Жаренов Евгений Андреевич

Магистрант

Направление: Информатика и вычислительная техника

Магистерская программа:Информационные системы

О средствах защиты цифровой и аналоговой информации

Аннотация. В настоящее время обслуживание пользователей компьютеров всё более происходит в форме удаленного доступа к ресурсам распределенной информационной системы, к числу которых относится телекоммуникационные и компьютерные сети. В силу этого обстоятельства увеличивается возможность утечки информации. В связи с этим возрастает роль создания эффективных мер защиты информации. Так же рассматриваются методы обеспечения безопасности данных и принципы их применения исследование современных технологий и подходы к защите информации, выявление преимущества и недостатки. Работа содержит рекомендации по выбору оптимальных средств защиты данных в различных сферах деятельности.

Ключевые слова: криптография, защита информации, кибербезопасность, шифрование, аутентификация

Современный мир цифровых технологий требует надежной защиты как цифровой, так и аналоговой информации. Существует множество средств защиты, которые помогают обеспечить конфиденциальность и целостность данных [1]. От криптографических алгоритмов до физических устройств, средства защиты информации играют важную роль в современном обществе. Оперативно-технические факультеты и специализированные компании разрабатывают и внедряют новейшие технологии для защиты данных от киберугроз. Понимание ключевых угроз и использование соответствующих средств защиты является неотъемлемой частью стратегии безопасности предприятий. В данной статье рассмотрим различные средства защиты цифровой и аналоговой информации, их особенности и применение в современном мире технологий [2].

Антивирусное программное обеспечение играет важную роль в защите компьютерных систем от вредоносных программ и вирусов. Оно сканирует файлы и программы на наличие угроз, блокирует вредоносные действия и предотвращает потенциальные атаки. Антивирус помогает обнаруживать и удалять вирусы, трояны, шпионские программы и другие вредоносные объекты, обеспечивая безопасность данных и конфиденциальность информации. Без антивирусного ПО компьютер остается уязвимым перед угрозами из сети, поэтому его установка и регулярное обновление являются необходимыми мерами для обеспечения безопасности информации.

Шифрование данных играет ключевую роль в обеспечении конфиденциальности и защите информации от несанкционированного доступа. Путем преобразования информации в зашифрованный вид, шифрование обеспечивает ее безопасность при передаче по сети или хранении на устройствах. Только авторизованные пользователи с доступным ключом могут расшифровать данные и прочитать их. Благодаря шифрованию, даже в случае утечки информации, злоумышленники не смогут прочитать ее без ключа. Это позволяет предотвратить утечку конфиденциальных данных и обеспечить их целостность [3].

Биометрическая аутентификация и использование паролей - два основных метода защиты информации. Биометрическая аутентификация основана на уникальных физиологических или поведенческих характеристиках человека, таких как отпечатки пальцев, сетчатка глаза или голос. Пароли, с другой стороны, представляют собой комбинацию символов, которые должен знать пользователь для доступа к информации. Биометрическая аутентификация обычно считается более безопасным методом, так как биометрические данные сложнее подделать или украсть, чем пароль. Однако, биометрическая аутентификация может быть менее удобной в использовании и требовать специального оборудования. Пароли, с другой стороны, могут быть украдены или подобраны злоумышленниками. Поэтому комбинация биометрической аутентификации и паролей может обеспечить более надежную защиту информации.

Многофакторная аутентификация - это метод защиты информации, который требует от пользователя предоставить несколько форм идентификации для доступа к системе. Это может включать в себя сочетание, что пользователь знает, например, пароль или отпечаток пальца. Этот подход делает взлом системы более сложным для злоумышленников, так как им нужно обойти несколько уровней защиты. Многофакторная аутентификация становится все более популярной в сфере кибербезопасности, так как обеспечивает более надежную защиту данных и информации.

Внедрение систем мониторинга безопасности позволяет постоянно отслеживать активность в сети и на компьютерах, выявлять подозрительные действия и атаки в реальном времени. Это помогает оперативно реагировать на угрозы и предотвращать утечку конфиденциальной информации. Системы мониторинга позволяют анализировать данные, обнаруживать несанкционированный доступ и вредоносные программы, а также контролировать действия пользователей. Внедрение таких систем повышает уровень безопасности организации и помогает предотвратить угрозы для информации и данных [4].

Таким образом, изучение современных средств защиты цифровой и аналоговой информации позволяет сделать вывод об их разнообразии и специфике применения. Сравнительный анализ показал, что каждое средство имеет свои преимущества и недостатки, и выбор конкретного зависит от конкретных потребностей и условий использования. Рекомендуется комбинировать различные средства защиты для обеспечения более надежной защиты информации. Дальнейшие исследования в этой области могут способствовать разработке новых эффективных средств защиты информации и повышению уровня информационной безопасности в целом.

Литература

1. Малюк А.А. Защита информации: современные проблемы // Безопасность информационных технологий. Т. 17. № 1(2010). С. 5-8.

2. Средства защита цифровой информации / Электронный ресурс / URL: https://pro-spec.ru/poleznaya-informaciya/152-sredstva-zashchita-tsifrovoj-informatsii.

3. Исаев А.Б. Современные технические методы и средства защиты информации: Учеб.пособие. - М.: РУДН, 2008. - 253 с.

4. Безопасность предприятий: ключевые угрозы и средства защиты / Электронный ресурс / URL: https://habr.com/ru/articles/529178/.