Дата поступления рукописи в редакцию: 23.03.2026 г.
Дата принятия рукописи в печать: 25.04.2026 г.
DOI: 10.24412/2782-3849-2026-4-228-231

МАКАРОВА Елена Николаевна,

заместитель начальника кафедры криминалистических экспертиз и исследований, полковник полиции, кандидат юридических наук, Санкт-Петербургский университет МВД,

e-mail: n.manikin@mail.ru

ПИРОГОВА Елена Николаевна,

старший преподаватель кафедры тактико-специальной подготовки Волгодонского филиала РЮИ МВД России, подполковник полиции,

e-mail: pirogova-81@mail.ru

КРЫЛОВ Марк Александрович,

старший преподаватель кафедры тактико-специальной, огневой и физической подготовки Тверского филиала Московского ордена Почёта университета МВД России им. В.Я. Кикотя, подполковник полиции,

e-mail: kurkin @yandex.ru

СОВРЕМЕННЫЕ ПОДХОДЫ В СЛУЖБЕ ППС К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ ГОСУДАРСТВА

Аннотация. *В условиях стремительного развития информационных технологий и всё более активного использования цифровых ресурсов, обеспечение киберзащиты становится приоритетной задачей для государственных структур, коммерческих организаций и частных лиц. Статья посвящена современным подходам информационной безопасности. Раскрываются приемы, которые применяются в служба физической и технической защиты (ППС) для комплексного обеспечения кибербезопасности в различных сферах деятельности. Работа начинается с теоретической базы, в которой рассматриваются основные понятия и принципы киберзащиты, а также роль службы ППС в её обеспечении. Авторы проводят сравнительный анализ традиционных методов обеспечения безопасности и новых подходов, включая интеграцию ИИ и машинного обучения, использование блокчейн-технологий, внедрение систем управления идентификацией и доступом.*

Ключевые слова: *безопасность, информации, систем, защиты, подразделениями , сотрудники полиции, цифровая безопасность.*

MAKAROVA Elena Nikolaevna,

Deputy Head of the Department of Forensic Examinations and Research, Police Colonel, Candidate of Law, St. Petersburg University of the Ministry of Internal Affairs

PIROGOVA Elena Nikolaevna,

Senior Lecturer, Department of Tactical and Special Training, Volgodonsk Branch of the RUI of the Ministry of Internal Affairs of Russia, Police Lieutenant Colonel

KRYLOV Mark Alexandrovich,

Senior Lecturer, Department of Tactical, Special, Fire and Physical Training, Tver Branch of the Moscow Order of Honor of the University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot, Police Lieutenant Colonel

MODERN APPROACHES IN THE PPP SERVICE TO ENSURING THE CYBERSECURITY OF THE STATE

Annotation. *In the context of the rapid development of information technologies and the increasingly active use of digital resources, ensuring cybersecurity has become a priority for*

government agencies, commercial organizations, and individuals. This article focuses on modern approaches to information security. It explores the techniques employed by the Physical and Technical Protection Service (PPS) to comprehensively ensure cybersecurity in various fields. The article begins with a theoretical framework that introduces the fundamental concepts and principles of cybersecurity, as well as the role of the PPS in its implementation. The authors conduct a comparative analysis of traditional security methods and new approaches, including the integration of AI and machine learning, the use of blockchain technologies, and the implementation of identity and access management systems.

Key words: *security, information, systems, protection, divisions, police officers, digital security.*

Современная среда информационной безопасности в органах внутренних дел МВД характеризуется стремительной динамикой изменений, требующей постоянного совершенствования инструментов защиты и адаптации организационных подходов. Увеличение объёмов обрабатываемой информации и рост сложности киберугроз создают необходимость интеграции передовых технологий, которые выходят за рамки традиционных методов обеспечения безопасности. В частности, активное внедрение искусственного интеллекта и машинного обучения способствует улучшению обнаружения аномалий, автоматизации реагирования на инциденты и прогнозированию угроз с учетом новых сценариев атак [1].

Ещё одним важным направлением является применение блокчейн-технологий для повышения прозрачности и неизменности записей в системах учёта и обмена информацией. Это позволяет создавать распределённые регистры, устойчивые к фальсификациям, что особенно актуально для обеспечения целостности данных в правоохранительных органах. Кроме того, внедрение единых архитектур информационных систем МВД способствует устранению ранее существовавших барьеров между отдельными подразделениями, упрощая совместный доступ к необходимым данным и повышая оперативность принятия решений. Формирование систем, объединяющих процессы сбора, обработки и анализа информации в рамках централизованных платформ, стимулирует повышение качества работы и снижает дублирование ресурсов [2].

Нормативно-правовая база также претерпевает существенные изменения: законодательство и внутренние положения МВД адаптируются под новые технологические реалии, устанавливая более жёсткие требования к безопасности информационных систем и порядку обработки персональных данных. Современные стандарты предусматривают необходимость регулярного аудита и сертификации систем защиты, а также обязательного обучения сотрудников новым методам работы с цифровой информацией. Законодательные инициативы отражают переход от реактивных мер к проактивному управлению рисками, что повышает своевременность и эффективность контрмер [3].

Технологическая модернизация МВД не ограничивается только программным обеспечением. В 2025–2026 годах активно внедряются инновационные технические средства, такие как беспилотные летательные аппараты для оперативного мониторинга и пресечения правонарушений, а также интеллектуальные системы распознавания автомобильных номеров, установленные на патрульных машинах. Эти разработки интегрируются в информационные экосистемы ведомства и дополнительно повышают возможности сбора и анализа информации в реальном времени, что существенно расширяет возможности профилактики и расследования преступлений [4].

В совокупности, перспективы развития информационной безопасности МВД опираются на системный подход, объединяющий инновационные технологии, обновлённое нормативное регулирование и комплексную модернизацию технической базы. В этом контексте особую роль играет подготовка сотрудников ППС, которые должны регулярно повышать квалификацию и осваивать новые инструменты и методы работы с информацией. Способность оперативно адаптироваться к изменяющимся условиям и вызовам цифровой эпохи становится необходимым компонентом профессионализма, обеспечивающим защиту государства и граждан в условиях сложной и быстро меняющейся информационной среды [3] [4][4][6].

Информационные ресурсы в деятельности патрульно-постовой службы МВД представляют собой основу для организации оперативной работы, координации действий и принятия управленческих решений. В процессе несения службы сотрудники ППС используют разнообразные информационные системы, содержащие данные о правонарушениях, маршрутах патрулирования, установленных объектах охраны, а также базы персональных

данных граждан и служебную документацию. Эти ресурсы обеспечивают взаимодействие между подразделениями МВД, контроль за выполнением служебных задач и оперативное реагирование на происшествия.

Важнейшими объектами защиты информации в ППС являются информационные системы, которые обеспечивают автоматизацию служебных процессов и поддерживают функционирование Единой цифровой платформы МВД. В частности, это специализированные базы данных о зарегистрированных правонарушениях, сведения об административных протоколах и материалы служебных расследований, а также системы связи и передачи данных между подразделениями. Значительное внимание уделяется сохранности и конфиденциальности персональных данных граждан, поскольку нарушение их защиты может привести к нарушению прав человека и привести к юридическим последствиям для сотрудников и организационных структур МВД.

Помимо цифровых информационных систем, к объектам информационной безопасности относят служебные документы, бланки и распоряжения, используемые в работе ППС. Их защита необходима для предотвращения фальсификаций, утечки информации и нарушения установленных процедур ведения документации. Технические средства, включая мобильные устройства и специализированное программное обеспечение, также подпадают под охрану, учитывая угрозы взлома, несанкционированного доступа и воздействия вредоносного программного обеспечения [4].

Особое значение имеет защита информации, связанной с объектами массового пребывания граждан, которые находятся под охраной ППС. Согласно нормативным актам, к таким объектам применяются комплексные меры антитеррористической безопасности, включая контроль состояния информационных систем мониторинга и связи. Информационные потоки, поступающие от систем видеонаблюдения, охраны периметра и контроля доступа, должны обеспечивать целостность и доступность данных для оперативного управления и анализа обстановки в реальном времени. Нарушение безопасности данной информации могло бы скомпрометировать систему охраны и привести к угрозам безопасности граждан и работников служб [5].

Служба ППС также связана с обеспечением информационной безопасности режимных и особо важных объектов, что предполагает применение дополнительных мер защиты для информационных систем с повышенными требованиями к конфиденциальности, целостности и доступности. Координация действий в этом направлении осуществляется с другими подразделениями МВД и ведомственными структурами, что требует надежных средств защиты информационных ресурсов и обмена данными на основе централизованного управления и строгого протоколирования событий [7].

Таким образом, для эффективного построения системы информационной безопасности в деятельности ППС необходимо четко определить и классифицировать объекты защиты. Это включает не только информационные системы и базы данных, но и служебные материалы, технические средства и информационные потоки, обеспечивающие контроль и управление оперативными процессами. Выявление и детальное изучение данных объектов является отправной точкой для разработки комплексных мер по защите информации, что позволит снизить риски утечки, искажения и несанкционированного доступа в условиях динамичной оперативной деятельности ППС МВД.

Список литературы:

[1] Белевский Роман Александрович Перспективы развития системы информационной безопасности в органах внутренних дел // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2024. №4 (101). URL: https://cyberleninka.ru/article/n/perspektivy-razvitiya-sistemy-informatsionnoy-bezopasnosti-v-organah-vnutrennih-del (27.05.2025).

[2] Основные тенденции развития информационных технологий... [Электронный ресурс] // student-servis.ru - Режим доступа: https://student-servis.ru/spravochnik/osnovnye-tendentsii-razvitiya-informatsionnyh-tehnologij-i-elektronnogo-zashhishhennogo-dokumentooborota-v-organah-vnutrennih-del/, свободный. - Загл. с экрана

[3] Министерство внутренних дел российской федерации [Электронный ресурс] // lib.eioskuimvd.ru - Режим доступа: http://lib.eioskuimvd.ru/jirbis2/_docs_file (свободный. - Загл. с экрана)

[4] Проблемы и перспективы развития... [Электронный ресурс] // scilead.ru - Режим доступа: https://scilead.ru/article/9203-problemi-i-perspektivi-razvitiya-informatsion, свободный. - Загл. с экрана

[5] Защита ведомственных мобильных устройств на Android [Электронный ресурс] // www.anti-malware.ru - Режим доступа: https://www.anti-malware.ru/analytics/Technology_Analysis/Protection_departmental_mobile_devices_Android, свободный. - Загл. с экрана

[6] Общие вопросы обеспечения [Электронный ресурс] // futurepubl.ru - Режим доступа:

https://futurepubl.ru/ru/storage/download/48093, свободный. - Загл. с экрана
[7] Сайт: ви.мвд.рф/institute/Pravovoy_razdel/Pravovoj_likbez/Normativno... [Электронный ресурс] // ви.мвд.рф - Режим доступа: https://ви.мвд.рф/institute/Pravovoy_razdel/Pravovoj_likbez/Normativno_pravovie_akti_po_napravleniju/Obespechenie_informacionnoj_bezopasnosti, свободный. - Загл. с экрана

References:

[1] Belevsky Roman Aleksandrovich Prospects for the development of an information security system in the internal affairs bodies//Scientific Bulletin of the Oryol Law Institute of the Ministry of Internal Affairs of Russia named after V.V. Lukyanov. 2024. №4 (101). URL: https://cyberleninka.ru/article/n/perspektivy-razvitiya-sistemy-informatsionnoy-bezopasnosti-v-organah-vnutrennih-del (27.05.2025).
[2] Key IT Trends... [Электронный ресурс] // student-servis.ru - Режим доступа: https://student-servis.ru/spravochnik/osnovnye-tendentsii-razvitiya-informatsionnyh-tehnologij-i-elektronnogo-zashhishhennogo-dokumentooborota-v-organah-vnutrennih-del/, свободный. - Zagl. from the screen
[3] Ministry of Internal Affairs of the Russian Federation [Electronic resource]// lib.eioskuimvd.ru - Access mode: http://lib.eioskuimvd.ru/jirbis2/_docs_file (free. - Zagl. from the screen)
[4] Challenges and development prospects... [Электронный ресурс] // scilead.ru - Режим доступа: https://scilead.ru/article/9203-problemi-i-perspektivi-razvitiya-informatsion, свободный. - Zagl. from the screen
[5] Protection of departmental mobile devices on Android [Electronic resource]// www.anti-malware.ru - Access mode: https://www.anti-malware.ru/analytics/Technology_Analysis/Protection_departmental_mobile_devices_Android, free. - Zagl. from the screen
[6] General security issues [Electronic resource]// futurepubl.ru - Access mode: https://futurepubl.ru/ru/storage/download/48093, free. - Zagl. from the screen
[7] Сайт: ви.мвд.рф/institute/Pravovoy_razdel/Pravovoj_likbez/Normativno... [Электронный ресурс] // ви.мвд.рф - Режим доступа: https://ви.мвд.рф/institute/Pravovoy_razdel/Pravovoj_likbez/Normativno_pravovie_akti_po_napravleniju/Obespechenie_informacionnoj_bezopasnosti, свободный. - Zagl. from the screen

