ФГАОУ ВО «СПбПУ»

Институт биомедицинских систем и биотехнологий

Угрозы информационной безопасности

Подготовили:

Назарова Анна

Можаева Виктория

4731204/50002

Актуальность проблемы

- Мы живем в эпоху цифровой трансформации, где информация стала ключевым активом.
- Рост числа подключенных устройств, объемов данных и онлайн-транзакций создает новые векторы для атак.
- Информационная безопасность (ИБ) перестала быть проблемой только IT-специалистов; она касается каждого — от крупных корпораций до обычных пользователей.
- Ключевой вопрос: Какие угрозы являются наиболее серьезными сегодня и как от них защититься?

Цели и задачи

Цели:

- 1. Классифицировать основные типы современных угроз информационной безопасности.

- 2. Проанализировать механизмы и последствия наиболее распространенных кибератак.

- 3. Сформулировать базовые принципы и методы защиты от рассмотренных угроз.

Задачи:

- Рассмотреть виды вредоносного программного обеспечения.

Классификация угроз информационной безопасности

- Программные угрозы: Вирусы, черви, трояны, ransomware.
- Угрозы, связанные с человеческим фактором: Социальная инженерия, фишинг, инсайдерские угрозы.
- Физические угрозы: Кража оборудования, несанкционированный доступ в помещения.
- Сетевые угрозы: DDoS-атаки, взлом сетей Wi-Fi, перехват данных.

Вредоносное программное обеспечение

- Вирусы и черви: Саморазмножающиеся программы, нарушающие работу систем.

- Трояны: Маскируются под легальное ПО для кражи данных или создания "бэкдоров".

- Программы-вымогатели (Ransomware): Шифруют данные пользователя с требованием выкупа. (Пример: WannaCry).

- Шпионское ПО (Spyware): Тайно собирает информацию о пользователе.

Социальная инженерия

- Манипулирование людьми для получения конфиденциальной информации.

- Фишинг: Массовая рассылка писем от имени легитимных отправителей (банков, сервисов) с целью кражи логинов и паролей.

- Целевой фишинг (Spear Phishing): Точечная атака на конкретного сотрудника или организацию.

- Претекстинг: Создание вымышленного сценария для получения информации.

- Почему это работает? Люди склонны доверять и совершать ошибки под давлением.

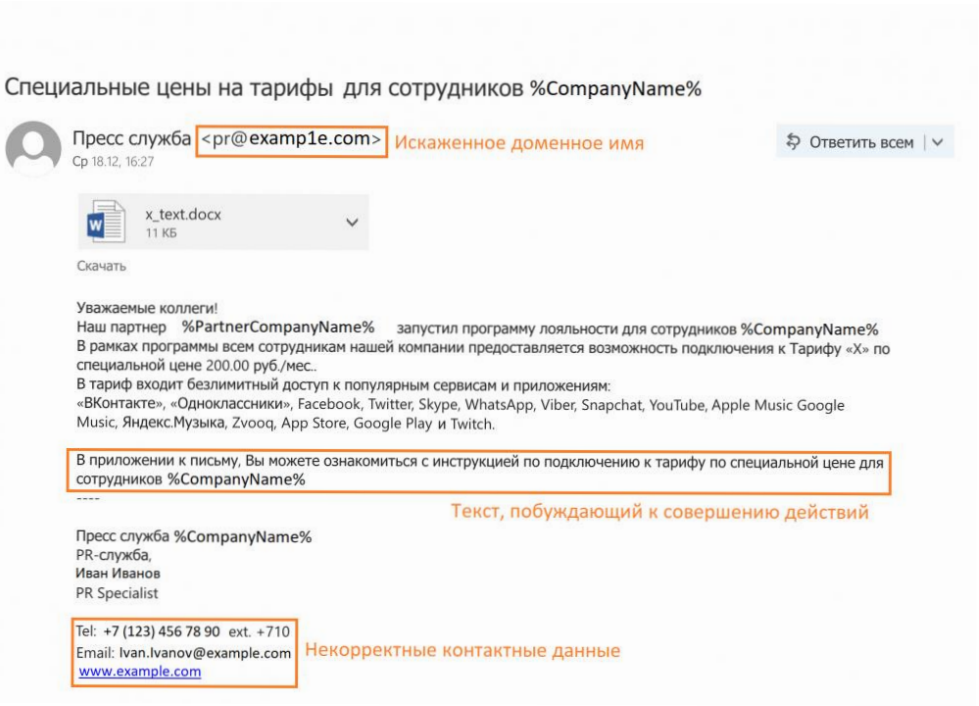

Рис.1. «Фишинг»

Атаки на сетевые ресурсы

- Манипулирование людьми для получения конфиденциальной информации.
- Фишинг: Массовая рассылка писем от имени легитимных отправителей (банков, сервисов) с целью кражи логинов и паролей.
- Целевой фишинг (Spear Phishing): Точечная атака на конкретного сотрудника или организацию.
- Претекстинг: Создание вымышленного сценария для

Угроза изнутри

Исходит от настоящих или бывших сотрудников, подрядчиков.

- Умышленные действия: Кража данных, саботаж из-за недовольства.
- Неумышленные действия: Потеря устройства, случайная отправка данных не тому адресату, попадание на удочку фишеров.
- Почему опасна? У инсайдеров уже есть легитимный доступ к системам и данным.

Базовые принципы защиты

- Технический уровень:
- Антивирусное ПО и брандмауэры: Базовая защита от известных угроз.
- Шифрование данных: Защита информации при передаче и хранении.
- Регулярное обновление ПО: Установка патчей для устранения уязвимостей.
- Системы обнаружения и предотвращения вторжений (IDS/IPS).

Организационный и человеческий фактор

- Организационный уровень:
- Политика безопасности: Четкие правила и процедуры для сотрудников.
- Разграничение прав доступа: Принцип минимальных привилегий.
- Резервное копирование: Регулярное создание бэкапов для восстановления после атак (особенно ransomware).
- Человеческий фактор:
- Обучение и повышение осведомленности: Самый важный элемент борьбы с социальной инженерией.

Выводы

1. Классификация угроз позволяет систематизировать подходы к защите, выделяя программные, человеческие и сетевые векторы атак.

2. Анализ механизмов атак показывает, что современные угрозы стали комплексными, часто сочетая технические уязвимости и методы социальной инженерии.

3. Эффективная защита требует комплексного подхода, включающего не только технические средства (антивирусы, шифрование), но и строгую организационную политику и постоянное обучение пользователей.