**Попов Юрий Леонидович,** г.п Доцент 1 кафедры,
к.и.н, доцент, профессор АВН
Филиал Военного учебно-научного центра
Военно-воздушных сил «Военно-воздушная академия имени
профессора Н.Е. Жуковского и Ю.А. Гагарина» в г. Челябинске

**Ткачёв Артём Андреевич**,
курсант 221 учебной группы 2 факультета
Филиал Военного учебно-научного центра
Военно-воздушных сил «Военно-воздушная академия имени
профессора Н.Е. Жуковского и Ю.А. Гагарина» в г. Челябинске

**Хабибулин Глеб Игоревич,**
курсант 221 учебной группы 2 факультета,
Филиал Военного учебно-научного центра
Военно-воздушных сил «Военно-воздушная академия имени
профессора Н.Е. Жуковского и Ю.А. Гагарина» в г. Челябинске

# СОВРЕМЕННЫЕ УГРОЗЫ И МЕХАНИЗМЫ ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

**Аннотация:** В статье рассматриваются актуальные угрозы безопасности государственной тайны в условиях стремительного развития цифровых технологий. Анализируются основные способы утечки секретной информации, а также современные технические и правовые механизмы её защиты. Особое внимание уделено киберугрозам, вопросам информационной безопасности и необходимости повышения уровня подготовки специалистов в области охраны государственной тайны.

**Ключевые слова:** государственная тайна, защита информации, цифровизация, киберугрозы, информационная безопасность, утечка данных, шпионаж, правовое регулирование, технические средства защиты, безопасность государства, криптография, конфиденциальность.

Государственная тайна – это не просто перечень засекреченных документов или сведений, имеющих ограниченный доступ. Это фундаментальный элемент системы национальной безопасности, опора суверенитета, стратегический актив государства и гарантия его политической, военной и экономической стабильности. Вокруг института государственной тайны выстраивается целый комплекс межведомственного взаимодействия, правового регулирования, технологического обеспечения и идеологического осмысления. От того, насколько эффективно функционирует система охраны секретной информации, зависит не только успех отдельных ведомств или проектов, но и способность государства защищать свои интересы в условиях глобальной конкуренции и скрытых угроз [2].

В условиях стремительной цифровизации, которая трансформировала все сферы – от государственного управления до оборонной промышленности, – защита государственной тайны стала задачей системного и стратегического характера. Век бумажных архивов, печатей и сейфов остался в прошлом. Сегодня государственные секреты хранятся на серверах, передаются по защищённым и, увы, не всегда надёжным каналам связи, интегрируются в облачные вычисления, становятся частью больших данных, которые ежедневно обрабатываются миллионами строк кода. При этом сами угрозы приобрели качественно новый характер: если в прошлом речь шла о физическом проникновении, шпионаже или

предательстве, то теперь на первый план выходят кибератаки, вредоносные алгоритмы, манипуляция поведенческой логикой пользователей и инструменты искусственного интеллекта [3].

Современное государство действует в условиях тотальной информационной взаимосвязанности: границы между внутренней и внешней средой стираются, а киберпространство стало ареной скрытых конфликтов, где используются не ракеты, а коды, не пушки, а пакеты данных. В этих условиях сама государственная тайна становится мишенью глобального масштаба. Информация – это валюта, оружие, стратегический ресурс и уязвимость одновременно. Разглашение сведений, составляющих государственную тайну, в современных реалиях может иметь последствия, сопоставимые с масштабным вооружённым нападением: подрыв боеспособности армии, утечка данных о военных разработках, компрометация энергетической или транспортной инфраструктуры, раскрытие внешнеполитических стратегий или потеря научно-технического лидерства [4].

Цифровые технологии не только усложнили задачи защиты, но и расширили само понимание того, что может быть отнесено к государственной тайне. Сегодня это не только оборонные документы или разведданные, но и алгоритмы, модели поведения, шаблоны принятия решений, источники метаданных, информация о критически важных объектах, параметры экономической устойчивости, сведения о кибервоенных возможностях страны и даже данные об организациях, участвующих в производственных цепочках для нужд обороны [5] При этом многие из этих сведений могут быть раскрыты не в результате прямого вторжения, а через косвенный сбор информации – так называемую "мозаичную угрозу", при которой внешние аналитики, собирая, обрабатывая и интерпретируя данные из открытых источников, способны реконструировать скрытые механизмы работы целых систем.

В этой новой реальности государственная тайна требует переосмысления не только как объект охраны, но и как явление, живущее в цифровом контексте. Оно стало гибким, динамичным, подвижным, исчезая и проявляясь в потоках данных, моделях коммуникации, контексте обработки. Традиционные методы защиты, основанные исключительно на физическом доступе, бумажном документообороте и нормативных запретах, утратили свою абсолютную эффективность [1] Их необходимо дополнять высокотехнологичными средствами защиты, продвинутыми методами цифровой гигиены, развитой системой внутреннего мониторинга и постоянным юридическим и технологическим совершенствованием.

Кроме того, государственная тайна – это не только технический и правовой объект, но и идеологический конструкт. Она связана с доверием между государством и его служащими, с моральной ответственностью граждан, с уровнем правовой культуры и сознания общества. Чем выше общий уровень информированности о рисках и ответственности, тем прочнее фундамент системы безопасности. Поэтому эффективная защита государственной тайны невозможна без комплексного подхода, в котором сочетаются три уровня: нормативно-правовой, технологический и человеческий. Именно на стыке этих компонентов и рождается современная система противодействия угрозам, которые раньше казались фантастическими, а сегодня становятся реальностью.

Законодательство Российской Федерации формирует прочную правовую основу охраны государственной тайны. Центральным актом остаётся Федеральный закон от 21 июля 1993 года № 5485-1 «О государственной тайне», определяющий государственную тайну как сведения, разглашение которых может нанести ущерб безопасности Российской Федерации в сферах обороны, внешней политики, разведки, экономики и иных стратегических направлений. Конституция РФ в статье 29, устанавливая свободу информации, подчёркивает, что эта свобода ограничивается требованиями охраны государственной тайны, что демонстрирует баланс между правами человека и защитой государства [2].

Однако основная трансформация угроз произошла с началом цифровой эры. Сегодня сведения, ранее хранившиеся в сейфах и папках под грифом «особой важности», переместились в цифровые базы данных, ведомственные облачные системы, распределённые реестры и даже нейросетевые среды. Такой переход многократно увеличил поверхность атаки – теперь не нужен физический доступ к архиву, достаточно уязвимости в ПО, фишинга или манипуляции персоналом. Именно поэтому государственная тайна оказалась под ударом новых, высокотехнологичных угроз – от кибершпионажа до аналитики больших данных [6].

Один из наиболее тревожных векторов – использование искусственного интеллекта в разведывательной деятельности. Современные ИИ-системы способны в реальном времени анализировать огромные массивы утёкших, частично засекреченных и даже открытых данных, выявляя связи, тренды и потенциальные объекты. Так, по метаданным, размещённым в открытом доступе, по публикациям в научных журналах и резюме сотрудников можно восстановить структуру секретных НИИ, раскрыть тематику их исследований и определить ключевые фигуры. Эффект «мозаичной угрозы» – когда совокупность незначительных сведений раскрывает стратегическую информацию – становится одним из основных вызовов эпохи [3].

В условиях этих рисков ключевую роль играет система допуска к государственной тайне. С 1 марта 2022 года действует новое "Положение о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне", утверждённое Постановлением Правительства РФ от 30 декабря 2021 года № 2572. Документ отменил ранее действовавшее Постановление № 63 от 2010 года и значительно обновил подходы к проверке, обучению и контролю доступа. Согласно Положению, допуск оформляется в рамках трёх форм: первой, второй и третьей – в зависимости от степени секретности (особой важности, совершенно секретно, секретно). Проверка кандидатов на допуск включает запросы в МВД, ФСБ, налоговые органы, анализ сведений о судимости, гражданстве, имущественном положении, возможных контактах с иностранными государствами, в том числе – в цифровой среде. Обязательным этапом является прохождение инструктажа и обучение по правилам обращения с секретной информацией, а также подписание обязательства о неразглашении.

Тем не менее, практика показывает, что допуск – это лишь формальный барьер, а настоящие угрозы кроются в человеческом факторе и технических уязвимостях. Так, несмотря на жёсткое законодательство, только в 2023 году, по данным ФСБ, было возбуждено более 300 уголовных дел, связанных с утечкой, незаконным доступом или разглашением государственной тайны. Основные причины – небрежность, использование незащищённых каналов связи, передача документов через личные почты, несоблюдение регламента работы с конфиденциальной информацией. Один из резонансных случаев – сотрудник оборонного предприятия отправил рабочие документы на свою домашнюю почту для "удобной работы на выходных". Суд признал его виновным по статье 283 УК РФ, назначив условное лишение свободы и пожизненный запрет на работу с гостайной.

Технические меры защиты информации регулируются требованиями ФСТЭК и ФСБ России. В организациях внедряются сертифицированные средства защиты информации (СЗИ), реализующие контроль доступа, криптографическую защиту, мониторинг сетевого трафика и предотвращение вторжений. Используются отечественные криптоалгоритмы: ГОСТ 28147-89, ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2012. Применяются системы типа SIEM, DLP, IDS/IPS, разграничение прав доступа по принципу минимальных привилегий. Однако даже технически защищённые системы могут быть уязвимы, если пренебрегать человеческой дисциплиной или если сотрудники не проходят регулярного переобучения в связи с обновлением угроз.

Особую озабоченность вызывает использование иностранного программного обеспечения и облачных сервисов в госструктурах. В условиях санкционного давления и дефицита импортозамещения, у ряда организаций нет технической возможности перейти на

полностью отечественные решения. Это повышает риск утечки данных через «бэкдоры» или программные закладки в коде, а также через сервисы обновлений, находящиеся под контролем иностранных юрисдикций. В ряде случаев наблюдаются конфликты между требованиями к безопасности и удобством – в пользу последнего, что недопустимо при работе с гостайной.

Кадровая составляющая остаётся одной из наиболее уязвимых. Несмотря на то, что федеральные ведомства формально проводят обучение, его содержание часто не соответствует уровню современных угроз. Курсы сводятся к чтению устаревших методичек, отсутствуют тренажёры, кейсы и практическое моделирование инцидентов. Между тем, цифровая грамотность сотрудников, особенно на местах, находится на критически низком уровне. В одном из исследований было установлено, что свыше 60% работников, имеющих доступ к секретной информации, не могут отличить фишинговое письмо от настоящего.

С учётом вышеизложенного, очевидна необходимость системной реформы подходов к защите государственной тайны в цифровую эпоху. Во-первых, требуется пересмотр Доктрины информационной безопасности РФ с учётом развития ИИ, квантовых технологий и биометрических систем. Во-вторых, необходимо создать национальные платформы мониторинга поведения пользователей с доступом к гостайне, с применением поведенческой аналитики, риск-профилирования и адаптивной политики контроля доступа. В-третьих, важнейшим направлением становится формирование национальной ИТ-экосистемы с полной независимостью от зарубежных компонентов – от железа до прошивки. В-четвёртых, образовательные инициативы должны быть перезапущены: только внедрение интерактивных тренажёров, ситуационного моделирования, междисциплинарных курсов (право + кибербезопасность + психология) способно создать новое поколение специалистов.

Век информации стал веком уязвимости. Никогда ранее человечество не сталкивалось с таким масштабом угроз, в которых данные – сырьё, инструмент и цель одновременно. Государственная тайна, будучи ядром суверенитета, не просто является объектом правовой охраны – она становится эквивалентом стратегической стабильности, символом независимости государства и фактором выживания в условиях глобальной турбулентности. Утечка одной критически важной информации может привести не только к срыву оборонного контракта, но и к потере технологического превосходства, дипломатическому скандалу, подрыву общественного доверия или даже прямому вторжению [3].

Современная Россия, находящаяся в эпицентре геополитической трансформации, не имеет права на ошибку в вопросах защиты государственной тайны. Новая архитектура угроз, в основе которой лежат цифровые технологии, кибершпионаж, социальная инженерия и поведенческая аналитика, требует от государства системного подхода, где каждая составляющая – право, технология, человек, политика – должна работать как часть единого защитного механизма. Привычные барьеры – сейфы, допуски, грифы – более не гарантируют сохранности информации. В игру вступают коды, алгоритмы, машинное обучение, человеческий фактор, и лишь их гармоничное сочетание способно дать необходимый уровень безопасности.

Оценка рисков сегодня невозможна без переосмысления роли человека в системе. Сотрудник с допуском к государственной тайне должен быть не просто дисциплинированным исполнителем, но высококвалифицированным профессионалом, осознающим, что каждое действие, каждый клик мыши, каждое слово – это потенциальная воронка для утечки. Мы живём в эпоху, когда вред может нанести не шпион с микрофильмом, а обычный сотрудник, случайно сохранивший файл на облачное хранилище или не распознавший фишинговое письмо. Поэтому стратегически важно не только совершенствовать технологии защиты, но и формировать культуру безопасности – в каждой организации, в каждом ведомстве, в каждом человеке.

Не менее важным является вопрос суверенитета технологий. Санкционное давление и зависимость от западных цифровых продуктов делают уязвимой саму инфраструктуру хранения и обработки секретных данных. Сегодня безопасность государственной тайны невозможна без собственной технологической базы: отечественных операционных систем, криптографических библиотек, систем видеонаблюдения, средств передачи и анализа данных. Импортозамещение в этой сфере – не экономическая мера, а вопрос национальной безопасности. Поддержка и развитие отечественной ИТ-индустрии – это фундамент, на котором должна строиться вся архитектура современной защиты [5].

Защита государственной тайны в XXI веке – это живой, адаптивный, эволюционирующий процесс. Он требует постоянного пересмотра нормативной базы, обновления методов контроля, развития образовательных программ, повышения ответственности всех участников – от рядового оператора до министра. И, что особенно важно, этот процесс не может быть статичным: киберугрозы развиваются с бешеной скоростью, и государство должно быть готово действовать на опережение, создавая не просто щит, а интеллектуальную, высокотехнологичную систему упреждающей обороны.

В заключение, можно с полной уверенностью сказать: судьба государственной тайны – это не только судьба конкретного документа, но и судьба государства как целостной, суверенной, самостоятельной системы. В эпоху, когда мир переходит от гонки вооружений к гонке алгоритмов, и когда один взломанный сервер может нанести ущерб, сравнимый с массированной атакой, только глубоко интегрированная, многоуровневая система защиты способна гарантировать сохранность критически важной информации. Будущее безопасности – за теми странами, которые смогут объединить силу закона, инновации технологий и зрелость человеческого сознания. Россия должна быть в их числе – и не на периферии, а в авангарде.

*Список литературы:*

1. Назмеева Л. Р. Современные проблемы безопасности национальной экономики в условиях её цифровой трансформации // *Вестник Казанского юридического института МВД России*. – 2022. – Т. 13, № 3 (49). – С. 69–78.
2. Дзанагова М. К., Бетеева М. М. Деятельность государственных органов по защите государственной тайны // *Право и государство: теория и практика*. – 2021. – № 4 (196). – С. 316–317.
3. Мирончуковская В. В., Темешев А. Г. Вопросы правовой регламентации деятельности государств по обеспечению национальной безопасности в цифровом пространстве: опыт России и Японии // *Право и государство: теория и практика*. – 2022. – № 8 (224). – С. 123–128.
4. Гаджиев Н. Г., Коноваленко С. А., Трофимов М. Н. Угрозы в сфере обеспечения экономической безопасности государства. Пути их нейтрализации // *Вестник экономической безопасности*. – 2022. – № 3 (15). – С. 45–52.
5. Кузьминов А. Н. Параметры экономической безопасности в условиях цифровой трансформации предприятий // *Russian Journal of Management*. – 2024. – № 4. – С. 592–597.
6. Брызгалов А. А., Козырев П. А., Ульянов В. В. Применение концепции "нулевого доверия" для защиты коммерческой тайны на предприятии в условиях цифровизации // *Вызовы цифровой экономики: технологический суверенитет и экономическая безопасность: сб. науч. тр.* – Белгород: Белгородский ГАУ, 2023. – С. 70–77.
7. Крохичева Г. Е., Шумилина В. Е. Основные вызовы и угрозы экономической безопасности // *Вестник экономической безопасности*. – 2023. – № 2 (10). – С. 33–41.
8. Гребенко Е. Д., Фролов А. А. Современные цифровые технологии: социальные и политические аспекты // *Возможности и угрозы цифрового общества: сб. науч. тр.* – СПб.: СПбГУ, 2023. – С. 68–75.