Современные методы защиты информации ограниченного доступа в государственных органах, включая органы критической информационной инфраструктуры

Романычев Никита Олегович
аспирант, Российский государственный университет правосудия имени В. М. Лебедева, n.romanychev@yandex.ru

В данной статье акцентируется внимание на задачах обеспечения безопасности государственных органах и их информационных система, в том числе объектов критической информационной инфраструктуры. Надежность этих систем должна быть на высочайшем уровне, так как от них зависит безопасность государства с учетом глобализации и интеграции информационных технологий в государственное управление, экономику, финансы и промышленность. Рассмотрены основные нормативные акты, регулирующие защиту информации ограниченного доступа, в том числе с использованием искусственного интеллекта.
Ключевые слова: DLP-системы, информационная безопасность, объекты критической информационной инфраструктуры, государственные органы, государственные информационные системы.

Введение

В последние годы в мире возрастает опасность киберугроз. Рост целенаправленных атак на государственные органы Российской Федерации тоже не остается не замеченным. В связи с этим во многих странах в последние годы происходит доработка нормативного обеспечения в сфере кибербезопасности и защиты информации ограниченного доступа с целью адаптации к современным требованиям цифровизации общества. Не малую часть в этом играет развитие информационных технологий и их проникновение во все сферы жизнедеятельности как человека в отдельности, так и государства в целом.

Одним из направлений информационной безопасности активно развивающимся в последние годы в России, является безопасность государственных органов и их автоматизированнх информационных систем. В эту область входят так же органы критических информационных инфраструктур (далее – КИИ) и вопросы их безопасности.

Основная часть

Согласно Федеральному закону по ФЗ №187 «О защите критической инфраструктуры» к субъектам КИИ относятся: федеральные и региональные органы власти,

- государственные и муниципальные учреждения (больницы, МФЦ, вузы),
- государственные и муниципальные унитарные предприятия (ГУПы, МУПы),
- хозяйственные общества с государственным участием, если государство владеет контрольным пакетом акций или имеет решающее влияние,
- любые юридические лица, работающие в сфере здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности,
- российские юридические лица, которые обеспечивают взаимодействие указанных систем или сетей.

В своих информационных системах государственные органы обрабатывают и хранят огромные массивы информации, как персональных данных, так и различной информации ограниченного доступа.

К информации с ограниченным доступом относятся сведения, составляющие **персональные** данные, **коммерческую** тайну **государственную** тайну, иную охраняемую законом тайну (например, тайну усыновления (удочерения) (статья 139 Семейного кодекса Российской Федерации), **врачебную** тайну (статья 13 Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»), а также иные сведения, доступ к которым ограничен на основании федерального закона (например, сведения о лицах, подлежащих государственной защите в соответствии с Федеральным законом от 20 августа 2004 года № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства»).

Таким образом информационная безопасность – крайне важное направление деятельности государства и защита организаций, которые имеют у себя подобные

данные и информационные системы, является вкладом в национальную безопасность, подход к которой описан в Доктрине обеспечения национальной безопасности Российской Федерации [1], которая утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

Защита как объектов КИИ, так и персональных данных необходима для соблюдения прав граждан и организаций, функционирования экономики и осуществления государственного управления.

В эпоху цифровых технологий защита данных в государственных органах требует комплексного подхода, который включает в себя не только технические меры, но и организационные аспекты.

Важно не допускать утечек информации ограниченного доступа из государственных органов, так как такие утечки подрывают доверие граждан к государству и вызывают множество дальнейших проблем. Например, только одна утечка вызовет расходы на расследование, оценку ущерба, привлечение внешних экспертов. Затем необходимо уведомить пострадавших и всех необходимых регуляторов (Роскомнадзор, ФСБ, Б, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации). Возможно, потребуется выплата после компенсации.

Основные угрозы для данных в государственных органах включают кибератаки, внутренние нарушения безопасности, физические утечки информации, а также устаревшее программное обеспечение и оборудование.

Существующие угрозы реализуются через уязвимости, самые слабые места в защите информационной системы. По отношению к государственным органам можно выделить четыре основные уязвимости:

1) В программном обеспечении — ошибки в коде, уязвимости конфигурации, архитектуры.

2) В технических средствах — уязвимости программного обеспечения, микропрограмм, базовой системы ввода-вывода.

3) В протоколах сетевого взаимодействия и каналах передачи данных — уязвимости, обусловливающие наличие технических каналов утечки информации.

4) Организационные — отсутствие организационных мер защиты информации, несоблюдение правил эксплуатации системы.

Статья Горбатова В.С. с соавторами [2, с. 12-26] выделяет основными угрозами и уязвимостями вредоносное ПО, уязвимостями в текущем ПО, DDoS-атаки и атаки при помощи социальной инженерии. Они предлагают комплексный подход, включающий межсетевые экраны, сегментацию сетей, шифрование, обновление ПО и обучение персонала. Так же в статье подчеркивается важность взаимодействия заинтересованных сторон и постоянного совершенствования методов защиты для противодействия киберугрозам.

В рамках оценки рисков информационной системы, следует изучить уязвимости и оценить, какая из них вероятней всего будет использована для реализации угрозы.

В государственных органах используется масса различных мер защиты, для лучшего понимания и анализа необходимо их обозначить и классифицировать

Меры защиты информации можно разделить на организационные и технические:

К организационным мерам относятся те меры, которые реализуются путем организации работы аппарата органа определенным образом. К организационным мера можно отнести такие меры как:

- Выделение помещений с ограниченным доступом. Также установка сейфы, сигнализации, видеонаблюдения, определение порядок доступа сотрудников.
- Обучение сотрудников правилам обработки данных и процедурам безопасной работы.
- Ограничение доступа к персональным данным тем сотрудникам, которым это не требуется для выполнения обязанностей.
- Статья 13 N 152-ФЗ добавляет требование «создать информационную систему персональных данных.» На практике это требование реализуется через различные ГИС – государственные информационные системы, например ГАС «Правосудие» в судебных органах;
- Назначаются лица, ответственные за организацию обработки персональных данных. В структурных подразделениях аппарата органа ими являются руководители структурных подразделений;
- Разработка политики обработки персональных данных и локальных нормативных актов, регулирующих категории и перечень обрабатываемых данных, способы, сроки обработки и хранения, порядок уничтожения данных после достижения целей обработки, процедуры выявления и устранения нарушений.
- Работникам госоргана запрещается выносить из здания документы или материалы, принадлежащие госоргану, без соответствующего на то разрешения.
- Стирание или обезличивание персональных данных
- Запрет госслужащим на разглашение привилегированной информации, ставшие им известными в связи с осуществлением своих полномочий.

К техническим средствам защиты относятся меры, которые реализуются через применения конкретных технологий в работе государственного органа. К ним относятся:

- Шифрование данных при передаче и хранении.
- Резервное копирование данных.
- Внедрение систем предотвращения утечек (DLP-систем).
- Использование средств антивирусной защиты.
- Регистрацией и учетом всех действий, совершаемых с персональными данными в автоматизированных информационных системах персональных данных;
- Специализированное оборудование по разделению каналов связи;
- Персонификация доступа к информационным ресурсам госоргана
- Использование лицензионного программного обеспечения;
- Обнаружение фактов несанкционированного доступа к персональным данным.

Большая часть этих мер регламентирована приказом ФСТЭК России от 18 февраля 2013 № 21, который регулирует защиту персональных данных у операторов персональных данных, к которым также относятся государственные органы.

Также участвует приказ ФСТЭК № 17, который устанавливает требования к обеспечению защиты информации ограниченного доступа от утечки по техническим каналам, несанкционированного доступа и других воздействий при её обработке в государственных информационных системах.

Однако с 1 марта 2026 года приказ №17 утратит силу и будет заменен приказом ФСТЭК России от 11.04.2025 №117, который установит требования для защиты информации некриптографическими методами, предотвращения несанкционированного доступа к ней и специальных воздействий на носители информации, а самое главное он распространит требования к обеспечению безопасности информации не только на операторов государствен-

ных информационных систем, но и на большинство государственных и муниципальных учреждений, использующих информационные системы, обрабатывающие информацию ограниченного доступа.

В целом имеется тенденция приведения требований к информационной безопасности к единому, достаточно высокому уровню. В июне 2025 года Министерство цифрового развития направило в адрес администраций письмо с требованием организовать применение «Методики оценки технической защиты информации», утвержденной ФСТЭК России 2 мая 2024 года. В этом требовании отмечается, что методика должна применяться ко всем информационным система госорганов, а не только объектов КИИ.

К организациям КИИ также добавляются требования приказа ФСТЭК № 239, направленный на обеспечение устойчивого функционирования значимых объектов при проведении в отношении них компьютерных атак

Кроме того, для субъектов КИИ, стратегических и системообразующих предприятий, органов власти Указом Президента РФ № 250 установлен запрет на использование средств защиты информации, странами происхождения которых являются недружественные иностранные государства.

Вышеуказанные приказы устанавливают требования к мерам защиты информации путем описания функции, которую должна выполнять мера. Однако для выполнения требований о защите информации ограниченного доступа необходимо контролировать работу с информацией в течение всего цикла ее обработки, в месте с действиями пользователей информационной системы. Для этого применяются современные системы защиты информации:

- Системы аудита и защиты данных на стадии хранения (DCAP-системы);
- Системы для предотвращения утечек, контроля действий и коммуникаций пользователей (DLP-системы);
- Системы управления событиями информационной безопасности (SIEM системы)

Статистика по использованию средств защиты Эксперты «СёрчИнформ» [3] выяснили, какие средства защиты данных использовали российские компании в 2024 году. В 100% опрошенных компаний используются антивирусные системы, в 80% – DLP-системы, в 74% – NGFW (Firewall, Proxy). Более чем в половине уже внедрены SIEM-системы

Разберем по отдельности функции каждой из систем защиты:

1. Системы аудита и защиты данных на стадии хранения (DCAP-системы);

DCAP-системы (Data-Centric Audit and Protection) используются в госорганах для аудита и защиты данных на стадии хранения, в том числе конфиденциальной информации. Эти системы ориентированы на безопасность самих данных, а не на безопасность инфраструктуры, и помогают выполнять требования регуляторов к защите информации

Рассмотрим функции **DCAP-системы:**

- **Контроль прав доступа** к информации. Более того, система выявляет избыточные права доступа, неактивные учётные записи с сохранёнными правами;
- **Контроль политик хранения** чувствительных данных;
- **Контроль использования конфиденциальных данных:** система предоставляет информацию о том, кто, когда и с какой целью имел доступ к файлам;
- **Оптимизация хранения данных**: DCAP-системы позволяют выявлять файлы, которые давно не использовались или уже неактуальны

Такие системы проходят сертификацию в Минцифры, например Makves DCAP, которая выполняет часть требований приказа ФСТЭК №117 к защите информации в государственных информационных системах, имеет такой сертификат.

2. Системы для предотвращения утечек, контроля действий и коммуникаций пользователей (DLP-системы);

DLP-система (Data Loss Prevention, «предотвращение утечек данных») работает на основе контроля и анализа всех возможных каналов утечки.

В частном секторе часто используются так называемые DLP – системы, это системы по защите от утечек.

Система отслеживает действия пользователей: копирование, печать, загрузку в облако, пересылку писем, использование внешних носителей. Это позволяет выявлять подозрительные операции и предотвращать инциденты на ранней стадии, путем приостановки передачи данных при подозрительных действиях. Информация об инциденте передается администратору, который его проверяет и затем разрешает, либо запрещает дальнейшую передачу данных.

Такую же систему можно добавить к текущим автоматизированным информационным системам. При этом есть несколько вариантов, как это можно осуществить, ДЛП – системы могут работать как с ИИ, так и без него. Но в любом случае использование такой системы рекомендуется добавить, как меру защиты в соответствующий единый акт. А в случае применения системы с ИИ, требуется обеспечить контроль человека над системой.

Российские решения в этой области также проходят сертификацию ФСТЭК и могут быть использованы госорганами.

3. Системы управления событиями информационной безопасности (SIEM системы)

Современные системы SIEM (Security Information and Event Management) — это программные комплексы, обеспечивающие сбор, нормализацию и корреляцию событий безопасности в реальном времени из различных источников (серверы, брандмауэры, антивирусы). Они используют агенты или безагентный сбор данных (то есть сбор данных с использованием дополнительных программ или без них), а также искусственный интеллект для обнаружения угроз и автоматического уведомления, работая через веб-интерфейсы.

SIEM-система объединяет в себе функцию сбора журналов, корреляцию событий и анализ в реальном времени.

Современные SIEM являются неотъемлемой частью центров мониторинга безопасности (SOC).

Сами же системы SOC (Security Operations Center) — это экосистема для защиты бизнеса (или же госоргана), объединяющая людей, процессы и технологии для активного обнаружения и реагирования на киберугрозы. Помимо SIEM в нее входит

IRP/SOAR (Incident Response Platform) **– платформа для** автоматизации процессов реагирования на инциденты, для минимизации ручного труда.

Также в системе SOC есть анализы индикаторов для выявления актуальных атак и инструменты мониторинга для отдельных рабочих инструментов, напрмимер для облачных сервисов.

Ожидаемая замена приказа ФСТЭК №17 на № 117 с расширением субъектов, к которым относятся требования по защите информации означает не только необходимость пересмотра модели угроз, но и внедрение инструментов мониторинга — в том числе SIEM-системы как обязательного компонента архитектуры защиты.

Использование ИИ и автоматизация:

Многие современные системы защиты информации применяют искусственный интеллект для автономного анализа и масштабирования защиты.

Также они активно используют машинное обучение для анализа поведения предполагаемых киберпреступников.

Так, например в работе Зуева В.Н. [4, с. 91-97] исследуется применение ИИ на в рамках использования методов глубокого обучения для обнаружения аномалий в сетевом трафике. Предлагается использовать сверточную нейронную сеть (CNN) для анализа сетевого трафика в режиме реального времени. Предоставленные результаты на наборах данных в публичном доступе показывают, что метод Зуева В. Н. обеспечивает более высокую точность обнаружения аномалий по сравнению с традиционными методами.

Обратимся к исследованию "Frontier AI Trends Report" [5] от AI Security Institute (AISI), в котором проанализированы результаты тестирования передовых моделей ИИ за период с 2024 по 2025 годы.

Согласно этому исследованию, современные модели ИИ существенно улучшили свои способности в задачах по обеспечению информационной безопасности.

Как указано, в начале 2024 г. такие системы могли выполнить задачу в 10% случаев, то к концу 2025 года они выполняют задачи такого же уровня в 50% случаев, причем без помощи человека. Более того, В 2025 году протестировали первую модель, которая могла успешно выполнять задачи экспертного уровня, обычно требующие от человека-практика более чем 10-летнего опыта.

Исследователями отмечается интересная закономерность: по их оценке, каждые 8 месяцев возможности ИИ удваиваются.

Таким образом современные SOC системы становятся более самостоятельными и автономными, за счет искусственного интеллекта.

Рассмотрим статью, [6] анализирующую проблему обнаружения аномалий в киберфизических системах. Автор Vegesna V. V. отмечает, что «традиционные методы обнаружения аномалий на основе правил и пороговых значений часто оказываются неэффективными для сложных киберфизических систем с большим объемом разнородных данных.» Чтобы решить эту проблему, снова используются подходы машинного обучения. Проведено экспериментальное сравнение различных методов машинного обучения на реальных данных: вероятностные модели и гибридные подходы, глубокие нейронные сети для анализа временных рядов, методы изоляционных лесов для выявления выбросов. Автор выводит, что наибольший результат показывает гибридный метод, и что он является перспективным для защиты критической инфраструктуры и обнаружения аномалий в киберфизических системах.

В заключение хочется отметить, что сфера защиты информации быстро развивается, а методы защиты с помощью искусственного интеллекта остается активной междисциплинарной областью исследований. Важно отметить, что дальнейшее развитие информационных систем государственных органов связно с использованием новых технологий, в том числе систем ИИ. Необходимо разрабатывать свои системы и перенимать зарубежный опыт, чтобы создать наиболее эффективную систему обработки данных в госорганах и подготовить для них современные методы защиты.

Реализация этих мер позволит сформировать эффективную, современную и доступную модель управления данными, которая отвечает требованиям времени и ожиданиям общества, укрепляет доверие граждан к государственной системе и способствует защите их прав и законных интересов.

Литература

1. Указ Президента РФ от 2 июля 2021 г. N 400 "О Стратегии национальной безопасности Российской Федерации" // СПС «Гарант» URL: https://base.garant.ru/401425792/
2. Горбатов В. С. и др. Кибербезопасность сетевого периметра объекта критической информационной инфраструктуры // Безопасность информационных технологий. 2022. Т. 29. №. 4. С. 12-26
3. «77% ИБ-специалистов согласны использовать в работе возможности ИИ» // ООО «СёрчИнформ» URL: https://searchinform.ru/news/company-news/2024/5/29/77-of-it-specialists-agree-to-use-ai-capabilities-in-their-work/
4. Зуев В. Н. Обнаружение аномалий сетевого трафика методом глубокого обучения // Программные продукты и системы. 2021. Т. 34. №. 1. С. 91-97.
5. AI Security Institute (AISI) – «Frontier AI Trends Report» // Институт безопасности искусственного интеллекта (AISI) URL: https://www.aisi.gov.uk/frontier-ai-trends-report
6. Vegesna V. V. Machine Learning Approaches for Anomaly Detection in Cyber-Physical Systems: A Case Study in Critical Infrastructure Protection // International Journal of Machine Learning and Artificial Intelligence. 2024. vol. 5. №. 5. Pp. 1-13.

Modern methods of protecting information with limited access in government agencies, including agencies of critical information infrastructure.

Romanychev N.O.

Lebedev Russian State University of Justice

This article focuses on the tasks of ensuring the security of government agencies and their information systems, including critical information infrastructure facilities. The reliability of these systems must be at the highest level, as the security of the state depends on them, taking into account globalization and the integration of information technologies into public administration, economics, finance and industry. The main regulatory acts regulating the protection of information with limited access, including the use of artificial intelligence, are considered.

Keywords**:** DLP systems, information security, critical information infrastructure facilities, government agencies, government information systems.

References

1. Decree of the President of the Russian Federation dated July 2, 2021 No. 400 "On the National Security Strategy of the Russian Federation" // SPS "Garant" URL: https://base .garant.ru/401425792/
2. Gorbatov V. S. and others. Cybersecurity of the network perimeter of a critical information infrastructure facility // Information technology security. 2022. Vol. 29. No. 4. pp. 12-26
3. "77% of IBM information technology specialists use the capabilities of And in their work" // Sarchinform LLC URL: https://searchinform.ru/news/company-news/2024/5/29/77-of-it-specialists-agree-to-use-ai-capabilities-in-their-work/
4. Zuev V. N. Detection of network traffic anomalies by deep learning method // Software products and systems. 2021. Vol. 34. No. 1. pp. 91-97.
5. Institute of Artificial Intelligence Security (AISI) – "Report on advanced trends in artificial Intelligence" // Institute of Artificial Intelligence Security (AISI) URL: https://www.aisi.gov.uk/frontier-ai-trends-report
6. Vegesna V. V. Approaches to machine learning for anomaly detection in cyberphysical systems: a practical example of critical infrastructure protection // International Journal of Machine Learning and Artificial Intelligence. Volume 2024. 5. No. 5. pp. 1-13.