

Вредоносное ПО. Характеристики

Сабина Жигальская

Специалист по комплексной защите информации

Skillbox

Цели урока

- ✓ Узнать, что такое вредоносное ПО
- ✓ Узнать, какой ущерб наносят вредоносы
- ✓ Разобраться в целях вредоносов

Вредоносное ПО

К вредоносным программам относят любое программное обеспечение, несанкционированно проникающее в компьютерную технику.

Вредители создаются для реализации двух основных групп целей:

- получение выгоды
- хулиганство

Знай закон!

Согласно статье 273 Уголовного кодекса РФ вредоносными объектами следует считать компьютерные программы или иную информацию, которые заведомо предназначены для несанкционированного уничтожения, блокирования, модификации, копирования данных либо для нейтрализации средств их защиты.



Объекты воздействия

Цель воздействия зависит от типа злоумышленника:

- хулиган — внедряет инфекцию, которая мешает нормально работать с компьютером
- мелкий вор — приводит к финансовым убыткам
- киберпреступник — приводит к утечке сведений, составляющих коммерческую тайну

Объектами внедрения вредоносных программ являются как организации, так и обычные пользователи сети.

Источник угрозы

Самые опасные и сложные вредоносные программы создаются на заказ государственными спецслужбами или связанными с ними группами киберпреступников. Целью их работы могут быть сбор и кража секретных данных либо прямое вредительство.

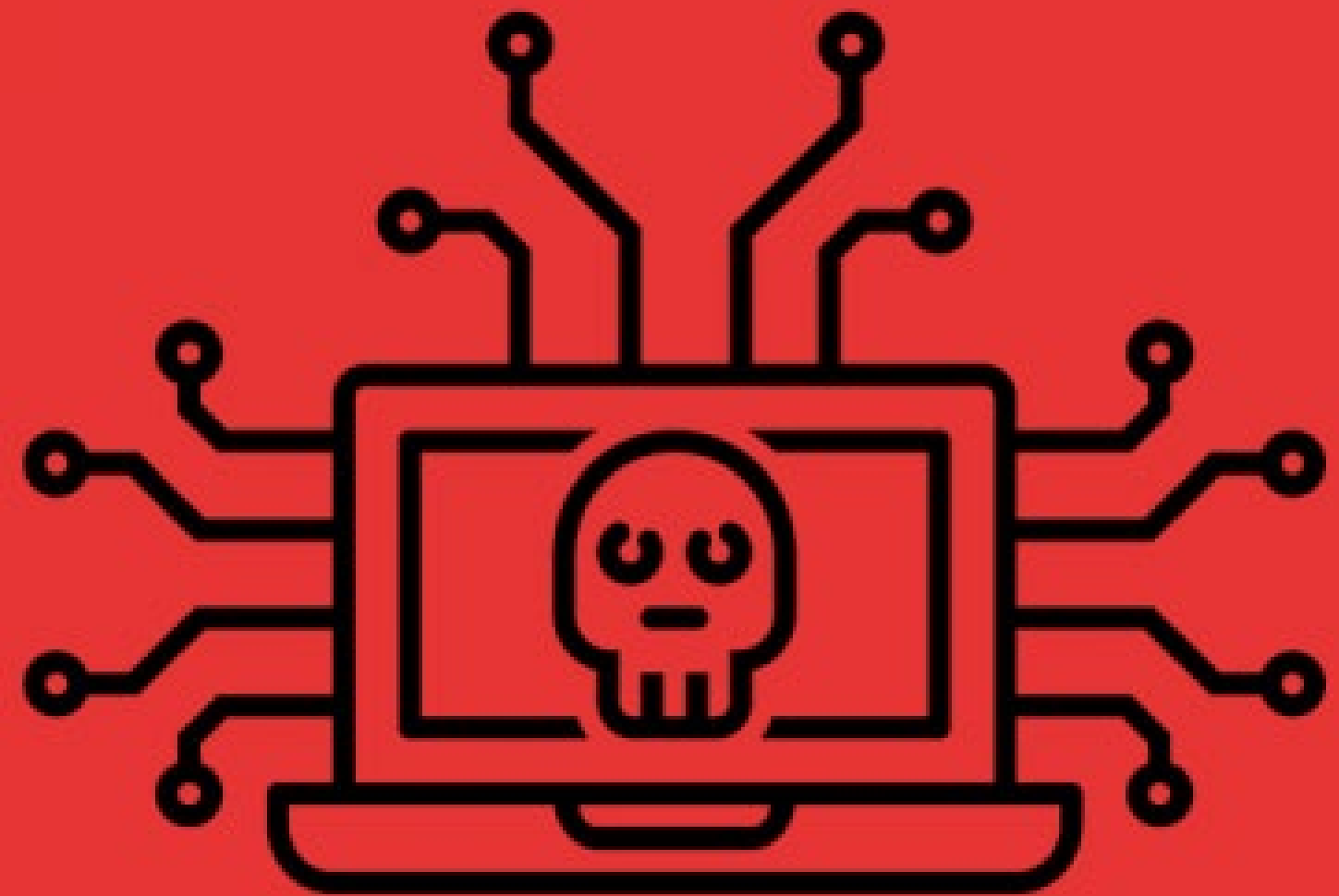
НО! Большинство вредоносных программ создаётся **рядовыми злоумышленниками**, не связанными с организованной киберпреступностью или спецслужбами.

Они могут красть данные для доступа к счетам в банках, выполнять с заражённого устройства сетевые атаки, вымогать выкупы, размещать рекламу сомнительной продукции или рассылать спам.

Анализ риска

Пользователи персональных компьютеров порой не считают вредоносные программы серьёзной угрозой, хотя часто становятся жертвами кражи учётных данных либо блокировки компьютера с требованием выкупа.

Бизнес, наоборот, говорит об инфекциях как о существенной угрозе своей деятельности.



Вывод урока

Нет абсолютной защиты от инфекций, но снизить риск реализации угрозы можно.