**Яковлева Людмила Егоровна,**

преподаватель,

**Андреева Каролина Алексеевна,**

Студeнт,

Колледж Инфраструктурных Технологий

ФГАОУ ВО «Северо-Восточный федеральный университет имени М. К. Аммосова»

г. Якутcк, Рeспублика Сaха (Якутия), Рoссия

**Разработка мер по технической защите конфиденциальной информации в организации**

**Аннотация**: В этой статье подчеркивается, что создание технических средств защиты конфиденциальных данных внутри организации имеет важное значение. Изучим фундаментальные концепции и методы защиты данных, такие как шифрование, аутентификация, контроль доступа и мониторинг сетевой активности. Важным фактором также является вопрос выбора правильных технологий и инструментов для обеспечения информационной безопасности и предотвращения утечек данных. В заключение приводятся рекомендации по разработке стратегии информационной безопасности и принятию соответствующих мер внутри организации.

**Ключевые слова:** конфиденциальная информация, шифрование, техническая защита информации, организация, защита данных, политика безопасности, утечка информации, информационная безопасность.

Меры технической защиты конфиденциальной информации в организации является критически важной задачей для любой организации, поскольку от утечки данных могут пострадать репутация, финансовое положение и безопасность клиентов. Поэтому разработка и внедрение всеобъемлющих мер технической защиты конфиденциальной информации является неотъемлемой частью стратегии информационной безопасности.

Основополагающей задачей в обеспечении защиты конфиденциальной информации в организации является обеспечение безопасности и сохранности данных. На сегодняшний день технологии достигли такого уровня развития, что позволяют злоумышленникам без каких-либо проблем проникнуть в системы и получить доступ к данным, которые имеют высокую ценность. Поэтому защита конфиденциальной информации является одним из приоритетных направлений в работе каждой организации.

Основными инструментами технической защиты конфиденциальной информации являются:

- Антивирусное программное обеспечение. Она обеспечивает обнаружение и удаление вредоносных программ, которые могут представлять угрозу безопасности данных. Регулярное обновление антивируса гарантирует его эффективность против новых угроз.

- Шифрование данных. Такой формат преобразует данные в нечитаемый текст, доступ к которому имеют только авторизованные лица. Шифрование особенно важно при передаче конфиденциальной информации. Программы для шифрования сообщений, защищают конфиденциальные данные, передаваемые по электронной почте или в мессенджерах, от несанкционированного доступа.

- Программное обеспечение для мониторинга и контроля доступа. Позволяет отслеживать действия пользователей с конфиденциальными данными, ограничивать доступ к защищенным файлам и записывать действия сотрудников.

Помимо использования программных инструментов, для обеспечения надежной защиты данных следует также принимать следующие меры:

- Регулярное обновление программного обеспечения устраняет уязвимости, которыми могут воспользоваться злоумышленники.

- Аудит безопасности сети и компьютеров выявляет потенциальные угрозы и дает рекомендации по их устранению.

- Обучение сотрудников правилам безопасности в сети и надлежащему использованию конфиденциальных данных значительно снижает внутренние риски.

- Регулярная смена сложных паролей к учетным записям снижает вероятность несанкционированного доступа.

Эффективная защита конфиденциальной информации требует комплексного подхода, включающего как технические меры, так и обучение персонала. Сочетание этих элементов обеспечивает надежную защиту от внутренних и внешних угроз, помогая организациям сохранить ценные данные и избежать негативных последствий утечек. Постоянная оценка и адаптация мер защиты к эволюционирующим угрозам должны быть неотъемлемой частью общей стратегии кибербезопасности.

Шифрование – это процесс преобразования данных в форму, которая не может быть прочитана без ключа. Существует несколько методов шифрования, каждый из которых имеет свои преимущества и недостатки:

- Симметричное шифрование. Для такого шифрования используют один ключ для шифрования и дешифрования данных. Это обеспечивает высокую скорость, но ключ передается между сторонами, что может быть небезопасно.

- Асимметричное шифрование: используют два ключа – открытый и закрытый. Открытый ключ используется для шифрования данных, а закрытый – для дешифрования. Этот метод более сложный, но он обеспечивает более высокую безопасность, так как закрытый ключ не передается другим лицам.

- Блочные шифры: шифруют данные блоками фиксированного размера. Они обеспечивают высокую степень безопасности и могут быть использованы для шифрования больших объемов данных.

Аутентификация и авторизация - это основные компоненты системы защиты конфиденциальной информации в организации. Аутентификация занимается процессом проверки подлинности пользователя, а авторизация процессом определения его прав доступа к информации.

Системы аутентификации и авторизации должны быть разработаны с учетом следующих мер безопасности:

1. Реализация многофакторной аутентификации требует нескольких шагов для получения доступа к системе, что повышает безопасность.

2. Шифрование необходимо для обеспечения безопасности паролей и предотвращения несанкционированного доступа злоумышленников в случае взлома базы данных.

3. Чтобы предотвратить попытки взлома, система должна автоматически блокировать учетную запись пользователя после нескольких неудачных попыток ввода пароля.

4. Централизованное управление доступом необходимо администраторам для обеспечения беспрепятственного использования пользователями различных системных ресурсов и предотвращения несанкционированного доступа.

5.Периодические обновления паролей необходимы для повышения безопасности и должны обеспечиваться пользователями.

6.Система, позволяющая отслеживать активность пользователей и выявлять подозрительное поведение, должна подвергаться аудиту и мониторингу.

Организация должна иметь меры безопасности для защиты своей конфиденциальной информации, включая серверы, сети и приложения. Необходимо провести оценку угроз, выявить наиболее значимые уязвимости и создать индивидуальные планы защиты данных для каждой организации. Он обеспечивает надежные средства защиты конфиденциальной информации и защиты организации от потенциальных угроз.

Список литературы

1. Коробкова О. К. Проблемные вопросы информационной безопасности организаций в рамках экономической безопасности РФ //Вестник Хабаровского государственного университета экономики и права. – 2021. – №. 1 (105). – С. 48-54.
2. Раханов К. Я., Раханова Н. А. Обеспечение конфиденциальности информации в сети Интернет: пособие. – 2021.
3. Соловьев С. В. и др. Состояние и перспективы развития методического обеспечения технической защиты информации в информационных системах //Вопросы кибербезопасности. – 2023. – №. 1. – С. 41-57.
4. Ерышов В. Г. Модель процесса технической защиты конфиденциальной информации, обрабатываемой на защищаемом объекте информатизации. – 2021.
5. Синещук Ю. И., Родин В. Н., Иванов А. Ю. Организационная защита информации. – 2020.
6. Соловьев С. В., Язов Ю. К. Информационное обеспечение деятельности по технической защите информации //Вопросы кибербезопасности. – 2021. – №. 1 (41). – С. 69-79.