ВУНЦ ВВС «ВВА» в г. Челябинске

**НАУЧНАЯ СТАТЬЯ**

|  |  |
| --- | --- |
| по | Защите государственной тайны |
| название дисциплины |
|  |
| Основы технической защиты информации. Этапы развития технической защиты информации в области защиты государственной тайны |
| тема |

 Научный руководитель: Попов Ю.Л.

 Выполнили: Рахматуллин Т.Ф.

 Фаттахов Р.Р.

Челябинск 2025г.

# Содержание

[Содержание](#_Toc0)

[Введение](#_Toc1)

[Основные понятия и принципы технической защиты информации](#_Toc2)

[Определение технической защиты информации](#_Toc3)

[Классификация методов защиты информации](#_Toc4)

[Принципы построения систем защиты информации](#_Toc5)

[Заключение](#_Toc18)

[Список литературы](#_Toc19)

# Введение

В современном мире информация стала одним из ключевых ресурсов, определяющих развитие общества и государства. С ростом цифровизации и внедрения информационных технологий увеличивается объем данных, которые требуют защиты. В условиях глобализации и технологического прогресса обеспечение безопасности информации приобретает первостепенное значение. Особую важность приобретает защита государственной тайны, так как утечка информации такого рода может нанести значительный ущерб национальной безопасности. Техническая защита информации становится неотъемлемой частью систем безопасности, обеспечивая сохранность данных от несанкционированного доступа и других угроз.

Современные угрозы информационной безопасности многообразны и включают в себя как внутренние, так и внешние факторы. Кибератаки, вирусные программы, утечки данных и ошибки человеческого фактора являются основными вызовами для систем защиты информации. Сложность угроз возрастает с развитием технологий, что требует постоянного совершенствования методов и средств защиты. В условиях цифровой трансформации особое внимание уделяется созданию комплексных систем, способных противостоять современным вызовам.

Техническая защита информации играет ключевую роль в обеспечении безопасности государственной тайны. Она включает в себя комплекс мер, направленных на предотвращение утечек, защиту от несанкционированного доступа и обеспечение целостности данных. Использование современных технологий, таких как шифрование, системы контроля доступа и мониторинг, позволяет минимизировать риски и повысить уровень безопасности. Эти технологии являются основой для создания надежных систем защиты государственной тайны.

Целью данного исследования является анализ основ технической защиты информации и исторических этапов ее развития в контексте защиты государственной тайны. Исследование направлено на изучение принципов, методов и технологий, которые обеспечивают безопасность информации. Задачи исследования включают в себя выявление ключевых аспектов технической защиты информации, анализ исторических этапов ее развития и рассмотрение современных тенденций и технологий в данной области.

Выбранная тема исследования актуальна в условиях современных вызовов информационной безопасности. Анализ основных аспектов технической защиты информации позволит не только понять ее значение, но и определить направления для дальнейшего развития технологий защиты.

# Основные понятия и принципы технической защиты информации

## Определение технической защиты информации

Техническая защита информации включает в себя комплекс методов, средств и мероприятий, направленных на предотвращение несанкционированного доступа, утечек, искажений и уничтожения данных. Это понятие начало формироваться в 1970-х годах в СССР, когда развитие вычислительных систем потребовало создания специализированных подходов для защиты информации. С тех пор техническая защита информации стала основополагающей частью обеспечения информационной безопасности и продолжает развиваться в ответ на современные вызовы.Профессия специалиста по информационной безопасности и защите информации становится все более актуальной в IT-индустрии. Курс «Физические основы защиты информации» помогает сформировать первичные представления о целях и задачах защиты данных, а также о ключевых методах защиты, что подчеркивает значимость этой области в свете современных требований (Сиротский, 2013. 123 с.).

Основной целью технической защиты информации является обеспечение конфиденциальности, целостности и доступности данных. Для достижения этой цели необходимо предотвратить несанкционированный доступ, минимизировать риски утечек информации, защититься от внешних и внутренних угроз, а также обеспечить непрерывность работы информационных систем. Это особенно актуально в контексте защиты государственной тайны, где нарушения безопасности могут иметь критические последствия.В этой связи следует учитывать, что «в области защиты информации следует предусмотреть не только меры, связанные с информационными технологиями (криптозащиту, программные средства администрирования прав пользователей, их идентификации и аутентификации, брандмауэры для защиты входов–выходов сети и т. п.), но и меры административного и технического характера» (Замкова, 2005. 59 с.). Таким образом, комплексный подход к защите информации включает как технологические, так и управленческие аспекты, что позволяет более эффективно справляться с угрозами безопасности.

Техническая защита информации направлена на предотвращение множества угроз, включая кибератаки, вредоносное программное обеспечение, физическое повреждение оборудования и утечку данных. Согласно отчету IBM, в 2021 году наибольший ущерб от утечки данных составил 5 миллиардов долларов, что подчеркивает необходимость защиты информации. Угрозы могут исходить как извне, так и изнутри организации, и их эффективное предотвращение требует использования современных технологий и методов. Гуляев отмечает, что «защита государственной тайны требует применения современных методов и технологий, которые обеспечивают безопасность информации и предотвращают утечки» (2023, с. 55). В связи с этим внедрение инновационных решений становится ключевым фактором в обеспечении информационной безопасности.

Для обеспечения технической защиты информации применяются разнообразные технологии, включая шифрование данных, системы обнаружения вторжений и устройства контроля доступа. Шифрование, впервые получившее широкое распространение в военных системах США во время Второй мировой войны, продолжает оставаться основным методом защиты информации. Современные системы защиты также интегрируют искусственный интеллект и машинное обучение, что позволяет эффективно анализировать угрозы и предотвращать атаки. Важно учитывать специфику использования компьютера как орудия доступа к социальной памяти, что подчеркивает необходимость адаптации к условиям широкого применения новых информационных технологий (Сурхаев, 2013, с. 141).

## Классификация методов защиты информации

Физические методы защиты информации представляют собой меры, направленные на предотвращение несанкционированного доступа к объектам, где хранится или обрабатывается информация. Эти методы включают использование различных инженерных решений, таких как системы контроля и управления доступом, видеонаблюдение, охранная сигнализация и физические барьеры. Согласно исследованию 2022 года, около 60% организаций применяют физические методы защиты для предотвращения утечек данных. Эффективность таких методов обусловлена их способностью предотвращать физическое проникновение к объектам информации, что является важным аспектом общей безопасности.С другой стороны, в контексте защиты государственной тайны в Российской Федерации необходимо учитывать потенциальные угрозы. В статье рассматриваются эти угрозы, а также предлагаются варианты решения проблемных вопросов защиты государственных секретов от утечки по техническим каналам (Смирнова и др., 2021, с. 2).

Технические методы защиты информации включают специализированное оборудование и технологии для обеспечения безопасности данных. Одним из ключевых направлений является применение криптографических протоколов, таких как Advanced Encryption Standard (AES), которые обеспечивают шифрование данных и предотвращают их несанкционированное использование. Эти методы составляют основу современных систем безопасности и широко применяются в финансовых, государственных и военных структурах для защиты конфиденциальной информации. В статье также рассматриваются практические рекомендации по совершенствованию информационного обеспечения деятельности по раскрытию и расследованию преступлений, включая использование современных информационных технологий (Паршина, 2004, с. 12).

Программные методы защиты информации включают использование программного обеспечения для предотвращения угроз и обеспечения целостности данных. К таким методам относятся антивирусные программы, системы обнаружения и предотвращения вторжений, а также брандмауэры. Более 70% решений в области IT-безопасности основаны на этих методах, что подчеркивает их значимость. Эти инструменты играют ключевую роль в защите информации от вредоносного программного обеспечения и кибератак.При организации и ведении технической защиты информации необходимо решать широкий круг задач, включая категорирование защищаемой информации и оценку угроз безопасности, как отмечают Соловьев, Тарелкин, Текунов и Язов (2022, с. 3).

Организационные методы защиты информации сосредоточены на разработке и внедрении процедур и правил, которые минимизируют риски утечки данных. К таким мерам относятся обучение сотрудников, формулирование политик безопасности и проведение регулярных аудитов. Согласно отчету Международного института кибербезопасности, эти меры могут снизить вероятность инцидентов на 30%. Важно отметить, что «цель статьи: определение основных направлений разработки, состава и структуры перспективного методического обеспечения в части решения задач организации и ведения технической защиты информации в информационных системах» (Соловьев, Тарелкин, Текунов, Язов, 2022. 1 с.). Организационные методы играют ключевую роль в дополнении технических и программных решений, что обеспечивает комплексный подход к защите информации.

Интеграция различных методов защиты в единые комплексные системы позволяет значительно повысить общую эффективность обеспечения безопасности. Такие системы объединяют физические, технические, программные и организационные методы, создавая многослойную защиту. Исследования Gartner показывают, что комплексные системы повышают эффективность защиты на 40%. Этот подход особенно важен в условиях современных угроз, когда требуется учитывать разнообразие потенциальных атак и уязвимостей.

## Принципы построения систем защиты информации

Принцип многослойной защиты, также известный как принцип «глубокой обороны», предполагает построение системы защиты информации таким образом, чтобы она состояла из нескольких слоев, каждый из которых выполняет свою функцию. Этот подход был впервые предложен в 1970-х годах в рамках военных систем США для обеспечения национальной безопасности. Применение многослойной защиты позволяет создать барьеры на пути злоумышленников, усложняя доступ к защищаемым данным. Например, использование комбинации физической, технической и программной защиты обеспечивает более высокий уровень безопасности, чем применение каждого метода по отдельности.

Принцип минимизации привилегий заключается в предоставлении пользователям и процессам минимально необходимого уровня доступа для выполнения их функций. Это снижает вероятность несанкционированных действий и уменьшает возможный ущерб от потенциальных угроз. Современные операционные системы, такие как Windows и Linux, активно используют этот принцип, ограничивая права пользователей и процессов, что предотвращает их возможность совершать действия, которые могут нарушить безопасность системы.

Принцип адаптивности систем защиты предполагает способность системы изменяться и подстраиваться под новые угрозы и условия эксплуатации. Адаптивные системы защиты особенно эффективны в противодействии динамическим угрозам, таким как полиморфные вирусы, которые изменяют свою структуру, чтобы обходить традиционные методы обнаружения. Такие системы используют методы машинного обучения и анализа поведения для своевременного выявления и нейтрализации новых угроз.

Принцип резервирования и отказоустойчивости направлен на обеспечение непрерывности работы системы даже в случае частичного отказа её компонентов. Это достигается за счёт создания резервных копий данных и использования дублирующих систем. Инциденты, такие как сбои серверов Amazon в 2011 году, продемонстрировали важность резервирования для предотвращения потерь данных и обеспечения стабильности работы систем.При этом внедрение ИИ и машинного обучения в России замедляется из-за недостатка вычислительных мощностей и невысокого уровня автоматизации (Мухина, Серебрянский, б. г. 7 с.). Это указывает на то, что для достижения надежности и отказоустойчивости систем необходимо учитывать не только технические аспекты, но и инфраструктурные ограничения.

Принцип регулярного мониторинга и обновления основывается на постоянном наблюдении за состоянием системы защиты и своевременном обновлении её компонентов. Это особенно актуально в условиях увеличения числа кибератак, таких как атака WannaCry в 2017 году, которая использовала уязвимости в устаревших системах. Регулярное обновление программного обеспечения и мониторинг состояния системы способствуют минимизации рисков, связанных с эксплуатацией уязвимостей. Необходимость постоянного анализа и адаптации мер защиты государственной тайны к новым вызовам и угрозам цифровой безопасности подчеркивается в современных исследованиях (Гуляев, 2023, с. 55).

# Список литературы

1. Губарев В. В. Построение автоматной модели системы допуска к государственной тайне на основе IDEF0-модели // Информационная безопасность. — 2021. — С. 77–82. — DOI: 10.37468/2307-1400-2021-4-77-82.
2. Гуляев Г. Ю. НАУЧНЫЕ ИССЛЕДОВАНИЯ 2023: сборник статей VII Международной научно-практической конференции. — Пенза: МЦНС «Наука и Просвещение», 2023. — 292 с.
3. Замкова Т.В. Проблемы защиты информации в современных информационных системах // Материалы конференции Современные наукоемкие технологии. — 2005. — № 3. — С. 58–59.
4. Мухина Е. Р., Серебрянский Д. И. Этапы развития искусственного интеллекта по отношению к экономической безопасности частного и государственного секторов // [б. и.]. — [б. м.], [б. г.]. — [б. с.].
5. Паршина Е.Н. Проблемы информационного обеспечения и защиты информации в предварительном расследовании преступлений: Автореферат диссертации на соискание ученой степени кандидата юридических наук. — Ижевск, 2004. — [б. с.].
6. Преподавание информационных технологий в Российской Федерации: материалы Одиннадцатой открытой Всероссийской конференции (16 – 17 мая 2013 г). — Воронеж: Воронежский государственный университет, 2013. — 332 с.
7. Сборник статей XIX Международной научной конференции «Свобода и право» / под ред. Никитина П. И. — Кемерово: Издательский дом «Плутон», 2017. — 300 с.
8. Смирнова К.С., Кривошеин А.А., Плешивцев А.Ю., Челпух Э.А. К вопросу об обеспечении защиты государственной тайны на современном этапе // Вопросы российского и международного права. — 2021. — Том 11. — № 6А. — С. 156-162. — DOI: 10.34670/AR.2021.40.90.021.
9. Соловьев С.В., Тарелкин М.А., Текунов В.В., Язов Ю.К. Состояние и перспективы развития методического обеспечения технической защиты информации в информационных системах // Вопросы кибербезопасности. — 2022. — № 1(53). — С. 41–57. — DOI:10.21681/2311-3456-2023-1-41-57.
10. Соловьев С.В., Язов Ю.К., Теплинских А.А. Математические модели для оценки показателей качества информационного обеспечения деятельности по технической защите информации // Вопросы кибербезопасности. — 2023. — № 6(58). — С. 81–95. — DOI: 10.21681/2311-3456-2023-6-81-95.
11. Федеральный закон РФ от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» (ред. от 10.01.2003) // Собрание законодательства РФ. — 1995. — № 8. — Ст. 609.