУРА

1. Борьба с религиозным экстремизмом и обеспечение политической стабильности общества. Электронный ресурс:URL: https://rtsu.tj/news/?ELEMENT_CODE=1649

2. Выступление Президента Республики Таджикистан Эмомали Рахмона на военном параде в честь 30-й годовщины образования Пограничных войск 28.05.2024. URL: http://www.president.tj/ru/node/33529 (дата обращения 29.05.2024).

3. Майтдинова Г. М. Реализация Стратегии противодействия экстремизму и терроризму в Республике Таджикистан на 2021–2025 года: права человека и верховенство закона /Г. М. Майтдинова/ Постсоветские исследования. Т.5. № 6 (2022). С.573-583.

4. Рахими Ф.К. Проблемы борьбы с религиозным экстремизмом и международным терроризмом в выступлениях и посланиях Президента Республики Таджикистан уважаемого Эмомали Рахмона. Республиканская научно – теоретическая конференция на тему Позиция Республики Таджикистан в противодействии религиозному экстремизму и международному терроризму. Электронный ресурс:URL: https://ifppanrt.tj/tj/ilm-va-navidho/(дата обращения 29 октября 2024)

5. Ризоён Ш. Ш. Опыт Таджикистана в профилактике экстремизма: проблемы и перспективы. Электронный ресурс:URL: http://berlek-nkp.com/tadzhikistan/7932-opyt-tadzhikistana-v-profilaktike-ekstremizma-problemy-i-perspektivy.html (дата обращения 21 февраля 2024)

6. Сафарзода Х.С., Ањёзода Ш.Т., Мирзомуродзода А.М. Пешгирии шомилшавии љавонон ба ташкилотњои экстремистї-террористї: Дастури таълимї-методї.-Душанбе: «Торус»,2021. С.57-58.

СВЕДЕНИЯ ОБ АВТОРЕ

Абдуллозода Неъматулло Рахматулло. Начальник кафедры оперативно-розыскной деятельности факультета № 4. Кандидат юридических наук.

Академия МВД Республики Таджикистан.

E-mail: nematullo.abdulloev@mail.ru

Abdullozoda Nematullo Rahmatullo. Head of the Department of Operational-Investigative Activities Faculty № 4. Candidate of Legal Sciences.

Academy of the Ministry of Internal Affairs of the Republic of Tajikistan,

E-mail: nematullo.abdulloev@mail.ru

Ключевые слова. Экстремизм; экстремист-вербовщик; безопасность; компьютерные технологии; кибербезопасность; искусственный интеллект; социальные сети; средства массовой информации; информационно-коммуникационные технологии.

Keywords. Extremism; extremist recruiter; security; computer technology; cybersecurity; artificial intelligence; social networks; mass media; information and communication technologies.

УДК 004.056

Ализода Мухаммад Маджид,
адъюнкт

О НЕОБХОДИМОСТИ ВЫБОРА КРИТЕРИЕВ ЭФФЕКТИВНОСТИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ ОБЕСПЕЧЕНИИ ОХРАНЫ ОБЩЕСТВЕННОГО ПОРЯДКА

ON THE NEED TO SELECT CRITERIA FOR THE EFFECTIVENESS OF DECISION-MAKING IN ENSURING THE PROTECTION OF PUBLIC ORDER

Приводится описание о необходимости в выборе критериев эффективности принятий решений при обеспечении охраны общественного порядка. Для осуществления процесса выбора критериев эффективности, предлагается использовать автоматизированный программный комплекс. Приведены примеры использования такого программного продукта.

The article describes the need to select criteria for the effectiveness of decision-making in ensuring the protection of public order. To implement the process of selecting performance criteria, it is proposed to use an automated software package. Examples of using such a software product are given.

В сегодняшних реалиях обеспечение общественной безопасности при проведении различных массовых мероприятий требует наличия более жестких правил и требований.

Охрану общественного порядка можно представить как сложную систему, в которой на результат влияют несколько критериев одновременно.

Для выбора критериев, на которые следует обращать внимание при подготовке проекта решения, разработан и опубликован алгоритм [1]. Блок-схема алгоритма расчета критериев эффективности приведена на рис. 1.

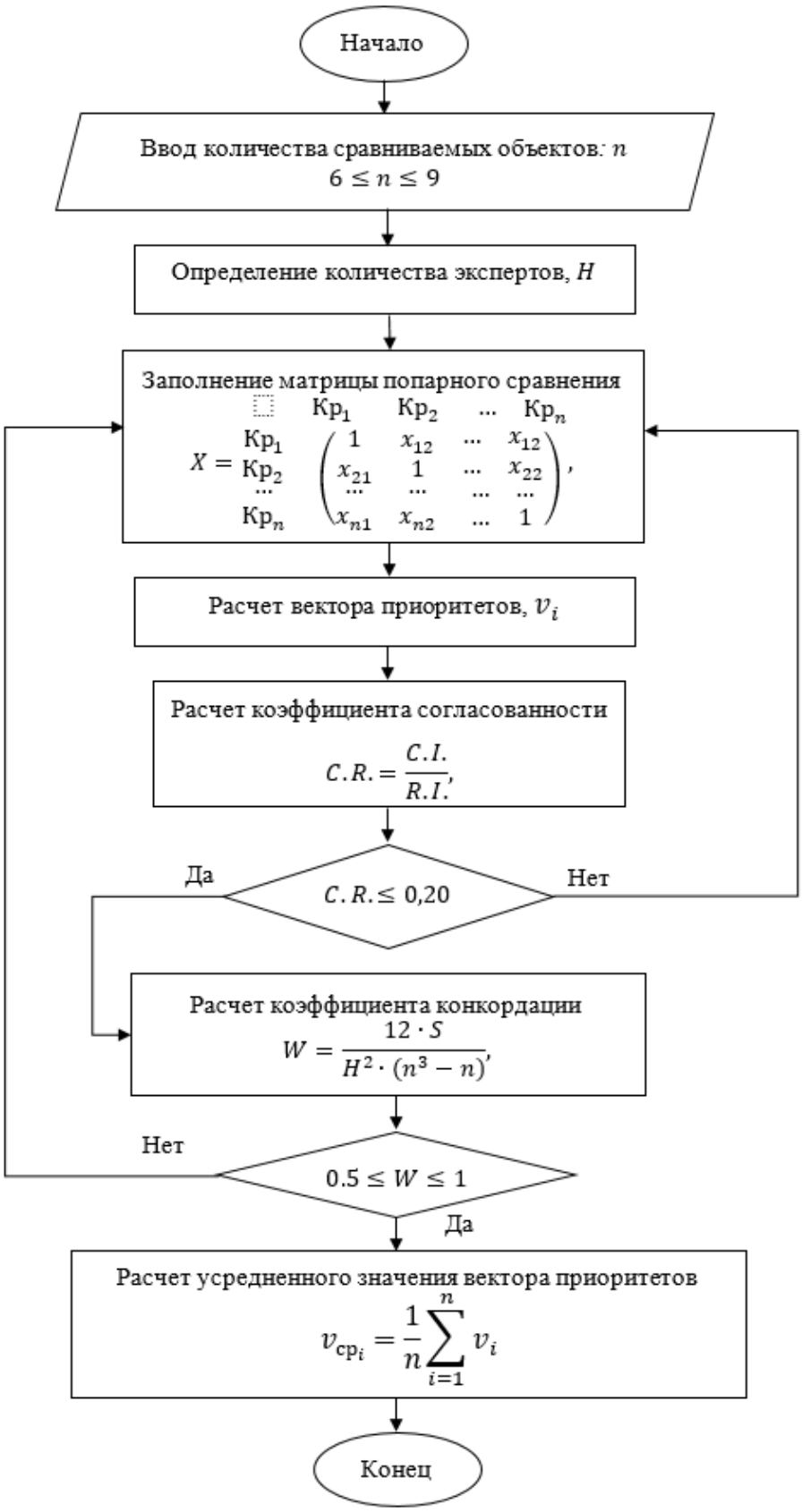
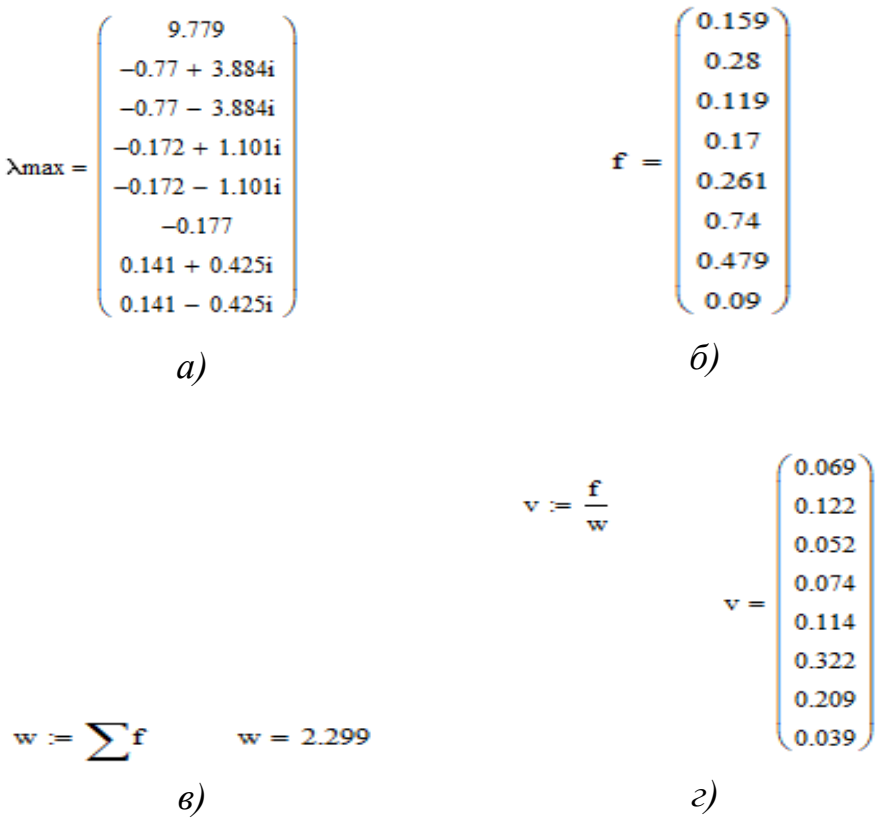


Рис. 1. Блок-схема алгоритма выбора критерия эффективности при принятии решений

В качестве объектов сравнения в данной работе предлагается использовать следующие критерии эффективности, отобранные из открытых источников [2-4]:

1. Минимальное время реагирования на совершенное преступление (t_{min});
2. Минимальное количество жертв со стороны мирных жителей ($К_{жерт_{min}}$);
3. Минимальное количества правонарушений ($К_{прав_{min}}$);
4. Максимальное число профилактических мероприятий ($К_{пр\_мер_{min}}$);
5. Максимальная удовлетворённость жителей в действиях сотрудников милиции ($Удв_{max}$);
6. Максимальный уровень безопасности граждан в общественных местах ($Ур_{без_{max}}$);
7. Максимальный уровень уверенности граждан в защищенности своих личных и имущественных интересов ($Ур_{защ_{max}}$);
8. Максимальный уровень качества в деятельности сотрудников милиции ($Ур_{кач\_деят_{max}}$).

При выборе критериев эффективности можно использовать различные программные средства, которые позволяют автоматизировать определенные вычислительные операции, например программе Mathcad. Скриншоты проведения вычислений приведены на рис. 2.



а) *б)* *в)* *г)*

Рис. 2. Результаты расчетов v_i для первой матрицы в программе Mathcad
а – расчет максимальное собственное число матрицы λ_{max}; б – расчет собственного вектор матрицы; в – нахождение координаты собственного вектора для нормирования приоритетов; г – расчет вектор приоритетов.

Но при использовании таких программных продуктов необходимо осуществлять ввод данных для каждого шага алгоритма для каждого эксперта вручную, что безусловно затрудняет и затягивает процесс выбора критериев эффективности. Охрана общественного порядка – это сложный процесс и проекты решений для урегулирования того или иного вопроса могут потребоваться в кратчайшие сроки. Поэтому для автоматизации ранее разработанного алгоритма предлагается разработать свое программное средство, которое автоматизирует весь процесс полностью и позволит сократить время обработки данных в разы. Скриншоты работы такого программного продукта приведены ниже на рис. 3-5.

Рис. 3 – Стартовое окно программы

Рис. 4 – Окно ввода информации об объектах сравнения (описание критериев эффективности)

Ввод информации об объектах сравнения позволит экспертам, принимающим решения, давать более корректные значения при сравнении данных объектов между собой. Данная возможность минимизирует нарушения транзитивности суждений экспертов и получения более объективных оценок.

Рис. 5 – Окно расчета вектора приоритетов

После ввода дополнительной информации об объектах сравнения пользователь (эксперт) попадает в окно расчета данных. Программа разработана таким образом, что для каждого эксперта выделено отдельное окно для ввода данных, а с правой стороны окна программы приводится пояснение, что означает каждый из объектов сравнения, для упрощения процедуры сравнения объектов между собой.

В конце программа автоматически выводит результаты как по каждому эксперту в отдельности, так и общий результат с графическим представлением данных. Для того чтобы полученные данные дальше можно было использовать, программа полученные отчеты генерирует в формат excel.

Данный программный продукт в настоящее время отправлен в федеральную службу по интеллектуальной собственности для регистрации.

ЛИТЕРАТУРА

1. Ализода М. М., Никулина О. А. Алгоритм выбора критерия эффективности при принятии решений по обеспечению охраны общественного порядка // Вестник Воронежского института ФСИН России. 2024. – № 4. – С. 31-40.

2. Об утверждении государственной программы Российской Федерации «Обеспечение общественного порядка и противодействие преступности» : постановление Правительства Российской Федерации от 15 апреля 2014 г. № 345. – URL: https://base.garant.ru/70644264/ (дата обращения: 10.10.2024).

3. Дубровин А. К. Деятельность полиции по охране общественного порядка в Российской Федерации / А. К. Дубровин, Ю. Р. Бальжинимаев // Право и государство: теория и практика, 2020. – № 9(189). – С. 160-162.

4. Боер В. М. Теоретико-правовое обеспечение общественного порядка и общественной безопасности в современных условиях / В. М. Боер, В. Н. Шамрай // Бизнес в законе – 2012. – № 3. – С. 161-164.

СВЕДЕНИЯ ОБ АВТОРЕ

Ализода Мухаммад Маджид. Адъюнкт 2 курса 3 факультета.
Академия управления МВД России.
E-mail: faridjun@mail.ru.

Alizod Muhammad Majid. 2st year adjunct, 3rd faculty.
Academy of Management of the Ministry of Internal Affairs of Russia.
E-mail: faridjun@mail.ru

Ключевые слова: охрана общественного порядка, критерии эффективности, экспертный опрос, информационные технологии.

Keywords: public order protection, performance criteria, expert survey, information technology.

УДК 004.04

Гилев Игорь Владимирович;
Абдрахманова Эльвина Ринатовна

ПРОЕКТИРОВАНИЕ СИСТЕМЫ НАВИГАЦИОННОГО ОБЕСПЕЧЕНИЯ В ИНТЕРЕСАХ УПРАВЛЕНИЯ МВД РОССИИ ПО Г. УФЕ РЕСПУБЛИКИ БАШКОРТОСТАН

DESIGN OF A NAVIGATION SYSTEM IN THE INTERESTS OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA IN THE CITY OF UFA OF THE REPUBLIC OF BASHKORTOSTAN

Статья посвящена рассмотрению проектированию системы навигационно-мониторингового обеспечения. Рассмотрены основные этапы проектирования спутниковых навигационно-мониторинговых систем органов

внутренних дел в программном обеспечении NAPs Emulator.

The article is devoted to the consideration of the design of the navigation and monitoring support system. The main stages of designing satellite navigation and monitoring systems of internal affairs agencies in the NAPs Emulator software are considered.

Проектирование – это совокупность работ, целью которого является подготовка и получение технической документации, позволяющей реализовать новый или модернизируемый объект с заданными свойствами и с заданной работоспособностью в заданных условиях. В нашем случае реализуется проектирование системы навигационного обеспечения, представляющее собой процесс разработки проекта и его технико-экономическое обоснование, а также инженерных решений, которые обеспечат надежную работу будущей навигационно-мониторинговой системы (НМС) [2].

Результатом навигационной задачи является установление местонахождения объекта и параметров его передвижения, которое обеспечивается с помощью навигационной аппаратуры потребителя (НАП), принимающей и обрабатывающей радионавигационные сигналы со спутников. В настоящее время глобальное покрытие обеспечивают четыре спутниковые системы позиционирования: ГЛОНАСС, NAVSTAR (или GPS), Galileo и BeiDou [3].

НМС – это комплекс технических и аппаратно-программных средств на основе НАП глобальных спутниковых навигационных систем, реализующей возможность контроля и наблюдения в центре мониторинга состояния и местоположения объекта. Принцип работы НМС основан на получении от НАП, находящейся у сотрудников или установленной на транспортных средствах, информации о местоположении подвижных объектов. Эти данные отправляются по каналам связи в центр мониторинга (ЦМ). Полученная навигационная информация обрабатывается аппаратно-программным комплексом (АПК) и на мониторе на фоне электронной карты местности отображаются местоположение, маршруты движения объектов и состояние НАП [4]. Общий принцип работы НМС показан на рис. 1.

Рис. 1. Общий принцип работы НМС

Для проектирования системы мониторинга подвижных объектов воспользуемся программным обеспечением «NAPs Emulator» (рис. 2).

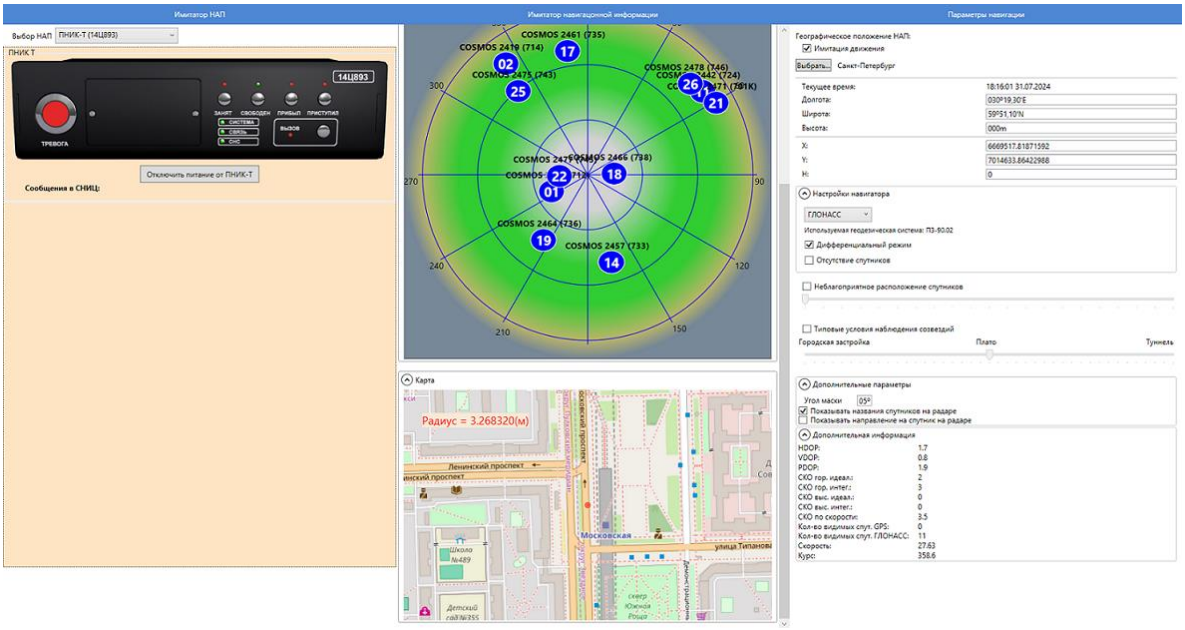


Рис. 2. Интерфейс программы NAPs Emulator

В качестве НАП в МВД России используются радионавигационное оборудование «Навик-Про» и «Навик-Про М», но в программном обеспечении NAPs Emulator данных бортовых оборудований нет, поэтому используем потребительский навигационно-информационный комплект (ПНИК-Т) (рис. 3).

Принцип действия аппаратуры основан на параллельном приеме и обработке 32 измерительными каналами сигналов навигационных космический аппаратов (НКА) систем ГЛОНАСС и GPS. Аппаратура обеспечивает формирование измерительной информации по сигналам стандартной и высокой точности системы ГЛОНАСС в частотном диапазоне L1 (от 1598,0625 до 1605,375 МГц), по сигналам С/А-кода (coarse/acquisition) системы GPS на частоте L1 (1575,42 МГц) [5].

Рис. 3. Внешний вид аппаратуры

Для успешного функционирования программного обеспечения необходимо задать следующие параметры навигации:

1. Выбираем населённый пункт – г. Уфа;
2. Дата, время и координаты проставляются автоматически системой;
3. В настройках навигатора устанавливаем ГНСС «ГЛОНАСС»;
4. Устанавливаем флажок на параметре «дифференциальный режим»;
5. Типовые условия наблюдений созвездий ставим «плато».

При данных параметрах конфигурации наблюдаем следующий уровень навигационных сигналов со спутников и выбранный объект на фоне электронной карты местности (рис. 4).

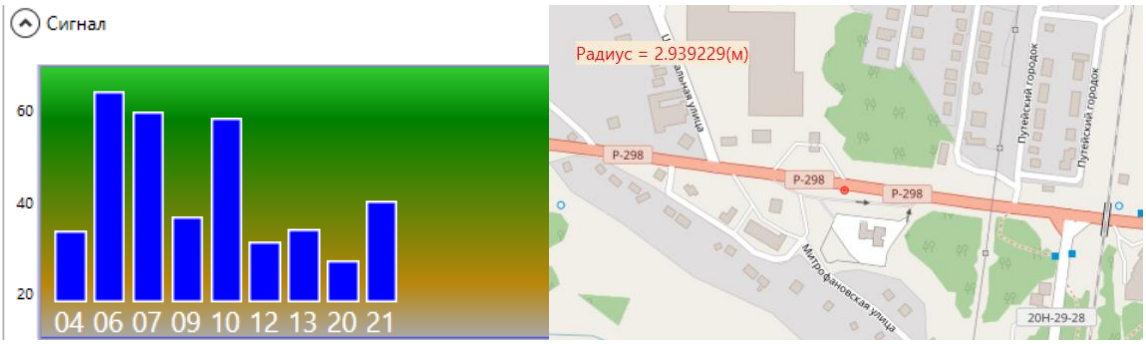


Рис. 4. Уровень сигналов и наблюдаемый объект

В современных условиях наблюдаемый объект не всегда может быть в зоне видимости большого числа спутников, так как этому препятствует огромное количество зданий и сооружений, расположенных в городе. Уровень сигнала в таких случаях будет меньше, так как информация о положениях спутников, поступающая в навигационном сообщении на приемное оборудование транспортного средства, будет приходить уже от меньшего числа НКА (рис. 5).

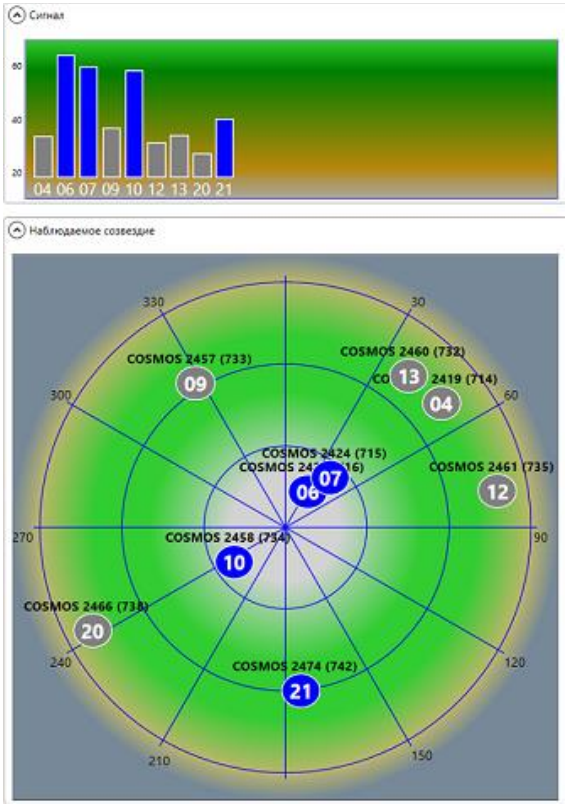


Рис. 5. Уровень сигнала и видимое количество спутников

Исходя из вышеописанного, можно сделать вывод, что данная программа подходит при моделировании систем навигационного обеспечения на первоначальном этапе проектирования. В МВД России таким программным обеспечением является «Автоматизированная система мониторинга объектов на базе Государственной автоматизированной информационной системы «ЭРА-ГЛОНАСС» («АСМ ЭРА»), обеспечивающая передачу данных о местоположении транспортного средства в СОДЧ ИСОД МВД России [4].

Таким образом, для того чтобы оснастить подразделение полиции устойчиво функционирующей системой навигационного обеспечения, необходимо выполнить качественный проект в соответствии с действующими требованиями стандартов. Требования, предъявляемые к спутниковым навигационно-мониторинговым системам, определены Приказом МВД России от 31.12.2008 г. № 1197 «Об утверждении и использовании общих тактико-технических требований к спутниковым навигационно-мониторинговым системам для органов внутренних дел Российской Федерации и внутренних войск МВД России» [1].

ЛИТЕРАТУРА

1. Об утверждении и использовании общих тактико-технических требований к спутниковым навигационно-мониторинговым системам для органов внутренних дел Российской Федерации и внутренних войск МВД России: Приказ МВД России от 31 декабря 2008 г. № 1197 // Собрание законодательства Российской Федерации. - 2008.

2. Компания СтройКад [Электронный ресурс]. - URL: https://stroykad.com/etapy-proektirovaniya-svyazi/ (дата обращения:01.12.2024).

3. Прикладной потребительский центр ГЛОНАСС [Электронный ресурс]. - URL: https://glonass-iac.ru/ (дата обращения:01.12.2024).

4. Хохлов Н. С. Спутниковые навигационно-мониторинговые системы : учебное пособие / Н. С. Хохлов, О. В. Пьянков, С. В. Канавин - Воронеж : Воронежский институт МВД России, 2021. - 132 с.

5. ALL-Pribors.ru [Электронный ресурс]. - URL: https://all-pribors.ru/opisanie/50871-12-pnik-t-indeks-14ts893-
8 (дата обращения:01.12.2024).

СВЕДЕНИЯ ОБ АВТОРАХ

Гилев Игорь Владимирович. Преподаватель кафедры инфокоммуникационных систем и технологий.

Воронежский институт МВД России.

E-mail: gileviv@bk.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Абдрахманова Эльвина Ринатовна. Слушатель 5 курса радиотехнического факультета.

Воронежский институт МВД России.

Gilev Igor Vladimirovich. Lecturer at the chair of Infocommunication Systems and Technologies.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: gileviv@bk.ru

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

Abdrakhmanova Elvina Rinatovna. 5th year student at the Faculty of Radio Engineering.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

Ключевые слова: проектирование; системы навигации; ГЛОНАСС; НМС.

Key words: design; navigation systems; GLONASS; NMS.

УДК 004

Гилев Игорь Владимирович;
Аброськин Егор Владимирович

НЕКОТОРЫЕ АСПЕКТЫ ПРОЕКТИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ВИБРОАКУСТИЧЕСКОМУ КАНАЛУ В ЗАЩИЩАЕМОМ ПОМЕЩЕНИИ

DESIGNING A SYSTEM FOR PROTECTING SPEECH INFORMATION FROM LEAKAGE VIA A VIBROACOUSTIC CHANNEL IN A PROTECTED ROOM

Статья посвящена рассмотрению проектированию системы защиты информации в защищаемом помещении от утечки информации по виброакустическому каналу. Рассмотрены основные принципы и факторы, влияющие на построение такой системы, а также содержание основных мероприятий по защите информации.

The article is devoted to the consideration of the design of the information protection system in the protected premises from information leakage via the vibroacoustic channel. The main principles and factors influencing the construction of such a system, as well as the content of the main measures for information protection are considered.

Защита речевой информации от утечек по виброакустическому каналу — важная и актуальная задача, особенно для организаций, работающих с конфиденциальной информацией, например, таких как органы внутренних дел. В условиях стремительного развития технологий и увеличения угроз безопасности необходимость в надёжных системах защиты становится более чем очевидной. Утечка данных может привести к серьёзным последствиям, включая компрометацию операций, утрату доверия со стороны граждан и даже угрозу национальной безопасности.

Виброакустический канал представляет собой метод перехвата информации, основанный на регистрации вибраций, возникающих в результате звуковых волн речи. Когда человек говорит, звуковые волны распространяются в воздухе и взаимодействуют с окружающими конструкциями — стенами, потолками и полами. В таких конструкциях происходят колебания, которые могут быть зафиксированы электронными устройствами негласного получения информации, такими как вибродатчики, что делает виброакустический канал одним из наиболее сложных для блокирования методов утечки информации [1].

Звуковые волны, несущие речевую информацию, взаимодействуют с различными средами — газами, жидкостями и твёрдыми телами. Каждая из них обладает упругостью, что позволяет звуковым волнам возбуждать волны

упругой деформации. Если вторичные волны возбуждаются в объектах значительной протяжённости, вероятность их распространения вдоль всего объекта возрастает, что создаёт серьёзные риски для конфиденциальности информации.

Для защиты речевой информации от утечки по виброакустическим каналам применяются как пассивные, так и активные методы.

Пассивные методы направлены на улучшение виброизоляции конструкций помещений. Они включают использование звукопоглощающих материалов и специальных конструкций для уменьшения передачи звука через стены и другие ограждающие конструкции. Например, экранирование помещений с использованием модульных конструкций значительно улучшает качество защиты.

Активные методы защиты включают системы акустического зашумления, которые создают искусственные помехи для маскировки речевого сигнала. Эти системы могут быть адаптивными и реагировать на уровень шума в помещении. Например, система активации по голосу может автоматически включать генераторы шума при обнаружении звука выше определённого порога [2].

Особое внимание следует уделять факторам защищенности технического канала утечки информации (ТКУИ). Под ТКУИ следует понимать совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств получения защищаемой информации. Контролируемая зона должна исключать неконтролируемое пребывание посторонних лиц и транспортных средств [3].

Нормативные требования, регламентирующие виброакустическую защиту, охватывают широкий спектр аспектов, связанных с технической защитой информации и обеспечением конфиденциальности в помещениях. Основные документы и стандарты, регулирующие эту область, включают в себя федеральные законы, постановления и рекомендации различных государственных органов.

Одним из ключевых документов является Федеральный закон Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (ред. от 08.08.2024), который устанавливает требования к защите информации с ограниченным доступом и определяет ответственность за утечку таких данных. Согласно этому закону, организации обязаны принимать необходимые меры для обеспечения конфиденциальности персональных данных и предотвращения их несанкционированного распространения. Кроме того, важным нормативным актом является постановление Федеральной службы по техническому и экспортному контролю (ФСТЭК) России, которое содержит требования к техническим средствам защиты информации. Требования касаются как физической защиты помещений, так и защиты информации от утечек по техническим каналам, включая виброакустические.

В рамках государственной системы защиты информации также разработаны методические рекомендации и стандарты, которые описывают

процедуры оценки защищенности объектов информатизации, в которых содержатся указания по проведению аудита безопасности, включая анализ уязвимостей помещений к утечкам по виброакустическим каналам.

Среди других важных аспектов можно выделить необходимость проведения регулярных проверок и тестов на проникновение для выявления слабых мест в системе защиты, что включает в себя использование специализированных средств для оценки акустической защищенности помещений и проверки эффективности применяемых методов защиты.

Оценка уязвимости помещений к утечкам по виброакустическому каналу включает анализ различных факторов защищенности. К ним относятся физическая безопасность (система охраны и контроля доступа), акустическая защита (использование специальных материалов и активных систем шумоподавления) и электромагнитная совместимость (экранирование помещений) [4].

Технический контроль акустической защищенности позволяет документально подтвердить возможность утечки информации из проверяемого помещения. В процессе контроля необходимо провести анализ архитектуры помещения и его конструктивных особенностей для выявления уязвимых мест.

Защита речевой информации от утечек по виброакустическим каналам является многогранной задачей, требующей комплексного подхода и постоянного совершенствования методов защиты. Только так получится обеспечить надежную защиту конфиденциальной информации в условиях современных вызовов информационной безопасности. Подходы к защите должны быть многоуровневыми: от физической безопасности помещений до внедрения современных технологий мониторинга и анализа данных.

В конечном итоге успешная реализация системы защиты требует не только технических решений, но и организационных мер — от повышения осведомленности сотрудников до разработки четких регламентов доступа к конфиденциальной информации. Таким образом, создание безопасной среды для работы с речевой информацией становится не просто технической задачей, а важным аспектом управления информационной безопасностью в целом.

ЛИТЕРАТУРА

1. Бузов Г. А. Защита от утечки информации по техническим каналам: Учебное пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. – М.: Горячая линия – Телеком, 2005. – 416 с.

2. Методы и средства защиты речевой информации от утечки по акустическому и виброакустическому каналам. [Электронный ресурс]. – URL: https://www.dvfu.ru/upload/medialibrary/3b2/f1n15qjclb3pxqzch 71y0rv7hhisqzpv /НТПП%202022%20-%20Сборник.pdf (дата обращения: 06.12.2024).

3. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436 с.

4. Гатчин Ю.А., Климова Е.В. Основы информационной безопасности: учебное пособие. – СПб: СПбГУ ИТМО, 2009. – 84 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Гилев Игорь Владимирович. Преподаватель кафедры инфокоммуникационных систем и технологий.

Воронежский институт МВД России.

E-mail: gileviv@bk.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Аброськин Егор Владимирович. Слушатель 5 курса радиотехнического факультета.

Воронежский институт МВД России.

Россия, 394065, Воронеж, проспект Патриотов, 53.

Gilev Igor Vladimirovich. Lecturer at the chair of Infocommunication Systems and Technologies.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: gileviv@bk.ru

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

Abroskin Egor Vladimirovich. 5th year student at the Faculty of Radio Engineering.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

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

Ключевые слова: проектирование; речевая информация; утечки по виброакустическому каналу.

Key words: design; speech information; leakage through the vibroacoustic channel.

УДК 004

Гилев Игорь Владимирович;
Денисова Анна Александровна

РАЗРАБОТКА ТЕХНИЧЕСКОЙ РЕАЛИЗАЦИИ СИСТЕМЫ DNSSEC ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ

DEVELOPMENT OF TECHNICAL IMPLEMENTATION OF THE DNSSEC SYSTEM FOR PROTECTING INFORMATION FROM LEAKAGE

Статья посвящена рассмотрению реализации системы DNSSEC в интересах органов внутренних дел. Рассмотрены основные этапы внедрения данной технологии, а также их содержание. Изложены перспективы применения данной технологии в защищенных информационных системах.

The article is devoted to the consideration of the implementation of the DNSSEC system in the interests of internal affairs agencies. The main stages of the implementation of this technology, as well as their content, are considered. The prospects for the use of this technology in secure information systems are outlined.

В современном мире, где информационные технологии играют ведущую роль в жизни общества, обеспечение безопасности данных становится одной из ключевых задач. Среди многочисленных угроз кибербезопасности особое место занимает атака типа «DNS-спуфинг», направленная на подмену адресов DNS-серверов с целью перенаправления пользователей на фишинговые или вредоносные сайты, что в свою очередь может привести к утечке конфиденциальной информации [1, 3].

Актуальность исследования определяется тем, что сетевые атаки, основанные на манипуляции с DNS, продолжают совершенствоваться, становясь всё более изощренными и сложными для обнаружения. Это требует постоянного обновления методов и механизмов защиты, а также разработки новых подходов к обеспечению безопасности информационных систем [2].

Для улучшения защиты от DNS-спуфинга в МВД России можно предложить разработку продвинутой системы DNSSEC. Domain Name System Security Extensions (DNSSEC) обеспечивает криптографическую защиту DNS-записей, предотвращая их подмену. Для МВД России важно обеспечить полную и правильную реализацию DNSSEC на всех уровнях DNS-инфраструктуры. Это включает в себя не только защиту собственных доменов, но и проверку подлинности всех получаемых DNS-ответов. Обновление и управление ключами DNSSEC должны быть автоматизированы для минимизации человеческого фактора и повышения надежности системы. Для успешного внедрения продвинутой системы DNSSEC в МВД России необходимо провести несколько этапов, включающих подготовительные работы, техническую реализацию и последующее сопровождение [5].

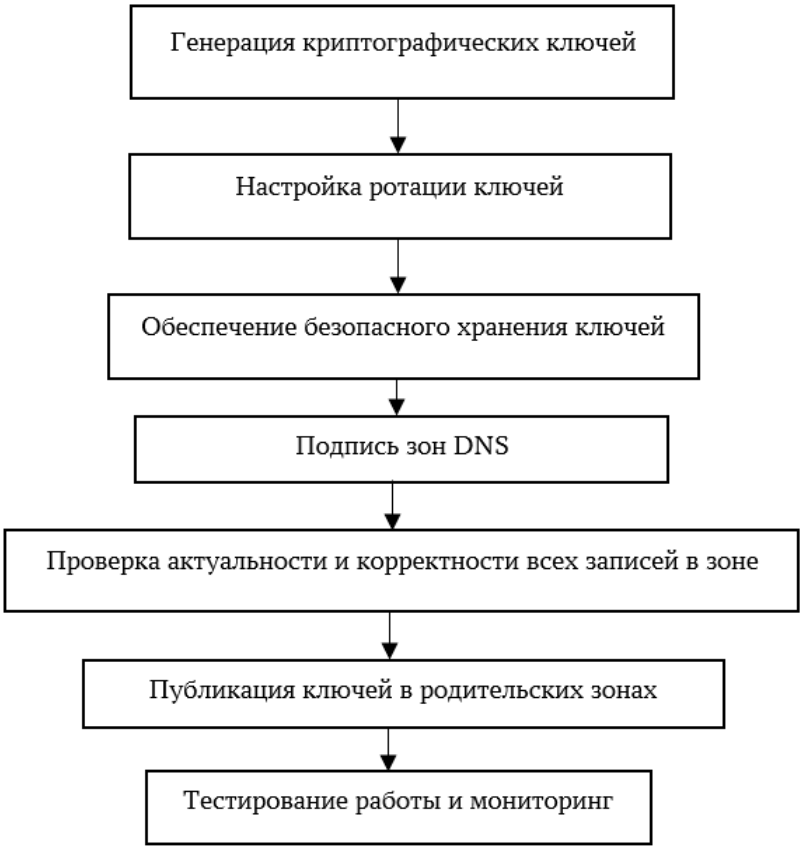


Рис. 1. Этапы технической реализации системы DNSSEC

Техническая реализация системы DNSSEC включает в себя этап генерации криптографических ключей (рис. 1). Необходимо создать ключи для каждой зоны: Key Signing Key (KSK) используется для подписи DNSKEY-записей. Zone Signing Key (ZSK) используется для подписи остальных записей в зоне. Далее настраивается ротация ключей, для этого выполняется определение политики ротации ключей для KSK и ZSK, настройка автоматизированных процессов ротации ключей с использованием инструментов управления ключами. Кроме того, важно обеспечить безопасное хранение и управления сгенерированными ключами, используя защищенные хранилища или аппаратные модули безопасности [4].

Чтобы осуществить подпись зон DNS, подготавливаются зоны для подписи: обновляются конфигурационные файлы зон, добавив записи DNSKEY, RRSIG и других необходимых записей для DNSSEC.

После подготовки осуществляется проверка на то, что все записи зоны актуальны и корректны.

Для публикации ключей в родительских зонах необходимо провести экспорт DS-записей, передать DS-записи регистратору, налаживание связи с регистратором домена для публикации DS-записей в родительских зонах. Проверка, что записи DS успешно опубликованы и доступны для проверки.

Проведение тестирования работы DNS-серверов с DNSSEC осуществляется с использованием инструментов проверки и мониторинга.

Внедрение системы DNSSEC в инфраструктуру МВД России представляет собой важный шаг в укреплении информационной безопасности и защите от атак типа DNS-спуфинг. Благодаря использованию криптографических методов и обеспечению целостности и аутентичности DNS-записей, DNSSEC существенно повышает уровень защиты сетей и данных. Внедрение DNSSEC в МВД России является передовым подходом к обеспечению кибербезопасности. Этот проект показывает, что при правильном планировании и исполнении можно добиться значительного повышения уровня защиты информационных систем. В дальнейшем, поддержка и обновление системы DNSSEC, а также адаптация к новым угрозам и технологиям, будут ключевыми аспектами для поддержания высокого уровня безопасности.

ЛИТЕРАТУРА

1. Об информации, информационных технологиях и о защите информации : федеральный закон от 27.07.2006 г. № 149-ФЗ // Собрание законодательства РФ от 31 июля 2006 г. № 31 (часть I) ст. 3448.
2. ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов от 18 декабря 2008 г. – URL: https://docs.cntd.ru/document/1200075568 (дата обращения: 15.11.2024).
3. Анализ и классификация основных угроз информационной безопасности автоматизированных систем на объектах информатизации органов внутренних дел / А. В. Бацких, И. Г. Дровникова, Е. С. Овчинникова, Е. А. Рогозин // Безопасность информационных технологий. – 2020. – Т. 27. – № 1. – С. 40-50.
4. Попов А. Д. Модели и алгоритмы оценки эффективности систем защиты информации от несанкционированного доступа с учетом их временных характеристик в автоматизированных системах органов внутренних дел: дис. канд. техн. наук: 05.13.19, Попов Антон Дмитриевич. Воронеж, 2018. – 163 с.
5. Официальный сайт ФСТЭК России. Банк данных угроз безопасности информации. – URL: https://bdu.fstec.ru/threat (дата обращения: 20.11.2024).

СВЕДЕНИЯ ОБ АВТОРАХ

Гилев Игорь Владимирович. Преподаватель кафедры инфокоммуникационных систем и технологий.

Воронежский институт МВД России.

E-mail: gileviv@bk.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Денисова Анна Александровна. Слушатель 5 курса радиотехнического факультета.
Воронежский институт МВД России.
Россия, 394065, Воронеж, проспект Патриотов, 53.

Gilev Igor Vladimirovich. Lecturer at the chair of Infocommunication Systems and Technologies.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: gileviv@bk.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Denisova Anna Alexandrovna. 5th year student at the Faculty of Radio Engineering.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: Система DNSSEC; DNS-сервер; защита информации.

Key words: DNSSEC system; DNS server; information security.

УДК 004

Ерошенко Денис Александрович;
Галуза Максим Андреевич;
Климов Александр Иванович,
доктор технических наук, профессор

ПЛОСКАЯ АНТЕННА ДИАПАЗОНА КВЧ С ВЫСОКИМ КОЭФФИЦИЕНТОМ УСИЛЕНИЯ

HIGH GAIN EHF BAND FLAT ANTENNA

Приведены результаты имитационного моделирования плоской антенной решетки вытекающей волны диапазона КВЧ с коэффициентом усиления не менее 33,5 дБ в полосе частот 60–61 ГГц. Антенна может быть использована в аппаратуре помехозащищенных систем радиосвязи прямой видимости.

The results of computer simulation of a flat EHF leaky wave antenna array with a gain at least 33,5 dB in the frequency band 60–61 GHz are presented. The antenna can be used in the equipment of noise-proof line-of-sight radio communication systems.

В настоящее время диапазон крайне высоких частот (КВЧ) все интенсивнее используется для построения различных радиотехнических систем передачи информации, включая помехозащищенные системы радиосвязи с радиолиниями прямой видимости, работающими в окрестности частоты 60 ГГц, на которой в силу резонансного поглощения энергии радиоволн молекулами кислорода резко возрастает погонное ослабление радиосигнала на приземной трассе. Соответственно, для повышения энергетического потенциала и помехозащищенности таких радиолиний необходимо применение антенн с высоким коэффициентом усиления (КУ) и низким уровнем боковых лепестков диаграммы направленности (ДН). Традиционно в аппаратуре подобных радиосистем применяются зеркальные антенны различных типов, что не всегда приемлемо с учетом требований к массогабаритным характеристикам аппаратуры. Альтернативу зеркальным антеннам составляют компактные плоские антенные решетки, в частности, волноводно-щелевые и полосковые. При этом в числе плоских полосковых антенных решеток особый интерес представляют собой полосковые антенные решетки вытекающей волны (ПАРВВ) линейной поляризации на основе плоского диэлектрический волновода (ПДВ) и полосковой дифракционной решетки (ДР), обладающие высоким коэффициентом полезного действия КПД) в диапазонах СВЧ и КВЧ, благодаря чему их КУ (у известных на данный момент антенн) достигает 28–30 дБ в относительной полосе частот до 1–2 % [1, 2]. В силу самого принципа построения простых по конструкции ПАРВВ с параллельно-последовательным питанием дальнейшее увеличение

коэффициента направленного действия (КНД) и КУ до 33–36 дБ путем увеличения площади раскрыва ПАРВВ приводит к не всегда допустимому сужению полосы рабочих частот [2]. В одной из предшествующих работ [1] нами был исследован вариант построения ПАРВВ с большой площадью раскрыва, предполагающий объединение четырех подрешеток вытекающей волны с помощью четырехканального параллельного сумматора/делителя мощности лучевого типа. Применительно к ПАРВВ для полосы частот 24–24,25 ГГц это позволило увеличить КУ до 34 дБ и обеспечить при этом формирование ДН с уровнем боковых лепестков порядка –18 дБ [1].

В данной работе представлены предварительные результаты имитационного моделирования с помощью программы ANSYS HFSS ПАРВВ, аналогичной описанной в [1], но рассчитанной для полосы частот 60–61 ГГц. Антенна разработана по методике [3] с использованием хорошо известного в электродинамике и теории антенн принципа электродинамического подобия. Новая антенна представляет собой масштабную копию антенны для полосы частот 24–24,25 ГГц с соответственно уменьшенными размерами раскрыва до 90,4×89,2 мм^2. Внешний вид антенны показан на рис. 1, ее основные электрические характеристики (частотная характеристика КСВ, частотные характеристики КНД, КУ с учетом только тепловых потерь и реализуемого КУ с учетом качества согласования по входу, а также пример ДН в E- и H-плоскостях на частоте 60,25 ГГц) иллюстрируются рис. 2–4.

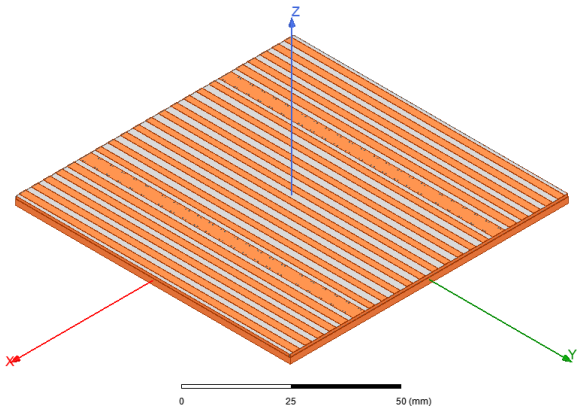


Рис. 1. ПАРВВ КВЧ, составленная из четырех подрешеток вытекающей волны с параллельным питанием

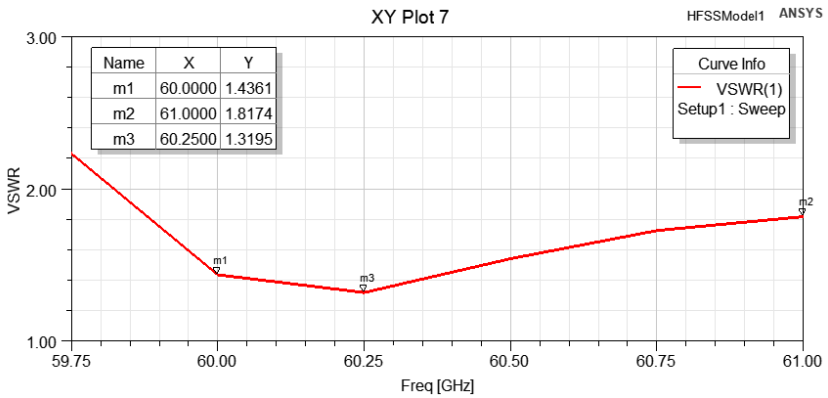


Рис. 2. Частотная характеристика КСВ

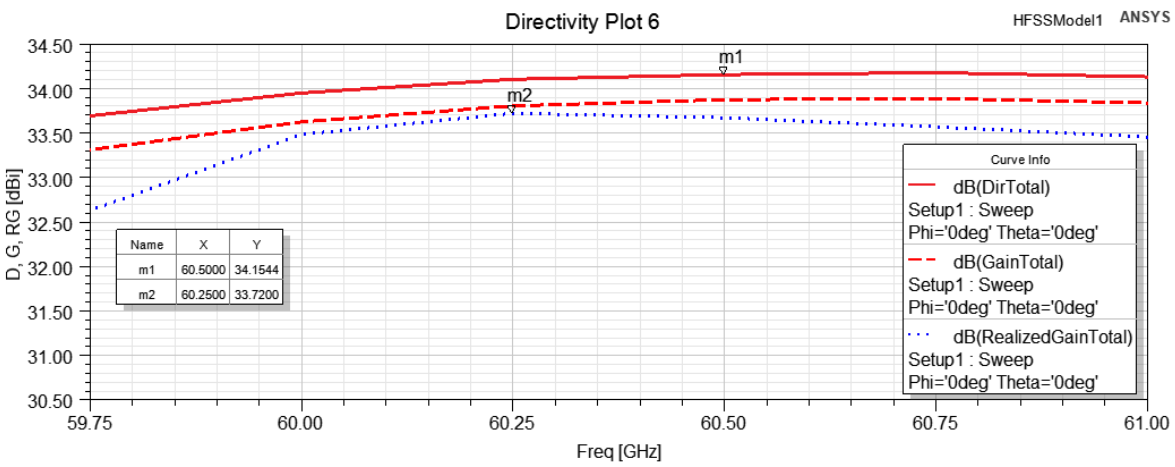


Рис. 3. Частотные характеристики КНД и КУ

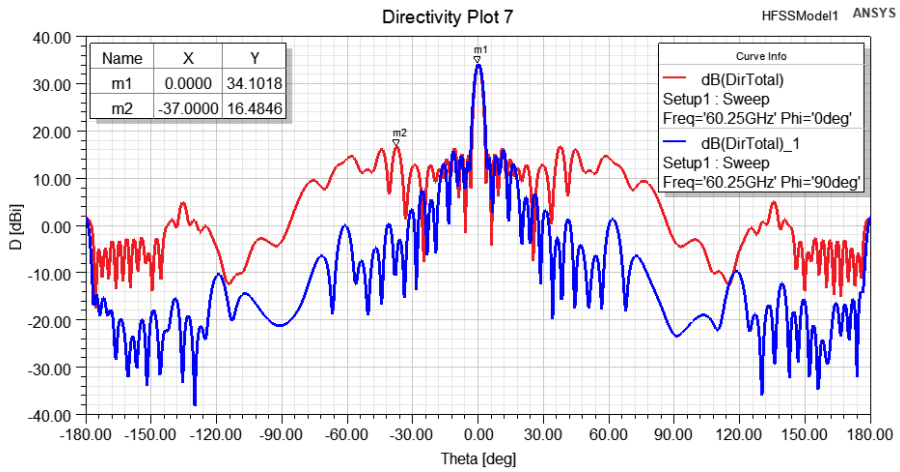


Рис. 4. ДН антенны на частоте 60,25 ГГц

Как видно из представленных на рис. 2 и 3 характеристик, в полосе частот 60–61 ГГц коэффициент стоячей волны напряжения на входе антенны (КСВ) не превышает 1,8; максимальный реализуемый КУ составил 33,7 дБ на частоте 60,25 ГГц, причем в полосе 60–60,75 ГГц КУ оказывается не менее 33,5 дБ. Анализ ДН антенны в полосе частот 60–60,75 ГГц показал, что уровень боковых лепестков в Е- и Н-плоскостях не превышает –16,3 дБ, а на частоте 60,25 ГГц (рис. 4) снижается до –17,6 дБ. Рассчитанное значение

эффективности излучения антенны (как произведения КПД и коэффициента использования поверхности) на частоте 60,25 ГГц составило 0,533. Стоит отметить, что, судя по форме ДН, есть резерв увеличения КНД и, соответственно, КУ антенны до 34–35 дБ.

Полученные результаты позволяют сделать вывод о том, что разработанная антенна представляется довольно перспективной альтернативой зеркальным антеннам в плане использования в аппаратуре помехозащищенных систем радиосвязи прямой видимости диапазона КВЧ.

ЛИТЕРАТУРА

1. Ерошенко Д.А. Плоская антенна СВЧ с высоким коэффициентом усиления и низким уровнем боковых лепестков диаграммы направленности / Д.А. Ерошенко, М.А. Галуза, А.И. Климов // Вестник Воронежского института МВД России. – 2022. – № 4. – С. 124–133.

2. Галуза М.А. Характеристики плоской антенны СВЧ, составленной из четырех подрешеток вытекающей волны / М.А. Галуза, А.И. Климов // Вестник Воронежского института МВД России. – 2019. – № 4. – С. 152–157.

3. Галуза М.А. Антенные решетки СВЧ с управляемой диаграммой направленности для аппаратуры систем радиосвязи и радиоуправления: Методические рекомендации / М.А Галуза, А.И. Климов, А.С. Лукьянов // Воронеж: Воронежский институт МВД России. – 2024. – 50 с.

СВЕДЕНИЯ ОБ АВТОРАХ

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

Воронежский институт МВД России.

E-mail: den1is_90@mail.ru

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

Галуза Максим Андреевич.

ФКУ НПО «СТиС» МВД России.

E-mail: q0mezon@gmail.com

Россия, 111024, г. Москва, ул. Пруд Ключики, 2.

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

Воронежский институт МВД России.

E-mail: alexserkos@inbox.ru

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

Eroshenko Denis Aleksandrovich. Head of the editorial section of the editorial and publishing department.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: den1is_90@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Galuza Maksim Andreevich.
Federal government institution scientic and production association Special equipment and telecoms of the Ministry of the internal affairs of the Russian Federation.
E-mail: q0mezon@gmail.com
Work address: Russia, 111024, Moscow, Prud-Klyuchiki str., 2

Klimov Alexander Ivanovich. Professor of the Chair of Infocommunication Systems and Technologies. Doctor of Sciences (Radio Engineering), Professor.
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: плоская антенная решетка; вытекающие волны; коэффициент направленного действия; коэффициент усиления; диаграмма направленности.

Key words: flat antenna array; leaky waves; radiation efficiency; directivity; gain; radiation pattern.

УДК 621.396.67

Жайворонок Денис Александрович,
кандидат технических наук, доцент;
Лозовой Иван Сергеевич;
Шишлянников Владимир Андреевич;
Яровой Александр Александрович

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТРАНСПОРТНОГО УРОВНЯ

ENSURING INFORMATION SECURITY AT THE TRANSPORT LEVEL

В работе приведены основные аспекты обеспечения информационной безопасности транспортного уровня.

The paper presents the main aspects of ensuring information security at the transport level.

На сегодняшний день практически у всех коммерческих организаций, у большинства государственных организаций и у многих физических лиц есть собственные вебсайты. Число пользователей и компаний, имеющих доступ в Интернет, стремительно растет, и все эти пользователи обладают графическими веб-браузерами. В результате коммерческие организации со все возрастающим интересом рассматривают возможность использования интернет-пространства для электронной коммерции. Однако в реальности всемирная паутина и корпоративные сети подвержены разнообразным атакам. Если коммерческая организация собирается использовать интернет не только для распространения информации, но и в других целях (например, для электронной коммерции), ей требуются надежные механизмы обеспечения безопасности.

Все большую популярность завоевывает универсальное решение проблемы безопасности, заключающееся в использовании протокола, функционирующего между протоколом транспортного уровня (TCP) и приложением. Наиболее известным примером такого протокола являются интернет-стандарт, известный как TLS. Здесь возможны два варианта реализации. Для полной универсальности протокол стандарт TLS может быть реализован как часть нижележащего стека протоколов и, таким образом, быть прозрачным для приложений. Альтернативный подход заключается во внедрении TLS в конкретные пакеты. Например, веб-браузеры Netscape и Microsoft поставляются со встроенной поддержкой TLS 1.3, и большая часть веб-серверов также поддерживает этот протокол. И хотя протокол TLS может применяться не только для транзакций через интернет, сегодня он, как правило, включается в состав веб-браузеров и веб-серверов, и, таким образом, его использование ограничено веб-трафиком.

Протокол TLS был разработан компанией Netscape. При работе над третьей версии этого протокола учитывались отзывы пользователей и

рекомендации производителей, после чего протокол был опубликован в виде проекта Интернет-стандарта. Позднее, когда был достигнут консенсус, в рамках группы IETF сформировалась рабочая группа TLS для подготовки общего стандарта. Текущая работа этой группы направлена на создание начальной версии Интернет-стандарта. В первой версии стандарта TLS специфицируется версия протокола SSLv3.1, очень близкая к SSLv3. Стандарт TLS описывает механизм, при помощи которого TLS-сущность может работать и по протоколу SSLv3.0; в этом смысле протокол TLS является обратно совместимым с SSL.

Работа протокола TLS прозрачна для пользователя. Механизмы безопасности реализованы поверх базовой службы TCP/IP. Использующее протокол TCP программное обеспечение, как правило, специфицирует сокет на каждом конце соединения. На этом уровне протокол TLS может быстро и прозрачно шифровать все передаваемые между сокетами данные, то есть он может обеспечивать безопасность, практически, для любого приложения интернета. В частности, протокол TLS может использоваться для защиты электронной почты всемирной паутины. При взаимодействии клиента и сервера протокол TLS обеспечивает защиту на уровне линии связи или канала, а не на уровне документа или транзакции.

Большая часть работы выполняется протоколом TLS на начальной стадии (во время процедуры, так называемого, «рукопожатия») в ходе установки защищенного канала. Протокол начинает свою работу с того, что клиент запрашивает у сервера аутентификацию. В запросе клиента указывается понимаемый клиентом алгоритм шифрования, а также помещается некий случайный набор символов, которые сервер должен зашифровать. Так клиент может убедиться в том, что на его запрос действительно отвечает сервер, знающий шифр. Сервер отвечает на запрос сертификатом, содержащим электронную подпись сервера, для чего используется шифрование с открытым ключом. Сервер также помещает в ответ предпочитаемые им алгоритмы шифрования. Затем клиент генерирует основной ключ, зашифровывает его открытым ключом сервера и посылает на сервер. Этот ключ используется для генерирования ключей, используемых для шифрования пересылаемых сообщений. Процесс рукопожатия также может включать этап аутентификации клиентом сервера. Этот этап полностью противоположен первому этапу. Сервер посылает клиенту случайный набор байтов, а клиент подтверждает свою личность, подписывая полученный случайный текст своей электронной подписью, а также посылает серверу сертификат своего открытого ключа. Используемые на стадии аутентификации цифровые подписи основаны на алгоритме шифрования с открытым ключом RSA. Однако после завершения процедуры рукопожатия для шифрования пересылаемых данных используется система шифрования с симметричным ключом, например, DES или Triple DES.

При анализе исходного текста HTML-документа, нужно обратить внимание, на то, что ссылки на другие веб-страницы обозначаются при

помощи команды HREF=<URL>, помещенной внутрь тега A (Anchor – якорь). В большинстве случаев, эти ссылки указывают на другие документы при помощи протокола HTTP (HyperText Transfer Protocol – протокол передачи гипертекста). Для того чтобы открыть новый документ, веб-браузер инициирует новый сеанс с TCP-портом номер 80 (это один из, так называемых, «хорошо известных» номеров порта протокола HTTP) получателя (сервера). В некоторых случаях может быть вызван подключаемый модуль, с которым веб-браузер обменивается данными. Для этого браузер инициирует сеанс с TCP-портом подключаемого модуля. Протокол TLS вызывается, когда ссылка начинается следующим образом: HREF=https://.,, Символ «s» после префикса «http» означает, что данные должны передаваться при помощи протокола TLS. Когда пользователь щелкает мышью на этой ссылке, браузер инициирует сеанс с TCP-портом номер 443 сервера. Протокол TLS пытается согласовать параметры установки защищенного канала и передать по нему данные. Если согласование заканчивается неудачно, данные передаваться не будут. Как правило, браузер указывает, что запрашивается безопасное соединение. Так, различные версии веб-браузеров могут сообщает об этом пользователю такими способами как: синяя рамка вокруг страницы, либо нарисованным ключиком в левом нижнем углу окна или изображением закрытого замка в нижней части строки состояния. Такой значок означает, что информация в окне браузера была доставлена при помощи протокола TLS.

ЛИТЕРАТУРА

1. Таненбаум, Эндрю. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл . – 5-е изд. – М. ; СПб. ; Н.Новгород ; Воронеж [и др.] : Питер, 2015. – 955 с. : ил. – (Классика computer science) .– Библиогр.: с.935-946. Алф. указ.: с.947-955 .– ISBN 978-0132126953.
2. Столлингс, Вильям. Передача данных / пер. с англ. М. Глазов, А. Леонтьев . – 4-е изд. – М. [и др.] : Питер, 2004 .– 749 с. : ил., табл. – (Классика computer science) .– Алфав. указ.: с.735-749.
3. Модель комплекса средств противодействия угрозам информационной безопасности в сетях связи специального назначения / О. И. Бокова, Д. А. Жайворонок, С. В. Канавин, Н. С. Хохлов // Моделирование, оптимизация и информационные технологии. – 2020. – Т. 8, № 2(29). – DOI 10.26102/2310-6018/2020.29.2.040. – EDN PPWMAG.
4. Жайворонок, Д. А. Программные продукты обеспечения безопасности виртуальных частных сетей / Д. А. Жайворонок, А. С. Лукьянов // Вестник Воронежского института высоких технологий. – 2018. – № 3(26). – С. 44-46.
5. Жайворонок, Д. А. Повышение эффективности управления потоком данных спутникового мониторинга транспортных средств / Д. А. Жайворонок // Инновации в автомобильном транспорте : материалы Всероссийской научно-технической конференции, Воронеж, 19–20 мая 2022

года. – Воронеж: Воронежский государственный лесотехнический университет им. Г.Ф. Морозова, 2022. – С. 16-22. – DOI 10.34220/IRT2022_16-22.

СВЕДЕНИЯ ОБ АВТОРАХ

Жайворонок Денис Александрович. Заместитель декана автомобильного факультета по учебной работе. Кандидат технических наук, доцент.
Воронежский государственный лесотехнический университет.
E-mail: dzhaivoronok@bk.ru
Россия, 394087, г. Воронеж, ул. Тимирязева, 8.

Лозовой Иван Сергеевич. Студент 3 курса.
Воронежский государственный лесотехнический университет.
Воронежский институт МВД России.
E-mail: Natali.Lozovaya@mail.ru
Россия, 394087, г. Воронеж, ул. Тимирязева, 8.

Шишлянников Владимир Андреевич. Студент 3 курса.
Воронежский государственный лесотехнический университет.
Воронежский институт МВД России.
E-mail: chelovek1987a@yandex.ru
Россия, 394087, г. Воронеж, ул. Тимирязева, 8.

Яровой Александр Александрович. Студент 3 курса.
Воронежский государственный лесотехнический университет.
Воронежский институт МВД России.
E-mail: alexandr.yarovoy2006@gmail.com
Россия, 394087, г. Воронеж, ул. Тимирязева, 8.

Ключевые слова: транспортный уровень; информация; протокол; безопасность, приложение, веб-браузер, данные, модуль.

Key words: phase-manipulated signal; interfering signals; phase detector; processing algorithm.

УДК УДК 621.396.41.

Канавин Сергей Владимирович,
кандидат технических наук, доцент;
Маркелов Даниил Игоревич

ПРОЕКТИРОВАНИЕ ЗАЩИЩЁННОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ МОНИТОРИНГА И РЕАГИРОВАНИЯ НА АТАКИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

DESIGNING A SECURE TELECOMMUNICATION SYSTEM FOR MONITORING AND RESPONSE TO ATTACKS IN COMPUTER SYSTEMS

Статья посвящена проектированию системы мониторинга компьютерных атак в локально-вычислительных сетях. Рассмотрены архитектура телекоммуникационной системы, а также преимущества SOAR и SIEM.

The article is devoted to the design of a system for monitoring computer attacks in local area networks. The architecture of the telecommunications system, as well as the advantages of SOAR and SIEM are considered.

Телекоммуникационные системы играют важную роль в функционировании различных сфер деятельности человека, обеспечивая надежность передачи информации и её сохранность. Это крайне важно для органов внутренних дел, где обеспечение надлежащего уровня защиты, как самой информации, так и её передачи, является одним из главных факторов для выполнения государственными структурами своих основных функций. Таким образом, отделы полиции нуждаются в защищенной телекоммуникационной сети, которая сможет автоматически производить мониторинг и реагирование на угрозы безопасности.

Так как угрозы для телекоммуникационных систем возрастают, а информации, циркулирующей внутри этих систем, становится всё больше и больше, то разработка систем защиты приобретает особое значение в соответствии с законодательством о защите информации [1]. Современные телекоммуникационные системы должны обладать высокой скоростью передачи информации, отличным качеством связи, надежностью и защищенностью для минимизации рисков.

Под телекоммуникационными системами понимаются структуры и средства, предназначенные для передачи больших объёмов информации, по линиям связи или с использованием радиоволн [3]. Эти системы проектируют для безопасной передачи информации между различными устройствами на различных расстояниях.

Телекоммуникационная система состоит из [2]:

1) передающего и приемного устройств (например, компьютер);
2) среды передачи информации (например, Интернет);
3) программного обеспечения для взаимодействия с информацией.

Архитектура телекоммуникационной системы может быть разделена по уровням [4]:

1) физический уровень (включает в себя физическое оборудование, такое как серверы, маршрутизаторы, коммутаторы);
2) сетевой уровень (отвечает за передачу данных между устройствами и включает в себя сетевые протоколы, маршрутизацию и управление трафиком);
3) прикладной уровень (включает в себя программное обеспечение и приложения, используемые для работы с данными);
4) уровень управления и мониторинга (включает в себя системы, отвечающие за управление безопасностью, мониторинг активности в сети и реагирование на инциденты).

Для обеспечения безопасности информации, циркулирующей в системах связи, необходимо обнаружить саму угрозу и устранить её, при этом минимизировав ущерб. Для этих целей возможно применение специализированного программного обеспечения, которое позволяет автоматизировать процесс и увеличить скорость реагирования.

Под таким программным обеспечением имеют ввиду программные продукты классов SIEM (Security Information and Event Management) и SOAR (Security Orchestration, Automation and Response).

SIEM – это программный продукт, предназначенный для сбора и анализа информации о событиях безопасности.

Задачами этих систем являются:

1) отслеживание в режиме реального времени сигналов тревоги, поступающих от сетевых устройств и приложений;
2) выявление отклонения в контролируемых системах;
3) оповещение специалиста об обнаруженных инцидентах.

SIEM способны собирать данные о событиях безопасности несколькими способами: с помощью специальных приложений, напрямую из файлов с логами, напрямую с сетевых устройств или с помощью протоколов потоковой передачи данных.

Преимущества использования SIEM:

1) выявление угроз в реальном времени;
2) управление инцидентами;
3) соответствие стандартам;
4) позволяет анализировать безопасность на основе ранее имеющихся данных и генерировать отчеты.

Недостатки использования SIEM:

1) высокие затраты на внедрение и поддержку системы;
2) сложность настройки
3) необходима соответствующая квалификация для специалистов;

4) возможные проблемы с производительность из-за обработки огромных объемов информации.

SOAR – это программный продукт, предназначенный для автоматизации и ускорения процессов обнаружения и реагирования на атаки в системах.

Функции SOAR:

1) объединение внешних и внутренних инструментов;
2) автоматизация процессов;
3) обеспечение сбора информации об угрозах, их локализация и устранение;
4) создание и хранение отчетов об инцидентах, их статусе и реакции на них.

Преимущества использования SOAR:

1) автоматизация позволяет значительно ускорить реагирование на угрозы;
2) снижает нагрузку на специалистов;
3) устранение человеческих ошибок и улучшение качества реагирования на инциденты;
4) интеграция с другими инструментами для комплексного управления безопасностью.

Недостатки использования SOAR:

1) высокие затраты на внедрение и поддержку системы;
2) автоматические процессы должны быть тщательно настроены, иначе ошибки могут привести к непредсказуемым результатам;
3) необходимость в продумывании сценариев автоматизации и оркестрации для предотвращения возможных ошибок.

SOAR автоматизирует анализ инцидентов и помогает оперативно принимать решения, что позволяет снизить нагрузку на специалистов и минимизировать риски.

Таким образом, программные компоненты SIEM и SOAR отлично дополняют друг друга, что помогает специалистам не только отслеживать различные инциденты и своевременно реагировать на них, а также анализировать слабые места в системе. Но также эти компоненты требуют высоких затрат на внедрение и поддержку, высокопроизводительные системы для их работы и квалифицированных специалистов. Дальнейшее исследования в этой области помогут создать гибкую экосистему для защиты телекоммуникационной системы как от существующих угроз, так и от тех, которые могут появиться в будущем.

ЛИТЕРАТУРА

1. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ. – Текст : электронный. // URL:

https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 04.11.2024).

2. Галас В. П. Вычислительные системы, сети и телекоммуникации / В. П. Галас. – Владимир : Издательство ВлГУ, 2017. − 284 с. – Текст: непостредственный.

3. Барановская, Т. П. Архитектура компьютерных систем и сетей / Т. П. Барановская, В. И. Лойко. – Москва : Финансы и статистика, 2013. – 256 с. – Текст : непосредственный.

4. Крухмалев, В. В. Основы построения телекоммуникационных систем и сетей: учебное пособие для вузов / В. В. Крухмалев. – Москва : ИнформоКомКнига, 2012. – 310 с. – Текст : непосредственный.

СВЕДЕНИЯ ОБ АВТОРАХ

Канавин Сергей Владимирович. Доцент кафедры инфокоммуникационных систем и технологий. Кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: sergejj-kanavin@rambler.ru

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

Маркелов Даниил Игоревич. Слушатель 5 курса радиотехнического факультета.

Воронежский институт МВД России.

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

Kanavin Sergey Vladimirovich. Associate Professor. Candidate of Technical Sciences.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: sergejj-kanavin@rambler.ru

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

Markelov Daniil Igorevich. 5th year student at the Faculty of Radio Engineering.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

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

Ключевые слова: проектирование; мониторинг; защищенная телекоммуникационная система; компьютерные атаки.

Key words: design; monitoring; secure telecommunication system; computer attacks.

УДК 004.056

Лемайкина Светлана Владимировна

ПРОБЛЕМЫ РАСПОЗНАВАНИЯ ЛИЦ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

PROBLEMS OF FACE RECOGNITION IN LAW ENFORCEMENT

В статье рассматривается технология распознавания лиц, проанализировано применение технологии во всех сферах, в том числе и в правоохранительной. С учетом того, что технология распознавание лиц сопряжена с проблемами, указано решение по применению биометрических технологий.

The article examines facial recognition technology, analyzes the use of technology in all areas, including law enforcement. Considering that facial recognition technology is associated with problems, a solution for the use of biometric technologies is indicated.

По определению, распознавание лиц — это технология, способная идентифицировать или подтвердить личность человека по изображению, видео или любому другому аудиовизуальному элементу его лица. Распознавание лиц — это процесс идентификации или подтверждения личности человека по его лицу. Оно фиксирует, анализирует и сравнивает шаблоны, основанные на чертах лица человека.

Процесс распознавания лиц является важным этапом, поскольку он позволяет обнаруживать и находить человеческие лица на изображениях и видео. Данный процесс преобразует аналоговую информацию (лицо) в набор цифровых данных (информации), основанных на чертах лица человека. Цель распознавания лиц состоит в том, чтобы по поступающему изображению найти серию данных об одном и том же лице в наборе обучающих изображений в базе данных. Система распознавание лиц использует сгенерированные компьютером фильтры для преобразования изображений лиц в числовые выражения, которые можно сравнивать для определения их сходства. Эти фильтры обычно создаются с помощью глубокого «обучения», которое использует искусственные нейронные сети для обработки данных. Компьютер может сравнить отпечатки лиц на двух отдельных изображениях, чтобы попытаться определить, принадлежат ли они одному и тому же человеку. Он также может попытаться определить другие характеристики (например, пол и эмоции) человека по отпечатку лица. Наиболее распространённый метод распознавания лиц часто называют «сопоставлением лиц». Сопоставления лица выражается в проверке: принадлежат ли два лица одному и тому же человеку. Данный момент считается самым естественным из всех биометрических

измерений. Идентификация отвечает на вопрос: «Кто вы?» Аутентификация отвечает на вопрос: «Действительно ли вы тот, за кого себя выдаёте?»

Технология распознавания лиц за последнее время значительно усовершенствовалась, и её использование стремительно растёт как в коммерческих продуктах в России, так и в зарубежных странах. Российская компания NtechLab, разработчик в области биометрических технологий, создала решение, способное распознавать лица, скрытые на 40% - например, маской, платком, шлемом или бородой. Продукты компании востребованы в сферах общественной и корпоративной безопасности, розничной торговли, финансового сектора, индустриях развлечений и гостеприимства. Компания работает с более чем 30 крупными клиентами в более чем 15 странах СНГ, Ближнего Востока, Латинской Америки, Юго-Восточной Азии. [1] По словам гендиректора NtechLab Сергея Сучкова, 62 региона России использовали системы распознавания лиц в 2021-2023 годах. Последствия пандемии COVID-19 породили программное обеспечение для распознавания лиц путем бесконтактной системы отслеживания посещаемости в режиме реального времени. Реальность, связанная с коронавирусом, побудила китайских технологических компаний, таких как «SenseTime» и «Minivision», с головой погрузиться в коммерческое внедрение механизмов распознавания лиц в таких условиях. [2] Новые алгоритмы могли не только распознавать людей в масках, но и определять тех, кто носит шарфы, очки, шапки и накладные бороды. Также в Китае система мониторинга «Skynet» была разработана для повышения безопасности городских жителей и эффективности выявления преступников полицией. Система массового мониторинга «Skynet» работает с помощью более 600 миллионов камер, установленный в Китае.[3]

Распознавание лиц используется при выдаче документов, удостоверяющих личность, и чаще всего в сочетании с другими биометрическими технологиями, такими как отпечатки пальцев (для предотвращения мошенничества с документами, удостоверяющими личность, и кражи личных данных). В связи со вспышкой COVID-19, эта технология заменяет билеты и позволяет бесконтактно проходить на стадионы и посещать спортивные мероприятия в Нью-Йорке и Лос-Анджелесе. Распознавание лиц используется при пограничном контроле для сравнения портрета в оцифрованном биометрическом паспорте с лицом владельца. Система быстрого пересечения внешней границы «PARAFE», основанная на технологии биометрической аутентификации, использует распознавание лиц, чтобы путешественники могли проходить автоматизированные пограничные формальности при въезде в Шенгенскую зону или выезде из неё. Французское правительство уже почти десять лет помогает внедрять систему «PARAFE», которая позволяет путешественникам самостоятельно пересекать границы по упрощённой процедуре проверки личности.[4]

Преимущества систем распознавания лиц для правоохранительных органов очевидны. Это выявление и предотвращение преступлений. Сегодня правительства и компании в международном плане сталкиваются с

различными угрозами безопасности. Распознавание лиц — ключевой инструмент для борьбы с этими угрозами.

Биометрические данные лица также могут использоваться при проверках в полиции, хотя в Европе их применение строго контролируется. В 2016 году «человек в шляпе», ответственный за теракты в Брюсселе, был опознан благодаря программе распознавания лиц ФБР [5]. Начиная с финала Лиги чемпионов УЕФА в 2017 году полиция Южного Уэльса использовала автоматическую систему распознавания лиц. Порядка 100 арестов и обвинений за 12 месяцев были сделаны при помощи данной системы. [6] По результатам оценки системы был сделан вывод, что данная система помогает полиции распознавать так эффективно, что не было возможности делать это другими способами.

Дроны с камерой в сочетании с аэрофотосъёмкой представляют собой интересную комбинацию для распознавания лиц на больших территориях, например, во время массовых мероприятий. Компания «Face-Six» разработала программное обеспечение, которое с помощью дрона помогает идентифицировать людей по заданным фотографиям в режиме онлайн. В марте 2024 года стало известно о разработке инженера-энтузиаста Луиса Венуса из американского Сан-Франциско, который совместно с программистом Робертом Лукошко создал воздушный дрон с искусственным интеллектом, который распознает человека по лицу, и даже может его преследовать.

Системы видеонаблюдения с функцией распознавания лиц могут значительно ускорить работу сотрудников полиции, позволяя им добавлять фото, предоставленное родителями пропавшего ребёнка, и сопоставлять его с лицами на видео. Полиция может использовать распознавание лиц для поиска видеозаписей (так называемая видеоаналитика) предполагаемого места и времени пропажи ребёнка. Полицейские могут лучше понять, как ребёнок перемещался до пропажи, и определить, где его видели в последний раз. Оповещение в режиме реального времени может срабатывать при обнаружении совпадения. Затем полиция может подтвердить его достоверность и сделать всё необходимое для поиска пропавших детей. Тот же процесс можно применить и к потерявшимся взрослым (например, с деменцией, амнезией, эпилепсией или болезнью Альцгеймера). Выделение появлений конкретных людей в видеоряде имеет решающее значение. Это также может ускорить работу сотрудников полиции в делах, связанных с эксплуатацией детей. Видеоаналитика может помочь составить хронологию, отслеживать активность на карте, выявлять детали и неочевидные связи между участниками дела. В МВД России активно используется технологии компании «NTechLab» для распознавания лиц. Система идентифицирует личность и определяет место проживания и маршрут передвижения по городу. В МВД России также разрабатывается система распознавания людей по татуировкам, по радужной оболочке глаз, по голосу и по движению тела [7].

Но распознавание лиц сопряжено и со многими трудностями. Для эффективной системы распознавания лиц необходимы обширная цифровая библиотека или база данных лиц, отличная камера для съёмки лиц, надёжная и быстрая связь, а также мощный процессор для алгоритмов сопоставления и выдачи результатов в режиме реального времени. Добавьте к этому проблемы, связанные с плохой видимостью, изменениями в окружающей обстановке, качеством фотографий и, наконец, алгоритмом обучения.

Система распознавания лиц может быть обманутой и уязвимым для взлома. Пользователь может применить фильтр, который изменяет определённые пиксели на изображении перед публикацией в интернете. Эти изменения незаметны для человеческого глаза, но сбивают с толку алгоритмы распознавания лиц. В России сотрудник «Яндекса» Григорий Бакунов изобрёл сервис, препятствующий идентификации лица любого пользователя, системой распознавания лиц. Он разработал алгоритм, который создаёт специальный макияж, чтобы обмануть программное обеспечение. Однако из этических соображений и опасений он решил не выводить свой продукт на рынок [8].

Распознавание лиц стремительно развивается, хотя алгоритмы могут обеспечивать очень высокую производительность в контролируемых условиях, многие системы демонстрируют более низкую производительность при использовании в реальных условиях. Распознавание лиц никогда не бывает идеальным, но оно с пугающей частотой даёт сбои. Так, молодого человека – преподавателя кандидата филологических наук Федора Ермошева задержали сотрудники МВД России по подозрению в совершении преступления. Однако после того, как его доставили в отдел полиции, было установлено, что произошла ошибка идентификации. При этом сотрудники полиции заявили, что система распознавания лиц подтверждала схожесть 70% между преступником и ошибочно задержанным разыскиваемым лицом [9]. Для исключения таких ошибок в идентификации человека необходимо анализировать несколько биометрических параметров человека, сравнивая параметры в соотношении их к конкретному человеку [10].

Прогнозируется, что система использования распознавания лиц в правоохранительных и других сферах будет стремительно развиваться. Кроме того, распознавание лиц часто предпочитают другим биометрическим технологиям, таким как распознавание голоса, текстуры кожи, радужной оболочки глаза и сканирование отпечатков пальцев из-за его бесконтактной процедуры и простоты внедрения. Ожидается, что в больших масштабах будут внедряться новые сценарии использования, такие как биометрический вход в систему, общественная безопасность, безопасность путешествий, авторизованные медицинские услуги, платформы электронного обучения и многие другие системы распознавания лиц.

Решение указанных проблем видится в усовершенствовании работы по применению биометрических технологий.

ЛИТЕРАТУРА

1. НТЕХ ЛАБ | Участник проекта «Сколково» [Электронный документ] https://navigator.sk.ru/orn/1122197 Дата ознакомления: 18.11.2024.

2. Медицинская маска больше не спасает от распознавания лица [Электронный документ] Хабр https://habr.com/ru/companies/globalsign/articles/489928/ Дата ознакомления: 18.11.2024.

3. Британские репортеры тестируют Скайнет | U-Technology Group [Электронный документ] Дзен https://dzen.ru/a/Y00TrHy2Dzzsu6I5 Дата ознакомления: 18.11.2024.

4. В парижских аэропортах начала работать система автоматического распознавания лиц [Электронный документ] https://tvrgomel.by/news/v-parizhskikh-aeroportakh-nachala-rabotat-sistema-avtomaticheskogo-raspoznavaniya-lits/ / Дата ознакомления: 18.11.2024.

5. Задержанный в Брюсселе Фейсал Шеффу опознан как «человек в шляпе», сопровождавший террористов. Новости. Первый канал [Электронный документ] https://www.1tv.ru/news/2016-03-26/161958-zaderzhannyy_v_bryussele_feysal_sheffu_opoznan_kak_chelovek_v_shlyape_soprovozhdavshiy_terroristov Дата ознакомления: 18.11.2024.

6. Как технология распознавания лиц помогает полиции [Электронный документ] / Хабр https://habr.com/ru/articles/434280/ Дата ознакомления: 18.11.2024.

7. В РФ стали применять систему распознавания лиц и силуэтов людей и машин - Российская газета [Электронный документ] https://rg.ru/2021/06/24/v-rf-stali-primeniat-sistemu-raspoznavaniia-lic-i-siluetov-liudej-i-mashin.html Дата ознакомления: 18.11.2024.

8. Сотрудник «Яндекса» придумал способ обмануть систему распознавания лиц [Электронный документ] | AdYummy! | Новости | AdIndex.ru https://adindex.ru/news/adyummy/2017/07/19/161085.phtml

9. Худшие ошибки системы распознавания лиц [Электронный документ] / Skillbox Media https://skillbox.ru/media/business/5-sluchaev-kogda-sistema-raspoznavaniya-lits-edva-ne-razrushila-zhizn-cheloveka-po-oshibke/#stk-1 Дата ознакомления: 18.11.2024.

10. Кулаевский А.В. О проблемах использования биометрических технологий при установлении следователем лица, совершившего преступление // Журнал правовых и экономических исследований. Journal of Legal and Economic Studies, 2023, 4: 102–105 https://giefjournal.ru/node/2159.

СВЕДЕНИЯ ОБ АВТОРЕ

Лемайкина Светлана Владимировна. Старший преподаватель кафедры информационного обеспечения ОВД.

Ростовский юридический институт МВД России.

E-mail: lemajkina67@mail.ru
Россия, 344015 Ростов-на-Дону, Еременко 83.

Lemaikina Svetlana Vladimirovna. Head of the Department of Information Support of the Internal Affairs Directorate.
Rostov Law Institute of the Ministry of Internal Affairs of Russia.
E-mail: lemajkina67@mail.ru
Russia, 344015 Rostov-on-Don, Eremenko 83.

Ключевые слова: распознавание лиц; технология; идентификация; биометрические данные; системы видеонаблюдения; база данных.

Key words: face recognition; technology; identification; biometric data; video surveillance systems; database.

УДК: 004.932.2

Пахомова Ангелина Александровна

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ОПТИМИЗАЦИИ РАСПРЕДЕЛЕНИЯ РАБОТ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ

COMPARATIVE ANALYSIS OF ALGORITHMS FOR OPTIMIZING THE DISTRIBUTION OF MAINTENANCE WORK

Рассматриваются вопросы планирования технического обслуживания средств связи и автоматизации в подразделениях органов внутренних дел Российской Федерации. Предлагаются эвристические правила, позволяющие уменьшить объем вычислений для построения оптимального плана-графика технического обслуживания. Проводится сравнительный анализ разработанных ранее алгоритмов оптимизации распределения технического обслуживания. Приводятся результаты вычислительного эксперимента построения плана-графика средств связи и автоматизации двухэтапным алгоритмом. Оцениваются эффективность работы алгоритмов и возможности их практического применения.

The issues of planning the maintenance of communications and automation facilities in the departments of the internal affairs bodies of the Russian Federation are considered. Heuristic rules are proposed to reduce the amount of calculations to build an optimal maintenance schedule. A comparative analysis of previously developed algorithms for optimizing the distribution of maintenance is carried out. The results of a computational experiment of constructing a schedule of

communication and automation facilities using a two-stage algorithm are presented. The effectiveness of the algorithms and the possibilities of their practical application are evaluated.

Полноценное функционирование государства целиком и полностью в нынешних реалиях зависит от использования технических средств. В МВД России для выполнения возложенных на него задач по осуществлению правоохранительной деятельности, применяются средства связи и автоматизации (ССиА), которые могут выходить из строя или отказывать в работе без проведения технического обслуживания (ТО) [1]. Для обеспечения своевременно проводимого ТО в органах внутренних дел разрабатываются планы-графики. Сложность заключается в том, что в связи с большим объемом, используемых ССиА, требований предъявляемых к проведению ТО, не всегда удается построить оптимальный план-график за короткий промежуток времени.

В настоящее время выделяют три вида ТО ежеквартальное – ТО № 1, полугодовое – ТО № 2, годовое – ТО № 3, причем в каждом последующем ТО входит предыдущее, т.е. ТО № 2 включает в себя ТО № 1 [2]. В год производится 4 плановых ТО, допустимые стратегии их проведения по кварталам представлены в таблице 1.

Таблица 1

Допустимые стратегии проведения технического обслуживания в квартале

№ стратегии	I квартал	II квартал	III квартал	IV квартал
1	ТО № 1	ТО № 2	ТО № 1	ТО № 3
2	ТО № 1	ТО № 2	ТО № 3	ТО № 1
3	ТО № 1	ТО № 3	ТО № 1	ТО № 2
4	ТО № 1	ТО № 3	ТО № 2	ТО № 1
5	ТО № 2	ТО № 1	ТО № 1	ТО № 3
6	ТО № 2	ТО № 1	ТО № 3	ТО № 1
7	ТО № 3	ТО № 1	ТО № 1	ТО № 2
8	ТО № 3	ТО № 1	ТО № 2	ТО № 1

Число вариантов технического обслуживания для одного ССиА для одной стратегии:

$$C_1 = 3^4 = 81, \quad (1)$$

где 3 – количество вариантов размещений ТО по месяцам в каждом квартале, а 4 – число кварталов.

Для 8 допустимых стратегий, рассмотренных в таблице 1, число вариантов проведения технического обслуживания для одного ССиА составит:

$$C_8 = 8C_1 = 648. \quad (2)$$

Таким образом, для n ССиА количество вариантов различных планов-графиков будет определяться следующим выражением:

$$C_n = C_8^n = 648^n. \quad (3)$$

Существуют различные варианты построения планов-графиков, такие, как полный перебор [3], эвристический алгоритм и двухэтапный алгоритм. Проведем их сравнительный анализ.

Выберем в качестве критерия оценки эффективности работы указанных методов количество ССиА, для которых можно построить план-график не более, чем за сутки. Для проведения вычислительного эксперимента для каждого алгоритма были созданы соответствующие программы для ЭВМ в среде Delphi 12 Community Edition [4]. Исходные данные, подобранные случайным образом, представлены в таблице 2.

Таблица 2

Исходные данные для вычислительного эксперимента

№ п/п	Наименование ССиА	Продолжительность, мин		
		ТО № 1	ТО № 2	ТО №3
1.	Прибор 1	10	26	49
2.	Прибор 2	5	18	33
3.	Прибор 3	7	20	44
4.	Прибор 4	12	37	52
5.	Прибор 5	9	23	47
6.	Прибор 6	13	27	60
7.	Прибор 7	20	40	72
8.	Прибор 8	17	33	58

9.	Прибор 9	15	27	48
10.	Прибор 10	19	25	44
11.	Прибор 11	24	47	89
12.	Прибор 12	33	57	90
13.	Прибор 13	10	31	77

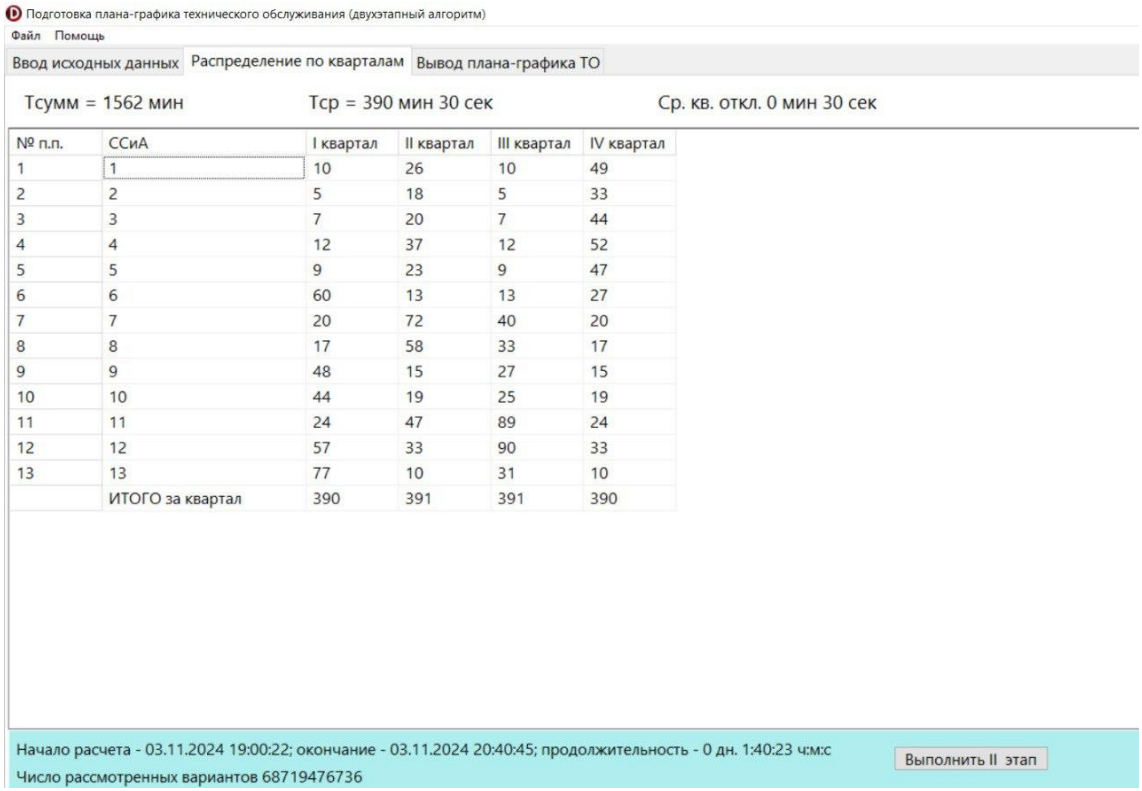
В ходе работы алгоритмов на ПЭВМ (процессор Intel Core i5-8300H CPU 2.30 GHz, оперативная память 8 ГБ, ОС Windows 10 Корпоративная) получены следующие результаты эксперимента (см. таблицу ниже).

Таблица 3

Результаты эксперимента

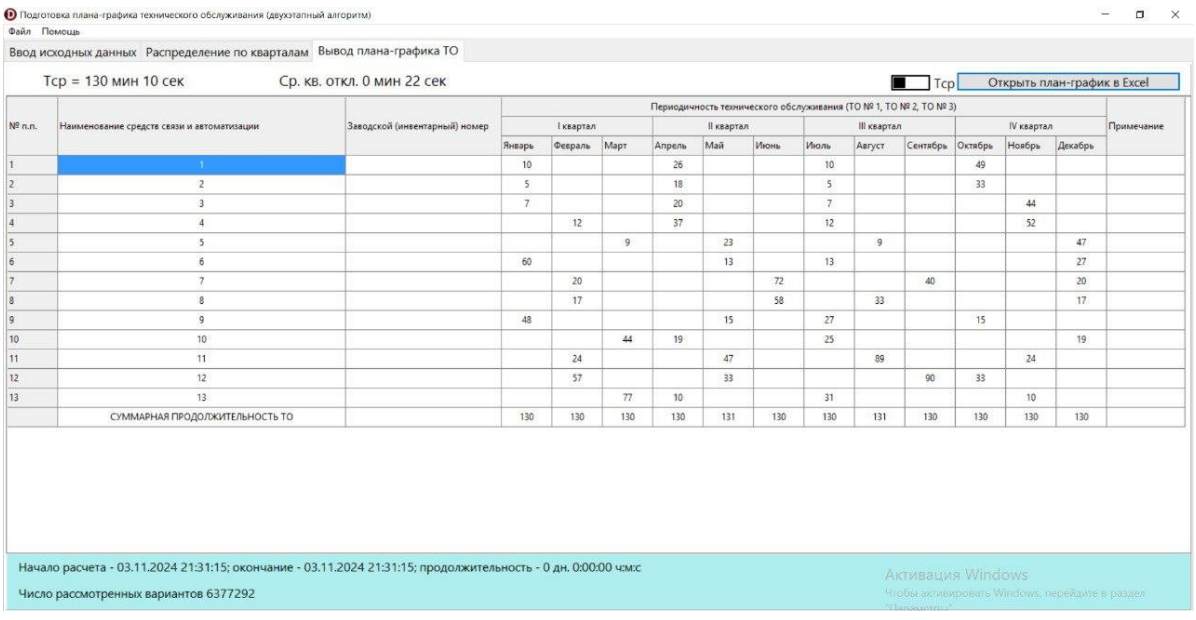
№ п/п	Кол-во ССиА	Полный перебор	Эвристический алгоритм	Двухэтапный алгоритм
1.	1	0	0	0
2.	2	0	0	0
3.	3	1 мин 7 сек	0	0
4.	4	52 ч 6 мин 8 сек	0	0
5.	5	-	0	0
6.	6	-	48 сек.	0
7.	7	-	5 ч. 8 мин. 14 сек.	0
8.	8	-	-	0
9.	9	-	-	8 сек.
10.	10	-	-	1 мин. 12 сек.
11.	11	-	-	9 мин. 54 сек.
12.	12	-	-	1 ч. 29 мин. 9 сек.
13.	13	-	-	1 ч. 40 мин. 23 сек.

На рисунке 1 и 2 представлены результаты работы программы по построению плана-графика двухэтапным алгоритмом для 13 ССиА.



№ п.п.	ССиА	I квартал	II квартал	III квартал	IV квартал
1	1	10	26	10	49
2	2	5	18	5	33
3	3	7	20	7	44
4	4	12	37	12	52
5	5	9	23	9	47
6	6	60	13	13	27
7	7	20	72	40	20
8	8	17	58	33	17
9	9	48	15	27	15
10	10	44	19	25	19
11	11	24	47	89	24
12	12	57	33	90	33
13	13	77	10	31	10
	ИТОГО за квартал	390	391	391	390

Рис. 1. Распределение по кварталам (двухэтапный алгоритм)



№ п.п.	Наименование средств связи и автоматизации	Заводской (инвентарный) номер	Периодичность технического обслуживания (ТО № 1, ТО № 2, ТО № 3)												Примечание
			I квартал			II квартал			III квартал			IV квартал			
			Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь	
1	1		10			26			10			49			
2	2		5			18			5			33			
3	3		7			20			7				44		
4	4			12		37			12				52		
5	5				9		23			9				47	
6	6		60				13		13					27	
7	7			20				72			40			20	
8	8			17				58		33				17	
9	9		48				15		27			15			
10	10				44	19			25					19	
11	11			24			47			89			24		
12	12			57			33				90	33			
13	13				77	10			31				10		
	СУММАРНАЯ ПРОДОЛЖИТЕЛЬНОСТЬ ТО		130	130	130	130	131	130	130	131	130	130	130	130	

Рис. 2. План-график (двухэтапный алгоритм)

Таким образом, двухэтапный алгоритм несомненно превосходит другие рассмотренные методы. Однако, его применение возможно лишь при незначительном числе средств связи и автоматизации, используемых в подразделениях органов внутренних дел. Требуются дополнительные

исследования по разработке эффективных вычислительных методов и алгоритмов построения оптимального плана-графика технического обслуживания ССиА с применением современных компьютерных технологий.

ЛИТЕРАТУРА

1. Организация технической эксплуатации защищенных систем связи : учебник / О. В. Пьянков / Воронеж : Воронежский институт МВД России, 2024. – 109 с. ISBN 978-5-00229-094-9. Текст: непосредственный.
2. Об утверждении Наставления по технической эксплуатации средств связи и автоматизации территориальных органов Министерства внутренних дел Российской Федерации : приказ МВД России № 772. – СТРАС «ЮРИСТ» (дата обращения: 20.08.2024). Текст: электронный.
3. Пьянков О.В. Разработка алгоритма оптимизации технического обслуживания средств связи и автоматизации / О.В. Пьянков, А.А. Быковских // Вестник Воронежского института МВД России – 2024. – № 3. – С. 68-75.
4. URL: https://www.embarcadero.com/ru/products/delphi/starter – Delphi 12 Community Edition (дата обращения: 01.10.2024).
5. Аттетков, А. В. Методы оптимизации : учеб. для вузов / А. В. Аттетков, С.В. Галкин, В. С. Зарубин / под ред. В. С. Зарубина, А. П. Крищенко. – Москва : МГТУ им. Н.Э. Бауман, 2003. – 440 с. – Текст: непосредственный.

СВЕДЕНИЯ ОБ АВТОРЕ

Пахомова Ангелина Александровна. Инженер кафедры инфокоммуникационных систем и технологий.
Воронежский институт МВД России.
E-mail: pahomova.angelina2013@yandex.ru
Россия, 394065, г. Воронеж, пр. Патриотов, 53.

Pakhomova Angelina Alexandrovna. Engineer of the Department of Information and Communication Systems and Technologies.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: pahomova.angelina2013@yandex.ru
Work address: Russia, 394065, Voronezh, Patriotov Avenue, 53.

Ключевые слова: техническое обслуживание; план-график; эвристические правила; оптимизация; вычислительный эксперимент.

Key words: maintenance; schedule; heuristic rules; optimization; computational experiment.

УДК 519.6

Попов Алексей Вячеславович,
кандидат технических наук;
Кучеряева Валерия Романовна

АНАЛИЗ ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ

ANALYSIS OF DESIGN OF A SECURE TELECOMMUNICATION SYSTEM

Статья посвящена рассмотрению вопросов проектирования защищенной телекоммуникационной системы органов внутренних дел. Рассмотрены основные элементы архитектуры безопасной телекоммуникационной системы.

The article is devoted to the consideration of issues of designing a secure telecommunications system for internal affairs agencies. The main elements of the architecture of a secure telecommunications system are considered.

В настоящее время телекоммуникационные системы стали неотъемлемой частью обеспечения надежного и безопасного обмена информацией. Это особенно важно для государственных органов, таких как органы внутренних дел, где высокий уровень защиты информации и связи является ключевым фактором для поддержания общественного порядка и защиты населения. К примеру, отдел полиции №5 МВД России по городу Воронеж, выполняя важную функцию в системе правоохранительных органов, требует надёжной и защищённой телекоммуникационной сети, которая сможет противостоять современным угрозам безопасности.

Значимость разработки системы защиты в сфере телекоммуникаций возрастает по мере усиления киберугроз, роста объемов информационных потоков и потребности в соответствии с законодательством о защите информации [1]. Современная телекоммуникационная инфраструктура не должна ограничиваться лишь скоростью и качеством связи, она также должна гарантировать безопасность передаваемых данных, защищая их от неавторизованного доступа, утечек и прочих рисков.

Телекоммуникационные системы – это комплекс оборудования, программного обеспечения и технологических решений, предназначенных для эффективной передачи информации на дальние расстояния [2]. Такие системы служат для моментального или запрограммированного обмена данными между разнообразными устройствами и пользователями, гарантируя бесперебойное взаимодействие в режиме онлайн или посредством отложенного обмена сообщениями.

Основными компонентами телекоммуникационных систем являются [3]:

1) передающие устройства (например, телефоны, модемы, радиостанции);

2) приемные устройства (например, компьютеры, телефоны);

3) сети передачи данных (например, телефонные сети, интернет, спутниковые сети);

4) программное обеспечение для обработки и управления данными.

Обеспечение безопасности данных в системах связи стоит в ряду приоритетных задач, так как это гарантирует сохранение секретности, неприкосновенности и возможность доступа к информации.

Исходя из этого, можно сказать, что основные принципы защиты информации включают в себя:

1) обеспечение конфиденциальности;

2) обеспечение целостности;

3) обеспечение доступности;

4) аутентификацию;

5) мониторинг и реагирование;

6) обучение и осведомленность;

7) политики и процедуры (например, разработка политик безопасности, соблюдение стандартов для управления информационной безопасностью);

8) физическая безопасность.

В эпоху стремительных технологических прогрессов и роста уровня угроз для безопасности, телекоммуникационные сети остро нуждаются в внедрении передовых защитных технологий и средств.

Рассмотрим следующие ключевые технологии и средства, используемые для обеспечения безопасности телекоммуникационных систем [4]:

1) шифрование данных (например, симметричное и асимметричное шифрование, VPN);

2) системы предотвращения и обнаружения вторжений (например, IDS (Intrusion Detection System)), IPS (Intrusion Prevention System));

3) файрволы (например, аппаратные, программные или следящие файрволы);

4) аутент ификация и контроль доступа (например, многофакторная аутентификация, системы управления доступом);

5) антивирусные и антишпионские программы (например, антивирусные решения, антифишинг);

6) системы резервного копирования и восстановления;

7) облачные технологии и безопасность;

8) искусственный интеллект и машинное обучение.

Основные элементы архитектуры безопасной телекоммуникационной системы состоят из нескольких важнейших компонентов [3]:

1) сетевое оборудование (маршрутизаторы, коммутаторы, точки доступа, которые гарантируют обмен информацией между сетевыми узлами);

2) системы безопасности периметра (системы обнаружения и предотвращения атак (IPS), отслеживающие и фильтрующие поток данных, защищая сеть от внешних атак);

3) технологии шифрования (аппаратные и программные средства для кодирования информации во время передачи и хранения, что гарантирует её секретность);

4) серверы и хранилища данных (безопасные серверы, где размещаются ключевые приложения и базы данных, а также системы резервного копирования для защиты информации);

5) персональные компьютеры и мобильные устройства (средства, используемые сотрудниками для доступа к информации и приложениям, которые должны быть защищены антивирусной защитой и инструментами контроля доступа).

Архитектура защищенной телекоммуникационной системы может быть структурирована по уровням [4]:

1) физический уровень (включает в себя физическое оборудование, такое как серверы, маршрутизаторы, коммутаторы и другие устройства);

2) сетевой уровень (отвечает за передачу данных между устройствами и включает в себя сетевые протоколы, маршрутизацию и управление трафиком);

3) прикладной уровень (включает в себя программное обеспечение и приложения, используемые для работы с данными);

4) уровень управления и мониторинга (включает в себя системы, отвечающие за управление безопасностью, мониторинг активности в сети и реагирование на инциденты).

Разработка схемы защиты информации включает несколько этапов:

1) анализ угроз и уязвимостей;
2) определение требований к безопасности;
3) разработка архитектуры защиты;
4) внедрение и тестирование;
5) мониторинг и обновление.

Таким образом, дальнейшие исследования в данной области могут быть направлены на изучение инновационных методов защиты данных и создание стратегий для объединения различных систем безопасности в единую защищенную структуру. Это позволит системе быть гибкой в ответ на эволюцию киберугроз и усилит её защитные качества против потенциальных атак.

ЛИТЕРАТУРА

1. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ. – Текст :

электронный. // URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 04.11.2024).

2. О связи : Федеральный закон от 7 июля 2003 г. № 126-ФЗ. – Текст : электронный. // URL: https://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 04.11.2024).

3. Барановская, Т. П. Архитектура компьютерных систем и сетей / Т. П. Барановская, В. И. Лойко. – Москва : Финансы и статистика, 2013. – 256 с. – Текст : непосредственный.

4. Крухмалев, В. В. Основы построения телекоммуникационных систем и сетей: учебное пособие для вузов / В. В. Крухмалев. – Москва : ИнформоКомКнига, 2012. – 310 с. – Текст : непосредственный.

СВЕДЕНИЯ ОБ АВТОРАХ

Попов Алексей Вячеславович. Преподаватель кафедры инфокоммуникационных систем и технологий. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: Alex_std_ex@mail.ru

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

Кучерява Валерия Романовна. Слушатель 5 курса радиотехнического факультета.

Воронежский институт МВД России.

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

Popov Aleksey Vyacheslavovich. Lecturer of Infocommunication systems and technologies Department. Candidate of Technical Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: Alex_std_ex@mail.ru

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

Kucheryava Valeria Romanovna. 5th year student at the Faculty of Radio Engineering.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

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

Ключевые слова: проектирование; телекоммуникационная система; сетевое оборудование; защита информации.

Key words: design; telecommunication system; network equipment; information security.

УДК 004

Попов Алексей Вячеславович,
кандидат технических наук;
Гаджиев Шахбан Гамзатович

РАЗРАБОТКА МОДЕЛИ АНАЛИЗА СЕТЕВОЙ ИНФРАСТРУКТУРЫ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

DEVELOPMENT OF A MODEL FOR ANALYSING THE NETWORK INFRASTRUCTURE OF INTERNAL AFFAIRS BODIES

В работе используется системный подход к исследованию и анализу сетевой инфраструктуры органов внутренних дел. Разрабатывается модель реализации комплекса мероприятий по выявлению и устранению неисправностей в сетях связи. В качестве примера реализации модели рассматривается использование сетевых сканеров для обеспечения безопасности узлов сети.

The paper uses a systematic approach to research and analyse the network infrastructure of internal affairs bodies. The model of implementation of a set of measures to identify and eliminate faults in communication networks is developed. The use of network scanners to ensure the security of network nodes is considered as an example of the model implementation.

Оценка эффективности сети связи важна для принятия управленческих решений по оптимизации производительности и обеспечения ее надежности при проведении мероприятий по охране общественного порядка и обеспечению общественной безопасности. Для органов внутренних дел обеспечение безопасности сетевой инфраструктуры является приоритетной задачей. Сети связи МВД России содержат критически важные данные, которые требуют высокого уровня защиты от несанкционированного доступа и кибератак. В целях повышения оперативности реализации комплекса мероприятий по выявлению и устранению неисправностей в сетях связи предложим модель M, представляющую собой кортеж:

$$M = \langle C, P, S, O, K, \rangle,$$

где $C = \{c_1, c_2, \dots, c_n\}$ – множество целей сканирования; $P = \{p_1, p_2, \dots, p_n\}$ – множество используемых программно-аппаратных средств для сканирования и достижения целей c_i; $S = \{s_1, s_2, \dots, s_n\}$ – множество типов сканирования; $O = \{o_1, o_2, \dots, o_n\}$ – множество используемых опций; $K = \{k_1, k_2, \dots, k_n\}$ – множество сетевых параметров.

К элементам c_i множества C можно отнести:

– c_1 – определение несанкционированных узлов в сети,

– c_2 – проверка доступности всех необходимых узлов,

– c_3 – обеспечение безопасности узлов сети,

– и другие;

к элементам $p_i \in P$:

– p_1 – Network Mapper (Nmap) – утилита с открытым исходным кодом для исследования сети и проверки безопасности, которая была разработана для исследования сети и проверки безопасности [4],

– p_2 – Netcat – сетевая утилита, используемая для чтения и записи данных по сети через TCP или UDP протоколы,

– p_3 – Nessus – сетевой сканер уязвимостей, предназначенный для обнаружения и оценки уязвимостей в сетевых устройствах,

– p_4 – Advanced IP Scanner – инструмент сканирования сети, предназначенный для быстрого и эффективного обнаружения устройств в локальной сети и получения информации от них;

– и другие;

к элементам $s_i \in S$:

– s_1 – TCP Connect Scan – установление полного TCP-соединения с целевым портом,

– s_2 – TCP SYN Scan – отправка SYN-пакета на целевой порт,

– s_3 – TCP Null Scan – отправка TCP-пакета с пустыми флагами,

– s_4 – TCP FIN Scan – отправка TCP-пакета с флагом FIN, для обнаружения фильтрующих межсетевых экранов,

– s_5 – TCP Xmas Scan – отправка TCP-пакета с флагами FIN, PSH и URG, для обнаружения фильтрующих межсетевых экранов,

– s_6 – TCP ACK Scan – отправка TCP-пакета с флагом ACK, для определения межсетевых экранов и их конфигурации,

– s_7 – UDP Scan – отправка UDP-пакета с целью обнаружения открытых UDP-портов,

– s_8 – ICMP Echo Scan – отправка ICMP Echo Request-пакетов, для обнаружения активных устройств,

– s_9 – ARP Scan – использование Address Resolution Protocol (ARP) для обнаружения устройств в локальной сети,

– s_{10} – SNMP Scan – использование Simple Network Management Protocol для получения информации о сетевых устройствах [2];

Положим, что в процессе эксплуатации сети связи у нас появляется необходимость выявить уязвимости сети, чтобы в дальнейшем их устранить. В таком случае, используя предложенную модель, определяем цель c_3, достижение которой может быть осуществлено согласно схеме (рис. 1).

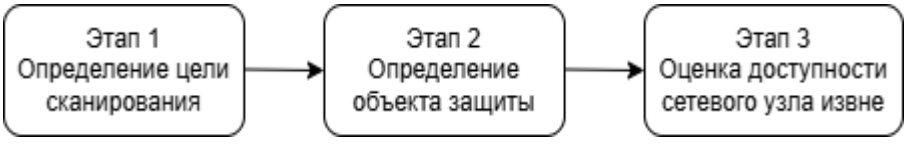


Рис. 1. Поэтапная схема обеспечения безопасности узлов сети

В частном случае в качестве объекта сканирования на этапе 2 выберем используемый в организации ubuntu-сервер. Выполнение 3 этапа сопряжено с использованием сетевых сканеров (утилит) p_1, p_2, p_3, p_4.

Из представленного перечня выберем p_1 (Nmap). Данная утилита полезна в области сетевой безопасности и администрирования. При помощи данной утилиты можно использовать различные методы сканирования. Данные методы используются в зависимости от конкретных требований и условий сканирования сети. Nmap обладает такими преимуществами, как:

– поддержка скриптов. Пользователь утилиты может использовать готовые скрипты или писать их самому для оптимизации задач по сканированию сети,

– утилита используется в различных операционных системах, таких как Linux, Windows и в Unix-подобных системах,

– для упрощения работы существует графический интерфейс утилиты Nmap под названием Zenmap,

– поддержка сканирования как IPv4, так и IPv6 сетей,

– Nmap имеет обширную документацию на официальном сайте;

Поскольку был выбран Nmap, для него характерны типы сканирования s_1, s_2, s_3, s_4, s_5 и s_6. Для достижения c_1 рационально использовать s_2, потому что SYN-сканирование быстрее и эффективнее, так как оно не требует полного установления соединения.

К опциям $o_i \in O$, используемым для достижения цели c_3, можно отнести:

– o_1 – -o (определение операционной системы),

– o_2 – -sV (определение версии используемого сервиса);

Данные опции будем использовать со следующими сетевыми параметрами $k_i \in K$:

– k_1 – тайм-ауты (--host-timeout),

– k_2 – скорость сканирования (-T4),

– k_3 – максимальное количество попыток сканирования (--max-retries);

Результат выполнения данной модели представлен на рисунке 2.

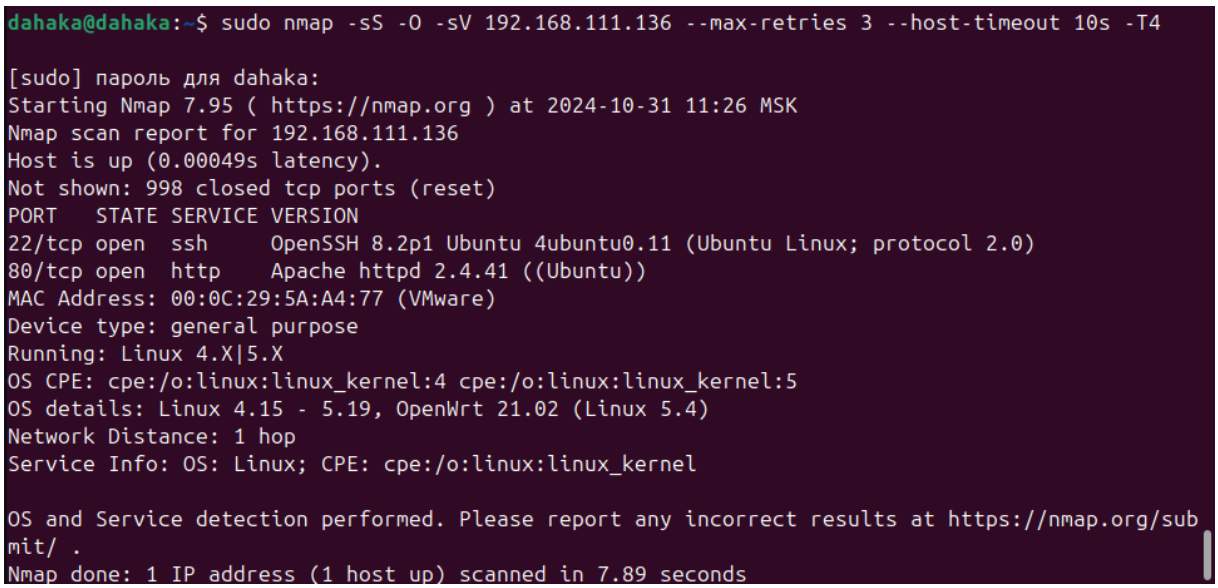


Рис. 2. Результаты реализации модели М

В результате мы получаем вывод информации об открытых портах, используемых сервисов и их версии. Также узнаем физический адрес устройства данной сети, используемую операционную систему и количество “скачков” до сканируемой сети.

Предложенная модель М позволяет повысить уровень безопасности и надежности сетевой инфраструктуры. Использование данной модели повышает оперативность реагирования на возникающие проблемы, используя системный подход к обеспечению безопасности, что способствует более эффективному управления сетевыми ресурсами и повышению общей эффективности работы правоохранительных органов. Внедрение подобных методов и инструментов в практику МВД России позволяет значительно улучшить качество и надежность сетевой инфраструктуры.

ЛИТЕРАТУРА

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник/ В. Г. Олифер, Н. А. Олифер. – Санкт-Петербург : Питер, 2021. – 1008с.

2. Зайцев А.П. Технические средства и методы защиты информации: учебник/ А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов – Москва: Горячая Линия – Телеком, 2018 – 442с.

3. Kaufman, C., Perlman, R., Speciner, M. Network Security: Private Communication in a Public World. — N. Y.: Prentice Hall, 2002. — 576 p.

4. Документация для пользователей утилиты Nmap: официальный сайт [Электронный ресурс]. – URL: https://nmap.org/ (дата обращения: 06.11.2024)

СВЕДЕНИЯ ОБ АВТОРАХ

Попов Алексей Вячеславович. Старший преподаватель кафедры инфокоммуникационных систем и технологий. Кандидат технических наук.
Воронежский институт МВД России.
E-mail: Alex_std_ex@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Popov Alexey Vyacheslavovich. Senior Lecturer, Department of Info-communication Systems and Technologies. Candidate of technical Sciences.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: Alex_std_ex@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Гаджиев Шахбан Гамзатович. Слушатель.
Воронежский институт МВД России.
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Gadzhiev Shahban Gamzatovich. Cadet.
Voronezh Institute Ministry of Internal Affairs of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: сети связи; модель; сетевой сканер; оптимизация; сетевая инфраструктура.

Key words: communication networks; model; network scanner; optimization; network infrastructure.

УДК 519-7

Пучков Геннадий Юрьевич
кандидат технических наук
ФКУ НПО «СТиС» МВД России

АНАЛИЗ ИССЛЕДОВАНИЙ В ОБЛАСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА, ПРОВЕДЕННЫХ В СИСТЕМЕ МВД РОССИИ В ПЕРИОД С 2020 ПО 2024 ГОД

ANALYSIS OF RESEARCH IN THE FIELD OF ARTIFICIAL INTELLIGENCE, CONDUCTED IN THE SYSTEM OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA DURING THE PERIOD FROM 2020 TO 2024

Аннотация*. В статье проводится анализ результатов исследований в области применения технологий искусственного интеллекта, проведенных в системе МВД России в период с 2020 по 2024 годы. Рассмотрены основные научные достижения и направления использования ИИ в борьбе с преступностью, включая анализ больших данных, выявление серийности преступлений, идентификацию личности по биологическому материалу и компьютерное зрение. Сделаны выводы о перспективах дальнейшего использования*
ИИ в ОВД РФ, определены направления внедрения технологий ИИ в деятельность ОВД РФ.

Abstract*. The article analyzes the results of research in the field of application of artificial intelligence technologies conducted in the system of the Ministry of Internal Affairs of the Russian Federation in the period from 2020 to 2024. The main scientific achievements and areas of AI use in the fight against crime are considered, including big data analysis, identifying serial crimes, identifying individuals by biological material and computer vision. Conclusions are made on the prospects for further use of AI in the Russian Internal Affairs Department, and directions for the implementation of AI technologies in the activities of the Russian Internal Affairs Department are determined.*

В последние годы искусственный интеллект (далее – ИИ) стал одной из ключевых технологий, определяющих дальнейшее развитие различных сфер общественной жизни. Учитывая, что общество становится все более зависимым от информационных ресурсов, злоумышленники перенесли существенную часть своей деятельности в информационное пространство, где начали активно использовать современные достижения в области ИИ.

Преступления в сети Интернет с использованием ИИ с каждым годом занимают все более заметное место в структуре всех зарегистрированных преступлений в стране. Если в 2018 году их удельный вес составлял порядка 9%,

то уже в 2023 году - почти 35 %. Наибольшее количество таких преступлений (почти 70 %) связано с хищениями собственности.

В системе МВД России исследования в области противодействия преступлениям с использованием ИИ находятся в настоящее время на начальной стадии своего развития. Период с 2020 по 2024 год можно охарактеризовать как первые попытки осознания, что такое ИИ и каким образом технологии ИИ могут быть использованы в борьбе с преступностью.

Цель настоящей статьи — проанализировать результаты и достижения исследований в области искусственного интеллекта, проведенных в системе МВД России в указанный период. Мы рассмотрим основные результаты, полученные в рамках этих исследований, а также попробуем сформулировать основные направления развития ИИ, которые могут быть использованы в борьбе с преступностью.

В период 2020 – 2024 годы в системе МВД России осуществлялись научно-технические и организационные мероприятия по реализации двух пилотных проектов федерального проекта «Искусственный интеллект» национальной программы «Цифровая экономика Российской Федерации».

Это исследования по определению индивидуальных анатомических признаков человека на основе анализа биологического материала, изъятого с мест совершения преступлений и исследования по выявлению признаков серийных преступлений.

В целях теоретического обеспечения успешного решения указанных задач ФКУ НПО «СТиС» МВД России выполнена НИР «Теоретические исследования по созданию комплекса технологических решений (искусственный интеллект) для обработки больших данных в сфере внутренних дел», шифр «Семантика».

В ходе выполнения НИР «Семантика» [1] получены следующие новые научные результаты:

исследованы возможности и механизмы применения технологий анализа больших данных, искусственного интеллекта и методов биоинформатики в целях реализации ведомственных пилотных проектов;

разработаны требования к формированию дата-сетов для выявления признаков серийности (сходства) определенных категорий преступлений;

разработаны требования к формированию дата-сетов для определения индивидуальных фенотипических признаков человека на основе анализа биологического материала, изъятого с мест совершения преступлений.

В результате проведенных исследований были разработаны два технических задания на НИР:

«Исследование применимости методов машинного обучения и анализа данных для выявления признаков серийности (сходства) определенных категорий преступлений», шифр «Серия»;

«Формирование требований к проведению работ по разработке методов определения индивидуальных фенотипических признаков человека на основе анализа биологического материала, изъятого с мест совершения преступлений», шифр «Анатомия 1».

В результате выполнения НИР «Серия» [2] было установлено наличие широких возможностей существующих технологий ИИ, способных обеспечить как автоматизацию выявления признаков серийности (сходства) преступлений, так и автоматизацию анализа больших данных, оцифровку текстовых документов, оцифровку и перевод в текстовый вид аудиозаписей и устной речи, выявление требуемой информации в составе документов (сущностей).

В ходе проведенного в рамках НИР «Серия» исследования получены следующие научные результаты:

выбраны и обоснованы способы применения технологий машинного обучения и семантического анализа данных по выявлению признаков серийных (сходных) категорий преступлений;

выбраны и обоснованы категории рассматриваемых преступлений (квартирные кражи, кражи из офиса, кражи транспортных средств);

подготовлены обучающие массивы данных по рассматриваемым категориям преступлений;

разработан макет информационной системы выявления признаков серийности (сходства) определенных категорий преступлений;

сформирован перечень признаков серийности (сходства) определенных категорий преступлений;

разработан макет информационной системы для проверки теоретических результатов исследований и наглядной демонстрации возможностей технологий ИИ, обеспечивающий выявление признаков серийности (сходства) определенных категорий преступлений (квартирных краж, краж из офисов, краж транспортных средств) позволяющий осуществлять выявление и отображение сведений о серийных (сходных) преступлениях:

– в табличном виде с перечислением соответствующих характеристик преступления;

– в виде интерактивного графа, позволяющего визуально определять взаимосвязи между преступлениями;

– на электронной географической карте.

Объектом исследования НИР «Анатомия 1» являлись методы определения индивидуальных фенотипических признаков человека на основе анализа геномной информации биологического материала, отраженные в современной научно-технической, нормативной, методической литературе, включая обзор научных информационных источников.

В ходе исследования получены следующие научные результаты [3]:

проведены теоретические исследования применения технологий искусственного интеллекта, биоинформатики в расследовании и раскрытии преступлений посредством анализа геномной информации;

разработана система классификации и формирования структурированного (формализованного) перечня индивидуальных фенотипических признаков человека с учетом традиционной криминалистической классификации признаков внешности человека;

разработаны требования к формированию анализируемой группы лиц, геномы которых подлежат секвенированию;

предложены требования к порядку сбора (описания) фенотипических признаков и сбору информации;

составлен список признаков, для которых возможно предсказание на основе анализа ДНК по генетическим и эпигенетическим маркерам для дальнейшего практического применения в криминалистике.

На основе результатов выполнения НИР «Серия» и «Анатомия 1» были сделаны следующие выводы:

применение технологий ИИ, позволит существенно повысить эффективность расследования, раскрытия и профилактики преступлений в части установления серийности преступлений, выявления и идентификации личности подозреваемых в совершении преступлений, а также установления личности неопознанных тел, лиц пропавших без вести, жертв террористических актов, природных и техногенных катастроф;

важнейшими условиями достижения эффективности данных мероприятий является наличие квалифицированных кадров в области ИИ и развитие отечественного ИИ в защищенном исполнении;

актуальной задачей в области развития и использования современных технологий искусственного интеллекта в системе МВД России является разработка и принятие следующих документов:

– нормативный правовой акт, регламентирующий применение доверенного искусственного интеллекта в оперативно-служебной деятельности подразделений МВД России;

– административные регламенты применения результатов, полученных с использованием искусственного интеллекта, при выработке процессуальных и управленческих решений;

– глоссарий терминов в области искусственного интеллекта.

В целях определения возможностей использования технологий ИИ для идентификации личности по татуировкам Воронежским институтом МВД России проведена НИР «Применение методов машинного обучения для обнаружения и классификации татуировок на фотоснимках человека», шифр «Татуировка».

В ходе НИР были осуществлены следующие мероприятия:

оценка возможности использования различных типов нейросетевых архитектур для обнаружения (детектирования) и классификации татуировок на фотоснимках человека;

подготовка обезличенного датасета для обучения нейросетевого детектора татуировок на фотоснимках человека;

разработка модели, предсказывающей расположение татуировок на фотоснимках человека и их классы;

подготовка аналитического обзора текущего состояния и перспектив автоматизации процессов обнаружения (детектирования) и классификации

татуировок на фотоснимках человека на основе применения технологий искусственного интеллекта;

анализ методов детектирования и классификации объектов при помощи технологии «компьютерного зрения», в числе которых алгоритмы обучения сверточных нейронных сетей: R-CNN, YOLOv4, SSD.

По результатам НИР:

сделан вывод о том, что для решения задач связанных с обнаружением и классификацией татуировок на фотоснимках человека с использованием методов машинного обучения необходимо использовать технологии компьютерного зрения и сверточные нейронные сети, а именно:

– использование методов каскадов Хаара с помощью библиотеки OpenCV;

– применение алгоритма обучения сверточных нейронных сетей YOLOv4;

установлено:

– алгоритм YOLOv4 позволяет обеспечить точность распознавания 63-78%, характеризуется относительно небольшим размером обученной модели (33,1 Mb) и низкой степенью ошибки, вместе с тем установлено также, что точность работы алгоритма зависит от разрешения изображения - чем выше качество изображения, тем точнее определяется область расположения рисунка и меньше степень ошибки;

– на фотографиях с одиночными изображениями татуировок классификатор с точностью до 98,9% обнаруживает искомый объект;

– с фотографиями человека, значительную часть туловища которого покрыта татуировками, классификаторы работают некорректно - большое количество «ложных» обнаружений предметов, не относящихся к татуировкам;

– оригинальная модель на основе сверточных нейронных сетей (20 слоев свертки) обеспечивает менее 30 процентов распознавания татуировок на тестовых фотографиях;

размечен и классифицирован набор фотографий с изображениями татуировок по классам: «крест», «кот», «тигр», «ангел», «буква», «дракон», «богородица», «звезда» и «змея». Датасет состоит из 2400 размеченных фотографий.

В настоящее время ФКУ НПО «СТиС» МВД России заканчивает НИР «Проведение анализа результатов выполнения Плана реализации основных направлений дальнейшего развития ИСОД МВД России на период с 2020 по 2024 год («дорожная карта»). Разработка предложений в План реализации основных направлений дальнейшего развития ИСОД МВД России на период с 2025 по 2028 годы», шифр «Направление», рамках которой в том числе проведен анализ состояния проблем использования технологий ИИ в деятельности органов внутренних дел Российской Федерации (далее – ОВД РФ), проведен опрос подразделений центрального аппарата МВД России о перспективах их использования в служебно-розыскной деятельности.

По итогом проведенного исследования сделан вывод о том, что в ближайшей перспективе современные технологии в области ИИ будут востребованы в деятельности ОВД РФ для решения следующих задач:

идентификация личности по фото- и видеоизображению;

идентификация личности по дактилоскопической информации;

выявление фейковых изображений;

поддержка процессов принятия решений;

семантическая обработка текстовой информации;

выявление серийного характера преступлений;

борьба с киберпреступностью и противоправным использованием информационно-коммуникационных технологий;

проведение анализа социальных сетей, различных интернет-ресурсов и мессенджеров с целью получения оперативно значимой информации;

оценка поведения человека, зафиксированного камерами видеонаблюдения, на соответствие заданным критериям.

В заключении необходимо отметить, что исследования, проведенные в системе МВД России в период с 2020 по 2024 годы, еще раз подтвердили необходимость и целесообразность применения технологий ИИ в борьбе с преступностью. В ходе выполнения научно-исследовательских работ «Семантика», «Серия», «Анатомия 1» были заложены основы использования ИИ для решения таких задач, как анализ больших данных, выявление серийности преступлений, идентификация личности по биологическому материалу.

Определены перспективы дальнейшего использования ИИ в деятельности ОВД РФ, включая такие направления как идентификация личности по различным биометрическим признакам, автоматизация анализа текстовой информации, борьба с киберпреступностью.

Определены ключевые проблемы, препятствующие активному применению ИИ в деятельности ОВД РФ – это дефицит квалифицированных кадров, слабое развитие отечественных технологий в защищенном исполнении и отсутствие нормативно-правовой базы, регулирующей использование ИИ в правоохранительной деятельности.

ЛИТЕРАТУРА

1. «Теоретические исследования по созданию комплекса технологических решений (искусственный интеллект) для обработки больших данных в сфере внутренних дел». Отчет о НИР «Семантика». – Москва: ФКУ НПО «СТиС» МВД России, 2021. – 125 с.

2. «Исследование применимости методов машинного обучения и анализа данных для выявления признаков серийности (сходства) определенных категорий преступлений». Отчет о НИР «Серия». – Москва: ФКУ НПО «СТиС» МВД России, 2022. – 153 с.

3. «Формирование требований к проведению работ по разработке методов определения индивидуальных фенотипических признаков человека

на основе анализа биологического материала, изъятого с мест совершения преступлений». Отчет о НИР «Анатомия 1» – Москва: ФКУ НПО «СТиС» МВД России, 2021. – 98 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Пучков Геннадий Юрьевич. Ведущий научный сотрудник ЦСИТ НИИСТ. Кандидат технических наук

Федеральное казенное учреждение «Научно-производственное объединение «Специальная техника и связь» МВД России,

E-mail: pgu7@ya.ru

Россия, 111024, Москва, Пруд Ключики, 2.

Puchkov, Gennady Yurievich. A leading researcher at the Scientific Research Institute of Special Technology. Candidate of Technical Sciences.

Federal Government Institution "Scientific and Production Association "Special Equipment and Communications" of the Ministry of Internal Affairs of Russia,

E-mail: pgu7@ya.ru

Russia, 111024, Moscow, Pond Klyuchiki, 2.

Ключевые слова: искусственный интеллект, серийные преступления, биометрическая идентификация, компьютерное зрение, киберпреступность, татуировки, геномный анализ.

Keywords: artificial intelligence; serial crimes; biometric identification, computer vision, cybercrime, tattoos, genomic analysis.

УДК 004.896

Терентьев Александр Андреевич,
кандидат технических наук;
Казанцева Ева Алексеевна

ВЫБОР ОПТИМАЛЬНОГО ОБОРУДОВАНИЯ ДЛЯ ОРГАНИЗАЦИИ СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

SELECTION OF OPTIMAL EQUIPMENT FOR THE ORGANIZATION OF A SPECIAL-PURPOSE COMMUNICATION NETWORK

Данная статья рассматривает подбор оборудований от разных производителей, состоящих на снабжении органов внутренних дел, расчет по методу попарного сравнения по определенным показателям, как сравнение устройств между собой, так и критерий. Определение значений вектора

приоритета и глобального вектора для выведения результатов о наилучшем оборудовании.

This article examines the selection of equipment from different manufacturers that supply law enforcement agencies, the calculation using the pairwise comparison method for certain indicators, both the comparison of devices with each other, and the criterion. Determining the values of the priority vector and the global vector to derive results about the best equipment.

Система специальной связи, на данный момент одно из важных аспектов функционирования органов внутренних дел. Для любого подразделения ОВД является главным критерием иметь защищенный канал передачи данных для осуществления своих непосредственных обязанностей по защиты граждан и обеспечение общественной безопасности. Для организации сегмента сети связи специального назначения требуется использовать средства, которые удовлетворяют всем требованиям предъявляемые современным обществом. На основании этого предлагается осуществить выбор актуальных средств связи при помощи математического аппарата – методом анализа иерархии [1, 2] для организации сегмента сети связи специального назначения.

В качестве критериев по котором будет осуществляется выбор оборудования предлагается использовать: пропускную способность и защищенность. При этом важным фактором является то, что данное оборудование обязательно должно быть допущено к использованию в системе МВД России. На основании проанализированным нормативно-правовых документов, сформируем перечень сетевого оборудования:

1. Маршрутизатор:
– Eltex;
– Huawei;
– D-Link;
2. Коммутатор:
– Eltex;
– Huawei;
– D-Link;
3. ПК устройства:
– IRU;
– KIOSK;
– DEPO.

Прежде чем приступать к методу принятия решений по подбору оборудований, сначала рассмотрим технические характеристики. В пример расчётов и характеристик будем рассматривать коммутаторы (табл. 1-3). С остальными характеристиками устройств можно ознакомиться на официальных сайтах производителей [3-5].

Таблица 1

Характеристики коммутатора Eltex MES2308P

Параметры	Значения
Пропускная способность	24 Гбит/с
Производительность на пакетах длиной 64 байта	17,7 MPPS
Таблица MAC-адресов	16384
Количество ARP-записей	820
Таблица VLAN	4094

Таблица 2

Характеристики коммутатора Huawei CloudEngine 8850-HAM

Параметры	Значения
Коммутационная ёмкость	19.2 Тбит/сек
Скорость передачи	4350 млн пакетов в секунду
Порты	32 порта 40/100GE QSFP28 или 32 порта 200 GE QSFP56, 8 портов 400GE QSFP-DD
IP маршрутизация	IPv4, IPv6
Количество портов	32
Тип коммутатора	Управляемый (Layer 3)

Таблица 3

Характеристики коммутатора D-Link DGS-3130-30S/DC

Параметры	Значения
Процессор	1,25 ГГц
Оперативная память	2 ГБ

Flash-память	256 МБ
Интерфейсы	24 порта 1000Base-X SFP 2 порта 10GBase-T 4 порта 10GBase-X SFP+ Консольный порт с разъемом RJ-45
Размер таблицы MAC-адресов	16K записей

Характеристики данных оборудований известны нам заранее. Теперь сравним показатели критериев между собой методом попарного сравнения. Для осуществления экспертного опроса воспользуемся фундаментальной шкалой [1], значения оценок будет от 1 до 9 и от 1/2 до 1/9. Согласно данному методу будет производится сравнение и выставляться оценка согласно фундаментальной шкале. Дадим определения критериям:

1. Пропускная способность – это показатель, который характеризует максимальную скорость передачи данных по выделенному каналу связи.

2. Защищенность – это уровень защиты информации, объектов и систем от несанкционированного доступа (НСД), злоумышленного воздействия, кибератак и других атак.

Первым этапом мы сравниваем показатели (табл. 4).

Таблица 4

Сравнение показателей между собой методом попарного сравнения

Показатели	S	D
S	1	3
D	1/3	1

S – максимальная пропускная способность;

D – защищенность.

Исходя из сравнения получаем итоговое значение – вектор приоритета (ВП) (табл. 5).

Таблица 5

Итоговое значение ВП

Показатели	ВП
S	0,596

D	0,308

Следующим этапом будет сравнение оборудований между собой для определения, наиболее подходящего для нас устройства. Как пример, возьмем коммутаторы и сравним их по установленным нами критериям. Сперва по критерию S (табл. 6).

Таблица 6

Сравнение коммутаторов, по показателю S

S	Коммутатор Eltex MES2308P	Коммутатор Huawei CloudEngine 8850-HAM	Коммутатор D-Link DGS-3130-30S/DC	ВП
Коммутатор Eltex MES2308P	1	7	8	0,777
Коммутатор Huawei CloudEngine 8850-HAM	1/7	1	3	0,153
Коммутатор D-Link DGS-3130-30S/DC	1/8	1/3	1	0,07

Значения приоритетов соответственно будут равны:

$$v_{\text{ком\_}S} = (0{,}777;\ 0{,}153;\ 0{,}07). \quad (1)$$

Аналогично проведем сравнение по показателю D (табл. 7).

Таблица 7

Сравнение коммутаторов, по показателю D

D	Коммутатор Eltex MES2308P	Коммутатор Huawei CloudEngine 8850-HAM	Коммутатор D-Link DGS-3130-30S/DC	ВП
Коммутатор Eltex MES2308P	1	7	8	0,777
Коммутатор Huawei CloudEngine 8850-HAM	1/7	1	3	0,153
Коммутатор D-Link DGS-3130-30S/DC	1/8	1/3	1	0,07

Значения приоритетов соответственно будут равны:

$$v_{\text{ком}\_D} = (0{,}756;\ 0{,}188;\ 0{,}056). \quad (2)$$

В заключении рассчитаем глобальный вектор, методом сравнения показателей и оборудований между собой, в котором и определим какое устройство будет использоваться в дальнейшем (табл. 8).

Таблица 8

Соотношение коммутатора и показателей

	S	D	Глобальные приоритеты
Коммутатор Eltex MES2308P	0,777·0,596=0,463	0,756·0,308=0,233	0,775
Коммутатор Huawei CloudEngine 8850-HAM	0,153·0,596=0,091	0,188·0,308=0,058	0.156

Коммутатор D-Link DGS-3130-30S/DC	0,07·0,596=0,042	0,056·0,308= 0,017	0.069

Выше были указаны остальные оборудования, которые аналогично данного мы примеру был произведен расчет. Подведем заключительные значения, исходя из наших вычислений.

Выбор коммутатора:

$$v_{\text{ком\_}S} = (0{,}741;\ 0{,}191;\ 0{,}069). \quad (3)$$
$$v_{\text{ком\_}D} = (0{,}747;\ 0{,}194;\ 0{,}059). \quad (4)$$
$$v_{\text{ком\_ГП}} = (0{,}742;\ 0{,}191;\ 0{,}067). \quad (5)$$

Выбор маршрутизатора:

$$v_{\text{маршр\_}S} = (0{,}757;\ 0{,}188;\ 0{,}054). \quad (6)$$
$$v_{\text{маршр\_}D} = (0{,}723;\ 0{,}206;\ 0{,}071). \quad (7)$$
$$v_{\text{маршр\_ГП}} = (0{,}754;\ 0{,}190;\ 0{,}056). \quad (8)$$

Выбор пользовательского компьютера:

$$v_{\text{пк\_}S} = (0{,}067;\ 0{,}160;\ 0{,}773). \quad (9)$$
$$v_{\text{пк\_}D} = (0{,}057;\ 0{,}166;\ 0{,}777). \quad (10)$$
$$v_{\text{пк\_ГП}} = (0{,}061;\ 0{,}170;\ 0{,}769). \quad (11)$$

В заключение сделаем следующий вывод: наиболее предпочтительным перечнем сетевых устройств при организации сегмента сети связи специального назначения в органах внутренних дел является:

– Коммутатор Eltex MES2308P;
– Маршрутизатор Eltex ESR-3100;
– ПК SZKIOSK PC4-21300.

Следует отметить, что все три позиции выделенного оборудования в процессе экспертного опроса является либо оборудованием российского производства, либо в списке разрешенного импорт замещённого оборудования. По сегодняшней ситуации в стране, а также в ближайших к ней регионах, этот факт является одним из преобладающим над другими.

ЛИТЕРАТУРА

1. Саати Т.Л. Принятие решений при зависимостях и обратных связях: Аналитические сети. Пер. с англ. / Науч. ред. А. В. Андрейчиков, О. Н. Андрейчикова. Изд. 3-е. – Москва : Книжный дом «ЛИБРОКОМ», 2011. – 360 с.

2. Терентьев А. А. Применение метода анализа иерархий для оценки степени конфликтности элементов инфокоммуникационных систем органов внутренних дел / А. А. Терентьев // Охрана, безопасность, связь. 2019. – № 4-2. – С. 73-77.

3. Eltex коммуникации. Официальный дилер Eltex. – URL: https://eltexcm.ru (дата обращения: 05.11.2024).

4. Huawei. – URL: https://www.huawei.ru/?ysclid=m559hs64v348611612 (дата обращения: 05.11.2024).

5. D-link/ – URL: https://dlink.ru/?ysclid=m559ll1s2l111318948 (дата обращения: 05.11.2024).

СВЕДЕНИЯ ОБ АВТОРАХ

Терентьев Александр Андреевич. Старший преподаватель кафедры инфокоммуникационных систем и технологий. Кандидат технических наук.
Воронежский институт МВД России.
E-mail: Alextt02021993@yandex.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

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

Terentev Aleksandr Andreevich. Senior lecturer of the chair of Infocommunication Systems and Technologies. Candidate of Technical Sciences.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: Alextt02021993@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

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

Ключевые слова: система связи специального назначения; максимальная пропускная способность; защищенность; вектор приоритета; глобальный вектор.

Key words: special purpose communication system; maximum bandwidth; security; priority vector; global vector.

УДК 519.816

Терентьев Александр Андреевич,
кандидат технических наук;
Купавцева Дарья Вячеславовна

КИБЕРПРЕСТУПЛЕНИЯ. СПОСОБЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ В 21 ВЕКЕ

CYBERCRIMES. WAYS TO COUNTER CYBERCRIME IN THE 21ST CENTURY

В статье рассмотрено понятие киберпреступлений, сущность и способы противодействия. Причины и факторы, способствующие росту киберпреступлений. Представлены рекомендации для борьбы с данной проблемой.

The article discusses the concept of cybercrimes, the essence and methods of counteraction. Causes and factors contributing to the growth of cybercrime. Recommendations for dealing with this problem are presented.

Век информационных технологий и цифровизации заставляет пересматривать нашу жизнь. Значительные изменения, которые распространяются в том числе на криминальную среду, создают новые возможности для развития новых способов совершения преступлений. С каждым годом объём и сложность киберугроз и кибератак растет, что ставит под сомнение безопасность личных данных. Сейчас же сеть, которая имеет много достоинств, порождает уязвимость общественных и государственных интересов. Это выражается в активном использовании всемирной «паутины» для организации беспорядков посредством телекоммуникации и повседневного использования интернета. Получается, что новые технологии могут сделать каждого жертвой киберпреступлений?

Для того чтобы противостоять виртуальной, но реальной угрозе, нужно знать о методах, которые используются преступниками и уметь правильно реагировать на них [1].

Киберпреступность охватывает широкий спектр противозаконных действий, включая несанкционированный доступ к данным, кражу личной информации, мошенничество, атаки на компьютерные сети и многие другие формы преступной деятельности, осуществляемой с использованием цифровых технологий.

Актуальность изучения киберпреступлений обуславливается не только уровнями угрозы, но и значительным воздействием на общественную безопасность и личные права граждан.

Киберпреступления представляют собой использование компьютерных и информационных технологий, а также генной инженерии, радиоэлектроники

в целях совершения преступлений, реализовывая сетевой принцип функционирования и распространения, с целью нарушения работы системы контроля и потери конфиденциальной информации и получения определенной выгоды. Их классификация может быть выполнена по нескольким критериям:

– По типу взаимодействия: киберпреступления включают внутренние преступления и внешние.

– По цели могут быть направлены на кражу данных, нанесение ущерба, финансовое мошенничество, шантаж.

– По методам осуществления: включают фишинг, вредоносное ПО, атаки «отказ в обслуживании» (DDoS), социальную инженерию и др.

Рост цифровизации и внедрение новых технологий вводит новые понятия, такие как Интернет вещей (IoT), облачные вычисления и искусственный интеллект. Основные угрозы представляют собой различные методики кражи личной информации. Фишинг – метод мошенничества, целью которого является получение конфиденциальной информации (например, паролей, номеров кредитных карт, личных данных) у пользователей под предлогом, что они взаимодействуют с официальным учреждением. Обычно фишинг осуществляется с помощью электронных писем, сообщений в мессенджерах или веб-сайтов, которые выглядят как официальные. Атаки на сети — это различные виды кибератак, направленные на компрометацию, повреждение или уничтожение сетевой инфраструктуры и данных, которые передаются по сетям. Эти атаки могут как нарушать работу, так и приводить к утечке или потере данных. Шантаж и вымогательство понимаются как виды преступной деятельности, при которых злоумышленники требуют от жертвы денежных средств под угрозой раскрытия компрометирующей информации, причинения вреда или использования силы. Эти методы часто применяются в киберпространстве, где преступники используют различные технологии для достижения своих целей [2].

Так, противодействие киберпреступлениям требует комплексного подхода, сочетающего технические, организационные и правовые меры. Разработка политики безопасности начинается с устранения уязвимостей информационной системы. Базовыми инструментами, позволяющими блокировать вредоносные программы и защищать компьютерные сети являются фаерволы и антивирусное ПО. Системы обнаружения и предотвращения вторжений (IDS/IPS): технологии, позволяющие мониторить сетевой трафик и обнаруживать подозрительную активность. Одним из самых высокоэффективных методов является использование криптографических методов для защиты конфиденциальной информации и предотвращения её от несанкционированного доступа. В последнее время использование искусственного интеллекта и машинного обучения так же включается в техническое противодействия таких преступлений, помогая анализировать большие объемы данных и предсказывать потенциальные угрозы.

Еще одним важным фактором, является улучшение кибербезопасности в личных и общественных целях. Допустим, создание многоуровневых систем

защиты информации, которая поможет справится с данной задачей. Метод, используемый данной системой, состоит в создании нескольких блоков. Контроль доступа, настройка шифрования сети, устройства слежения, понижают шансы взломщика на успех. так как хорошо защищенные системы сложнее подвергаются атакам.

Организационный подход рассматривает наиболее понятные пункты, включающие в себя: обучение сотрудников, разработку политик безопасности, а также регулярные проверки системы. Наличие четких инструкций и правил по работе с информацией и компьютерными системами помогает снизить уровень рисков и предотвратить возможные атаки [3].

Законодательство Российской Федерации создает и совершенствует правовые нормы регулирующие кибербезопасность, помогая обеспечить защиту граждан и их личную информацию.

Таким образом, киберпреступления продолжают оставаться серьезной угрозой для безопасности конфиденциальных данных в 21 веке. Эффективные меры противодействия должны быть комплексными и многоуровневыми. Вместе с тем в условиях постоянно меняющихся способов нарушения конфиденциальности, целостности и доступности информации, необходимо продолжать исследовать новые технологии и подходы. Только такой мультидисциплинарный подход позволит эффективно противостоять киберпреступникам и обеспечивать безопасность в цифровом пространстве.

ЛИТЕРАТУРА

1. Богданова И. А. Проблемы квалификации киберпреступлений // Вестник Санкт-Петербургского университета МВД России. – 2021. – № 1. – С. 23-28.

2. Драчев С.С. Киберпреступность и пути ее предупреждения // Вестник Московского университета. Серия 11. Право. 2019. – № 3. – С. 112-125.

3. Уголовный кодекс Российской Федерации (ст. 272-274.1). – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения:

4. «Об информации, информационных технологиях и о защите информации : федеральный закон от 27 июля 2006 г. № 149-ФЗ. – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/?ysclid=m56uc84kp2937007139 (дата обращения: 13.11.2024).

СВЕДЕНИЯ ОБ АВТОРАХ

Терентьев Александр Андреевич. Старший преподаватель кафедры инфокоммуникационных систем и технологий. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: Alextt02021993@yandex.ru

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

Купавцева Дарья Вячеславовна.
Воронежский институт МВД России.
E-mail: kupavtsevadaria@yandex.ru
Россия, 394006, г. Воронеж, Проспект Патриотов, 53.

Terentev Aleksandr Andreevich. Senior lecturer of the chair of Infocommunication Systems and Technologies. Candidate of Technical Sciences.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: Alextt02021993@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Kupavtseva Daria Vyacheslavovna
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: kupavtsevadaria@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53

Ключевые слова: киберпреступления; классификация киберпреступлений; кибербезопасность.

Key words: cybercrimes; classification of cybercrimes; cybersecurity.

УДК 004.056

Терентьев Александр Андреевич,
кандидат технических наук;
Бакулин Никита Сергеевич

АПРОБАЦИЯ ПРОГРАММНОГО КОМПЛЕКСА РАСПРЕДЕЛЁННОЙ ЭКСПЕРТНОЙ ОЦЕНКИ «DAS»

APPROBATION OF THE «DAS» DISTRIBUTED EXPERT ASSESSMENT SOFTWARE PACKAGE

В статье рассматривается апробация разработанного ранее программного комплекса для организации и проведения распределённой экспертной оценки.

This article discusses the approbation of a previously developed software package for organizing and conducting distributed peer review.

В рамках данной работы была проведена апробация разработанного ранее программного комплекса «DAS» [1], на основе разработанного

численного метода [2]. В ходе апробации были отобраны 10 экспертов - слушателей 5 курса радиотехнического факультета, обучающиеся по специальности «Информационная безопасность телекоммуникационных систем». Эксперты были разделены на две группы по 5 человек.

Обоим группам была поставлена задача осуществить сравнение 25 комплексов радиомониторинга и обнаружения закладочных устройств (таблица 1) [3], в целях выбора комплекса представляющего наибольший интерес в рамках образовательного процесса. Каждой из групп экспертов были выданы справочные материалы по всем сравниваемым объектам для достижения более точных результатов.

Таблица 1

Комплексы радиомониторинга и обнаружения закладочных устройств

Номер	Название комплекса
1	АСТРА
2	Кассандра WiFi
3	Кассандра-С30
4	Кассандра-С6
5	Кассандра-СО6
6	Кассандра-СО
7	Крона-М6
8	Крона-М12
9	Рубин-М
10	СИГНАЛ-РМ
11	ШЛЮЗ-ВЧН
12	СИРИУС-МК
13	ST 154
14	Анализатор МБС
15	Звезда
16	СПЕКТР-ЭКСПРЕСС

17	OSCOR Green - 8
18	OSCOR Blue 24
19	OSCOR Green - 24
20	ОМЕГА-КС4
21	МОЗАИКА-НВ
22	МИРАЖ
23	ОМЕГА-М5
24	Кассандра-К21
25	Кассандра К6

Попарное сравнение осуществлялось с использованием следующей системы оценивания:

- от 9 до 2 оценка в положительную сторону, где 9 максимально положительная оценка ;
- 1 равноценное отношение объектов без уклона в положительную или отрицательную сторону;
- от 0,1 до 0,5 оценка в отрицательную сторону, где 0,1 максимально отрицательная оценка.

Первая группа экспертов осуществляла попарное сравнение используя программный комплекс DAS, а именно его составляющую клиентское приложение «DAS CLIENT».

С помощью серверного приложения «DAS SERVER» осуществлялся контроль выполнения экспертами представленных задач.

По окончании всеми экспертами сравнения был проведён анализ полученных результатов и выгружен отчёт в формате xlsx документа.По оценочным значениям представленным экспертами программным комплексом были рассчитаны векторы направленности, исходя из полученных значений может быть определён наиболее предпочтительный по мнению экспертов объект(таблица 2).

Таблица 2

Векторы направленности сравниваемых объектов

S (сравниваемые объекты)	V (векторы направленности)	Описание

0	0,009	АСТРА
1	0,254	Кассандра WiFi
2	0,046	Кассандра-С30
3	0,053	Кассандра-С6
4	0,064	Кассандра-СО6
5	0,064	Кассандра-СО
6	0,016	Крона-М6
7	0,016	Крона-М12
8	0,019	Рубин-М
9	0,011	СИГНАЛ-РМ
10	0,004	ШЛЮЗ-ВЧН
11	0,027	СИРИУС-МК
12	0,022	ST 154
13	0,01	Анализатор МБС
14	0,01	Звезда
15	0,003	СПЕКТР-ЭКСПРЕСС
16	0,128	OSCOR Green - 8
17	0,036	OSCOR Blue 24
18	0,068	OSCOR Green - 24
19	0,046	ОМЕГА-КС4
20	0,042	МОЗАИКА-НВ
21	0,017	МИРАЖ
22	0,003	ОМЕГА-М5
23	0,003	Кассандра-К21

Рассчитанные данные визуализируется в отчёте за счёт построения диаграммы векторов направленности, из которой сразу можно определить наиболее подходящий по мнению экспертов объект (рисунок 1).

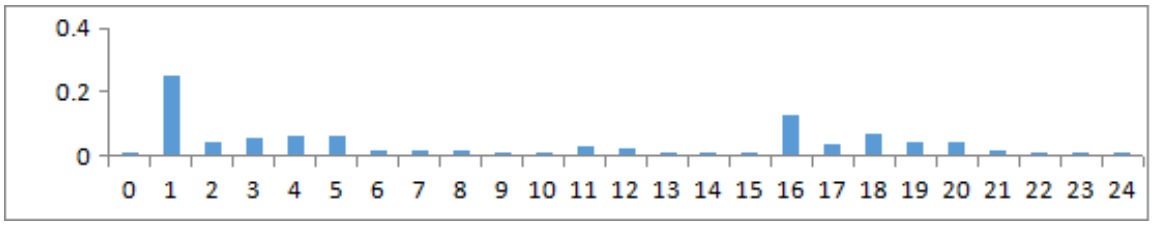


Рис. 1. Диаграмма векторов направленности

Исходя из представленной диаграммы можно сделать вывод что наибольший интерес в рамках образовательного процесса вызвал комплекс радиомониторинга и обнаружения закладочных устройств под индексом 1 - «Кассандра WiFi».

Также программный комплекс осуществляет фиксацию в отчёте временных показателей работы каждого из экспертов и перечень рассматриваемых каждым экспертом объектов (таблица 3).

Таблица 3

Данные о работе экспертов

Пользователь	Время начала работ	Время окончания работ	Список обрабатываемых объектов
Эксперт 1	13:15	13:34	0,1,2,3,4,5
Эксперт 2	13:15	13:36	0,6,7,8,9,10
Эксперт 3	13:16	13:32	0,11,12,13,14,15
Эксперт 4	13:16	13:35	0,16,17,18,19,20
Эксперт 5	13:17	13:40	0,21,22,23,24

Исходя из данных таблицы № 3, к работе первый эксперт приступил в 13:15, а последний эксперт закончил в 13:40, следовательно, общее затраченное время на осуществление экспертного сравнения 25 объектов 5 экспертами с помощью разработанного программного комплекса заняло 35 минут.

Вторая группа экспертов осуществляла сравнение объектов не используя средств автоматизации, в Exel таблице из 25 элементов. Из полученных данных были также рассчитаны векторы приоритетов (таблица 4).

Таблица 4

Векторы направленности сравниваемых объектов

<S> (сравниваемые объекты)	V (векторы направленности)	Описание
0	0,002	АСТРА
1	0,01	Кассандра WiFi
2	0,008	Кассандра-С30
3	0,023	Кассандра-С6
4	0,026	Кассандра-СО6
5	0,03	Кассандра-СО
6	0,014	Крона-М6
7	0,018	Крона-М12
8	0,044	Рубин-М
9	0,019	СИГНАЛ-РМ
10	0,059	ШЛЮЗ-ВЧН
11	0,05	СИРИУС-МК
12	0,007	ST 154
13	0,06	Анализатор МБС
14	0,222	Звезда
15	0,097	СПЕКТР-ЭКСПРЕСС
16	0,061	OSCOR Green - 8

17	0,018	OSCOR Blue 24
18	0,015	OSCOR Green - 24
19	0,017	ОМЕГА-КС4
20	0,023	МОЗАИКА-НВ
21	0,052	МИРАЖ
22	0,031	ОМЕГА-М5
23	0,03	Кассандра-К21
24	0,042	Кассандра К6

Далее для визуализации полученных данных была построена диаграмма векторов направленности (рисунок 2).

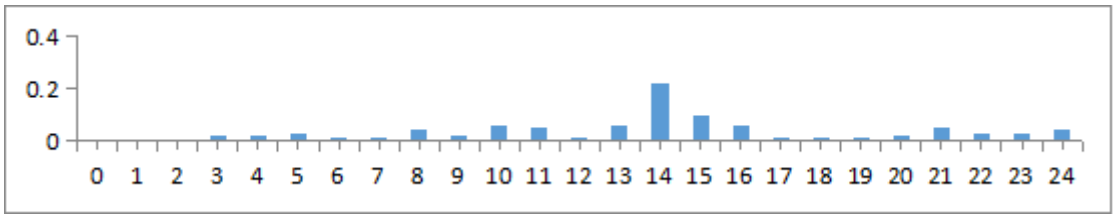


Рис. 2. Диаграмма векторов направленности

Исходя из представленной диаграммы можно сделать вывод, что наибольший интерес в рамках образовательного процесса вызвал комплекс радиомониторинга и обнаружения закладочных устройств под индексом 14 - «Звезда».

Для осуществления последующего анализа было зафиксировано время, затраченное экспертами на проведение сравнения без средств автоматизации.

Исходя из полученных данные вторая группа экспертов, осуществляющая сравнение без средств автоматизации, затратила на выполнение 58 минут.

В рамках апробации две группы экспертов из 5 человек получили одинаковое задание на экспертное сравнение 25 объектов. Первая группа используя разработанный программный комплекс выполнила поставленную задачу за 35 минут, вторая группа выполнила поставленную задачу за 58 минут, не используя средств автоматизации, что на 65,7% больше чем у первой группы.

Также нельзя забывать о том, что по выполнению первой группой экспертов экспертного сравнения отчёт по результатам сравнения и наиболее подходящий объект был сформирован за кратчайший промежуток времени (менее 2 секунд), результаты экспертного оценивания второй группы экспертов обрабатывались вручную, что также повлекло временные затраты, порядка 30 минут.

Исходя из всех полученных данных, можно сказать, что программный комплекс существенно автоматизирует процесс организации и проведения экспертного сравнения, уменьшая временные затраты на 151% (с учётом временных затрат на формирование отчёта), а с увеличением количества сравниваемых объектов данный показатель будет лишь увеличиваться, что подтверждает актуальность и целесообразность применения разработанного программного комплекса «DAS». Програмный комплекс прошёл регистрацию в ФИПС (Свидетельство о государственной регистрации программ для ЭВМ №2024660433) [5].

ЛИТЕРАТУРА

1. Бакулин Н.С., Терентьева А.А. Разработка автоматизированного программного комплекса распределённой экспертной оценки // Сборник Всероссийской научно-практической конференции курсантов и студентов «IV научно-педагогических чтений молодых ученых имени профессора С.В. Познышева». Воронеж, 2024. – С. 320-323.
2. Пьянков О.В. Разработка численного метода определения весов конфликтных взаимодействий / Пьянков О.В., Терентьев А.А. // Вестник Воронежского института МВД России. 2019. – № 1. – С. 69-74.
3. Стратегия развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года [Электронный ресурс]. – URL: https://digital.gov.ru/common/upload/Strategiya_razvitiya_otrasli_IT_2014-2020_2025.pdf. (дата обращения: 17.11.2023). – Текст : электронный.
4. 2. Об утверждении Ведомственной программы цифровой трансформации МВД России на 2021 - 2023 годы : Распоряжение МВД России от 29 декабря 2020 г. № 1/15065 – URL: http://www.consultant.ru/document/cons_doc_LAW_399116/ (дата обращения: 17.11.2023). – Текст : электронный.
5. Бакулин Н.С., Терентьев А.А. Автоматизированный программный комплекс распределённой экспертной оценки / Н.С. Бакулин, А.А. Терентьев // Свидетельство о регистрации программы для ЭВМ № 2024660433.

СВЕДЕНИЯ ОБ АВТОРАХ

Терентьев Александр Андреевич. Старший преподаватель кафедры инфокоммуникационных систем и технологий. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: alextt02021993@yandex.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Бакулин Никита Сергеевич. Слушатель 5 курса радиотехнического факультета.
Воронежский институт МВД России.
E-mail: nikita.bakulin.2001@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Terentyev Alexander Andreevich, lecturer at the Department of Information and Communication Systems and Technologies. Candidate of Technical Sciences.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
mail: alextt02021993@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Bakulin Nikita Sergeevich. 5th year student of the Radio Engineering Faculty.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: nikita.bakulin.2001@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: распределённая экспертная оценка; программный комплекс; апробация.

Key words: distributed expert assessment; software package; approbation.

УДК 004.42

Терентьев Александр Андреевич,
кандидат технических наук;
Бушланова Анастасия Сергеевна

МЕТОДИКА ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ С НОСИТЕЛЕЙ ИНФОРМАЦИИ

THE METHOD OF RESTORING INFORMATION FROM MEDIA

В статье рассматривается методика восстановления информации с носителей информации. Рассмотрены основные принципы и этапы процесса восстановления данных, включая анализ носителя, диагностику повреждений и выбор подходящих методов восстановления. Особое внимание уделено различным технологиям и инструментам, используемым специалистами для восстановления информации с различных типов носителей, таких как жесткие диски, флеш-накопители и т.д. Результаты исследования позволяют сделать вывод о важности профессионального подхода к восстановлению информации с носителей и его значении для современных информационных технологий.

This article discusses the method of restoring information from media. The basic principles and stages of the data recovery process are considered, including media analysis, damage diagnosis and selection of appropriate recovery methods. Special attention is paid to various technologies and tools used by specialists to recover information from various types of media, such as hard drives, flash drives, etc. The results of the study allow us to conclude about the importance of a professional approach to the recovery of information from media and its importance for modern information technologies.

При удалении файлов через стандартный менеджер стертая информация на самом деле не исчезает. При удалении лишь совершается присвоение соответствующим секторам статуса свободных, чтобы в будущем они были перезаписаны. Однако до тех пор, пока этого не произошло, файлы можно без особого труда восстановить при помощи разных методик.

Процесс, направленный на восстановление удаленной или поврежденной информации с электронных носителей, является одной из ключевых задач для правоохранительных органов. Преднамеренные действия правонарушителей, сбои программного обеспечения, физические повреждения носителей и вирусные атаки приводит к потере значимых данных.

В современном обществе существует несколько основных методик восстановления данных с носителей информации.

Программное восстановление данных подразумевает использование специализированного ПО для восстановления данных с поврежденных носителей информации. Такие программы имеют возможность восстановить удаленную или поврежденную информацию, предварительно просканировав на наличие таковой [1].

Например, *Recover My Files* сканирует выбранный диск или устройство на предмет удаленных файлов, используя алгоритмы для анализа файловой системы, которые могут обрабатывать ситуации как с файловыми структурами NTFS, так и FAT. Recover My Files ищет остаточные данные об удаленных файлах, используя сигнатуры файлов и другие методы. После завершения сканирования пользователю предоставляется список найденных файлов, а возможность предварительного просмотра позволяет выбрать именно те файлы, которые мы хотим восстановить, после чего указывается место сохранения отобранных данных.

Также можно привести в пример *R – Studio,* которая представляет собой целый набор утилит, призванных выполнять восстановление файлов, расположенных на внутренних жестких дисках, внешних накопителях (USB – флешки, CD, DVD), ZIP дисках. При этом не имеет значения, каким образом был удален тот или иной файл – в результате деятельности вирусных программ или наличия сбоя внутри самой системы. R – Studio также имеет удобный и интуитивно понятный интерфейс, что делает его доступным для широкого круга пользователей, включая начинающих пользователей и профессиональных специалистов. Программа поддерживает работу на различных операционных системах, включая Windows, Mac и Linux. Поиск и восстановление удаленных файлов может выполняться двумя основными способами. Сканирование диска выдаст пользователю перечень папок и файлов, имеющихся в выбранном разделе диска. Напротив удаленных файлов находится пометка в виде красного крестика. А для того чтобы выполнить восстановление того или иного файла, требуется пометить его галочкой (можно отметить сразу несколько папок), после чего нажать «Восстановить помеченные». Пользоваться R – Studio также можно, применяя сигнатуры. Если на диске не были найдены нужные файлы, это значит, что их структура уже повреждена. Следовательно, просмотр содержимого диска результата не даст. В этом случае проблему часто можно решить, запустив сканирование по сигнатурам. После чего R – Studio отобразит список найденных файлов, подлежащих восстановлению.

В добавок к предшествовавшему можно упомянуть и об Undelete 360 — специальная программа для восстановления файлов. Ее основные отличия от других программ аналогичного направления заключаются в том, что она использует наиболее эффективный алгоритм для поиска, сканирования и восстановления потерянных данных. Этот алгоритм позволяет значительно уменьшить время, которое используется для предварительного сканирования имеющихся на компьютере жестких дисков. Данное приложение работает

также с внешними HDD, с флеш-накопителями, CD и DVD приводами, с картами памяти и др. [2].

Работать с программой очень просто. Для этого вам нужно всего лишь выбрать диск, на котором требуется восстановить файлы, и нажать на запуск процесса предварительного сканирования. Когда программа закончит свою работу, она выведет список тех удаленных файлов, которые подлежат восстановлению. В приложении также имеется очень удобный фильтр, с помощью которого результаты поиска можно вывести в рассортированном виде — по типам файлов или в виде дерева. Программа Undelete 360 выводит по каждому элементу краткую информацию — имя файла и путь к нему. Но это еще не все. Приложение предоставляет возможность посмотреть свойства того или иного элемента в подробном виде. Иногда очень проблематично бывает вспомнить по названию содержимое файла. Для решения этой проблемы в приложении имеется очень интересная и полезная функция — это встроенный модуль для предварительного просмотра той информации, которую нужно восстановить. Еще одно дополнение штатного функционала приложения — интегрированный в программу шестнадцатеричный просмотровщик, с помощью которого можно сделать побайтный анализ содержащейся в удаленном файле информации.

Существует огромное количество специализированных ПО, являющихся незаменимым инструментом для восстановления информации [3].

Для этого требуется произвести выбор из вышеперечисленных программ с целью определения наиболее эффективной и качественной программы методом попарного сравнения [4].

Расчет вектора приоритетов v осуществляется следующим образом:

- определяется максимальное собственное число матрицы λ_{max}

$$\lambda_{max} = eigenvals(B) \quad (1)$$

- рассчитывается вектор приоритетов

$$v = eigenvec(B, \lambda_{max}) = (v_1, v_2, \dots, v_N) \quad (2)$$

- нормирование вектора приоритетов

$$v_{\text{н}} = (v_{1\text{н}}, v_{2\text{н}}, \dots, v_{N\text{н}}), \text{ где } v_{i\text{н}} = \frac{v_i}{\sum v_i}, \ i = 1,2, \dots, N. \quad (3)$$

Для этого каждому эксперту был выдан бланк, на котором была таблица с программами, а также фундаментальная шкала, которая содержала оценочную школу от 1 до 9 и от 1/2 до 1/9. Согласно методу попарного сравнения, эксперт сравнивал каждую программу между собой и выставлял оценку согласно фундаментальной шкале.

Пример заполнения таблицы одним экспертом для определения программы, наиболее подходящей для выполнения конкретных задач, учитывая их функциональность, удобство использования, цену и другие критерии (см. табл. 1).

Таблица 1

Результаты экспертного опроса для первого эксперта

Программы	Recover My Files	PC – 3000 Portable	Recuva	R – Studio	Undelete 360
Recover My Files	1	1/5	4	1/6	4
PC – 3000 Portable	5	1	5	3	7
Recuva	1/4	1/5	1	1/6	3
R – Studio	6	1/4	6	1	5
Undelete 360	1/4	1/7	1/3	1/5	1

Усредненные значения вектора приоритетов приведем ниже:

$$v = (0{,}121; 0{,}465; 0{,}064; 0{,}31; 0{,}039) \quad (3.4)$$

Исходя из полученных данных, мы однозначно можем сказать, что PC – 3000 Portable, весовое значение данный объект сравнения имеет 0,465. Таким образом, данный программный продукт, по мнению экспертов, является наиболее надежным и предпочтительным средством для восстановления потерянной или удаленной информации.

Аппаратное восстановление данных включает использование специализированного оборудования для восстановления данных с поврежденных носителей информации. К такому способу восстановления данных можно отнести линейку инструментов и решений, разработанных компанией «Элекс», которая используется в основном для восстановления данных с поврежденных или неисправных жестких дисков и других носителей информации. PC – 3000 Portable включает в себя аппаратные компоненты, которые позволяют специалистам в области восстановления данных выполнять сложные операции по извлечению информации. Кроме того комплекс поддерживает накопители из диапазона более 10 лет. Дополнительно, PC – 3000 Portable позволяет создавать имидж – копии данных с накопителей HDD, SSD, USB – Flash, в том числе без использования управляющего компьютера. Ведется протоколирование всех операций и создание отчетов, которые в дальнейшем могут быть сохранены или распечатаны. Данная программа имеет множество функций, например: диагностика и анализ состояния носителей; восстановление данных с поврежденных устройств; создание образов дисков для дальнейшего анализа; работа с RAID – массивами и отдельными дисками. PC – 3000 Portable широко используется экспертами в правоохранительных органах и профессиональных лабораториях по восстановлению данных разных IT–корпораций.

Безусловно, самый простой способ уничтожения данных с USB – флеш-накопителей, HDD и SSD подразумевает под собой радикальные меры, а именно механическим, термическим или химическим воздействием, и тут на помощь приходит физическое восстановление данных, которое сочетает в себе различные физическое манипуляции с носителем информации. Такой процесс является энергозатратным, трудоемким и дорогим, поэтому он менее популярен по сравнению с вышеперечисленными. Данная методика используется, когда носитель имеет видимые повреждения и требуется замена каких-либо его механических элементов или, в лучшем случае, снятие с поверхности диска поврежденного слоя защитного покрытия. К сожалению, при физическом поражении накопителя данных не всегда возможно восстановить необходимую информацию.

Методика восстановления информации с носителей информации включает несколько этапов, начиная от оценки состояния носителя и заканчивая сохранением восстановленных данных. В данной статье мы рассмотрели программные решения, такие как специализированные утилиты для восстановления файлов, которые позволяют эффективно восстанавливать данные с поврежденных или отформатированных носителей, аппаратные методы, включая использование специализированных лабораторий, обеспечивающих более глубокое восстановление данных, а также упомянули о физическом восстановлении информации в случаях физического повреждения носителей. Знание основных методов позволяет эффективно справляться с ситуациями потери данных и минимизировать риск их утраты.

ЛИТЕРАТУРА

1. Жуков М. М. Применение специальных знаний для получения значимой информации из компьютерных систем : учебно-методическое пособие / М. М. Жуков, А. Ю. Телков, А. А. Гущина, В. И. Парфенов, Д. И. Полухин, С. Е. Кривобокова. Воронежский институт МВД России, 2023. – 75 с.
2. Меньшаков Ю. К. Виды и средства иностранных технических разведок : учебное пособие. Под ред. М. П. Сычева. Москва : Изд.-во МГТУ им. Н. Э. Баумана, 2009. – 656 с.
3. Нестеровский О. И. Основы информационной безопасности в ОВД [Электронный ресурс] : учебное пособие / О. И. Нестеровский. Воронеж : Воронежский институт МВД России, 2015. - 32 с.
4. Саати Т.Л. Принятие решений при зависимостях и обратных связях: Аналитические сети. Пер. с англ. / Науч. ред. А. В. Андрейчиков, О. Н. Андрейчикова. Изд. 3-е. – Москва : Книжный дом «ЛИБРОКОМ», 2011. – 360 с.
5. Скляров Д. Искусство защиты и взлома информации / Д. Скляров. Санкт-Петербург : БХВ-Петербург, 2004. - 276 с.

6. Шалаева А. С., Терентьев А.А. Роль компьютерной экспертизы в органах втренних дел // Сборник материалов Всероссийской научно-практической конференции курсантов и студентов «IV научно-педагогические чтения молодых ученых имени профессора С.В. Познышева». Воронеж, 2024. – С. 500-504.

СВЕДЕНИЯ ОБ АВТОРАХ

Терентьев Александр Андреевич. Старший преподаватель кафедры инфокоммуникационных систем и технологий. Кандидат технических наук.
Воронежский институт МВД России.
E-mail: Alextt02021993@yandex.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Бушланова Анастасия Сергеевна. Курсант.
Воронежский институт МВД России.
E-mail: nastya.shalaeva.2002@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Terentev Aleksandr Andreevich. Senior lecturer of the chair of Infocommunication Systems and Technologies. Candidate of Technical Sciences.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: Alextt02021993@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Bushlanova Anastasia Sergeevna. The cadet.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: nastya.shalaeva.2002@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: Recover My Files; R – Studio PC – 3000 Portable; USB-накопитель; метод попарного сравнения; экспертный опрос.

Keywords: Recover My Files; R – Studio; PC – 3000 Portable; USB flash drive; pairwise comparison method; expert survey.

УДК 519.816

Тынянкин Сергей Иванович,
доктор технических наук;
Балюков Валерий Михайлович;
Скоморохов Виктор Викторович,
кандидат физико-математических наук;
Солдатенкова Надежда Алексеевна

ПЕРЕДАЧА ВИДЕОИНФОРМАЦИИ В УЗКОПОЛОСНЫХ КАНАЛАХ ЦИФРОВОЙ ПРОФЕССИОНАЛЬНОЙ ПОДВИЖНОЙ РАДИОСВЯЗИ

TRANSMISSIN OF VIDEO INFORMATION IN NARROWBAND CHANNELS DIGITAL PROFESSIONAL MOBILE RADIO COMMUNICATIONS

Средства узкополосной цифровой профессиональной подвижной радиосвязи, применяемые в МВД России, имеют ряд преимуществ по дальности действия и стоимостным параметрам. Однако, стандартная скорость передачи информации в них не превосходит единиц кбит/с, что не позволяет передавать видеоинформацию в реальном времени. Применение инновационного алгоритма передачи информации в узкополосных средствах радиосвязи обеспечивает повышение информационной скорости до десятков кбит/с и, как следствие, возможность передачи видеоинформации.

The means of narrowband digital professional mobile radio communications used in the Ministry of Intenal Affairs of Russia have a number of advantages in terms of range and cost parameters. However, the standart data transfer rate in them does not exceed units of kbits/s, which does not allow transmitting video information in real time. The use of an innovative algorithm for transmitting information in narrowband radio communications provides an increase in information speed to tens of kbits/s and, as a result, the possibiliting video information.

Подразделения МВД России в своей повседневной служебной деятельности (несение патрульно-постовой службы, осуществление контроля за дорожным движением и т.д.) широко используют средства радиосвязи. При этом сотрудниками МВД России используются средства как широкополосной, так и узкополосной радиосвязи.

Согласно разработанной стратегии развития оперативной радиосвязи органов внутренних дел Российской Федерации до 2035 года основной целью ведомственной оперативной радиосвязи является ее совершенствование с учетом требований к системе управления МВД России в современных условиях. Основные задачи включают в себя

переход от узкополосных цифровых систем связи к широкополосным цифровым системам.

Современные широкополосные радиотехнологии характеризуются спектральной эффективностью от 0,75 бит/с/Гц до 3 бит/с/Гц и более. Для обеспечения такой высокой пропускной способности радиолиний в них используются различные многопозиционные методы модуляции, расширенная полоса частот (до 28 МГц). Это позволяет передавать в реальном масштабе времени видеоинформацию о текущей обстановке, с места происшествия и в других случаях.

Вместе с тем применение средств широкополосной радиосвязи требует развертывания специальной инфраструктуры связи, которая, как правило, технически сложнее и существенно дороже относительно сетей узкополосной цифровой профессиональной подвижной радиосвязи (ЦППР). Кроме того, широкополосные сети требуют выделения бóльшего частотного ресурса, что в условиях высокой загруженности радиодиапазона зачастую является ключевым фактором, ограничивающим их создание и эксплуатацию. В связи с изложенным, в настоящее время в МВД России продолжается широкое применение узкополосных средств и систем ЦППР.

Поэтому несомненный практический интерес представляет возможность передачи видеоинформации по узкополосным радиоканалам радиосетей ЦППР. Реализация такого дополнительного функционала в узкополосных средствах ЦППР с шириной полосы частотного канала не превышающей 12,5 кГц позволит существенно повысить эффективность применения средстрв связи в повседневной деятельности подразделений МВД России.

Поставленная задача может быть решена за счёт реализации в узкополосных средствах ЦППР инновационного алгоритма передачи информации с использованием доработанного стека протоколов на физическом и канальном уровне, обеспечивающего существенное повышение скорости передачи информации.

В настоящее время активно развиваются различные методы сжатия как звука, так и видео, обеспечивающие передачу информации с мéньшими скоростями при вполне удовлетворительном качестве. Например, для создания систем видеосвязи используется кодек H.264, способный при информационной скорости 34 кбит/с передать видеоинформацию от мегапиксельных видеокамер в реальном времени.

Таким образом, повышение скорости передачи информации до 34 кбит/с для физического радиоканала с шириной полосы пропускания 12,5 кГц позволит организовывать видеовызовы между пользователями сети ЦППР. Для этого был разработан инновационный алгоритм, использующий на физическом уровне стека протоколов ЦППР современные сигнально-кодовые конструкции, в основе которых сигналы с

ортогональным частотным разделением каналов – OFDM (Orthogonal Frequency Division Multiplexing).

Алгоритм использует двухуровневый стек протоколов. На физическом уровне применяется мультиплексирование с ортогональным частотным разделением каналов. Ширина полосы частот, занимаемая передаваемым радиосигналом 12,5 кГц, и длительность одного таймслота, обеспечивающего многостанционный доступ с временным разделением каналов, не более 27,5 мс. Длительность полезной части символа OFDM составляет 24 мс, длительность защитного интервала 2,66 мс, длительность кадра передачи 400 мс.

Алгоритмом предусмотрена возможность задания различных значений следующих параметров: ширина полосы каналов, число и номера поднесущих, которые адаптируются в зависимости от занятости спектра. Возможно использование различных вариантов модуляции поднесущих как по амплитуде, так и по фазе (QAM – квадратурная амплитудная модуляция). Шаблоны модуляции могут иметь 64 состояния (6 битов, 64-QAM), 16 состояний (4 бита, 16-QAM) или 4 состояния (2 бита, 4-QAM).

Для адаптации параметров радиосигнала под импульсную характеристику канала и удовлетворительную демодуляцию каждой поднесущей определяется характеристика канала радиопередачи и он настраивается с использование эквалайзера. Для этого некоторые из поднесущих символов OFDM переносят пилот-сигналы.

Пилот-сигналы позволяют приемнику определить, принят ли сигнал; оценить сдвиг частоты; оценить канал радиопередачи. Число пилот-сигналов зависит от желательной устойчивости сигнала. Положение пилот-сигнала в каждом символе OFDM-кадра представляется определенным образом.

На канальном уровне формируются три потока данных для трех каналов: основной сервисный канал, канал быстрого доступа и канал описания служб.

Каналы предназначены для выполнения следующих функций:

основной канал передачи полезных данных содержит основную мультимедийную информацию: аудио, видео, изображение, текст;

канал быстрого доступа предоставляет технологическую информацию о ширине канала и других подобных параметрах, необходимую приемнику для демодуляции сигнала;

канал описания служб предоставляет информацию о способе декодирования основного сервисного канала и содержит служебную информацию, описывающую сервисы и службы макета системы.

Для экспериментальной проверки предлагаемого алгоритма передачи информации был разработан макет узкополосного приемопередающего тракта (на базе радиостанции Аксимут-100) с программным обеспечением, в основу которого был положен стек протоколов, использующий на физическом уровне радиосигналы,

передаваемые с помощью ортогонального мультиплексирования, модуляция поднесущих осуществлялась 64-QAM. В разработанном макете каждая поднесущая модулировалась по амплитуде и фазе: шаблоны модуляции имеют 64 состояния (6 битов, 64-QAM) или 4 состояния (2 бита, 4-QAM). Для передачи использовалось помехоустойчивое кодирование.

Возможность проведения экспериментальной проверки с использованием серийно изготавливаемых радиостанций Аксимут-100 обусловлено тем, что эти радиостанции построены по технологии программно-определяемого радио (англ. терминология SDR – Software Defined Radio) и представляют собой универсальные приемо-передающие платформы. Типы используемых сигналов и алгоритм работы радиостанции могут изменяться путем обновления или изменения программного обеспечения.

Экспериментальная проверка проводилась в УКВ диапазоне, на частоте 144,68 МГц, ширина полосы радиоканала 10 кГц, длина радиотрассы 20,1 км.

Параметры передающего тракта:

1. Выходная мощность передающего устройства – 20 Вт.
2. Высота подъема антенны передатчика – 24 метра над землей.
3. Тип передающей антенны – штыревая коллинеарная с круговой ДН.
4. Коэффициент усиления передающей антенны – 8,3 дБ.
5. Длина фидерной системы 50 метров.
6. Потери, вносимые коаксиальным кабелем – 2,45 дБ.
7. Класс работы усилителя мощности – АВ.

Параметры приемного тракта:

1. Высота подъема антенны приемника – 32 метра над землей.
2. Тип приемной антенны – штыревая коллинеарная с круговой ДН.
3. Коэффициент усиления приемной антенны – 8,3 дБ.
4. Длина фидерной системы – 50 метров.
5. Потери, вносимые коаксиальным кабелем – 2,45 дБ.
6. Чувствительность приемника при отношении сигнал/шум 10 дБ – 0,3 мкВ в полосе 10 кГц.

В ходе проведенных на реальной УКВ радиотрассе экспериментов с использованием серийно выпускаемого радиооборудования была впервые апробирована возможность обеспечения видеосвязи в узкополосной сети радиосвязи. При этом получены следующие результаты: осуществлена радиопередача видеоинформации в полосе 10 кГц с модуляцией поднесущих 64QAM, информационная скорость в канале составила 34,8 кбит/с. Видеоинформация передавалась в течение 27 сек с разрешением 320x240, 8 кадров/сек, видео/аудио битрейт в эксперименте составил 26 кбит/с.

Таким образом, в ходе экспериментальной проверки разработанного иннновационного алгоритма передачи информации была получена информационная скорость 34,8 кбит/с, что позволяет передавать видео в реальном времени в узкополосных сетях ЦППР.

СВЕДЕНИЯ ОБ АВТОРАХ

Тынянкин Сергей Иванович. Директор Центра исследования подвижной связи. Доктор технических наук, старший научный сотрудник.

Федеральное государственное бюджетное учреждение научно-исследовательский институт радио имени М.И. Кривошеева.

E-mail: tynyankinsi@niir.ru

Россия, 105064, Москва, ул. Казакова, д.16.

Балюков Валерий Михайлович. Заместитель директора Центра исследования подвижной связи.

Федеральное государственное бюджетное учреждение научно-исследовательский институт радио имени М.И. Кривошеева.

E-mail: balyukovvm@niir.ru

Россия, 105064, Москва, ул. Казакова, д.16.

Скоморохов Виктор Викторович. Ведущий специалист Центра исследования подвижной связи. Кандидат физико-математических наук.

Федеральное государственное бюджетное учреждение научно-исследовательский институт радио имени М.И. Кривошеева.

E-mail: vvs.tmb@mail.ru

Россия, 105064, Москва, ул. Казакова, д.16.

Солдатенкова Надежда Алексеевна. Научный сотрудник отдела средств связи центра средств и систем связи научно исследовательского института специальной техники.

ФКУ НПО «СТиС» МВД России.

E-mail: nsoldatenkova4@mvd.ru

Россия, 111024, г. Москва ул. Пруд-Ключики, д. 2.

Tynyankin Sergei Ivanovich. Director of the Mobile Communications Research Centre. Doctor of Sciences (Technical), Senior Researcher.

Federal State Budgetary Institution Scientific Research Institute of Radio named M. I. Krivosheev.

E-mail: tynyankinsi@niir.ru

Work address: Russia, 105064, Moscow, Kazakova str, 16.

Balyukov Valery Mihailovich. Deputy Director of the Mobile Radio Research Center.

Federal State Budgetary Institution Scientific Research Institute of Radio named M. I. Krivosheev.

E-mail: balyukovvm@niir.ru

Work address: Russia, 105064, Moscow, Kazakova str, 16.

Skomorohov Viktor Viktorovich. The leading specialist of the Research Center mobile communication. Candidate of Sciences (Physics and Mathematics).

Federal State Budgetary Institution Scientific Research Institute of Radio named M. I. Krivosheev.

E-mail: vvs.tmb@mail.ru

Work address: Russia, 105064, Moscow, Kazakova str, 16.

Soldatenkova Nadezhda Alekseevna. Researcher of the Department of Communications center of communication facilities and systems scientific research institute of special equipment.

Federal government institution scientic and production association Special equipment and telecoms of the Ministry of the internal affairs of the Russian Federation.

Work address: Russia, 111024, Moscow, Prud-Klyuchiki str., 2

Ключевые слова: профессиональная подвижная радиосвязь; многопозиционные сигналы; видеосвязь.

Key words: professional mobile radio communication, multi-position signals, video communication

УДК 621.396

Хохлов Николай Степанович,
доктор технических наук, профессор;
Пупкова Полина Сергеевна

ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННОЙ ИНФОРМАЦИОННОЙ СЕТИ ДЛЯ ВЗАИМОДЕЙСТВИЯ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

DESIGNING A SECURE INFORMATION NETWORK FOR INTERACTION OF INTERNAL AFFAIRS OFFICERS

Статья посвящена проектированию защищенной информационной сети в интересах сотрудников органов внутренних дел. Рассмотрена концепция, основной алгоритм построения, а также необходимые аппаратно-программные средства. Изложены требования к защищенности информации в проектируемой сети.

The article is devoted to the design of a secure information network in the interests of employees of internal affairs agencies. The concept, the basic algorithm for construction, as well as the necessary hardware and software are considered. The requirements for the security of information in the designed network are set out.

В данной работе будет рассмотрен вопрос актуальности проектирования прототипа Web-сервера для взаимодействия сотрудников ОВД РФ. Несмотря на все достоинства сервисов ИСОД, существуют определенные недостатки, мешающие идеализации системы. К главному недостатку возможно отнести отсутствие выхода пользователя в систему с мобильного устройства и домашнего персонального компьютера. Деловое общение в сервисе происходит исключительно с ведомственного оборудования, установленного в региональных подразделениях. Еще одним недостатком является отсутствие у курсантов образовательных организаций системы МВД пробной версии для работы с самим сервисом и др. Исходя из выше сказанного, у сотрудников, не имеющих доступа к системе, появляется необходимость делового коллективного общения в доступных социальных сетях Российской Федерации. К таким мы можем отнести: сервис «ВКонтакте», мессенджер «Telegram», «Viber». Такие системы зачастую подвержены атакам злоумышленников и перехвату служебной информации. Из-за перечисленных причин, предлагаем внедрение в ОВД Web-сервер «Вслужбе». Рассмотрим понятие веб-сервера и его принципы работы.

Веб-сервером можно назвать компьютерную систему, отвечающую за хранение, обработку, распространение файлов веб-сайтов в браузерах. Веб-серверы состоят как из аппаратных, так и программных компонентов и используют протокол передачи гипертекста (HTTP), для обработки запросов, поступающих от пользователей Интернета. С точки зрения аппаратного

обеспечения веб-сервер подключается к Интернету, что позволяет ему обмениваться данными или файлами с другими подключенными устройствами. Эти данные могут принимать различные формы, к примеру файлы HTML, изображения, файлы JavaScript, таблицы стилей CSS.

Принцип работы веб-сервера состоит в следующих шагах:

1. Пользователь в адресной строке браузера вводит название домена сайта
2. Браузер отправляет запрос на DNS-сервер для получения IP-адреса, соответствующего указанному адресу сайта.
3. DNS-сервера соответственно хранят информацию о том какому доменному имени какой IP-адрес сопоставлен.
4. Получив ответ от DNS-сервера браузер устанавливает соединение с соответствующим IP-адресом Web-сервера.
5. После установки соединения браузер формирует HTTP-запрос, который сообщает Web-серверу какую информацию необходимо предоставить.
6. Web-сервер принимает HTTP-запрос от браузера, проверяет его корректность и определяет запрашиваемый ресурс на основе указанного URL. При обработке запроса сервер может выполнять и обрабатывать программные скрипты, запрашивать данные из базы данных, считывать данные из файловой системы. Web-сервер формирует и отправляет браузеру HTTP-ответ, который включает статус ответа и его тело, содержащее ресурс. Принцип действия мы можем наблюдать на рис.1.

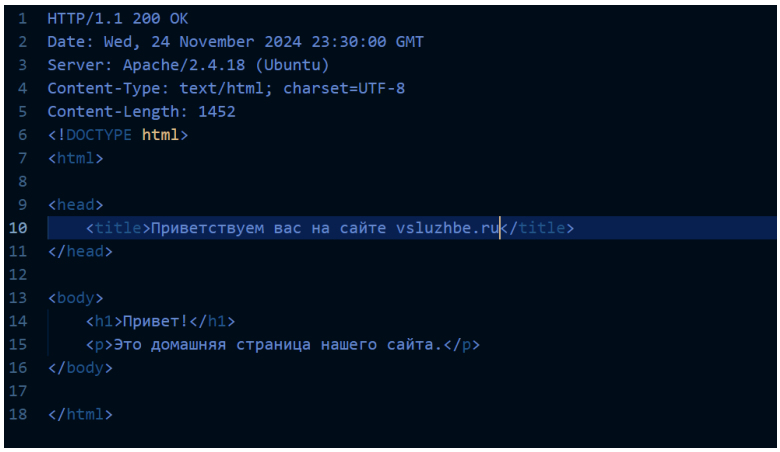


Рис.1 Пример ответа, содержащего в себе запрошенный ресурс

Рассмотрев вышеперечисленные шаги работы веб-сервера, далее в нашей работе рассмотрим необходимые программы для обеспечения динамической работы разрабатываемого сайта на сервер «Вслужбе» дополнительно можем предложить установку:

1. Языки программирования. PHP, Python, Java.
2. Фреймворки, в зависимости от выбранного языка программирования, для облегчения разработки веб-приложения.

3. Базы данных. Для хранения данных, обрабатываемых на сервере. MySQL.

4. CMS для быстрого создания скелета сайта.

5. Дополнительное программное обеспечение, удобное разработчику.

При проектировании предлагаемого нами прототипа веб-сервера, так же подразумеваются соответствующие методы защиты информации, хранящиеся на сервере. Конфиденциальность, целостность и доступность, как три главных постулата информационной безопасности определены в ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» [1]:

1. Конфиденциальность – это обеспечение того, чтобы передаваемая информация не могла быть доступна или прочитана незаконными лицами. Это может включать в себя шифрование данных, управление доступом и другие методы защиты от несанкционированного доступа.

2. Целостность – это обеспечение того, чтобы передаваемая информация не была изменена или повреждена в процессе передачи. Если данные подверглись изменению, это может привести к ошибкам или даже злонамеренным вмешательствам.

3. Доступность – это гарантирование доступности информации для легальных пользователей. Это включает в себя защиту от атак на доступность, такие как DDoS-атаки, которые могут привести к отказу в обслуживании.

Данные процедуры неукоснительно нужны в первую очередь для защиты персональных данных пользователей, зарегистрированных в системе. Под персональными данными следует понимать – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных) [2]. Такие методы, как разграничение доступа подразумевает под собой выделение некоторых ролей при функционировании сайта [3]. Администратор наделен максимумом полномочий, имеет доступ ко всем функциям сайта. Обычные пользователи, то есть зарегистрировавшиеся сотрудники имеют минимальный набор полномочий, для них доступен интерфейс сайта, в котором они могут преследовать свои цели, а именно такие как общение на форуме с другими сотрудниками их территориальных подразделений, либо межрегиональных. Ключевым аспектом можем выделить такую особенность, как доступ у бывших сотрудников к данному сервису. Приведем ситуацию, где бывший сотрудник по выходу на пенсию имеет желание поделиться своим профессиональным опытом и имеет возможность, зарегистрировавшись зайти на форум и оставить комментарий на интересующую его тему. В данный момент в ИСОД отсутствует возможность для взаимосвязи действующих сотрудников и покинувших службу. Следующая роль это модератор. Подразумевается, при регистрации, будет необходимо желающему ввести логин, пароль и электронную почту для двухфакторной аутентификации. Стоит отметить, что данный сайт будет использоваться как модуль, прилегающему к сервису ИСОД, при этом имеющий собственный веб-сервер

для распределения нагрузки. Во время регистрирования данные будут отправляться на электронные базы данных, принадлежащих системе МВД, где будет установлена личность пользователя и его принадлежность к ОВД РФ. При процедуре регистрации следует окно, в котором пользователь соглашается на отсутствие упоминания в диалогах сведений, составляющих служебную, государственную тайну, употребление ненормативной лексики и оскорблению других участников форума. Модератор должен следить за выполнением правил и вносить корректировки при их нарушении, тем самым блокируя пользователя и не давая ему дальнейшего использования сайта.

В дальнейшем при проектировании прототипа веб-сервера «Вслужбе» последует установка необходимых мер защиты сервера, технического обеспечения, фактического расположения центра, с необходимым оборудованием, создание непосредственно самого сайта «Вслужбе», которому будет установлена соответствующая категория защиты.

ЛИТЕРАТУРА

1. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». [Электронный ресурс]. – URL: https://ksc-alternativa.com.ru/wp-content/uploads/2019/08/ГОСТ-Р-50922-2006.pdf (дата обращения: 03.12.2024).
2. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных». – // Консультант. – URL: http://www.consultant.ru/document/cons_doc_LAW_ 61801/ (дата обращения: 25.11.2024)
3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Консультант. – URL: http://www.consultant.ru/document/cons_doc_LAW_61798 / (дата обращения: 25.11.2024).

СВЕДЕНИЯ ОБ АВТОРАХ

Хохлов Николай Степанович. Профессор кафедры инфокоммуникационных систем и технологий. Доктор технических наук, профессор.

Воронежский институт МВД России.

E-mail: nikolayhohlov@rambler.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Пупкова Полина Сергеевна. Слушатель 5 курса радиотехнического факультета.

Воронежский институт МВД России.

Россия, 394065, Воронеж, проспект Патриотов, 53.

Khokhlov Nikolay Stepanovich. Professor of the chair infocommunication systems and technologies. Doctor of Technical Sciences, Professor.
Voronezh Institute of Russian Ministry of Internal Affairs.
E-mail: nikolayhohlov@rambler.ru
Work adress: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Pupkova Polina Sergeevna. 5th year student at the Faculty of Radio Engineering.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
Work adress: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: проектирование; защищенная информационная сеть; веб-сервер; язык программирования.

Key words: design; secure information network; web server; programming language.

УДК 004.056

Шерстюков Сергей Анатольевич,
доктор технических наук, доцент

СПЕКТРАЛЬНОЕ СКАНИРОВАНИЕ РАДИОЧАСТОТНОГО ДИАПАЗОНА С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНО-ОПРЕДЕЛЯЕМОЙ РАДИОСИСТЕМЫ

SPECTRAL SCANNING OF THE RADIO FREQUENCY RANGE USING A SOFTWARE-DEFINED RADIO SYSTEM

Представлена функциональная схема комплекса радиоэлектронной разведки на базе программно-определяемой радиосистемы, реализующая в круговом азимутальном секторе спектральное сканирование радиочастотного диапазона беспилотных летательных аппаратов.

The functional diagram of the electronic reconnaissance complex based on the software-defined radio system is presented, implementing spectral scanning of the radio frequency range of unmanned aerial vehicles in a circular azimuth sector.

В соответствии с отчетом (SM.2152 от 09.2009) Сектора радиосвязи Международного союза электросвязи (МСЭ), занимающийся разработкой международных стандартов радиосвязи, телевизионного и радиовещания и международным распределением радиочастотного спектра и орбит спутников связи, в целях обеспечения общего понимания дано определение

радиоустройства с программируемыми параметрами (SDR – Software-defined radio, программно-определяемая радиосистема).

SDR – это радиопередатчик и/или радиоприемник, использующий технологию, позволяющую с помощью программного обеспечения устанавливать или изменять рабочие радиочастотные параметры, включая, в частности, диапазон частот, тип модуляции или выходную мощность, за исключением изменения рабочих параметров, используемых в ходе обычной предварительно определенной работы с предварительными установками радиоустройства, согласно той или иной спецификации или стандарта системы.

Принцип работы SDR основан на использовании специализированного ПО для обработки аналоговых радиосигналов, преобразованных в цифровые данные, которые обрабатываются на компьютере или вычислительном устройстве.

Основными компонентами SDR являются:

1. Антенна, с выхода которой принимаемые радиосигналы передаются для обработки в SDR устройство.

2. RF Front-End – аппаратная часть SDR, отвечающая за преобразование аналоговых радиосигналов в цифровой формат. В состав RF Front-End входят: усилители, фильтры, модуляторы и демодуляторы.

3. Analog-to-Digital Converter (ADC) – аналого-цифровой преобразователь.

4. Digital Signal Processor (DSP) – цифровой сигнальный процессор, выполняющий функции фильтрации, демодуляции, декодирования и др.

5. Baseband Processor (BP) – процессор постобработки цифрового сигнала после DSP, подготавливающий данные для вывода на динамик и дисплей.

6. Software – ПО SDR, выполняющее операции по обработке и декодированию сигналов.

7. Управляющее программное обеспечение – это ПО, которое управляет работой SDR, настраивает параметры приема и передачи сигналов.

Для обнаружения БПЛА в круговом азимутальном секторе с использованием SDR предлагается функциональная схема комплекса радиоэлектронной разведки (РЭР), изображенная на рис. 1.

В состав функциональной схемы входят следующие элементы:

- локальный объект (здание или комплекс зданий) в населенном пункте, располагающийся на ограниченной территории, или позиция вблизи линии боевого соприкосновения;

- SDR1 – SDR4 – аппаратные модули программно-определяемой радиосистемы;

- SA1 – SA4 – широкодиапазонные секторные антенны;

- Gain 1 – Gain4 – широкополосные усилители радиосигналов;

- Mini PC 1 – Mini PC 4 – персональные мини-компьютеры с установленной операционной системой Pentoo Linux и специализированным программным обеспечением gqrx;

- коммутатор;

- маршрутизаторы M1 и M2;

- сервер управления.

Широкий ДРЧ SDR позволяет: обнаруживать БПЛА на основных радиочастотах их управления, проводить спектральный анализ для идентификации типа БПЛА, определять характеристики сигналов управления и выполнять декодирование протоколов управления. Для автоматического обнаружения и классификации БПЛА без участия оператора имеется возможность сопряжения SDR с методами машинного обучения.

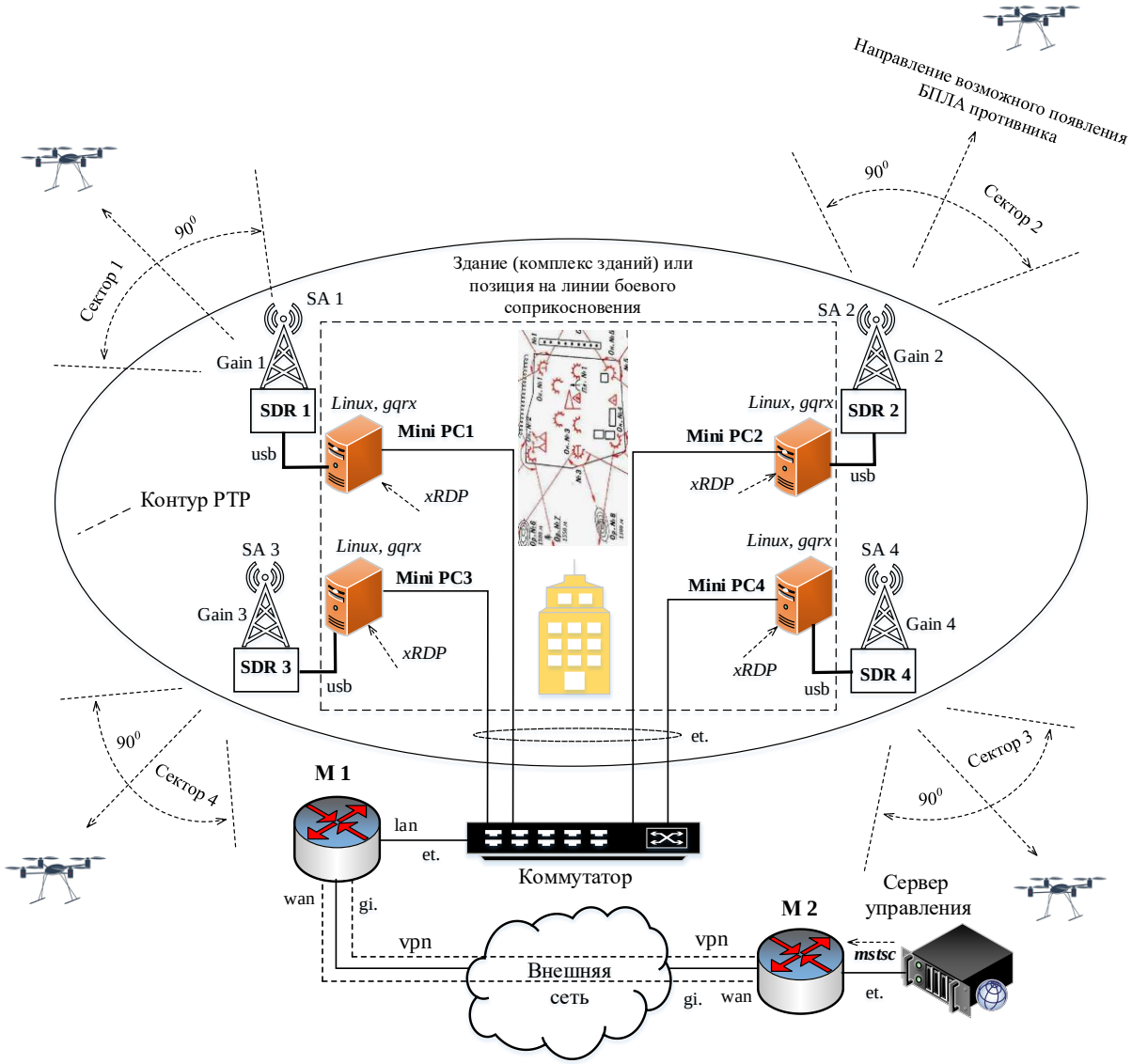


Рис. 1. Функциональная схема комплекса РЭР на базе аппаратной SDR, реализующая в круговом азимутальном секторе спектральное сканирование ДРЧ БПЛА

СВЕДЕНИЯ ОБ АВТОРЕ

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

Воронежский институт МВД России.

E-mail: sherserge@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Sherstyukov Sergey Anatolyevich. Professor of the chair of infocommunication systems and technologies. Doctor of technical sciences, assistant Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: sherserge@mail.ru

Work adress: Russia, 394065, Voronezh, Prospekt Patriotov, 53.

Ключевые слова: программно-определяемая радиосистема; беспилотный летательный аппарат.

Key words: software defined radio system; unmanned aerial vehicle.

УДК 621.396.62

Шерстюков Сергей Анатольевич,
доктор технических наук, доцент;
Лукьянов Александр Сергеевич,
кандидат технических наук;
Никулин Сергей Геннадьевич

ОСОБЕННОСТИ ДАЛЬНОСТИ СВЯЗИ ОБОРУДОВАНИЯ ПРИ РАЗМЕЩЕНИИ РЕТРАНСЛЯТОРОВ НА БПЛА

FEATURES OF THE COMMUNICATION RANGE OF THE EQUIPMENT WHEN PLACING REPEATERS ON UAVS

В материале предложены возможности цифровой системы радиосвязи с технологией дистанционного беспроводного энергоснабжения, которая позволяет увеличить время полета БПЛА с цифровыми mesh-ретрансляторами, а также получить высокую эффективность тракта передачи энергии.

The article suggests the possibilities of a digital radio communication system with remote wireless power supply technology, which allows you to increase the flight time of a UAV with digital mesh repeaters, as well as to obtain high efficiency of the energy transmission path.

В настоящее время одним из перспективных технологических направлений является создание систем дифракции быстрых электронов (ДБЭ) беспилотных летательных аппаратов (БПЛА), при размещении на них полезной нагрузки в виде ретрансляторов для систем радиосвязи. Оптимальной транспортной средой для дистанционной передачи электрической энергии является лазерное излучение, представляющее собой узконаправленный пучок монохроматического инфракрасного излучения. Лазер способен передавать энергию как для летящих, так и зависающих беспилотных аппаратов, что даёт им возможность неограниченное время находиться в воздухе и выполнять функции радио ретрансляторов [3].

Для размещения на БПЛА применялся mesh-ретранслятор компании Hitera E-pack100. Ретрансляторы Hytera E-pack имеют возможность размещения на базе БПЛА, благодаря конструктивному исполнению в виде пыле- и влагозащитного корпуса (IP67), невысокой мощности передатчика (от 5 Вт до 20 Вт), низкому потреблению электроэнергии и малому весу (от 1,5 до 3,6 кг с встроенным аккумулятором в зависимости от исполнения).

E-pack 100 – переносной цифровой автономный приемопередающий модуль. Ретранслятор разработан в виде интеллектуальной коммуникационной платформы, предлагающий максимальную универсальность для подключения различных систем и обеспечения их бесперебойного взаимодействия.

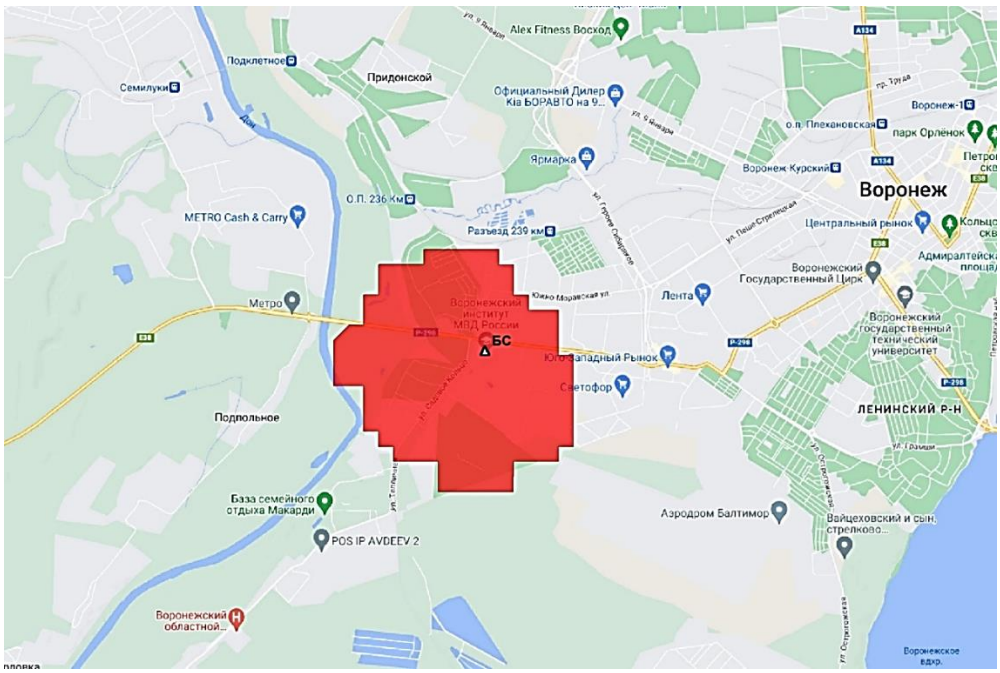
Парк абонентских радиостанций выполнен в виде компактной, легкой, с обтекаемой формой, обладают совместимостью с классом защиты IP67, выдерживают погружение на глубину до 1 м на 30 минут и более.

Для демонстрации расширения зоны покрытия сети радиосвязи при использовании ретранслятора, размещенного на борту БЛА, например, квадрокоптера, ниже приведены результаты моделирования зоны покрытия с помощью программного комплекса «Зона – подвижная радиосвязь». Данный комплекс успешно используется многими отечественными специалистами при проектировании сетей подвижной радиосвязи, в частности, работающих в ОВЧ и УВЧ диапазонах.

При моделировании предполагалось, что используется сравнительно маломощный ретранслятор с выходной мощностью радиопередатчика 5 Вт, с антенной вертикальной поляризацией с круговой азимутальной диаграммой направленности и максимальным коэффициентом усиления 4 дБи, а также носимая радиостанция с выходной мощностью радиопередатчика 2 Вт, с антенной вертикальной поляризации с круговой азимутальной диаграммой направленности и максимальным коэффициентом усиления 2 дБи, высота расположения антенны 1,7 м. Рабочие частоты прямого и обратного каналов связи 450 и 460 МГц. Остальные электрические характеристики приемопередающих трактов ретранслятора и носимой радиостанции взяты в пределах типовых для соответствующей аппаратуры, например, цифровых систем подвижной радиосвязи стандарта DMR. Ретранслятор на приведенных ниже рисунках обозначен как «БС», размещался на высотах 30 м и 100 м на территории Советского района г. Воронежа.

На рисунке 1 приведена Google-карта из комплекса «Зона», на которой обозначено положение ретранслятора и показана полученная в результате расчета конфигурация зоны покрытия в случае расположения антенны ретранслятора на высоте 30 м. Как видно из рисунка, наименьшую протяженность зона покрытия имеет в северо-восточном направлении, для которого характерны довольно плотная городская застройка многоэтажными зданиями высотой до 30-50 м, наличие высоких опор линий электропередачи.

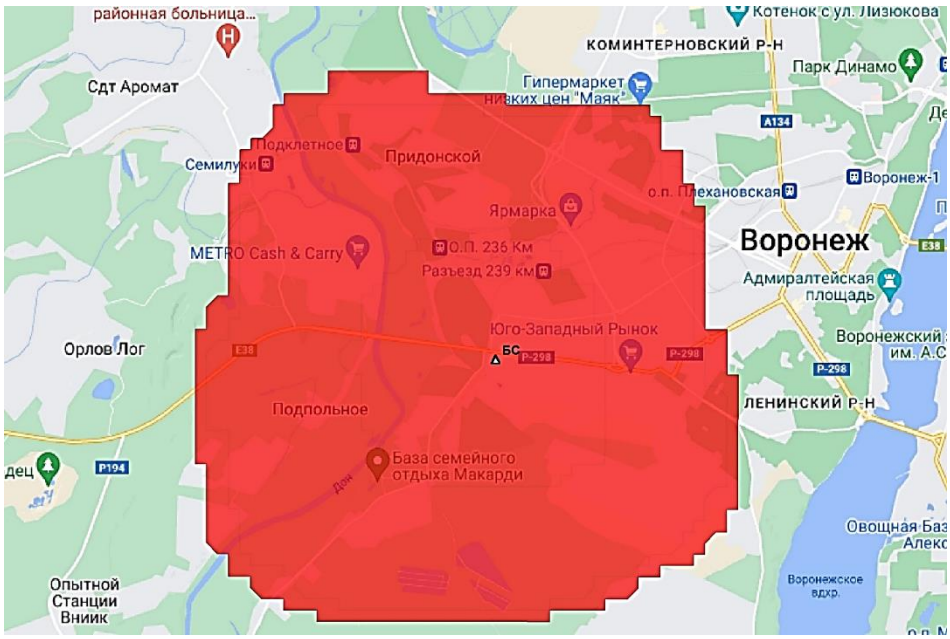
Как видно из рисунка 2, границы зоны существенно расширились, и, что особенно важно, в северо-восточном направлении, благодаря увеличению расстояния прямой видимости. В среднем расширение границ зоны покрытия по отношению к точке расположения ретранслятора составило около 3 раз, что подтверждает ожидаемый положительный эффект от подъема антенны ретранслятора.



Масштаб 1:150000

Рис. 1. Рассчитанная зона покрытия (подъема ретранслятора 30 м)

На рисунке 2 приведена Google-карта из комплекса «Зона», на которой также обозначено положение ретранслятора и показана полученная в результате расчета новая конфигурация зоны покрытия в случае расположения антенны ретранслятора на высоте 100 м.



Масштаб 1:200000

Рис. 2. Рассчитанная зона покрытия (подъема ретранслятора 100 м)

При решении задач радиосвязи с помощью БПЛА учитываются основные полетные характеристики: грузоподъемность (в пределах 0,1-7 кг), время полета и управляемость взлетом, посадкой и нахождением в точке зависания. Предлагаемая технология дистанционного беспроводного энергоснабжения позволит увеличить время полета БПЛА, работающих от аккумуляторов, вплоть до круглосуточного нахождения в воздухе без посадки, что позволит повысить эффективность использования БПЛА для системы радиосвязи.

Принцип действия структурной схемы заключается в следующем. Квадрокоптер с дополнительно установленным оборудованием за счет штатных аккумуляторных блоков поднимается на высоту от 20 до 100 метров относительно земной поверхности и фиксируется в точке зависания с помощью бортовой системы позиционирования. Допускается отклонение от исходной точки в пределах нескольких метров в зависимости от силы бокового ветра.

В процессе работы квадрокоптера происходит естественный процесс разряда аккумуляторных батарей, который с учетом веса дополнительно установленного оборудования ограничивает его полетное время. С целью поддержания полетного режима квадрокоптера вместо привязного питания может использоваться наземная система дистанционного энергоснабжения, в которой монохроматическое излучение источника формируется в малорасходящийся пучок, наводимый с помощью высокоскоростной цифровой видеокамеры с оптико-механическим объективом на приемник-преобразователь, закрепленный на летательном аппарате и подключенный к аккумуляторному блоку для его зарядки. Существует два типа дистанционного энергоснабжения – непрерывный и периодический.

Данная технология дистанционного беспроводного энергоснабжения позволит увеличить время полета БПЛА с цифровыми mesh-ретрансляторами, работающих от аккумуляторов, вплоть до нахождения в воздухе 24 часа в сутки без посадки. Основные преимущества – высокая эффективность тракта передачи энергии (до 40%), возможность использования небольших по размерам приемников (до 100 мм в диаметре), масса которых не превышает 0,1 кг.

Основными характеристиками системы лазерного питания, состоящей из полупроводниковых лазеров и фотоэлектрических преобразователей, являются: КПД, коэффициент отражения и коэффициент пропускания оптических компонентов системы формирования пучка.

Следовательно, на расстояниях порядка 1 км пятно излучения будет порядка $D_{1км}$=40 см. В ближней зоне (менее 500 метров) возможно уменьшение пятна путем фокусировки до 3-10 см без потери эффективности, что дает возможность использовать такую оптическую систему для дистанционного снабжения БПЛА, а небольшое фокусное расстояние позволяет сделать компактную систему.

Таким образом, при расстоянии от станции лазерного питания до квадрокоптера, равном 100 метрам, пятно излучения будет порядка $D_{100м}$=2 см без потери эффективности питающего аккумулятор излучения. В сочетании с применением LiFePO4-аккумуляторов очевиден экономический выигрыш.

ЛИТЕРАТУРА

1. T-motor Flame 60A ESC. – URL: https://www.foxtechfpv.com/t-motor-flame-60a-esc.html (дата обращения 17.10.2024). – Текст : электронный.

2. Айхлер, Ю. Лазеры. Исполнение, управление, применение / Ю. Айхлер, Г. И. Айхлер. – Москва : Техносфера, 2008. – 440 с. – Текст : непосредственный.

3. Шрёдер, Г. Техническая оптика / Г. Шрёдер, Х. Трайбер. – Москва : Техносфера, 2006. – 424 с. – Текст : непосредственный.

СВЕДЕНИЯ ОБ АВТОРАХ

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

Воронежский институт МВД России.

E-mail: sherserge@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Лукьянов Александр Сергеевич. Старший преподаватель кафедры инфокоммуникационных систем и технологий. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: las92@yandex.ru

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

Никулин Сергей Геннадьевич. Старший преподаватель кафедры тактико-специальной и огневой подготовки.

Казанский юридический институт МВД России.

Россия, 420108, Казань, ул. Магистральная, д. 35.

E-mail: kamenka_reds@mail.ru

Sherstyukov Sergey Anatolyevich. Professor of the chair of infocommunication systems and technologies. Doctor of technical sciences, assistant Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: sherserge@mail.ru

Work adress: Russia, 394065, Voronezh, Prospekt Patriotov, 53.

Lukyanov Alexander Sergeyevich. Senior teacher of department of infocommunication systems and technologies of the Voronezh institute of the Ministry of Internal Affairs of the Russian Federation.
E-mail: las92@yandex.ru
Work adress: Russia, 394065, Voronezh, Prospekt Patriotov, 53.

Nikulin Sergey Gennadievich. Senior lecturer at the Department of Special Tactics and Fire training.
Kazan Law Institute of the Ministry of Internal Affairs of the Russian Federation.
E-mail: kamenka_reds@mail.ru
Work adress: Russia, 420108, Kazan, Magistralnaya str. 35.

Ключевые слова: беспилотный летательный аппарат; радиосвязь; питание.

Keywords: unmanned aerial vehicle; radio communication; nutrition.

УДК 623.74

Научное издание

ОХРАНА,
БЕЗОПАСНОСТЬ, СВЯЗЬ

Сборник статей

Выпуск 10

Часть 1

В авторской редакции

Подписано в печать 28.03.2025
Формат 60х84 1/16
Усл. печ. л. 10,7
Тираж 60 экз.
Заказ № 41

Воронежский институт МВД России
394065, Воронеж, просп. Патриотов, 53

Типография Воронежского института МВД России
394065, Воронеж, просп. Патриотов, 53