Дата поступления рукописи в редакцию: 23.03.2026 г.
Дата принятия рукописи в печать: 25.04.2026 г.
DOI: 10.24412/2782-3849-2026-4-258-261

ПАРАМОНОВА Галина Владимировна,

доцент кафедры криминалистических экспертиз и исследований кандидат юридических наук, доцент,

e-mail: paramonovagalina@rambler.ru

ПИРОГОВА Елена Николаевна,

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

e-mail: pirogova-81@mail.ru

КИЯШКИН Павел Владимирович,

преподаватель кафедры тактико-специальной подготовки Краснодарского университета МВД России майор полиции,

e-mail: kurkin @yandex.ru

РОЛЬ ПАТРУЛЬНО-ПОСТОВОЙ СЛУЖБЫ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГРАЖДАН

Аннотация. *В статье рассматривается роль патрульно-постовой службы (ППС) в обеспечении и защите прав и свобод граждан в условиях правового государства. Анализируются основные функции ППС как одного из наиболее приближенных к населению подразделений правоохранительных органов, обеспечивающего общественный порядок, предупреждение правонарушений и оперативное реагирование на угрозы безопасности. Особое внимание уделяется правовым основам деятельности ППС, принципам законности, гуманизма и уважения прав человека. Раскрываются проблемы, связанные с превышением полномочий, недостаточным уровнем правовой культуры и взаимодействием с гражданами, а также предлагаются пути их решения, включая повышение профессиональной подготовки сотрудников и усиление контроля за их деятельностью. Делается вывод о ключевой роли ППС в укреплении доверия общества к государственным институтам и обеспечении реальной защиты прав и свобод личности.*

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

PARAMONOVA Galina Vladimirovna,

Associate Professor, Department of Forensic Examinations and Research, Candidate of Law, Associate Professor

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

KIYASHKIN Pavel Vladimirovich,

Lecturer, Department of Tactical and Special Training, Krasnodar University, Ministry of Internal Affairs of Russia, Police Major

THE ROLE OF THE PATROL AND GUARD SERVICES OF THE INTERNAL AFFAIRS BODIES IN ENSURING INFORMATION SECURITY FOR CITIZENS

Annotation. *The article examines the role of the Patrol and Watch Service (PWS) in ensuring and protecting the rights and freedoms of citizens in a legal state. It analyzes the main functions of the PWS as one of the closest law enforcement agencies to the population, which ensures public*

order, prevents offenses, and promptly responds to security threats. Special attention is given to the legal basis of the PWS's activities, the principles of legality, humanism, and respect for human rights. The article reveals the problems associated with abuse of authority, insufficient legal culture, and interaction with citizens, and suggests ways to solve them, including improving the professional training of employees and strengthening control over their activities. The article concludes that the police play a crucial role in building public trust in government institutions and ensuring the real protection of individual rights and freedoms.

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

Анализ и моделирование угроз информационной безопасности служат фундаментальным этапом построения эффективной системы защиты для сотрудников ППС МВД и ИСПДн. Модель угроз представляет собой формальное или концептуальное описание всех возможных нарушений конфиденциальности, целостности и доступности информации, которое позволяет систематизировать потенциальные источники опасности, оценить их воздействие и определить приоритеты в выборе средств защиты [1]. Такой аналитический подход обеспечивает комплексное понимание рисков и способствует формированию адекватных мер противодействия, исходя из специфики деятельности подразделений ППС.

В условиях МВД основными угрозами информационной безопасности выступают как случайные, так и преднамеренные действия, связанные с человеческим фактором. К ним относятся ошибки сотрудников ППС при работе с информационными системами, неправильное применение служебных полномочий и внутренние злоупотребления доступом к данным. Наличие внутриорганизационных рисков требует применения жестких процедур контроля и аудита всех операций с персональными данными и другими конфиденциальными сведениями, в том числе при использовании мобильных устройств, которые широко внедряются для оперативного взаимодействия и передачи информации [2].

Сетевая инфраструктура МВД подвержена угрозам, включающим попытки несанкционированного доступа, внедрение вредоносного программного обеспечения, а также атаки, направленные на отказ в обслуживании (Denial of Service). Последние особенно опасны для оперативных систем, так как сниженная доступность может привести к задержкам в передаче критически важной информации и нарушению координации действий сотрудников ППС в экстренных ситуациях. Для противодействия таким атакам в модели угроз учитываются параметры пропускной способности каналов связи, время отклика систем и возможности мониторинга сетевого трафика [3].

Уязвимости мобильных устройств, которые часто работают на платформе Android, представляют дополнительный вектор угроз. Отсутствие своевременных обновлений безопасности, недостаточный уровень защиты от эксплойтов и вирусов, а также слабая централизация контроля над используемым программным обеспечением требуют комплексных технических и организационных мер. В модели угроз они выделены как особая категория факторов, влияющих на уровень безопасности информационных процессов в подразделениях ППС [1][3].

Правовые и организационные аспекты занимают важное место в модели угроз, поскольку правильное регулирование доступа, ответственность за нарушение информационной безопасности и наличие нормативной базы способствуют снижению рисков и обеспечивают механизм реагирования на инциденты. Документы МВД и федеральные стандарты предписывают ответственность за информационные правонарушения и устанавливают требования к внутреннему контролю, что включается в модель угроз как обязательный элемент комплексной стратегии безопасности [4].

Модель угроз для ИСПДн и служб ППС МВД строится с учетом вероятностно-статистических методов, что позволяет прогнозировать вероятность реализации различных видов атак и отказов. Эволюционное и структурное моделирование способствует адаптации мер защиты под изменяющиеся условия, что крайне важно для динамичной оперативной среды МВД. Учет субъективных факторов, таких как человеческие ошибки и злонамеренные действия, повышает реалистичность модели и качество оценки рисков [4][3].

Вывод из анализа подчеркивает необходимость регулярного обновления и корректировки модели угроз с учетом технологических изменений, новых векторов атак и изменений в законодательном поле. Периодический пересмотр модели обеспечивает актуальность защиты и позволяет своевременно адаптировать методы и средства безопасности для сотрудников ППС. Только такой подход способствует своевременному выявлению и нейтрализации новых рисков, которые

возникают в условиях постоянного усложнения информационной среды МВД [7][3].

Методический подход к выбору средств защиты информации в деятельности ППС МВД базируется на комплексном анализе модели угроз и классификации информационных систем персональных данных (ИСПДн). Подразделения-операторы ИСПДн при создании или модернизации систем определяют их класс, что служит исходной точкой для подбора адекватных технических и организационных мер. Такой процесс позволяет учитывать специфику обрабатываемых данных, возможные риски и характер потенциальных атак, отталкиваясь от приоритетов, выявленных в модели угроз [5].

Выбор средств защиты ориентирован на обеспечение конфиденциальности, целостности и доступности информационных ресурсов. Технические меры включают применение сертифицированных криптографических средств, систем контроля и разграничения доступа, а также инструментов обнаружения и предотвращения сетевых атак, в том числе противодействие угрозам типа «человек посередине» и эксплойтам «нулевого дня». Эти решения интегрируются в единую информационную систему централизованной обработки данных (ЕИС ЦОД), построенную с использованием современных технологий виртуализации, облачных платформ и распределённых дата-центров, что требует усиленных мер защиты для сохранения высокой надежности и отказоустойчивости информационной инфраструктуры МВД [5][7].

Организационные методы заключаются в разработке и внедрении нормативно-методической базы, регламентирующей порядок обработки и защиты персональных данных, а также в обеспечении квалифицированной подготовки сотрудников. В частности, ведомственные учебные заведения реализуют специальные курсы и тренинги, направленные на повышение компетенций по работе с конфиденциальной информацией и соблюдение требований безопасности. Существенное внимание уделяется постоянному обновлению перечня защищаемых документов и ограничению доступа к секретной информации, предоставляя допуск только уполномоченным лицам в строгом соответствии с их служебными обязанностями [4].

Порядок выбора и реализации средств защиты регламентируется приказами МВД, такими как № 678 от 06.07.2012 и № 538 от 15.07.2013, которые устанавливают требования к процессам классификации ИСПДн и подбору соответствующих мер. Эти нормативные акты обеспечивают системность и прозрачность внедрения защиты, позволяет адаптировать меры под изменяющиеся условия эксплуатации и возникающие угрозы. Внедрение современных технических решений в сочетании с организационными мерами формирует комплексную систему защиты, учитывающую как внутренние, так и внешние риски [2][6].

Особое значение имеет учет специфики работы подразделений ППС, связанный с постоянным оперативным режимом, использованием мобильных устройств и необходимости быстрого доступа к информации. Поэтому выбранные меры защиты должны обладать гибкостью, позволяющей оперативно реагировать на инциденты и обеспечивать непрерывность доступа к критически важным данным без снижения уровня безопасности. Адаптация инструментов и процедур под реальные условия работы ППС является обязательным условием эффективного функционирования системы информационной безопасности в МВД.

Таким образом, методы и способы выбора средств защиты информации в ППС МВД представляют собой взаимосвязанный и динамичный процесс, комбинирующий анализ угроз, классификацию информационных систем, внедрение современных технических средств и организационных мероприятий, а также подготовку кадров.

Список литературы:

[1] Бабкин Александр Николаевич, Куличенко Анна Юрьевна, Широкий Александр Александрович Моделирование и прогнозирование угроз информационной безопасности регионального сегмента ИСОД МВД России // Вестник Воронежского института МВД России. 2020. №2. URL: https://cyberleninka.ru/article/n/modelirovanie-i-prognozirovanie-ugroz-informatsionnoy-bezopasnosti-regionalnogo-segmenta-isod-mvd-rossii (13.07.2025).

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

[3] Бабкин Александр Николаевич, Куличенко Анна Юрьевна, Широкий Александр Александрович Моделирование и прогнозирование угроз информационной безопасности регионального сегмента ИСОД МВД России // Вестник Воронежского института МВД России. 2020. №2. URL: https://cyberleninka.ru/article/n/modelirovanie-i-prognozirovanie-ugroz-informatsionnoy-bezopasnosti-regionalnogo-segmenta-isod-mvd-rossii (13.07.2025).

[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] Анализ и классификация основных угроз... [Электронный ресурс] // bit.spels.ru - Режим доступа: https://bit.spels.ru/index.php/bit/article/view/1250, свободный. - Загл. с экрана
[7] Диссертация на тему «Моделирование информационных...» [Электронный ресурс] // www.dissercat.com - Режим доступа: https://www.dissercat.com/content/modelirovanie-informatsionnykh-protsessov-v-kompyuternykh-sistemakh-organov-vnutrennikh-del-, свободный. - Загл. с экрана
[8] Приказ МВД РФ от 6 июля 2012 г. № 678 “Об утверждении...” [Электронный ресурс] // www.garant.ru - Режим доступа: https://www.garant.ru/products/ipo/prime/doc/70130320/, свободный. - Загл. с экрана

References:

[1] Babkin Alexander Nikolaevich, Kulichenko Anna Yuryevna, Shiroky Alexander Alexandrovich Modeling and forecasting threats to information security of the regional segment of the ISOD of the Ministry of Internal Affairs of Russia//Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. 2020. №2. URL: https://cyberleninka.ru/article/n/modelirovanie-i-prognozirovanie-ugroz-informatsionnoy-bezopasnosti-regionalnogo-segmenta-isod-mvd-rossii (13.07.2025).
[2] 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)
[3] Babkin Alexander Nikolaevich, Kulichenko Anna Yuryevna, Shiroky Alexander Alexandrovich Modeling and forecasting threats to information security of the regional segment of the ISOD of the Ministry of Internal Affairs of Russia//Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. 2020. №2. URL: https://cyberleninka.ru/article/n/modelirovanie-i-prognozirovanie-ugroz-informatsionnoy-bezopasnosti-regionalnogo-segmenta-isod-mvd-rossii (13.07.2025).
[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] Analyze and classify top threats... [Electronic resource]// bit.spels.ru - Access mode: https://bit.spels.ru/index.php/bit/article/view/1250, free. - Zagl. from the screen
[7] Thesis on “Modeling information...” [Электронный ресурс] // www.dissercat.com - Режим доступа: https://www.dissercat.com/content/modelirovanie-informatsionnykh-protsessov-v-kompyuternykh-sistemakh-organov-vnutrennikh-del-, свободный. - Zagl. from the screen
[8] Order of the Ministry of Internal Affairs of the Russian Federation of July 6, 2012 No. 678 “On approval...” [Electronic resource]// www.garant.ru - Access mode: https://www.garant.ru/products/ipo/prime/doc/70130320/, free. - Zagl. from the screen

