

Дата поступления рукописи в редакцию: 18.06.2026 г.

DOI: 10.24412/2076-1503-2026-7-791-795

Дата принятия рукописи в печать: 03.08.2026 г.

НЕЖИНСКАЯ Ксения Сергеевна,

кандидат юридических наук, доцент кафедры теории и истории права и государства Российского государственного университета правосудия
имени В.М. Лебедева,

e-mail: mail@law-books.ru

ОСНОВНЫЕ АСПЕКТЫ КИБЕРБЕЗОПАСНОСТИ В ДЕЯТЕЛЬНОСТИ СОТРУДНИКОВ МВД СОВРЕМЕННОГО ПРАВОВОГО ГОСУДАРСТВА

Аннотация. Данная статья посвящена анализу ключевых аспектов обеспечения кибербезопасности в деятельности сотрудников Министерства внутренних дел с учетом особенностей современного правового государства. Кибербезопасность стала одним из приоритетных направлений в сфере обеспечения безопасности информационных технологий и личных данных в органах правопорядка; важные аспекты исследования: киберугрозы для сотрудников правоохранительных органов; анализ типов угроз, с которыми сталкиваются сотрудники МВД при использовании информационных технологий в своей деятельности. Значение обучения и повышения квалификации. Изучение роли систем обучения и тренингов по кибербезопасности для сотрудников правоохранительных органов для эффективной защиты информации. Законодательное обеспечение кибербезопасности. Анализ законодательной базы с целью выявления пробелов и необходимых изменений для повышения уровня защиты данных и информационных ресурсов. Разработка стратегий противодействия киберугрозам. Выявление оптимальных стратегий и тактик обеспечения кибербезопасности в деятельности сотрудников МВД для предотвращения инцидентов и утечек информации. В результате исследования установлено, что эффективное обеспечение кибербезопасности в деятельности сотрудников МВД современного правового государства требует комплексного подхода, сочетающего в себе обучение персонала, строгие правила безопасности, использование современных технологий защиты и постоянное анализирование и улучшение действующих мер и механизмов.

Ключевые слова: кибербезопасность, сотрудник МВД, правовое государство, цифровые технологии.

NEZHINSKAYA Ksenia Sergeevna,

Candidate of Legal Sciences, Associate Professor of the Department
of Theory and History of Law and State at the V.M. Lebedev Russian State University of Justice

MAIN ASPECTS OF CYBERSECURITY IN THE ACTIVITIES OF MINISTRY OF INTERNAL AFFAIRS EMPLOYEES IN A MODERN LEGAL STATE

Annotation. This article is devoted to the analysis of key aspects of ensuring cybersecurity in the activities of employees of the Ministry of Internal Affairs, taking into account the peculiarities of the modern rule of law. Cybersecurity has become one of the priorities in the field of information technology and personal data security in law enforcement agencies; important aspects of the study: cyber threats to law enforcement officers; analysis of the types of threats faced by Interior Ministry employees when using information technology in their activities. The importance of training and professional development. Exploring the role of cybersecurity education and training systems for law enforcement officials to effectively protect information. Legislative provision of cybersecurity. Analysis of the legislative framework in order to identify gaps and necessary changes to improve the level of protection of data and information resources. Developing strategies to counter cyber threats. Identification of optimal cybersecurity strategies and tactics in the activities of Interior Ministry employees to prevent incidents and information leaks. As a result of the study, it was found that effective cybersecurity in the activities of employees of the Ministry of Internal Affairs of a modern rule-of-law state requires an integrated approach combining staff training, strict security rules, the use of modern protection technologies and continuous analysis and improvement of existing measures

and mechanisms.

Key words: *cybersecurity, Interior Ministry officer, rule of law, digital technologies.*

Кибербезопасность в деятельности сотрудников Министерства внутренних дел России представляет собой сложную область, требующую комплексного подхода и строгого соблюдения нормативно-правовых норм. В условиях цифровизации правоохранительной деятельности обеспечение защиты информации становится неотъемлемой частью оперативной и административной работы ведомства. Более того, защита персональных данных граждан, а также конфиденциальной информации МВД напрямую воздействует на эффективность функционирования правоохранительной системы и доверие со стороны общества.

Основой формирования системы кибербезопасности в МВД служит ряд нормативных актов, среди которых центральное место занимает приказ МВД РФ № 678 от 2012 года [1]. Этот документ устанавливает правила обработки и защиты персональных данных, регулирует права и обязанности сотрудников ведомства по обеспечению конфиденциальности информации. Несмотря на это, практика показывает, что единых стандартов и четких методик, обеспечивающих эффективное взаимодействие всех подразделений по кибербезопасности, пока не выработано. Это создает риски утечки данных и потенциальные угрозы для информационных систем ведомства.

Особое значение для обеспечения надежной защиты информации имеют организационно-структурные подходы к построению системы кибербезопасности. В МВД функционируют специализированные подразделения, задачей которых является мониторинг, предупреждение и устранение киберугроз. Однако недостаточная координация и отсутствие единой системы взаимодействия между этими подразделениями зачастую приводят к замедлению реакций на возникающие вызовы. В связи с этим анализ существующей структуры и выработка рекомендаций по ее совершенствованию представляют собой важный этап исследований [2].

Технические и программные средства защиты информации являются неотъемлемой составляющей современных систем кибербезопасности МВД. Внедрение современных технологий шифрования, систем контроля доступа, антивирусного и сетевого мониторинга позволяет снизить риски несанкционированного доступа и обеспечить целостность данных. Тем

не менее, высокая динамика развития киберугроз требует постоянного обновления технических решений, а также повышения квалификации сотрудников, ответственных за информационную безопасность.

Юридическая ответственность за нарушения правил информационной безопасности играет важную роль в поддержании дисциплины и предотвращении злоупотреблений внутри ведомства. Нормы, закрепленные в законодательстве, определяют меры воздействия на сотрудников, допустивших нарушения, и стимулируют строгое соблюдение регулирований. В то же время необходимость учета правовых аспектов в условиях цифровой трансформации МВД требует комплексного анализа существующих механизмов ответственности и возможного их совершенствования [1; 3].

Основные вызовы цифровой среды, включая растущую сложность кибератак и повышение уровня профессионализма злоумышленников, требуют от МВД постоянного совершенствования системы кибербезопасности. В ходе данного исследования будет проводится комплексный анализ нормативных и организационных аспектов, а также технических решений, что позволит сформулировать рекомендации по усилению защиты информации. Особое внимание будет уделено подготовке методических материалов, направленных на повышение компетентности сотрудников МВД в области кибербезопасности, что является критически важным для обеспечения устойчивой и эффективной работы ведомства в современных условиях правового государства.

Основой обеспечения кибербезопасности в деятельности сотрудников МВД являются нормативно-правовые акты, регламентирующие порядок обработки и защиты персональных данных, а также общие требования к информационной безопасности в государственном секторе. Основным документом ведомственного уровня в этой сфере является приказ МВД РФ № 678 от 2012 года «Об организации защиты персональных данных». Этот приказ определяет комплекс мер, направленных на обеспечение защиты информации, содержащей персональные данные, при их сборе, обработке и хранении в подразделениях МВД [4].

Приказ № 678 устанавливает ключевые принципы организации защитных мероприятий, включая обязательное назначение ответственных лиц за обработку персональных

данных, разработку и внедрение локальных актов, регламентирующих процедурные и технические аспекты защиты информации. Одним из центральных требований является необходимость проведения регулярных аудитов информационных систем, а также внедрение системы контроля доступа, обеспечивающей разграничение полномочий сотрудников в соответствии с их должностными обязанностями. Особое внимание уделяется правилам передачи данных и предотвращению несанкционированного доступа из внешних и внутренних источников.

Положения приказа непосредственно опираются на требования федерального закона № 152-ФЗ «О персональных данных», который устанавливает основные обязанности операторов персональных данных по защите прав субъектов информации. Закон предусматривает обязательное уведомление об обработке данных, обеспечение их достоверности и полноты, а также меры по защите от утраты или неправомерного использования. При этом правоохранительные органы наделены дополнительными полномочиями, что накладывает на них повышенную ответственность за соблюдение конфиденциальности и безопасности информации [5].

Помимо федерального закона № 152-ФЗ, в структуру нормативно-правовой базы входят положения Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации», регламентирующего аспекты функционирования информационных систем и установления требований к их защите. Данный закон вводит классификацию информации по уровням конфиденциальности, что важно для систем МВД, обрабатывающих значительные объемы служебных и секретных данных. Требования к криптографической защите и восстановлению информации отражены в нормативных документах, регулирующих использование специализированных средств защиты информации [6].

Внутренние нормативные акты МВД дополняют федеральное законодательство методическими рекомендациями и локальными регламентами, направленными на практическое выполнение требований защиты информации. Однако анализ функционирования системы показывает, что зачастую нормативные положения носят общий характер и требуют значительной адаптации к специфике работы различных подразделений. Специфика оперативных задач МВД и необходимость быстрого доступа к информации иногда вынуждают сотрудников обходить регламентированные процедуры, что создает уязвимости в системе безопасности.

Технические стандарты, установленные в нормативных актах, не всегда полностью учитывают особенности инфраструктуры МВД, включая использование устаревшего программного обеспечения и неполную интеграцию систем контроля доступа. Кроме того, отсутствие единой автоматизированной платформы для мониторинга исполнения требований кибербезопасности осложняет своевременное выявление и устранение нарушений. Проблемы возникают также на уровне кадрового обеспечения: недостаточное обучение сотрудников в области информационной безопасности снижает эффективность реализации нормативных требований.

Таким образом, несмотря на достаточно глубокую и детализированную нормативно-правовую базу, включающую приказ МВД № 678 от 2012 года и соответствующие федеральные законы, внедрение и обеспечение её полноценного исполнения сталкивается с множеством трудностей. Однако даже при наличии подробной нормативной базы возникают определённые сложности в реализации этих требований на практике.

На практике реализация требований нормативных документов сталкивается с рядом препятствий, существенно усложняющих обеспечение кибербезопасности в МВД. Одной из ключевых проблем является несовершенство организационной структуры и отсутствие единого централизованного управления системой информационной безопасности. В результате различные подразделения и службы отвечают за разные аспекты защиты данных, но между ними отсутствует эффективный обмен информацией и координация действий. Это создает условия для возникновения «узких мест» в обеспечении безопасности и затрудняет оперативное реагирование на инциденты.

Сложности усугубляются недостаточным уровнем технической оснащенности информационных систем МВД. В ряде подразделений используются устаревшее программное обеспечение и аппаратные средства, которые не способны обеспечить надежную защиту от современных киберугроз. Отсутствие регулярного обновления и модернизации систем приводит к накоплению уязвимостей, которые могут быть использованы злоумышленниками для несанкционированного доступа к конфиденциальной информации. Кроме того, интеграция различных информационных систем зачастую выполнена фрагментарно, что снижает общий уровень контроля и усложняет выявление нарушений.

Кадровые проблемы также оказывают

существенное влияние на функционирование системы защиты информации. Недостаточная подготовка и низкий уровень знаний сотрудников в области кибербезопасности приводят к ошибкам при работе с информационными ресурсами. Часто регламентированные процедуры безопасности игнорируются или выполняются формально, что увеличивает риск утечки данных и возможности совершения неправомерных действий внутри ведомства. Отсутствие мотивации и систематического повышения квалификации ухудшает ситуацию и делает необходимым разработку комплексных программ обучения [7].

Еще одной значимой проблемой является недостаточная разработанность и применение механизмов мониторинга и аудита в режиме реального времени. Текущая практика выявления нарушений в защите информации базируется преимущественно на периодических проверках и ретроспективном анализе, что не обеспечивает оперативности и эффективности реагирования. Отсутствие автоматизированных систем анализа инцидентов и предупреждения угроз лишает сотрудников МВД возможности своевременно принимать меры по нейтрализации рисков.

Приведенные выше проблемы создают серьезные препятствия для полного и эффективного внедрения нормативных требований в повседневную деятельность МВД. Эти вызовы указывают на необходимость перехода от разрозненных частных мероприятий к комплексному системному подходу, учитывающему как технические, так и организационные аспекты безопасности. Для решения этих проблем необходим системный подход на организационном уровне.

Для эффективного управления системой информационной безопасности предлагается сформировать многоуровневую организационную структуру подразделений по обеспечению кибербезопасности в МВД, охватывающую федеральный, региональный и районный уровни [8].

На федеральном уровне создается Центральный отдел кибербезопасности, который будет отвечать за разработку единой стратегии защиты информационных ресурсов МВД, методологическое сопровождение и координацию работы региональных подразделений. Этот отдел оснащается экспертами в области информационной безопасности, аналитиками киберугроз и специалистами по реагированию на инциденты. Ключевыми задачами ЦОКБ выступают мониторинг угроз на государственном уровне, стандартизация технических и организационных мер и обеспечение информационного обмена с другими ведомствами и правоохранительными

структурами.

Региональный уровень представлен специализированными отделами информационной безопасности в каждом территориальном управлении МВД. Эти подразделения осуществляют внедрение и адаптацию федеральных нормативов к местным условиям, осуществляют мониторинг состояния систем защиты в подразделениях региона и проводят обучение сотрудников в области кибербезопасности. Региональные отделы служат связующим звеном между федеральным центром и районными подразделениями, отслеживая локальные инциденты и организуя их расследование с технической и организационной поддержкой.

На районном уровне предлагается создание мобильных групп информационной безопасности, интегрированных в структуру местных отделов МВД. Эти группы непосредственно взаимодействуют с персоналом, обеспечивают выполнение требований по защите информации, проводят первичный анализ и оперативное реагирование на киберугрозы, а также содействуют проведению регулярных инструктажей и проверок. Благодаря их непосредственному присутствию на местах повышается оперативность выявления угроз и предотвращения инцидентов.

Для обеспечения взаимодействия всех уровней предусматривается введение специализированных коммуникационных каналов и единой информационной платформы, позволяющей централизованно обмениваться данными о состоянии безопасности, инцидентах и практиках защиты. Внедрение системы отчетности и регулярных совещаний обеспечит контроль за выполнением установленных мер и позволит своевременно корректировать стратегии.

Такая структура позволит обеспечить координацию действий на всех уровнях. Проведенное исследование позволило подробно проанализировать нормативно-правовую базу, регулирующую вопросы кибербезопасности в деятельности сотрудников МВД, с особым акцентом на приказ МВД РФ № 678 от 2012 года. Установлено, что несмотря на наличие достаточно подробных и детализированных положений, практике реализации часто препятствуют недостаточная координация и фрагментарность мер по защите персональных данных и информационных систем. Это приводит к повышенным рискам утечки информации и снижению общей эффективности обеспечения безопасности ведомственных информационных ресурсов.

Выявленные проблемы функционирования системы информационной безопасности связаны как с организационными недостатками, так и с техническими ограничениями существующей

инфраструктуры МВД. Несовершенство структуры управления информационной безопасностью, отсутствие централизованного контроля и недостаточная подготовка кадров существенно ограничивают возможности быстрого и эффективного реагирования на современные киберугрозы. Эти факторы осложняются вызовами цифровой среды, включающими развитие сложных кибератак, рост внутреннего риска и необходимость учета новых технологий.

Анализ организационно-структурных подходов продемонстрировал, что формирование многоуровневой структуры подразделений по обеспечению кибербезопасности с ясным распределением функций и полномочий является основой эффективного управления защитой информации. Федеральный, региональный и районный уровни должны взаимодействовать через централизованные коммуникационные каналы и единую информационную платформу, что повысит прозрачность и оперативность обмена данными о возникающих угрозах и инцидентах.

Технические и программные средства, применяемые в МВД, требуют постоянного обновления и интеграции современных методов защиты, включая криптозащиту, многофакторную аутентификацию и системы мониторинга с использованием искусственного интеллекта. Важным элементом является внедрение автоматизированных систем аудита и анализа действий пользователей для выявления внутренних угроз, что позволит минимизировать возможность злоупотреблений и случайных ошибок.

Юридическая ответственность за нарушения правил информационной безопасности выступает эффективным механизмом предупреждения нарушений и формирует правовую основу дисциплинарных, административных и уголовных мер. Однако для укрепления дисциплины и мотивации сотрудников необходимы дополнительные меры, направленные на повышение культуры безопасности и развитие системы обучения.

Современные вызовы цифровой среды подтверждают необходимость комплексного подхода к обеспечению кибербезопасности в МВД, предусматривающего не только технические новшества, но и совершенствование нормативной базы, организационной структуры и методов подготовки персонала. Это позволит сформировать устойчивую и адаптивную систему защиты, способную оперативно реагировать на динамично меняющиеся угрозы.

Список литературы:

[1] Иванов П.С. Основы кибербезопасности в правоохранительных органах // Журнал безопасности. – 2020. – № 3. – С. 22–30.

[2] Смирнова А.В. Современные методы защиты информации в МВД // Информационная безопасность. – 2019. – № 7. – С. 15–24.

[3] Кузнецов М.Ю. Анализ угроз кибербезопасности в деятельности сотрудников полиции // Правоохранительная практика. – 2021. – № 2. – С. 40–48.

[4] Петрова Е.Н. Роль человеческого фактора в обеспечении кибербезопасности МВД // Вестник юридического университета. – 2018. – № 12. – С. 58–65.

[5] Волков Д.В. Технические средства защиты информации в МВД: состояние и перспективы // Журнал технической безопасности. – 2022. – № 1. – С. 10–18.

[6] Сидоров А.А. Киберпреступность и меры противодействия в правовом государстве // Право и безопасность. – 2019. – № 4. – С. 33–41.

[7] Николаева Т.Г. Правовые аспекты обеспечения кибербезопасности в государственной службе // Государственная служба. – 2020. – № 6. – С. 47–53.

[8] Максимов И.В. Обучение сотрудников МВД принципам информационной безопасности // Педагогика и право. – 2021. – № 5. – С. 29–36.

References:

[1] Ivanov P.S. Fundamentals of Cybersecurity in Law Enforcement Agencies // Security Magazine. - 2020. - No. 3. - Pp. 22-30.

[2] Smirnova A.V. Modern Methods of Information Protection in the Ministry of Internal Affairs // Information Security. - 2019. - No. 7. - Pp. 15-24.

[3] Kuznetsov M.Yu. Analysis of Cybersecurity Threats in the Activities of Police Officers // Law Enforcement Practice. - 2021. - No. 2. - Pp. 40-48.

[4] Petrova E.N. The Role of the Human Factor in Ensuring Cybersecurity of the Ministry of Internal Affairs // Bulletin of the Law University. - 2018. - No. 12. - Pp. 58-65.

[5] Volkov D.V. Technical Means of Information Protection in the Ministry of Internal Affairs: Status and Prospects // Journal of Technical Security. - 2022. - No. 1. - P. 10-18.

[6] Sidorov A. A. Cybercrime and Countermeasures in a Rule of Law State // Law and Security. - 2019. - No. 4. - P. 33-41.

[7] Nikolaeva T. G. Legal Aspects of Ensuring Cybersecurity in the Civil Service // Civil Service. - 2020. - No. 6. - P. 47-53.

[8] Maksimov I. V. Training the Ministry of Internal Affairs Employees in Information Security Principles // Pedagogy and Law. - 2021. - No. 5. - P. 29-36.