Введение в компьютерную науку

Introduction to cybersecurity

Salymbekov University

Miss Aliia Beishenalieva

aliya.beiwenalieva@gmail.com

04.11.2024

Recap

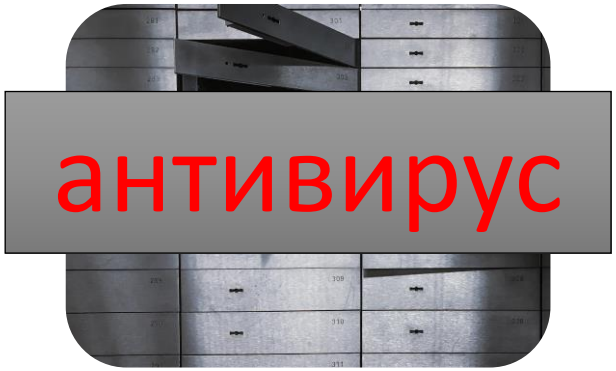
- Что мы прошли на прошлом уроке?

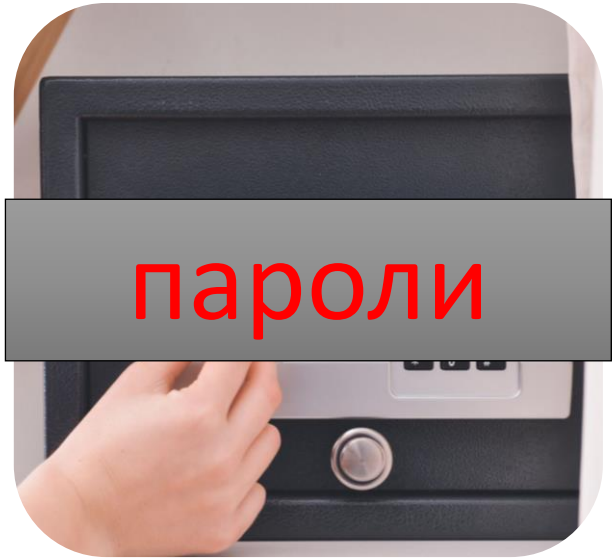
What is the cybersecurity?

Кибербезопасность — это защита компьютеров, серверов, сетей и данных от вредоносных атак, повреждений или несанкционированного доступа.

What is the cybersecurity?

What is the cybersecurity?

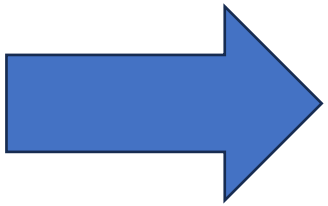




What is the cybersecurity?

Данные:

Банки
Здравохранение
Социальные сети
Государственные органы



Интернет

Без кибербезопасности хакеры могут взломать системы, украсть информацию, повредить системы или даже держать наши данные "в заложниках" (как цифровое похищение!)

The CIA triad: Триада CIA

Чтобы защитить цифровую информацию, специалисты по кибербезопасности фокусируются на трёх основных принципах, известных как **триада CIA**:

1.Конфиденциальность (Confidentiality) — Обеспечение того, чтобы информация была доступна только для авторизованных пользователей.

Подумайте о дневнике с замком. Только у вас (или у кого-то с ключом) есть возможность его прочитать.

2.Целостность (Integrity) — Обеспечение того, чтобы информация была точной и не подвергалась изменениям.

Представьте, что вы пишете письмо другу. Вы хотите быть уверены, что никто не изменит ваше сообщение перед его получением. В цифровом мире это может включать контрольные суммы или хеширование (можно представить как "цифровые отпечатки" для файлов).

3.Доступность (Availability) — Обеспечение того, чтобы информация была доступна, когда она необходима.

Если вы ведёте веб-сайт ресторана, вы хотите, чтобы он работал круглосуточно, чтобы клиенты могли забронировать стол в любое время. Кибератака может нарушить доступ, и клиенты не смогут сделать бронь.

Типы киберугроз

1. Вредоносное ПО (Malware)

   •**Вирусы**: Программа, которая прикрепляется к файлам и распространяется при их запуске.
   •**Программы-вымогатели (Ransomware)**: Блокируют доступ к файлам или системе до тех пор, пока не будет выплачен выкуп (представьте, что кто-то закрыл ваш дом и требует деньги, чтобы его открыть!).
   •**Шпионское ПО (Spyware)**: Незаметно собирает информацию о вас — ваши пароли, историю браузера и т.д. — без вашего ведома.

Представьте, что сотрудник компании нажимает на ссылку в письме, и внезапно все файлы на его компьютере заблокированы. Появляется сообщение с требованием выкупа для их разблокировки. Это действие программы-вымогателя.

Типы киберугроз

2. Фишинг

Фишинг — это когда злоумышленник притворяется легитимной организацией или человеком, чтобы обманным путём получить личную информацию, такую как логин к банку или номер социального страхования.

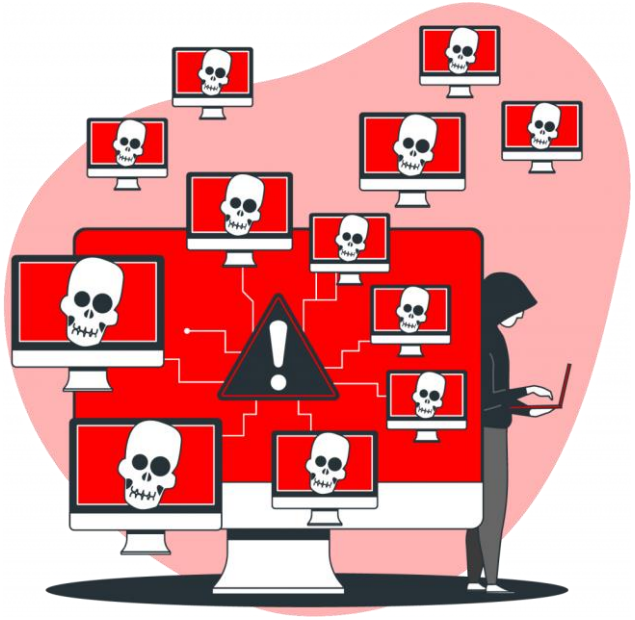
Вы получаете электронное письмо, которое выглядит как письмо от вашего банка, с просьбой подтвердить учётную запись, перейдя по ссылке. Перейдя по ссылке, вы попадаете на поддельный сайт, который фиксирует ваш пароль.

Типы киберугроз

4. Атаки типа "отказ в обслуживании" (DDoS)

   Атака DDoS направлена на перегрузку веб-сайта таким количеством запросов, что он становится недоступен для реальных пользователей.

Представьте, что сотни “людей” пытаются одновременно войти в магазин, блокируя доступ реальным клиентам. Примерно так работает атака DDoS на веб-сайты.



Как уберечь свои данные?

1. Надёжные пароли и менеджеры паролей

Используйте длинные и сложные пароли. Надёжный пароль может выглядеть случайно (например, G5&7b12@X).

Никогда не используйте один и тот же пароль на разных сайтах.

Используйте менеджеры паролей (например, LastPass или Bitwarden), чтобы надёжно хранить и создавать сложные пароли.

2. Многофакторная аутентификация (MFA)

MFA — это дополнительный уровень безопасности, требующий двух или более форм проверки для доступа к учётной записи. Обычно включает:

- ✓ Что-то, что вы знаете (пароль)
- ✓ Что-то, что у вас есть (код, отправленный на телефон)
- ✓ Что-то, что вы есть (отпечаток пальца)

Даже если кто-то узнает ваш пароль, MFA затрудняет ему доступ к вашей учётной записи без второго фактора.

Как уберечь свои данные?

4. Регулярные обновления программного обеспечения

Обновления программного обеспечения устраняют уязвимости в безопасности.

5. Резервное копирование

Регулярное резервное копирование защищает нас от потери важных файлов в случае атак программ-вымогателей или других происшествий. Это похоже на то, как иметь запасной ключ на случай, если основной потеряется.

Взлом информационных систем больших компаний

Взлом данных в компании Equifax

В 2017 году кредитное бюро под названием Equifax было взломано, что привело к компрометации личных данных 147 миллионов человек.

Последствия: Equifax столкнулась с судебными исками и потерей репутации. Этот случай подчеркивает, что кибербезопасность важна не только для IT-специалистов, но и для успешной работы любой организации.

Practice

- Найдите 3 кейса, где выло взломаны данные.
- Расскажите детально про эти инциденты.

Thank you for your attention

Introduction to cybersecurity

Salymbekov University

Miss Aliia Beishenalieva

aliya.beiwenalieva@gmail.com