

# Тема: Угрозы информационной безопасности

**Санкт-Петербургский  
политехнический  
университет Петра  
Великого**

Выполнили: Назатова М., 4731204/50003  
Ишкова С., 4731204/50003

# Актуальность

## Почему это важно?

- Объём цифровых данных растёт экспоненциально.
- Киберпреступность становится всё более профессиональной.
- Утечки данных ведут к финансовым и репутационным потерям.
- Законодательство ужесточает требования к защите информации.  
Каждый день в мире происходит более 2 000 кибератак.

# Объект, цель и задачи

**Объект:** Угрозы информационной безопасности

**Цель:** Сформировать системное представление об основных угрозах информационной безопасности и методах их нейтрализации.

**Задачи** исследования:

1. Определить ключевые понятия информационной безопасности
2. Классифицировать основные типы угроз
3. Рассмотреть реальные примеры инцидентов
4. Изучить методы защиты от угроз
5. Сформулировать рекомендации по повышению безопасности

# Основные понятия

**Информационная безопасность** — это состояние защищённости информации и инфраструктуры от случайных или преднамеренных воздействий, которые могут нанести ущерб.

**Угроза ИБ** — потенциальная возможность нарушения одного из ее свойств.

## Правила информационной безопасности



Используйте **сложный пароль**, длиной не менее 10 символов, состоящий из букв разного регистра, цифр и специальных символов. Храните его в **тайне** и не сообщайте третьим лицам.



**Блокируйте** компьютер, если покидаете рабочее место.



**Проверяйте** антивирусом внешние носители перед использованием.



Используйте **антивирус** для проверки подозрительных файлов. Не читайте письма от неизвестных источников.



**Не выкладывайте** в интернете внутренние, конфиденциальные и персональные данные.

Рис.1 Правила информационной безопасности

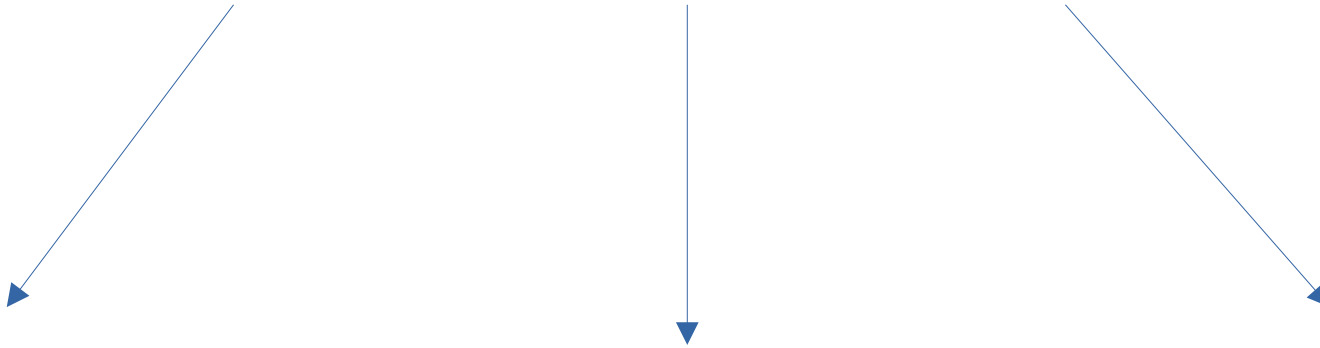
# Ключевые принципы

1. Конфиденциальность — доступ только уполномоченным лицам
2. Целостность — защита от несанкционированного изменения данных
3. Доступность — возможность получения информации по требованию



Рис.2 Триада информационной безопасности

# Классификация угроз



## По источнику:

- Внутренние (ошибки сотрудников, злонамеренные действия).
- Внешние (хакеры, вирусы, стихийные бедствия).

## По способу воздействия:

- Технические (вирусы, DDoS-атаки).
- Социальные (фишинг, претекстинг).
- Физические (кража оборудования).

## По цели:

- Нарушение конфиденциальности.
- Нарушение целостности.
- Нарушение доступности.

# Распространённые угрозы

1. Вирусы и вредоносное ПО — программы, повреждающие данные.
2. Фишинг — мошенничество с целью получения личных данных.
3. DDoS-атаки — перегрузка серверов для остановки работы.
4. Утечки данных — несанкционированное распространение информации.
5. Социальная инженерия — манипуляция людьми для доступа к данным.

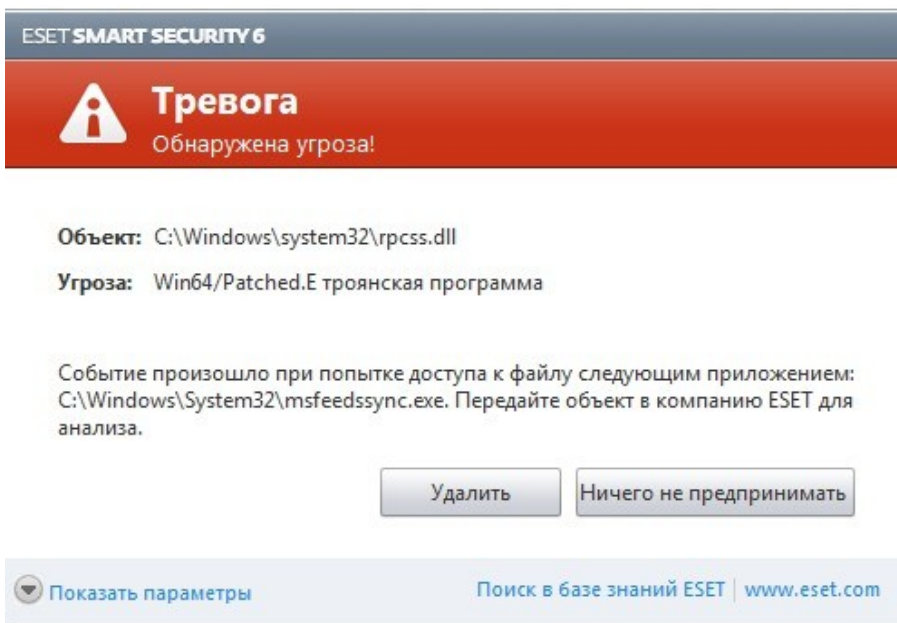


Рис.3 Обнаружение троянской программы

# Реальные примеры инцидентов

- 2023: Утечка данных 1 млрд пользователей соцсети — причина: уязвимость в API.
- 2022: Остановка работы больницы из-за ransomware-атаки — ущерб: \$10 млн.
- 2021: Фишинговая атака на корпорацию — потеря 500 000 записей клиентов.

Вывод: Даже крупные компании не застрахованы от угроз.

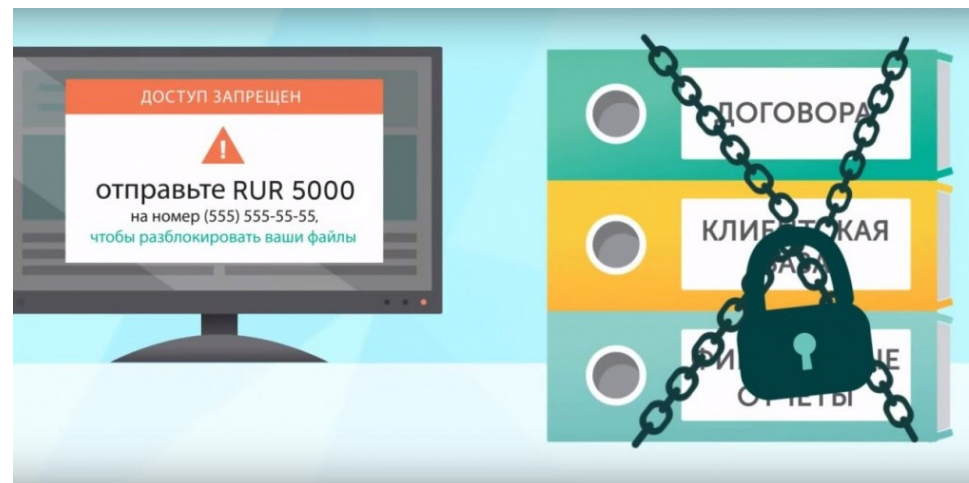


Рис.4 Работа программы-вымогателя

# Методы защиты

## Технические меры:

- Антивирусное ПО.
- Шифрование данных.
- Резервное копирование.
- Межсетевые экраны (firewalls).

## Организационные меры:

- Политики безопасности.
- Обучение сотрудников.
- Контроль доступа.

## Правовые меры:

- Соблюдение GDPR, Ф3-152.
- Договоры о неразглашении (NDA).



Рис.5 Антивирусы

# Рекомендации по усилению безопасности

1. Регулярно обновлять ПО.
2. Использовать многофакторную аутентификацию.
3. Проводить тренинги для сотрудников.
4. Тестировать уязвимости (пентесты).
5. Разработать план реагирования на инциденты.
6. Резервировать данные вне площадки.

# Выводы

1. Информационная безопасность обеспечивается тремя базовыми свойствами: конфиденциальностью, целостностью и доступностью данных. Угроза ИБ — это любая потенциальная возможность нарушения одного из этих свойств.
2. Угрозы делятся на внутренние/внешние, технические/социальные/физические. Каждая категория требует специфичных методов защиты.
3. Даже крупные организации уязвимы перед кибератаками. Наиболее частые причины инцидентов — уязвимости в ПО и человеческий фактор.
4. Эффективная защита требует комбинации технических, организационных и правовых мер.
5. Необходимо внедрять проактивные меры: пентесты, обновление ПО, резервное копирование; критично разработать план реагирования на инциденты.  
Инвестиции в защиту окупаются за счёт предотвращения убытков от утечек и атак.