Дата поступления рукописи в редакцию: 26.03.2026 г.
Дата принятия рукописи в печать: 25.04.2026 г.

DOI: 10.24412/2782-3849-2026-4-265-268

КАСАТКИНА Наталья Владимировна,

старший преподаватель кафедры криминалистических экспертиз и исследований Санкт-Петербургского университета МВД России,

e-mail: K7-nata@yandex.ru

СТАУРСКИЙ Станислав Станиславович,

к.э.н., доцент, преподаватель кафедры экономики и управления Российской академии народного хозяйства и государственной службы, филиал г. Омск,

e-mail: nparnyuk@mail.ru,

КИБЕРБЕЗОПАСНОСТЬ В СИСТЕМЕ МВД В СОВРЕМЕННОМ ПРАВОВОМ ГОСУДАРСТВЕ

Аннотация. *В данной статье рассматривается проблема кибербезопасность в системе МВД в современном правовом государстве. Цель исследования – определить причины информационной преступности. Авторами разрываются особенности организации и обеспечения кибербезопасности в МВД в условиях современного правового государства.. Особое внимание уделено особенностям,которые организуют и обеспечивыапют кибербезопасность в системе МВД в условиях современного правового государства. В рамках исследования рассмотрены ключевые направления и методы обеспечения кибербезопасности, проанализированы правовые основы и нормативные акты, регулирующие эту сферу. Авторы изучают перспективы применения данных метод, которые активизируют и способствуют более интенсивному контролю информационной безопасности. Исследование проведено с целью выявления ключевых проблем кибербезопасности в современном правовом государстве. Научная новизна заключается в изучении р правовой базы, организационных механизмов и практические методы обеспечения кибербезопасности в системе МВД, что позволит выявить ключевые проблемы и предложить пути их решения.*

Ключевые слова: *кибербезопасность в системе МВД, преступление, технических и правовых меры.*

KASATKINA Natalya Vladimirovna,

Senior Lecturer, Department of Forensic Examinations and Research, St. Petersburg University of the Ministry of Internal Affairs of Russia

STAURSKY Stanislav Stanislavovich,

Ph.D., Associate Professor, Lecturer, Department of Economics and Management, Russian Academy of National Economy and Public Administration, branch of Omsk

PROCESSING AND MANAGEMENT OF DOCUMENTS FOR PATROL AND GUARD OFFICERS

Annotation. *This article discusses the issue of cybersecurity in the Ministry of Internal Affairs system in a modern legal state. The purpose of the study is to identify the causes of information crime. The authors analyze the features of the organization and provision of cybersecurity in the Ministry of Internal Affairs in a modern legal state. Special attention is paid to the features that organize and ensure cybersecurity in the Ministry of Internal Affairs in a modern legal state. The study examines the key areas and methods of cybersecurity, as well as the legal framework and regulations governing this field. The authors explore the potential of these methods to enhance and promote more effective control of information security. The study was conducted in order to identify the key problems of cybersecurity in a modern legal state. The scientific novelty lies in the study of the legal framework, organizational mechanisms, and practical methods of ensuring cybersecurity.*

Key words: *Cybersecurity in the Ministry of Internal Affairs system, crime, and technical and legal measures.*

В современном мире информационные технологии стали неотъемлемой частью функционирования государственных институтов, включая правоохранительные органы. Министерство внутренних дел (МВД) как ключевой субъект обеспечения общественной безопасности и правопорядка активно использует цифровые ресурсы и информационные системы для выполнения своих задач. Однако рост зависимости от информационных технологий приводит к увеличению уязвимости государственных структур перед киберугрозами. Кибербезопасность в системе МВД становится стратегически важным направлением, обеспечивающим сохранность данных, надежность функционирования систем и защиту от внешних и внутренних угроз. Правовые основы обеспечения кибербезопасности в системе МВД представляют собой комплекс нормативно-правовых актов, регулирующих деятельность по защите информационных ресурсов и противодействию киберугрозам. В контексте современного правового государства важнейшим элементом становится гармонизация национального законодательства с международными стандартами и обязательствами. Основу правового регулирования составляют Конституция РФ, федеральные законы, указы Президента, постановления Правительства, а также ведомственные нормативные акты МВД.

Конституция Российской Федерации закрепляет основные принципы защиты прав и свобод граждан, включая право на неприкосновенность частной жизни и защиту персональных данных. Эти положения создают правовую рамку, в пределах которой МВД должно осуществлять свою деятельность по обеспечению кибербезопасности. Наряду с этим, конституционные нормы требуют соблюдения баланса между обеспечением национальной безопасности и защитой прав человека, что особенно важно при использовании технических средств контроля и мониторинга информационных систем [1].

Федеральный закон «О безопасности» и Федеральный закон «Об информации, информационных технологиях и защите информации» являются ключевыми нормативными актами, регулирующими вопросы кибербезопасности. Они устанавливают основные требования к защите информации, ответственность за нарушение правил и порядок взаимодействия государственных органов. В частности, в этих законах прописаны обязанности МВД по обеспечению безопасности государственных информационных систем, а также меры по предотвращению и расследованию киберпреступлений.

Важным элементом правового регулирования является Федеральный закон «О персональных данных», который регулирует порядок обработки и защиты персональной информации. В условиях цифровизации правоохранительной деятельности МВД активно использует персональные данные, что требует строгого соблюдения установленных норм для предотвращения злоупотреблений и утечек информации. Закон устанавливает требования к техническим и организационным мерам защиты, а также права субъектов данных на доступ и контроль за их использованием.

Международные правовые акты и стандарты также играют значительную роль в формировании национальной политики кибербезопасности. Россия участвует в ряде международных соглашений, направленных на сотрудничество в области противодействия киберпреступности и обмена информацией. В частности, Конвенция Совета Европы о киберпреступности (Будапештская конвенция) служит ориентиром для разработки национальных законов и практик. Однако особенности российского законодательства и суверенитет государства в области информационной безопасности приводят к необходимости адаптации международных норм к национальным реалиям.

Одним из вызовов правового регулирования является динамичность развития технологий и появление новых видов киберугроз. Законодательство часто отстает от технических инноваций, что создает пробелы в правовом поле. Для решения этих проблем в России разрабатываются специализированные нормативные акты, регулирующие использование криптографии, электронных подписей, защиты критической информационной инфраструктуры и других аспектов. МВД активно участвует в формировании и реализации этих правовых норм, обеспечивая их практическое применение.

Кроме того, особое значение имеет ведомственное регулирование. МВД разрабатывает собственные инструкции, регламенты и методические рекомендации, которые конкретизируют требования федерального законодательства и учитывают специфику работы правоохранительных органов. Ведомственные нормативы регулируют вопросы доступа к информации, порядок реагирования на инциденты, меры по обеспечению конфиденциальности и целостности данных. Это позволяет создавать эффективную систему кибербезопасности, адаптированную к специфике правоохранительной деятельности.

Таким образом, правовые основы

обеспечения кибербезопасности в системе МВД представляют собой сложный и многогранный комплекс нормативных актов, направленных на защиту информационных ресурсов и обеспечение безопасности государства и граждан. Их анализ показывает необходимость постоянного совершенствования законодательства, интеграции международного опыта и учета технических особенностей информационных систем МВД. Только при условии соблюдения правовых норм возможно эффективное и законное противодействие современным киберугрозам [2][3][4].

Организационные аспекты кибербезопасности в системе МВД являются ключевым элементом, обеспечивающим реализацию правовых норм и технических мер на практике. Эффективная организация работы по защите информационных ресурсов требует формирования специализированных подразделений, разработки комплексных программ и процедур, а также обеспечения высокого уровня квалификации сотрудников. В современных условиях кибербезопасность рассматривается как интегрированная система, включающая не только технические средства, но и человеческий фактор, организационную культуру и управленческие механизмы.

В структуре МВД функционируют специализированные подразделения, ответственные за кибербезопасность и информационную защиту. К ним относятся отделы информационной безопасности, центры мониторинга и реагирования на инциденты, а также подразделения по расследованию киберпреступлений. Эти структуры обеспечивают постоянный контроль за состоянием информационной безопасности, анализируют угрозы и разрабатывают меры по их нейтрализации. Организация взаимодействия между подразделениями позволяет оперативно реагировать на инциденты и минимизировать возможные последствия.

Важной составляющей является разработка и внедрение нормативных документов, регламентирующих порядок работы с информационными системами и средствами защиты. Ведомственные стандарты и инструкции определяют требования к техническим средствам, процедурам доступа, методам идентификации и аутентификации пользователей, а также алгоритмам реагирования на угрозы. Такие документы обеспечивают системный подход и позволяют унифицировать процессы обеспечения кибербезопасности на всех уровнях МВД.

Обучение и повышение квалификации персонала занимают центральное место в организационной структуре кибербезопасности. Поскольку технологии постоянно развиваются, а методы кибератак усложняются, сотрудники МВД должны обладать актуальными знаниями и навыками. Для этого реализуются программы профессиональной подготовки, курсы повышения квалификации и специализированные тренинги. Особое внимание уделяется развитию аналитических и технических компетенций, а также формированию культуры информационной безопасности среди всех сотрудников ведомства.

Важным аспектом является также сотрудничество МВД с другими государственными органами, научными учреждениями и частным сектором. Обмен информацией о новых угрозах, совместная разработка технологий защиты, участие в межведомственных рабочих группах способствуют повышению эффективности кибербезопасности. Взаимодействие с операторами критической информационной инфраструктуры и провайдерами позволяет своевременно выявлять и устранять уязвимости, а также проводить профилактические мероприятия.

Организационные меры включают также создание системы мониторинга и аудита информационной безопасности. Регулярные проверки состояния технических средств, анализ инцидентов, оценка рисков и уязвимостей позволяют выявлять слабые места и принимать своевременные меры. Внедрение современных средств автоматизации и аналитики способствует повышению оперативности и точности оценки угроз, что особенно важно в условиях постоянного изменения киберсреды [5][6][7].

Наконец, организационный аспект предусматривает разработку планов действий в чрезвычайных ситуациях, связанных с кибератаками. Наличие четко прописанных процедур реагирования, восстановления и минимизации ущерба обеспечивает устойчивость информационных систем МВД. Планирование и проведение учений позволяют отработать навыки взаимодействия и повысить готовность к реальным инцидентам.

Таким образом, организационные аспекты кибербезопасности в системе МВД представляют собой сложную и многоуровневую систему, объединяющую кадровый потенциал, нормативное регулирование, межведомственное взаимодействие и техническую поддержку. Эффективное управление этими элементами обеспечивает надежную защиту информационных ресурсов и способствует реализации задач МВД в условиях современных вызовов и угроз

Список литературы:

[1] Конституция Российской Федерации:

комментарий к статье 23. – М.: Юридическая литература, 2018. – 120 с.
[2] Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ.
[3] Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.
[4] Конвенция Совета Европы о киберпреступности (Будапештская конвенция), 2001.
[5] Орлов В.В. Организационные основы кибербезопасности в правоохранительных органах. – М.: Проспект, 2022. – 400 с.
[6] Кузнецова Н.П. Управление информационной безопасностью в МВД. – СПб.: Питер, 2020. – 350 с.
[7] Федоров Д.А. Кадровое обеспечение кибербезопасности: проблемы и решения. – М.: РАГС, 2019. – 290 с.

References:

[1] Constitution of the Russian Federation: Commentary to Article 23. - M.: Legal literature, 2018. - 120 s.
[2] Federal Law “On Information, Information Technologies and Information Protection” of 27.07.2006 No. 149-FZ.
[3] Federal Law “On Personal Data” dated 27.07.2006 No. 152-FZ.
[4] Council of Europe Convention on Cybercrime (Budapest Convention), 2001.
[5] Orlov V.V. Organizational foundations of cybersecurity in law enforcement. - M.: Prospect, 2022. - 400 s.
[6] Kuznetsova N.P. Information security management in the Ministry of Internal Affairs. - St. Petersburg: Peter, 2020. - 350 s.
[7] D.A. Fedorov. Cybersecurity staffing: problems and solutions. - M.: RAGS, 2019. - 290 s.

