Лихачев Максим Сергеевич, студент,
ФВУНЦ ВВС «ВВА», г. Челябинск

Пашков Кирилл Сергеевич, студент,
ФВУНЦ ВВС «ВВА», г. Челябинск

Попов Юрий Леонидович, к.и.н.,
ФВУНЦ ВВС «ВВА», г. Челябинск

ЗАЩИТА ГОСУДАРСТВЕННОЙ ТАЙНЫ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ: ПРАВОВЫЕ, ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ АСПЕКТЫ

Аннотация: В условиях активной цифровизации государственного управления защита государственной тайны приобретает новое значение. Настоящая работа посвящена комплексному анализу действующей системы защиты секретной информации в России с учетом современных вызовов информационной безопасности. Исследуются правовые основы, организационные и технические аспекты обеспечения режима секретности, включая участие ФСБ, ФСТЭК и других уполномоченных органов. Особое внимание уделено применению современных технологий защиты, таких как DLP- и SIEM-системы, криптографическая защита, а также принципу Zero Trust. Рассматривается международный опыт (НАТО, ISO/IEC 27001), выявлены актуальные проблемы и предложены рекомендации по модернизации системы. Работа основана на актуальных нормативных документах и практических примерах, что делает её полезной для практического применения в работе государственных органов и разработки новых мер по защите секретной информации в условиях цифровизации.

Ключевые слова: Государственная тайна, информационная безопасность, цифровизация, ФСБ, ФСТЭК, режим секретности, криптографическая защита, Zero Trust, DLP, SIEM, ISO/IEC 27001, защита информации, нормативная база, киберугрозы.

Введение

Защита государственной тайны – один из базовых элементов системы национальной безопасности. Цифровизация органов власти, облачные технологии, мобильные рабочие места и электронный документооборот значительно расширили поверхность потенциальных атак на защищаемые сведения. В условиях, когда объем обрабатываемых данных в органах управления растет, а киберугрозы становятся всё более сложными, традиционные методы защиты информации требуют пересмотра и усиления. Цель настоящей работы – комплексный анализ действующей системы защиты государственной тайны с учетом вызовов цифровой эпохи и выработка практических рекомендаций по ее совершенствованию.

1. Правовая основа защиты государственной тайны

1.1. Базовые нормативные акты

Фундаментальным документом является Федеральный закон от 21 июля 1993 г. № 5485-1 «О государственной тайне». Закон определяет перечень сведений, подлежащих засекречиванию, устанавливает степень секретности («особой важности», «совершенно секретно», «секретно»), регламентирует порядок допуска, хранения, передачи и уничтожения секретной информации. Дополняется он указами Президента РФ, постановлениями Правительства, приказами ФСБ и ФСТЭК, а также государственными стандартами, включая ГОСТ Р 51275-99, ГОСТ Р ИСО/МЭК 15408, ГОСТ Р ИСО/МЭК 27001.

1.2. Классификация сведений и грифы секретности

Сведения, отнесенные к государственной тайне, классифицируются по степени ущерба, который их разглашение может нанести безопасности РФ. «Особой важности» – наиболее чувствительная категория, разглашение которой может привести к катастрофическим последствиям. Документы маркируются грифами, предусматривающими различный уровень доступа, режимы хранения и ограничения по копированию и передаче.

1.3. Ответственность за нарушение режима секретности

Уголовный кодекс РФ содержит ряд статей, устанавливающих ответственность за утрату или разглашение государственной тайны. Статья 283 УК РФ предусматривает ответственность за умышленное или неосторожное разглашение сведений, составляющих государственную тайну, – до 4 лет лишения свободы. Статья 283.1 вводит ответственность за незаконное получение таких сведений. Помимо уголовной предусмотрена дисциплинарная, административная и материальная ответственность.

2. Организационно-правовой механизм обеспечения режима секретности

Эффективное обеспечение режима секретности в государственном управлении основывается на четкой регламентации полномочий органов власти, строгом порядке допуска к государственной тайне и комплексной системе внутренних мер в организациях. Рассмотрим каждый из этих аспектов подробнее.

2.1. Уполномоченные органы

В Российской Федерации действует многоуровневая система органов, обеспечивающих защиту государственной тайны. Их функции и взаимодействие регулируются законодательством и подзаконными актами.

Межведомственная комиссия по защите государственной тайны при Президенте РФ

Является координирующим органом, разрабатывающим стратегические направления государственной политики в области защиты секретной информации. Комиссия формирует методические рекомендации, участвует в разработке нормативных актов, контролирует выполнение программ обеспечения безопасности секретных сведений и координирует действия различных ведомств.

Федеральная служба безопасности Российской Федерации (ФСБ)

ФСБ играет ключевую роль в обеспечении режима секретности. Ее функции включают:

– проведение проверок граждан перед допуском к сведениям, составляющим государственную тайну;

– организацию и контроль за соблюдением режима секретности в подведомственных и иных учреждениях;

– разработку методических рекомендаций по защите информации;

– расследование нарушений режима и утечек информации.

Федеральная служба по техническому и экспортному контролю (ФСТЭК)

Основные функции ФСТЭК связаны с технической защитой информации, в том числе:

– установление требований к средствам защиты информации (СЗИ);

– сертификация и лицензирование организаций, осуществляющих деятельность в сфере технической защиты;

– проведение аттестации объектов информатизации, где обрабатываются сведения, составляющие государственную тайну;

– участие в разработке ГОСТов и других стандартов безопасности.

Министерство обороны РФ

Отвечает за защиту секретных сведений в вооруженных силах. Включает режимные службы, службы безопасности соединений, спецотделы и внутренние органы контроля.

Службы внутренней безопасности и режимные подразделения организаций

На местах защиту гостайны обеспечивают режимно-секретные отделы (РСО), создаваемые в организациях. Они контролируют соблюдение режима секретности, ведут учет носителей, оформляют допуск сотрудников, организуют инструктажи и внутренние проверки.

2.2. Порядок допуска к государственной тайне

Доступ к сведениям, составляющим государственную тайну, осуществляется по строго регламентированной процедуре. Этот механизм служит фильтром, позволяющим исключить потенциальные риски со стороны лиц, не отвечающих требованиям безопасности.

1. Наличие служебной необходимости

Сведения предоставляются только лицам, деятельность которых прямо связана с использованием соответствующей информации.

Письменное согласие гражданина

Форма согласия утверждена законодательно. Без добровольного согласия допуск невозможен.

Проверка органами ФСБ

ФСБ проводит комплексную проверку кандидата:

– анкетные и биографические данные;
– факты судимости, административных правонарушений;
– сведения о родственных связях, поездках за границу;
– данные о финансовой стабильности, контактах с иностранными структурами;
– психофизиологическое состояние.

Медицинское освидетельствование

Обязательная медицинская справка (форма 989н), включая психиатрическое и наркологическое заключение. Для отдельных форм допуска требуется прохождение полиграфа.

Подписание обязательства о неразглашении

Лицо подписывает документ, в котором подтверждает осведомлённость о последствиях разглашения тайны, и обязуется соблюдать режим секретности, включая сохранение сведений и после прекращения трудовых отношений.

Присвоение формы допуска

Существует три формы допуска, соответствующие степеням секретности:

– 1 форма – «особой важности»;
– 2 форма – «совершенно секретно»;
– 3 форма – «секретно».

Форма допуска определяет уровень доступа, объем проверок, ограничения в бытовой и профессиональной сфере (поездки за границу, участие в тендерах, работа по совместительству и пр.).

Периодический контроль и перепроверка

Форма допуска требует регулярного подтверждения благонадежности – как планово, так и в случае внешних признаков риска (долги, семейные обстоятельства, контакты с иностранцами). Перепроверка проводится в среднем раз в пять лет, но может быть назначена внепланово.

2.3. Режим секретности в организациях

На уровне конкретной организации защита гостайны реализуется через систему режимных, кадровых, технических и контрольных мер.

Внутренние локальные акты

Организация разрабатывает и утверждает:

– Положение о защите государственной тайны;

– Инструкции по работе с документами с грифами;
– Порядок доступа, передачи, хранения и уничтожения информации;
– Журналы учета носителей и допусков.

Режимные помещения

Выделяются специальные комнаты и зоны с ограниченным доступом, оборудованные:
– средствами контроля доступа (СКУД);
– видеонаблюдением;
– охранно-пожарной сигнализацией;
– блокировкой мобильной связи;
– сейфами и шкафами с кодовыми замками.

Учет и хранение носителей

Все носители (бумажные и электронные) подлежат регистрации, маркировке и хранению в специальных условиях. Секретные документы пересылаются только по закрытым каналам связи или нарочным способом, с фиксацией в журналах.

Обучение и инструктаж сотрудников

Сотрудники проходят обязательный инструктаж при приеме на работу, а затем ежегодное повторное обучение. Периодически проводятся учения по действиям в случае утраты документов или попыток проникновения.

Контроль перемещения информации

Применяются DLP-системы, предотвращающие несанкционированную передачу данных по электронным каналам. Запрещено использование личных устройств (смартфонов, флешек) в режиме работы с гостайной.

Применение шифросвязи и защищённых каналов

Используются криптографические средства защиты (КСЗИ), сертифицированные ФСБ и ФСТЭК. Внешний обмен ведется через закрытые защищенные каналы, включая ВИПНЕТ, Континент, СЗИ СМЭВ, а также специальные средства связи Минсвязи.

Работа с агентурной защитой

В учреждениях с высоким уровнем секретности действуют внутренние механизмы выявления угроз, включая взаимодействие с контрразведкой, анализ поведения сотрудников и проведение проверочных мероприятий.

Таким образом, организационно-правовой механизм защиты государственной тайны в Российской Федерации построен на принципе многослойности: от координации на высшем уровне до конкретных исполнительных процедур в учреждениях. В условиях цифровизации роль внутренних процедур и технических решений возрастает, и от их точного соблюдения зависит устойчивость всего режима секретности

3. Технические средства защиты

Обеспечение сохранности сведений, составляющих государственную тайну, в условиях цифровизации невозможно без применения высокоэффективных технических решений. Технические средства защиты информации являются неотъемлемым элементом комплексной системы безопасности, направленной на противодействие внутренним и внешним угрозам. Современные технологии позволяют выявлять, блокировать и документировать попытки несанкционированного доступа к информации, обеспечивать её конфиденциальность, целостность и доступность.

3.1. Средства криптографической защиты информации (СКЗИ)

Криптографическая защита – базовая и обязательная составляющая защиты государственной тайны в автоматизированных системах. Применение сертифицированных средств криптографической защиты информации (СКЗИ) регламентировано приказами

ФСТЭК и ФСБ России и осуществляется строго в соответствии с ГОСТами. Основной задачей СКЗИ является защита данных от перехвата и искажения при передаче и хранении.

Наиболее распространённые в РФ программно-аппаратные комплексы:

– **ВИПНЕТ** (ViPNet) – используется для построения защищённых сетей и каналов связи;

– **Континент** – система шифрования данных и межсетевого экранирования;

– **КриптоПро CSP** – криптопровайдер, обеспечивающий реализацию ГОСТ-алгоритмов в различных программных средах.

Все указанные средства должны быть сертифицированы по требованиям безопасности информации, а их установка и эксплуатация – осуществляться только специалистами с соответствующим уровнем допуска. Важно, что использование иностранных криптосредств в обработке информации, отнесённой к государственной тайне, запрещено.

3.2. Системы контроля утечек (DLP) и управления событиями безопасности (SIEM)

Современная система защиты информации невозможна без автоматизации процессов мониторинга и анализа действий пользователей и ИТ-инфраструктуры.

DLP-системы (Data Loss Prevention)

Позволяют контролировать все каналы утечки информации – электронную почту, флеш-накопители, мессенджеры, принтеры, мобильные устройства. Система проводит фильтрацию содержимого, сравнивает с базой шаблонов секретных документов, блокирует подозрительные действия (например, отправку закрытых сведений на внешние почты). DLP особенно важна в борьбе с инсайдерскими угрозами и халатностью персонала.

SIEM-системы (Security Information and Event Management)

Реализуют централизованный сбор, корреляцию и анализ событий безопасности, поступающих со всех компонентов ИТ-инфраструктуры (сервера, рабочие станции, маршрутизаторы, системы входа и доступа). Позволяют в реальном времени выявлять атаки, подозрительную активность, несанкционированные попытки доступа к защищаемой информации, а также обеспечивают аудит действий операторов.

Комбинация DLP и SIEM обеспечивает непрерывный контур наблюдения и реагирования на инциденты, необходимый в условиях работы с государственной тайной.

3.3. Аттестация объектов информатизации

Аттестация – это обязательная процедура подтверждения соответствия объектов информатизации (ОИ) требованиям по защите информации, содержащей государственную тайну. Аттестации подлежат:

– серверные комнаты и ЦОД;

– рабочие станции сотрудников;

– линии связи, включая каналы шифрованной передачи данных;

– помещения с режимом ограниченного доступа;

– программное обеспечение и автоматизированные системы.

Порядок аттестации регламентирован нормативными документами ФСТЭК и ФСБ. Он включает:

– анализ архитектуры и проектной документации;

– установку сертифицированных средств защиты информации;

– проведение испытаний на проникновение и тестов устойчивости;

– оформление протоколов, заключений и актов готовности.

По итогам выдается аттестат соответствия**,** действующий ограниченное время (обычно до 3 лет) при условии, что в системе не происходят существенные изменения. Аттестация подтверждает, что все элементы информационной инфраструктуры соответствуют нормам безопасности и могут использоваться для обработки сведений с грифом секретности.

3.4. Принцип Zero Trust в защите гостайны

Zero Trust – современная концепция кибербезопасности, отрицающая автоматическое доверие к любому пользователю или устройству, даже если они находятся внутри корпоративной сети. Принцип особенно актуален при защите сведений, составляющих государственную тайну, поскольку предполагает:

– постоянную аутентификацию и верификацию действий;
– минимизацию привилегий («не больше, чем нужно»);
– сегментацию сети для ограничения распространения инцидента;
– обязательное шифрование трафика и многофакторную аутентификацию (MFA);
– использование поведения как критерия безопасности (User Behavior Analytics).

Zero Trust предполагает, что угроза может исходить как извне, так и изнутри, а потому каждая сессия, транзакция или действие должно быть подтверждено и проверено. Эта модель становится всё более приоритетной для государственных структур, обеспечивающих защиту закрытых данных в условиях распределённых систем и удалённого доступа.

Технические средства защиты информации в контексте государственной тайны – это не просто оборудование или программные решения, а целостная система, включающая криптографическую защиту, активный мониторинг, формальные процедуры сертификации и принципы нулевого доверия. Только при их комплексном применении можно говорить о реально работающем механизме, способном противостоять современным цифровым угрозам. Сочетание этих решений с грамотной организацией и подготовкой кадров обеспечивает надежный щит от утечек и атак на критически важную информацию.

6. Международный опыт

Современные вызовы информационной безопасности в мире не ограничиваются национальными границами. Опыт зарубежных государств, особенно членов НАТО и стран с развитой системой управления безопасностью, представляет практический интерес для России в части совершенствования системы защиты государственной тайны.

6.1. Системы защиты в странах НАТО

Страны НАТО используют стандартизированную систему классификации секретной информации, закреплённую в рамках документов STANAG (Standardization Agreement). В рамках этой системы выделяются четыре основных уровня секретности:

– **Top Secret** (совершенно секретно);
– **Secret** (секретно);
– **Confidential** (конфиденциально);
– **Restricted** (ограниченного доступа).

Основной акцент делается на строгую унификацию подходов, процедур и терминологии в области информационной безопасности, что обеспечивает совместимость систем и возможность защищённого обмена данными между союзниками. Информационные системы строятся по принципу полной доверенной инфраструктуры, с обязательным шифрованием всех каналов связи, централизованным управлением доступом и тотальной аутентификацией. Стандарты безопасности распространяются не только на государственные учреждения, но и на подрядные организации, участвующие в реализации оборонных и инфраструктурных программ.

Особое внимание уделяется созданию единой среды реагирования на киберугрозы, постоянному обмену разведывательной информацией и совместным киберучениям. Такие меры позволяют оперативно реагировать на новые угрозы и адаптировать политику безопасности к изменяющимся условиям.

6.2. Стандарты ISO/IEC

Международный стандарт ISO/IEC 27001 представляет собой основу для построения системы управления информационной безопасностью (СУИБ) в организациях. Стандарт охватывает весь цикл защиты информации: от оценки рисков и классификации активов до внедрения технических и организационных мер.

Ключевые принципы ISO/IEC 27001:

– непрерывное улучшение процессов;
– подход на основе оценки рисков;
– вовлечение руководства в вопросы безопасности;
– документирование и контроль процедур;
– адаптивность к меняющимся условиям и угрозам.

На базе ISO/IEC 27001 в России разрабатываются и адаптируются собственные нормативные документы (например, ГОСТ Р ИСО/МЭК 27001-2021), применяемые в проектах цифровизации органов власти и реализации концепции «Цифровое государство». Несмотря на наличие отличий в правовой и организационной базе, ориентация на международный стандарт позволяет повысить уровень системности, транспарентности и управляемости процессов защиты государственной информации.ф

7. Рекомендации по совершенствованию системы защиты государственной тайны

1. Ужесточить требования к аттестации объектов информатизации, включая обязательное тестирование всех компонентов на устойчивость к киберугрозам и расширение перечня сертифицируемых программных решений.

2. Разработать новые ГОСТы, ориентированные на реалии облачных вычислений, мобильных платформ и удалённой работы с информацией, отнесённой к государственной тайне.

3. Повсеместно внедрить принципы Zero Trust в архитектуру информационных систем государственных органов: многофакторную аутентификацию, сегментацию сетей, динамический контроль политик доступа.

4. Реализовать комплексную систему кадровой подготовки: обязательная переподготовка не реже одного раза в три года, психологическая устойчивость, знание цифровых инструментов и правовых норм.

5. Установить более жёсткие меры контроля за внешними подрядчиками, временными работниками и сторонними поставщиками, в том числе через обязательную сертификацию и допуск по результатам проверок.

6. Активно внедрять искусственный интеллект и машинное обучение для мониторинга поведения пользователей, анализа инцидентов и предиктивной аналитики угроз, что позволит реагировать на риски до наступления последствий.

Заключение

Эффективная защита государственной тайны – это не статичная система, а живая, постоянно развивающаяся структура, отвечающая на вызовы времени. В условиях цифровизации и роста киберугроз её устойчивость возможна лишь при полной интеграции правовых норм, организационных регламентов, технических решений и человеческого ресурса. Российская система защиты гостайны обладает прочной нормативной основой и выстроенной вертикалью контроля, но для обеспечения её эффективности в XXI веке необходимо:

– усиление технической защищенности систем;
– модернизация подходов к обучению и проверке персонала;
– внедрение глобальных стандартов управления безопасностью;
– переход к новым архитектурным концепциям (Zero Trust, гибридная защита);
– активное использование современных аналитических систем.

Опыт стран НАТО и рекомендации международных стандартов показывают, что будущее защиты государственной тайны лежит в смещении акцента с «формального соблюдения требований» на «оперативное реагирование, устойчивость и управляемость рисками». Только гибкая и проактивная модель может обеспечить надёжную защиту интересов государства в условиях технологической трансформации общества.

Список литературы:

1. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Общие положения: утв. и введ. в действие Постановлением Госстандарта РФ от 05.03.1999 № 35-ст [Электрон. ресурс]. (дата обращения: 22.05.2025).
2. ГОСТ Р ИСО/МЭК 27001–2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности: утв. приказом Росстандарта от 29.10.2021 № 2148-ст
3. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учеб. пособие / Ю. Н. Загинайлов. – М.: Электронный учебник, 2021. – 320 с.
4. Мусиенко Н. О., Лысов Д. А., Кузина В. В. Сравнительный анализ сертифицированных и импортных средств защиты информации в контексте создания системы информационной безопасности для значимых объектов критической инфраструктуры // Информационная безопасность. – 2023. – № 1. – С. 45–58.
5. Методические рекомендации ФСБ России. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств. – 2023
6. Нестеров С. А. Информационная безопасность: учеб. пособие / С. А. Нестеров. – М.: Юрайт, 2021. – 224 с [Электрон. ресурс].
7. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электрон. ресурс].
8. Уголовный кодекс Российской Федерации: Федер. закон от 13 июня 1996 г. № 63-ФЗ (ред. от 30.12.2022). Ст. 283 «Разглашение государственной тайны»
9. Уголовный кодекс Российской Федерации: Федер. закон от 13 июня 1996 г. № 63-ФЗ (ред. от 30.12.2022). Ст. 283.1 «Незаконное получение сведений, составляющих государственную тайну»
10. Федеральный закон от 21 июля 1993 г. № 5485-1 «О государственной тайне» (ред. от 22.05.2025)