Информационная безопасность

Выполнил: Ковалев Всеволод, 9-1 класс

Наставник: Могилова Людмила Ильинична,

Учитель математики и информатики

Цель: рассмотреть проблемы информационной безопасности и возможные способы применения современных методов и средств защиты информационных ресурсов.

- Задачи:
- изучить и проанализировать литературу и источники интернета по теме проекта;
- выявить проблемы информационной безопасности и проанализировать пути решения данных проблем;
- Ознакомить учащихся с главными сведениями об информационной безопасности.

Мы живем во время развивающихся информационных технологий и компьютеризации, исходя из этого, информация – это один из самых ценных и важных активов любого предприятия, которая должна быть надлежащим образом защищена.

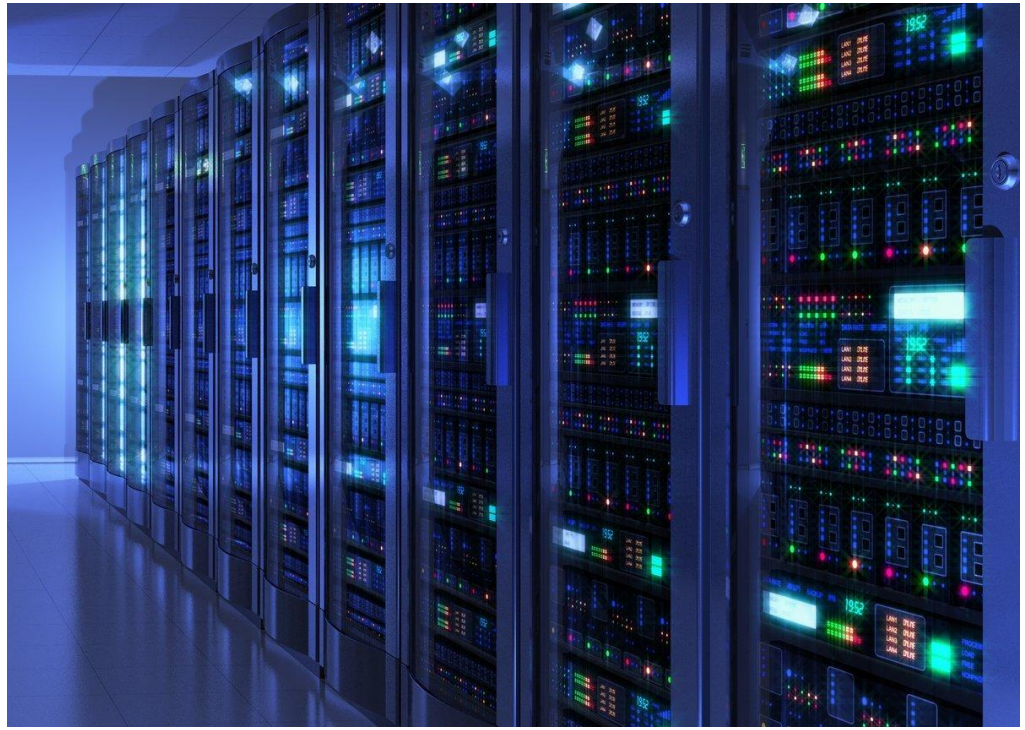
Информационная безопасность

- **Информационная безопасность (ИБ)** – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенных для использования, сбережения и передачи этой информации. Другими словами, это набор технологий, стандартов и методов управления, которые необходимы для защиты информационной безопасности.
- **Цель обеспечения информационной безопасности** – защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения. Информационная безопасность помогает обеспечить непрерывность бизнеса.

Главные принципы информационной безопасности

- **Конфиденциальность.** Это значит ввести в действие контроль, чтобы гарантировать достаточный уровень безопасности с данными предприятия, активами и информацией на разных этапах деловых операций для предотвращения нежелательного или несанкционированного раскрытия

- **Целостность.** Целостность имеет дело с элементами управления, которые связаны с обеспечением того, чтобы корпоративная информация была внутренне и внешне последовательной.
- **Доступность.** Доступность обеспечивает надежный и эффективный доступ к информации уполномоченных лиц. Сетевая среда должна вести себя предсказуемым образом с целью получить доступ к информации и данным, когда это необходимо.



Контроль информационной безопасности

- Обеспечить полноценную и надежную информационную безопасность предприятия можно только при условии применения комплексного и системного подхода. Система информационной безопасности должна быть построена с учетом всех актуальных угроз и уязвимостей, также с учетом тех угроз, которые могут возникнуть в будущем. Поэтому важно обеспечить поддержку непрерывного контроля, который должен действовать ежедневно и круглосуточно. Необходимым условием является обеспечение контроля на каждом из этапов жизненного цикла информации, начиная с момента ее поступления в инфраструктуру компании и заканчивая потерей ее актуальности или уничтожением данных.

Угрозы информационной безопасности

- Угрозы информационной безопасности можно разделить на следующие:

Искусственные:
-непреднамеренные (совершаются людьми по неосторожности или незнанию);
-преднамеренные (хакерские атаки, противоправные действия конкурентов, месть сотрудников и пр.).

Естественные (катаклизмы, не зависящие от человека: пожары, ураганы, наводнение, удары молнии и т.д.).

Вредоносные программы как угроза информационной безопасности

- Баранова Е.К и Бабаш А.В в своей книге "Информационная безопасность и защита информации" 3-е изд. (2016) утверждают, что Вредоносные программы - одна из главных угроз информационной безопасности. Это связано с масштабностью распространения этого явления и, как следствия, огромного ущерба, наносимого системам.
- Вредоносные программы создаются специально для несанкционированного пользователем уничтожения, блокирования, модификации или копирования информации, нарушения работы компьютеров или компьютерных сетей. К данной категории относятся вирусы и черви, троянские программы и иной инструмент, созданный для автоматизации деятельности злоумышленников.

Виды средств защиты информации

- Виды средств защиты информационной безопасности можно разделить на следующие:

Антивирусные программы

Облачный антивирус

Криптографические системы

Правовое регулирование защиты информации

- Правовую основу информационной безопасности обеспечивает государство. Защита информации регулируется международными конвенциями, Конституцией, федеральными законами и подзаконными актами.
- Государство также определяет меру ответственности за нарушение положений законодательства в сфере ИБ.

Практическая часть

- В ходе практической части был разработан буклет по данной теме.Его можно изучить всем желающим после выступления.

Информационная безопасность

В связи с развитием информационных технологий и компьютеризацией экономики одним из важнейших вопросов в деятельности компании становится обеспечение информационной безопасности.

Информация – это один из самых ценных и важных активов любого предприятия и должна быть надлежащим образом защищена.

МЕРЫ ПРЕДОСТОРОЖНОСТИ

1. Используйте надежные пароли. Не применяйте легко угадываемые или подбираемые комбинации.
2. Избегайте незащищенных Wi-fi сетей в общественных местах. В них вы уязвимы для атак man-in-middle(Человек перехватывает ваш траффик)
3. Не переходите по ссылкам, полученным от неизвестного отправителя. Опасность заключается в возможности заражения компьютера вредоносным программным обеспечением.
4. Используйте антивирусные программы. Антивирусное программное обеспечение имеет возможность обнаружения и предотвращения компьютерной угрозы.
5. Не открывайте почтовые вложения от неизвестных отправителей.

Информационная безопасность очень важна для комфортной жизни и успешного развития бизнеса. Особенно актуально это стало в компьютезированных отраслях (медицинские учреждение, образовательные учреждения и т.п) и бизнес-среде, где на передний план вышли информационные технологии, так как мы живем в эпоху цифровой экономики, без информационной безопасности невозможно их развитие

Информация сейчас подвергается все большему числу угроз и уязвимостей. Хакерские атаки, перехват данных по сети, воздействие вирусного программного обеспечения и другие угрозы приобретают более изощренный характер и набирают быстрый темп.

Вывод

- Информационная безопасность очень важна для комфортной жизни и успешного развития бизнеса. Особенно актуально это стало в компьютерезированных отраслях (медицинские учреждения, образовательные учреждения и т.п) и бизнес-среде, где на передний план вышли информационные технологии, так как мы живем в эпоху цифровой экономики, без информационной безопасности невозможно их развитие
- Информация сейчас подвергается все большему числу угроз и уязвимостей. Хакерские атаки, перехват данных по сети, воздействие вирусного программного обеспечения и другие угрозы приобретают более изощренный характер и набирают быстрый темп. Отсюда возникает необходимость внедрять системы информационной безопасности, которые могли бы защитить данные компании.

Список используемых источников

- **1. Информационная безопасность**
- (https://pirit.biz/reshenija/informacionnaja-bezopasnost)
- 2. Информационная безопасность
- (https://searchinform.ru/informatsionnaya-bezopasnost/)
- 3. Меры защиты информации
- (https://helpiks.org/9-884.html)
- 4. Информационная безопасность. Виды угроз и защита информации
- (http://galyautdinov.ru/post/informacionnaya-bezopasnost)
- **5. Юрий Родичев, «Информационная безопасность. Национальные стандарты Российской Федерации» [стр. 2-3]**
- 6. Баранова Е.К., Бабаш А.В. «Информационная безопасность и защита информации: учебное пособие» [стр. 62-63]
- 7.Евгений Касперский «Компьютерное зловредство»

Информационная безопасность

Выполнил: Ковалев Всеволод, 9-1 класс

Наставник: Могилова Людмила Ильинична,

Учитель математики и информатики