Дата поступления рукописи в редакцию: 28.08.2026 г.
Дата принятия рукописи в печать: 25.09.2026 г.

DOI: 10.24412/2782-3849-2026-9-39-43

ХОРОШЕВА Анна Владимировна,
кандидат физико-математических наук, доцент, начальник кафедры специальной техники и информационных технологий юридического факультета Владимирского юридического института ФСИН России, Владимир, Россия,
e-mail: d_anya@list.ru

ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СИСТЕМ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ИНФОРМАЦИИ В УЧРЕЖДЕНИЯХ И ОРГАНАХ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ

Аннотация. *В статье рассматриваются правовые и организационные основы применения систем обнаружения и предотвращения утечек информации (DLP-систем) в учреждениях и органах уголовно-исполнительной системы Российской Федерации (далее – УИС). Анализируется нормативно-правовая база, регламентирующая защиту информации ограниченного доступа в УИС, а также функциональные возможности современных DLP-решений. Особое внимание уделяется специфике деятельности пенитенциарных учреждений, обусловливающей повышенные требования к защите персональных данных осужденных, сотрудников и иных категорий лиц. На основе анализа научных публикаций и правовых актов делается вывод о необходимости системного внедрения DLP-систем как элемента комплексной системы информационной безопасности УИС.*

Ключевые слова: *DLP-системы, уголовно-исполнительная система, информационная безопасность, защита информации, персональные данные, утечка информации, внутренний нарушитель, ФСИН России.*

KHOROSHEVA Anna Vladimirovna,
candidate of physico-mathematical sciences, associate professor, head of the Department of Special Equipment and Information Technologies, of the Law Faculty of Vladimir Law Institute of the FPS of Russia, Vladimir, Russia

OPPORTUNITIES FOR USING INFORMATION LEAK DETECTION AND PREVENTION SYSTEMS IN INSTITUTIONS AND BODIES OF THE PENITENTIARY SYSTEM

Annotation. *The article discusses the legal and organizational foundations of the use of information leakage detection and prevention systems (DLP systems) in institutions and bodies of the penal system of the Russian Federation. It analyzes the legal framework governing the protection of restricted information in the penal system, as well as the functionality of modern DLP solutions. Special attention is given to the specific nature of the activities of penitentiary institutions, which requires increased protection of the personal data of convicts, employees, and other categories of individuals. Based on the analysis of scientific publications and legal acts, it is concluded that the systematic implementation of DLP systems as an element of the comprehensive information security system of the penal system is necessary.*

Key words: *DLP systems, penal system, information security, information protection, personal data, information leakage, internal violator, Federal Penitentiary Service of Russia.*

Информационная безопасность является одним из приоритетных направлений государственной политики Российской Федерации. В системе государственных органов Федеральная служба исполнения наказаний занимает особое место. Ее деятельность связана с обработкой значительных массивов информации ограниченного доступа, включая персональные данные осужденных, сотрудников и иных лиц, сведения, составляющие служебную и иную охраняемую законом тайну.

Обеспечение безопасности государственных органов и их автоматизированных информационных систем является одним из наиболее интенсивно развивающихся направлений в сфере защиты информации, так как надежность информационного обеспечения деятельности государственных органов является важным условием их развития.

В современных условиях деятельность

учреждений и органов УИС характеризуется высокой степенью информатизации. Телекоммуникационная система УИС охватывает все территориальные органы ФСИН России и большую часть подведомственных им учреждений. В эксплуатации находится значительное количество цифровых каналов передачи данных, функционируют автоматизированные информационные системы различного уровня, осуществляется электронный документооборот. Следует учитывать, что информационные системы УИС относятся к числу объектов, в которых обрабатываются данные ограниченного распространения, поэтому, согласно действующим правовым нормам, необходимо обеспечить защиту от несанкционированного доступа и любых форм внешнего вмешательства. При этом с марта 2026 года требования к безопасности данных, хранящихся и обрабатывающихся в информационных системах, стали более жесткими и распространились не только на государственные информационные системы, но и иные информационные системы государственных органов [1].

Параллельно с этим наблюдается устойчивая тенденция к наращиванию объемов обрабатываемой и передаваемой по каналам связи информации, связанной с деятельностью органов и учреждений УИС, что в свою очередь влечет за собой риски несанкционированного доступа к данным, а также утечек конфиденциальной информации, в том числе персональных данных.

Утечки данных можно считать одной из серьезных угроз, которая может принести разрушительные последствия для любой организации, а особенно для государственного сектора, которые включают финансовые потери, утрату репутации и доверия граждан.

Несмотря на то, что в настоящее время внимание акцентируется на кибератаках, инциденты информационной безопасности внутреннего характера занимают весьма существенное место среди всех видов угроз. По данным экспертно-аналитического центра InfoWatch в 2025 году в мире 28,7% утечек информации по вине внутренних нарушителей приходится на государственные организации, в России – 43,6% [2]. Для противодействия внутренним нарушителям необходимо внедрять системы, обеспечивающие полный контроль движения конфиденциальной информации, управления учетными записями, отслеживания поведенческих факторов и индикаторов риска.

Одним из способов защитить данные от утечки является использование систем обнаружения и предотвращения утечек информации (DLP-систем).

Функционально DLP-системы ориентированы на выявление и блокировку несанкционированного перемещения данных закрытого характера по любым доступным сетевым и физическим каналам. В зависимости от настроек, такие системы могут работать в режиме наблюдения или активного вмешательства, перекрывая передачу через почтовые сервисы, мессенджеры, а также при копировании на съемные носители или в облачные и сетевые папки. То есть это предотвращение угроз информационной безопасности, связанных с человеческим фактором, объем которых в настоящее время достаточно велик.

Принцип работы DLP-систем строится на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется [3, с. 46].

Необходимость применения DLP-систем в УИС обусловлена рядом факторов. Во-первых, учреждения и органы УИС обрабатывают персональные данные значительного числа субъектов – осужденных, подозреваемых, обвиняемых, сотрудников, что требует неукоснительного соблюдения требований Федерального закона № 152-ФЗ «О персональных данных». Во-вторых, сложная сетевая структура и территориальная распределенность компонентов информационных систем создают дополнительные уязвимости. В-третьих, большое количество пользователей, наделенных правами доступа к информационным ресурсам, включая не только сотрудников УИС, но и представителей иных государственных органов, создает предпосылки для реализации внутренних угроз.

В контексте УИС проблема внутренних нарушителей приобретает особое звучание. Сотрудники учреждений и органов УИС имеют санкционированный доступ к значительным объемам конфиденциальной информации, и любое нарушение правил обращения с такой информацией может повлечь серьезные последствия. Банк данных угроз ФСТЭК России определяет восемь категорий внутренних нарушителей, включая лиц, имеющих санкционированный доступ к информационной системе, зарегистрированных пользователей с различными полномочиями, программистов-разработчиков и иных лиц [4, с. 164]. В этой связи DLP-системы являются не только эффективным средством предотвращения утечек, но и инструментом контроля действий сотрудников.

Современный инструментарий DLP охватывает практически все аспекты защиты информации, востребованные в учреждениях и органах УИС. Одна из базовых возможностей таких систем – оценка уровня конфиденциальности документов, циркулирующих в сетевом трафике. Эта оценка строится на двух подходах: анализе формальных признаков (например, специальные

метки, грифы) и исследовании содержательной части документа. Помимо этого, комплекс фиксирует, как сотрудники расходуют рабочее время и ресурсы, проверяет законность их операций с данными, отслеживает служебную переписку с целью своевременного выявления отклонений, способных снизить результативность работы организации.

В качестве наиболее значимых для УИС функций можно выделить создание резервных копий конфиденциальных данных, пересылаемых по разным каналам, для последующего разбора инцидентов; пресечение попыток отправки таких сведений вовне; блокировка использования ведомственных ресурсов в неслужебных целях; обнаружение мест несанкционированного дублирования охраняемой информации. Расширенный функционал включает модуль сканирования файловых хранилищ на предмет документов с некорректно настроенными правами доступа, средства аудита пользовательских сессий для внутренних проверок, поведенческий анализ с элементами машинного обучения, а также речевую аналитику для регистрации фактов устной передачи данных ограниченного доступа.

Следует отметить, что вопрос о том, насколько правомерно применение DLP-систем в пенитенциарных учреждениях заслуживает отдельного внимания, потому что мониторинг информационных потоков неизбежно вступает в противоречие с конституционным правом сотрудников на тайну личной переписки и невмешательство в частную жизнь. В соответствии со статьями 23 и 24 Конституции РФ каждый гражданин имеет право на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений [4, с. 165].

Вместе с тем, в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» № 149-ФЗ, обладатель информации обязан принимать меры по защите информации, ограничивать доступ к информации, если такая обязанность установлена федеральными законами, что ведет к ограничению указанных прав. Кроме того, обладатель информации обязан обеспечить предотвращение несанкционированного доступа к информации и передачи ее лицам, не имеющим право доступа [5].

Следовательно, правовая база для развёртывания DLP-систем в учреждениях УИС закреплена на уровне федерального законодательства. Но здесь важно понимать: если внедрение не подкреплено грамотной локальной нормативной документацией, реальная ценность системы резко снижается, а значительная часть ее аналитического потенциала остается невостребованной.

Более того, последствия невнимательного подхода к этому вопросу могут быть двоякими: организация рискует не только допустить утечку конфиденциальных данных, но и столкнуться с исками со стороны сотрудников, уволенных с нарушением процедурных требований, даже если сами нарушения правил работы с данными были зафиксированы.

Правовое обеспечение работы DLP-систем требует выстроенной системы локальных актов. Начинается эта работа с того, что руководство организации закрепляет и документально оформляет перечень сведений ограниченного распространения, причём каждый сотрудник должен быть лично ознакомлен с этим перечнем под роспись. Набор документации, которую предстоит разработать, включает: собственно перечень охраняемых сведений; реестр лиц, уполномоченных на их обработку; внутренние положения о порядке обращения и защиты таких данных; приказы о введении соответствующих ограничительных режимов. Параллельно оформляются положения, включающие запрет на разглашение сотрудниками конфиденциальных сведений, ставшие доступными им по службе. Причём эта норма должна дублироваться как в базовых внутренних регламентах (трудовые контракты, правила распорядка, должностные обязанности), так и в специализированных актах, регламентирующих порядок защиты информации.

Именно поэтому особое значение приобретает формирование политики информационной безопасности учреждений и органов УИС, при формировании которой они самостоятельно определяют какие именно сведения подлежат защите и какие методы и средства защиты будут использоваться. При этом основная цель политики безопасности состоит в эффективном прогнозировании рисков для информации, а также в построении действенной системы эффективного противодействия всем данным рискам [6, с. 78].

В контексте УИС вопросы юридического оформления применения DLP-систем приобретают дополнительную значимость в связи с особым правовым статусом как сотрудников, так и иных лиц, взаимодействующих с информационными системами. При разработке проекта политики информационной безопасности учреждений УИС важно предусмотреть три взаимосвязанных блока: во-первых, чётко сформулированные цели; во-вторых, механизмы, посредством которых эти цели предполагается достичь; в-третьих, персональную ответственность сотрудников за нарушение положений документа.

Технические аспекты внедрения DLP-систем в УИС также требуют отдельного рассмотрения. На российском рынке представлен

широкий спектр DLP-решений, включая как зарубежные, так и отечественные разработки. Однако для использования в органах и учреждениях УИС необходимо выбирать отечественные решения, т.к. они обладают сертификацией ФСТЭК и удовлетворяют требованиям законодательства.

В числе российских DLP-систем, получивших сертификаты ФСТЭК, следует отметить Zecurion DLP, DeviceLock, InfoWatch , Traffic Monitor, Falcongaze SecureTower, СерчИнформ КИБ, Solar Dozor, Гарда DLP и другие.

Следует отметить, что в соответствии с законодательством органам государственной власти запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия [7]. Поскольку учреждения и органы УИС подпадают под действие законодательных ограничений, касающихся использования иностранного программного обеспечения, выбор DLP-решений для них объективно сужается до продуктов отечественной разработки, прошедших сертификацию.

Выбор конкретной DLP-системы для органов и учреждений УИС должен ориентироваться на несколько приоритетных параметров: эффективность обнаружения утечек данных; покрытие различных каналов передачи данных; варианты развертывания; управление политиками безопасности; возможности взаимодействия с иными средствами защиты информации; качество пользовательского интерфейса; возможности масштабируемости; соответствие нормативной правовой базе; аналитические возможности; финансовые затраты; наличие сертификатов ФСТЭК.

Важным аспектом применения DLP-систем в УИС является их интеграция с иными средствами защиты информации. Для эффективного мониторинга событий безопасности, своевременного выявления угроз, поддержания соответствия регуляторным требованиям и автоматизации рутинных операций предпочтительным оказывается интегрированное решение, объединяющее функциональные возможности трёх классов систем: SIEM (управление событиями и информацией безопасности), DCAP (аудит и защита данных на уровне их хранения) и DLP (контроль информационных потоков). При этом SIEM-система фиксирует отклонения в поведении пользователей и идентифицирует каналы получения доступа к данным, DLP-система анализирует содержание всех коммуникаций, а DCAP-система отслеживает операции с файлами и блокирует нежелательные действия. Именно такая высокоинтегрированная связка данных систем дает возможность максимально полно расследовать нарушения ИБ и собрать необходимую доказательную базу [8, с. 76].

Внедрение DLP-систем в учреждениях и органах УИС сопряжено с определенными организационными сложностями, связанными с практическим применением политики безопасности учреждения. Причин, по которым заявленная политика безопасности не работает в полной мере, может быть несколько. В одних случаях сам по себе текст документа безупречен с точки зрения формулировок, однако остается невостребованным на практике – его предписания игнорируются либо выполняются формально. В других – изначально допущены просчеты при разработке: положения либо недостаточно проработаны, либо не учитывают долгосрочные изменения в условиях функционирования учреждения. В связи с этим необходимо очень основательно и грамотно разрабатывать политику безопасности, принимая во внимание специфику работы организаций ФСИН России [6, с. 78].

Таким образом, DLP-системы могут служить надежной опорой в обеспечении информационной безопасности учреждений и органов УИС. Они дают возможность предупреждать утечки данных, осуществлять контроль действий сотрудников при работе с данными, проводить расследования инцидентов информационной безопасности. Вместе с тем успешное внедрение DLP-систем невозможно без должного правового обеспечения, включающего разработку политики информационной безопасности, принятие локальных нормативных актов, ознакомление сотрудников с установленными требованиями под роспись.

Особое значение для УИС имеет использование отечественных сертифицированных DLP-решений, соответствующих требованиям ФСТЭК России и учитывающих специфику деятельности пенитенциарных учреждений. Комплексный подход, сочетающий технические средства защиты информации (DLP, SIEM, DCAP) с организационными мерами (разработка политик безопасности, обучение персонала, юридическое оформление), позволит создать эффективную систему информационной безопасности, способную противостоять и внешним, и внутренним угрозам.

Перспективными направлениями развития DLP-систем в УИС представляются: дальнейшее совершенствование технологий анализа контента с применением искусственного интеллекта и машинного обучения; расширение функциональных возможностей по контролю новых каналов передачи данных; интеграция с иными системами защиты информации в рамках единой платформы информационной безопасности; развитие средств поведенческого анализа пользователей

для выявления аномалий на ранних стадиях. Реализация указанных направлений позволит существенно повысить уровень защищенности информационных ресурсов УИС и обеспечить надежную защиту информации ограниченного доступа, в том числе, персональных данных.

Список литературы:

[1] Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений : приказ ФСТЭК России от 11 апр. 2025 г. № 117 // Официальный интернет-портал правовой информации http://pravo.gov.ru, 17 июня 2025 г.

[2] Утечки данных вследствие действий внутренних нарушителей https://www.infowatch.ru/sites/default/files/analytics/files/utechki-dannykh-vsledstviye-deystviy-vnutrennikh-narushiteley.pdf.

[3] Миленчук, Я. В. Анализ функционала DLP-систем и целесообразность их внедрения в автоматизированную систему информационного обеспечения органов пограничной службы / Я. В. Миленчук, О. С. Полоцкая // Новые информационные технологии в телекоммуникациях и почтовой связи. – 2023. – Т. 1, № 1. – С. 46-47. – EDN BBJQQC.

[4] Митюшин, Д. А. Правовые вопросы применения систем защиты от утечки конфиденциальной информации на объектах информатизации / Д. А. Митюшин // Вестник Московского университета МВД России. – 2020. – № 5. – С. 163-168. – DOI 10.24411/2073-0454-2020-10283. – EDN ZBRAZV.

[5] Об информации, информационных технологиях и о защите информации: Федер. закон от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства Российской Федерации. – 2006. – № 31, ст. 3448.

[6] Перегудов, А. Н. Политика информационной безопасности в деятельности органов и учреждений уголовно-исполнительной системы / А. Н. Перегудов, С. А. Бокадаров // Вестник Воронежского института ФСИН России. – 2024. – № 3. – С. 78-81. – EDN QSGYPC.

[7] О дополнительных мерах по обеспечению информационной безопасности Российской Федерации : Указ Президента РФ от 1 мая 2022 г. № 250 // Собрание законодательства Российской Федерации. – 2022. – № 18, ст. 3058.

[8] Морозов, В. Е. Комплексные решения для минимизации внутренних угроз информационной безопасности / В. Е. Морозов, Н. Г. Милославская // Вопросы кибербезопасности. – 2024. – № 5(63). – С. 67-78. – DOI 10.21681/2311-3456-2024-5-67-78. – EDN PBSASV.

References:

[1] On approval of the Requirements for the protection of information contained in state information systems, other information systems of state bodies, state unitary enterprises, state institutions: order of the FSTEC of Russia dated April 11, 2025 No. 117 // Official Internet portal of legal information http://pravo.gov.ru, June 17, 2025.

[2] Утечки данных вследствие действий внутренних нарушителей https://www.infowatch.ru/sites/default/files/analytics/files/utechki-dannykh-vsledstviye-deystviy-vnutrennikh-narushiteley.pdf.

[3] Milenchuk, Ya. V. Analysis of the functionality of DLP systems and the feasibility of their introduction into the automated information support system of border service bodies/Ya. V. Milenchuk, O. S. Polotskaya // New information technologies in telecommunications and postal services. – 2023. - T. 1, NO. 1. - S. 46-47. – EDN BBJQQC.

[4] Mityushin, D. A. Legal issues of the use of protection systems against leakage of confidential information at informatization facilities/ D. A. Mityushin // Bulletin of Moscow University of the Ministry of Internal Affairs of Russia. – 2020. – № 5. - S. 163-168. – DOI 10.24411/2073-0454-2020-10283. – EDN ZBRAZV.

[5] On information, information technology and information security: Feder. Law of July 27, 2006 No. 149-FZ // Collection of Legislation of the Russian Federation. – 2006. - No. 31, Art. 3448.

[6] Peregudov, A. N. Information security policy in the activities of bodies and institutions of the penitentiary system/A. N. Peregudov, S. A. Bokadarov // Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia. – 2024. – № 3. - S. 78-81. – EDN QSGYPC.

[7] On additional measures to ensure information security of the Russian Federation: Decree of the President of the Russian Federation of May 1, 2022 No. 250 // Collection of legislation of the Russian Federation. – 2022. - No. 18, Art. 3058.

[8] Morozov, V. E. Comprehensive solutions to minimize internal threats to information security/ V. E. Morozov, N. G. Miloslavskaya // Cybersecurity issues. – 2024. – № 5(63). - S. 67-78. – DOI 10.21681/2311-3456-2024-5-67-78. – EDN PBSASV.