**Петрыга Александра Александровна**

Магистрант

**Направление:** Информатика и вычислительная техника

**Магистерская программа:** Сети ЭВМ и телекоммуникации

# Анализ основных программных средств защиты информации в информационных сетях

**Аннотация.** В статье рассматриваются методы защиты информации в компьютерных сетях. Ключевая идея заключается в выявлении основных угроз информационной безопасности и определении медов по их предотвращению. В настоящее время обеспечение безопасности информации является в телекоммуникационных и компьютерных сетях является основной проблемой человечества, так как основная часть информации хранится и передается в цифровом виде. В статье определены основные угрозы информационной безопасности, а также проанализированы методы защиты информации.

**Ключевые слова:** аутентификация, безопасность, доступность информации, защита данных, идентификация, информация, целостность информации, шифрование.

Информационная безопасность представляет собой комплекс мер, направленных на защиту информации от угроз и рисков, связанных с её использованием, хранением и передачей. Фундаментальными принципами информационной безопасности являются:

1. Конфиденциальность – обеспечение защиты информации от несанкционированного доступа.

2. Целостность – предотвращение несанкционированного изменения информации.

3. Доступность – гарантирование доступа к информации для авторизованных пользователей [4, с. 27].

Работа компьютерных сетей базируется на взаимодействии аппаратных и программных компонентов. К сожалению, программирование не застраховано от ошибок, которые становятся мишенью для кибер-атак. Использование этих уязвимостей наносит серьезный ущерб пользователям и компаниям.

Ситуация осложняется многообразием операционных систем и задержками в выявлении уязвимостей. Более того, даже выпущенные обновления часто не устанавливаются своевременно, открывая возможности для взлома сетей, распространения вирусов и изменения данных.

Увеличение числа пользователей и усложнение сетевой архитектуры приводит к росту угроз безопасности. Эта проблема затрагивает как программное, так и аппаратное обеспечение. В аппаратном аспекте уязвимыми становятся не только компьютеры, но и элементы сетевой инфраструктуры – оптоволоконные кабели и прочие средства передачи информации.

Нахождение сетевых компонентов в разных географических точках расширяет поле для направленных кибер-атак, способных причинить значительный вред. Отдельного внимания заслуживает проблема компьютерных вирусов, требующая бдительности от каждого пользователя сети.

Далее проведем анализ основных программных средств защиты информации в информационных сетях.

Безопасность компьютерных сетей серьезно страдает от вредоносных программ, среди которых особую опасность представляют вирусы и трояны. Эффективной защитой служит брандмауэр, который создает барьер между зараженными программами и компьютерной системой.

Брандмауэр функционирует как защитный экран, разделяющий внутренние и внешние сетевые соединения. При выявлении потенциальной атаки система позволяет пользователю запустить защитные протоколы для блокировки угрозы. Важно помнить о проблемах совместимости, которые могут возникнуть при интеграции брандмауэра с существующей инфраструктурой.

Антивирусное ПО представляет собой ключевой компонент в стратегии защиты сетевой инфраструктуры. Данное решение, получившее широкое

распространение среди пользователей, обеспечивает многоуровневую защиту от различных типов киберугроз.

Создание качественного антивирусного продукта требует соблюдения трех основных принципов: стабильности работы, простоты использования и быстрого реагирования на угрозы. Важно учитывать, что даже лучшие антивирусные программы малоэффективны в борьбе с уже проникшими в систему вирусами.

Цифровые данные постоянно находятся под угрозой повреждения или кражи, что делает антивирусную защиту необходимым элементом компьютерной безопасности. Для поддержания должного уровня защиты критически важно своевременно обновлять вирусные сигнатуры, обеспечивая защиту от новейших вредоносных программ [2, с. 210].

Инновационный метод шифрования служит современным решением для обеспечения защиты данных, препятствуя их неавторизованному использованию. Следует отметить, что эффективное предотвращение угроз информационной безопасности возможно лишь при оперативном внедрении защитных механизмов.

При улучшении системы безопасности сетевой инфраструктуры важно не только внедрять базовые меры защиты, но также принимать во внимание технические ограничения и вопросы сервисного обслуживания. Шифрование существенно усиливает приватность информации в сети, предупреждая возможные риски [3, с. 43].

Данные, защищенные с помощью криптографических алгоритмов при вводе и трансфере, значительно менее подвержены риску перехвата. Кроме того, критически важно обеспечивать защиту аппаратных компонентов через укрепление безопасности и внедрение специальных мер против вирусных атак.

В современных телекоммуникационных и компьютерных сетях используются различные способы аутентификации и идентификации пользователей для обеспечения надежной защиты данных. Данные механизмы составляют фундамент системы информационной безопасности в цифровой среде.

Процесс аутентификации служит для проверки подлинности заявленной пользователем личности, подтверждая соответствие субъекта предоставленным учетным данным.

Механизм идентификации выполняет функцию распознавания пользователей, ограничивая их доступ только разрешенными ресурсами. Комбинация этих технологий эффективно противодействует несанкционированному проникновению к защищенной информации и снижает вероятность успешных кибернетических атак. Разработанные методы аутентификации и идентификации также находят применение в научных работах, направленных на совершенствование систем информационной безопасности [1, с. 81].

Таким образом, анализ проблем безопасности компьютерных сетей показывает, что основными угрозами являются уязвимости системы, внешние атаки и вредоносное программное обеспечение. Для эффективной защиты информации необходимо применять многоуровневый подход, сочетающий различные технологии: брандмауэры, антивирусное ПО, шифрование данных, аутентификацию и идентификацию пользователей.

Информационная безопасность в современном мире становится критически важным аспектом как для частных лиц, так и для организаций. Недостаточное внимание к вопросам защиты данных может привести к серьезным последствиям: утечке конфиденциальной информации, финансовым потерям и репутационному ущербу.

Для усиления защиты компьютерных сетей рекомендуется разработать и внедрить комплексную стратегию безопасности, которая будет включать регулярное обновление программного обеспечения, обучение персонала правилам безопасности, проведение аудита систем и разработку политик реагирования на инциденты. Особое внимание следует уделить методам аутентификации и идентификации пользователей, которые являются первой линией защиты от несанкционированного доступа.

В связи с постоянным развитием угроз необходимо непрерывно совершенствовать системы защиты, следить за новыми тенденциями в сфере

информационной безопасности и оперативно адаптироваться к изменяющимся условиям. Только комплексный и проактивный подход к безопасности позволит обеспечить надежную защиту информации в компьютерных сетях.

**Литература**

1. Исмагилова А.С., Лушников Н.Д. Программная реализация защиты от несанкционированного доступа // Безопасность информационных технологий. 2023. Т. 30, № 1. С. 81-91.

2. Кравченко Ю.А. Защита информации в компьютерной сети / Современные тенденции развития науки и мирового сообщества в эпоху цифровизации: Сборник материалов XIII Международной научно-практической конференции, Москва, 10 апреля 2023 года. – М.: Общество с ограниченной ответственностью «Издательство АЛЕФ», 2023. С. 210-212.

3. Рихтер Т.В. Разработка модели системы обеспечения информационной безопасности в компьютерных сетях // International Journal of Advanced Studies in Computer Engineering. 2021. № 1. С. 43-54.

4. Чечулин А.А. Основные элементы методологии обеспечения информационной безопасности и защиты информации в компьютерных сетях // Информатизация и связь. 2022. № 3. С. 27-30.