Федеральное государственное автономное образовательное учреждение высшего образования
“Санкт-Петербургский политехнический университет Петра Великого“

Защита персональных данных

Работу выполнили: Царенко Евдокия
Исправникова Елена
Преподаватель: Горелов С.В.
Биоинженерия и биоинформатика 4750601/50001

Санкт-Петербург 2025

Введение

- Персональные данные — это важная часть нашей жизни. В условиях цифровизации безопасность этой информации становится критически важной. В этой презентации мы рассмотрим основные аспекты защиты персональных данных.

цели

- Понять, что такое персональные данные и почему их необходимо защищать
- Ознакомиться с основными угрозами безопасности персональных данных
- Изучить методы и инструменты защиты личной информации
- Рассмотреть законодательные нормы и ответственность за нарушения
- Дать практические рекомендации для пользователей и организаций

Что такое персональные данные?

- Это любая информация, которая прямо или косвенно относится к конкретному человеку.
- Примеры: ФИО, фотография, адрес, телефон, паспортные данные, e-mail.
- Цель защиты: обеспечить неприкосновенность частной жизни.

Рисунок 1. Пример персональных данных

Почему важно защищать персональные данные?

- Чтобы предотвратить их misuse (неправомерное использование).
- Защита от кражи личности, мошенничества, спама и шантажа.
- Сохранение нашей цифровой репутации и приватности.

Основные угрозы безопасности

- Взломы: несанкционированный доступ к базам данных.
- Вредоносное ПО (вирусы): крадут информацию с устройств.
- Фишинг: мошеннические письма и сайты, выманивающие данные.

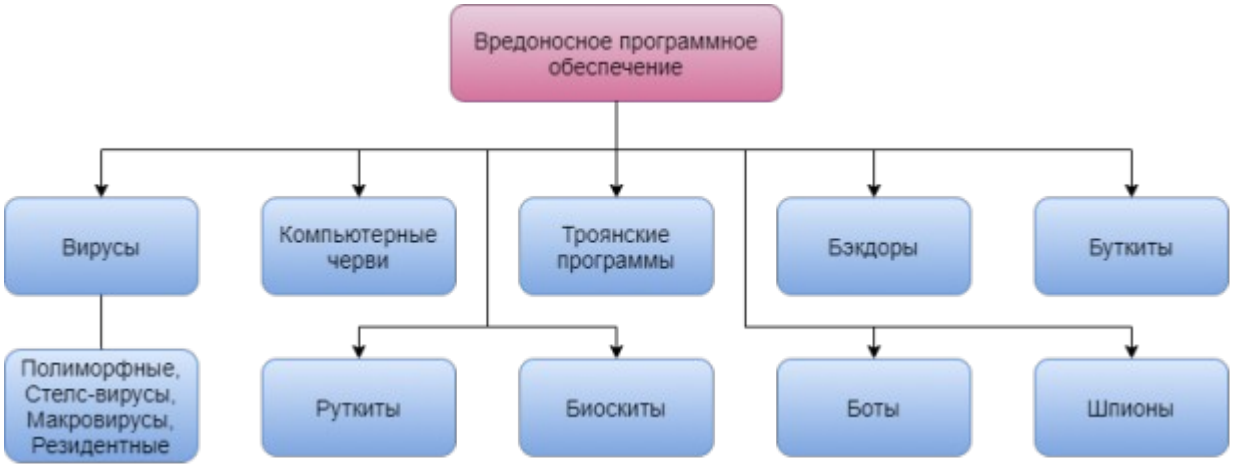

Рисунок 2. Примеры вредоносного ПО.

Стандарты и законодательство

- Деятельность по обработке данных регулируется законами.
- В России: Федеральный закон № 152-ФЗ «О персональных данных».
- В мире: GDPR (General Data Protection Regulation) в Евросоюзе.

Рисунок 3. Принципы GDPR.

Ответственность за нарушение закона

- Нарушители несут ответственность: административную, гражданско-правовую и даже уголовную.
- Последствия: крупные штрафы для компаний, компенсация морального вреда, ограничение свободы.

Технические методы защиты данных

- Шифрование: преобразование данных в нечитаемый код.
- Системы защиты: брандмауэры, антивирусы.
- Регулярное резервное копирование.

Рисунок 4. Пример работы шифрования.

Организационные меры защиты

- Разработка внутренней политики безопасности в компании.
- Обучение и информирование сотрудников.
- Разграничение доступа к информации («знать только необходимое»).

Роль пользователя в защите

каждый человек — главный защитник своих данных.

Что делать?

- Использовать сложные пароли и двухфакторную аутентификацию.
- Не переходить по подозрительным ссылкам.
- Ограничивать объем данных в соцсетях.

Примеры реальных инцидентов

- Крупные утечки данных у известных компаний:

  Yahoo: В 2013-2014 годах произошла крупнейшая в истории утечка данных, затронувшая около 3 миллиардов учетных записей пользователей.
- Последствия: падение репутации, многомиллионные штрафы, судебные иски, потеря доверия клиентов.

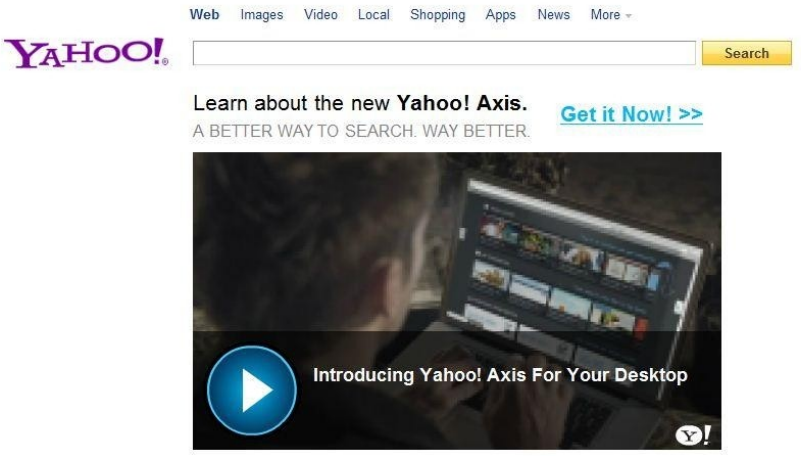

Рисунок 5. Поисковая система yahoo!

Выводы

- защита персональных данных — это не только задача государства и компаний, но и личная ответственность каждого.
- Соблюдение простых правил безопасности позволяет значительно снизить риски и защитить свою цифровую жизнь.