



МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ



Академия  
МИНПРОСВЕЩЕНИЯ РОССИИ



Информационные угрозы:

вредоносное ПО



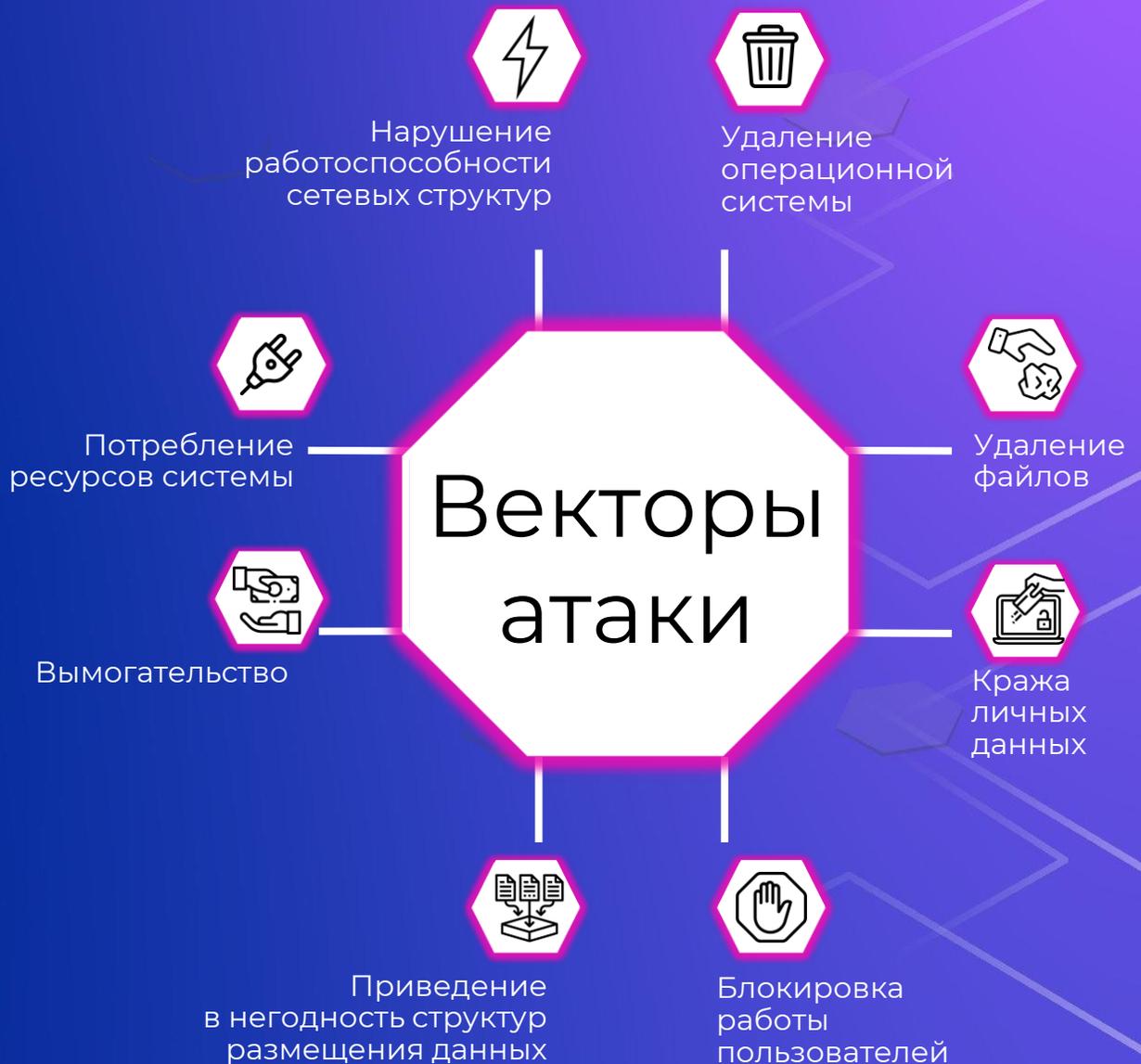
# Компьютерный вирус

Тип вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по различным каналам

Основная цель вируса – **распространение**



Даже если создатель вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям техники из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами



# Виды вредоносного ПО



## Троян

Вредоносный код, спрятанный внутри работоспособной оболочки, обычно — какой-то функционально полезной программы. Способен перехватить управление устройством и даже сетью, может быть переносчиком **компьютерных вирусов**, кейлоггеров и **руткитов**. Используются для сбора, уничтожения или модификации информации



# Виды вредоносного ПО



## Кейлоггер

**Клавиатурный шпион**, который записывает всё набираемое на клавиатуре и отправляет злоумышленникам. С помощью кейлоггеров преступники могут получить **доступ ко всем сервисам** с устройства пользователя, включая финансовые инструменты. К преступнику поступает отчет о нажатии каждой клавиши, а значит, он получает онлайн-доступ к переписке во всех мессенджерах и соцсетях, в том числе и конфиденциальной



# Виды вредоносного ПО



## Пиратское ПО

Это лицензионное программное обеспечение, защита которого была взломана с целью бесплатного распространения (как правило, через торренты). Так как среди хакеров довольно мало альтруистов, каждая «взломанная» или «вылеченная» программа, кроме работоспособной оболочки, может содержать дополнительную нагрузку в виде **трояна, эксплойта или загрузчика**



# Виды вредоносного ПО



## Загрузчик

Это своеобразный вирусный эмиссар, представляющий собой небольшую автономную часть вредоносного кода. Пробравшись за линию защиты, он «перетягивает» к себе «родственников» — остальные компоненты программы, — собирается воедино и устанавливает свою полную версию. Попасть на устройство загрузчик может вместе с письмом, которое пришло по электронной почте или **даже при просмотре зараженной картинки**



# Виды вредоносного ПО



## Червь

Эта вредоносная программа похожа на своего офлайн-тёзку: она перемещается по сетям, **ищет уязвимые места в защите**, если находит, то пролезает внутрь, «откладывает личинку» и ползет дальше. Обладает огромным деструктивным потенциалом



# Виды вредоносного ПО



## Шифровальщик

Самая опасная разновидность вредоносного **руткита**.  
Получив контроль над устройством, программа зашифровывает все размещенные на нём данные, после чего начинает шантажировать пользователя уничтожением информации, требуя перечисления денег на счет вымогателя



# Виды вредоносного ПО



## Эксплойт

Компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для **проведения атаки на вычислительную систему**



# Виды вредоносного ПО



**Спам** (англ. spam)

**Массовая рассылка**  
корреспонденции рекламного  
характера лицам, не выразившим  
желания её получить

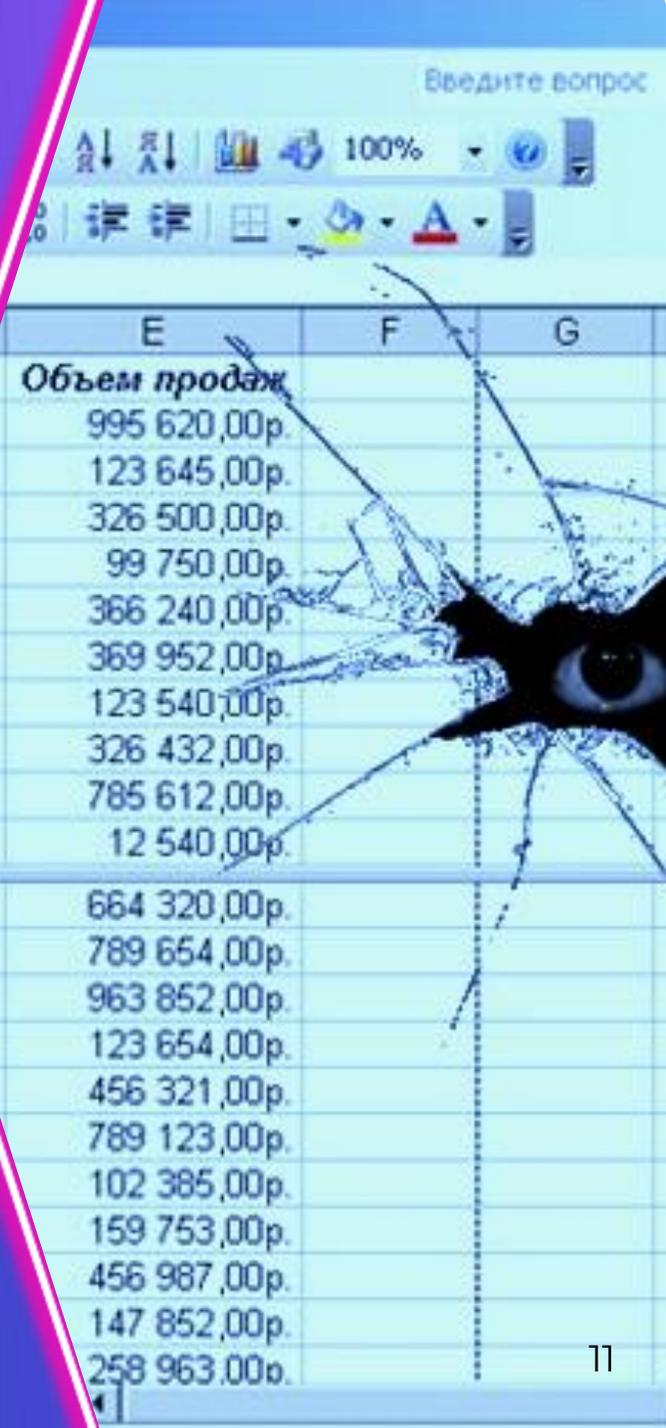


# Виды вредоносного ПО



## Макровирусы

Особенность этого типа вредоносных программ - кроссплатформенность. Макровирусы с равным успехом могут обитать во всех операционных системах, где есть текстовые или табличные редакторы со встроенным языком макрокоманд. Макровирус невидим для стандартных алгоритмов защиты, его главное уязвимое место — **он всегда требует запуска «вручную»**



# Виды вредоносного ПО



## Бэкдор

**Бэкдор** (англ. backdoor) – задняя дверь

Дефект алгоритма, который встраивается в код разработчиком с целью получить аварийный доступ к управлению устройством

**BACKDOOR**

# Виды вредоносного ПО



## РутКИТ (англ. «Rootkit»)

«Чемоданчик суперпользователя», набор программных средств, позволяющих осуществить полный **перехват управления устройством**. Записывает себя в служебные области памяти, поэтому очень плохо и неохотно обнаруживается антивирусными программами



ROOTKIT

# Виды вредоносного ПО



## Ботнет

Масштабная распределенная сеть компьютерных модулей. Пока она расширяется, модули «спят» в гибернации. Затем по ставшей огромной нервной системе проходит сигнал — и сотни тысяч клонов одновременно идут в атаку.

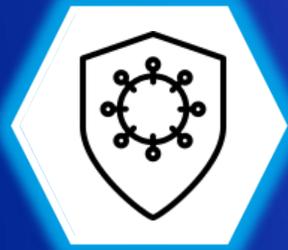
**98% владельцев атакующих устройств даже не догадываются** о том, что их смартфон, компьютер или система освещения умного дома **подключены к ботнету**



# Рекомендации по защите от технологических угроз



Почтовые  
фильтры



Антивирус



Резервные копии  
важных данных



Лицензионные программы  
и данные, полученные  
из надежных источников



Надежные, регулярно  
обновляемые  
пароли



## Почтовые фильтры

Предназначены для фильтрации и удаления спама и зараженных писем во входящей корреспонденции. Как правило, включаются и настраиваются автоматически

**НЕ ОТКЛЮЧАЙТЕ И НЕ ИЗМЕНЯЙТЕ**  
установки почтовых фильтров. **НЕ**  
**ОТКРЫВАЙТЕ И НЕ ИССЛЕДУЙТЕ**  
папку «спам»



Лицензионные программы и данные, полученные из надежных источников

Пиратские копии и нелегальное программное обеспечение — самый простой и быстрый способ получить сразу несколько типов вредоносного программного обеспечения на свои устройства

Самый распространенный – **троян**, который функционирует внутри почти каждой работоспособной оболочки «взломанной» платной программы. Но при меньшем везении вместе с пиратским ПО можно получить и **руткит**, и **шифровальщик**, и **кейлоггер**



# Антивирус

Антивирусные процессоры сегодня – это **сложные интегрированные программные комплексы**, которые включают в себя сразу несколько ступеней защиты устройства – начиная от фильтрации входящего интернет-трафика (сетевые фильтры), заканчивая эвристическими алгоритмами поиска резидентных программ в служебных областях памяти

Антивирус как таковой – это **алгоритм, проверяющий все файлы на устройстве** в поисках элементов кода, который может быть частью вредоносной программы. Оптимальной защитой любого устройства является максимально полный, платный антивирусный пакет с официальной лицензией



Надежные,  
регулярно  
обновляемые  
пароли

Для современного уровня технологического развития существуют определенные стандарты и нормативы, которые делают пароль криптоустойчивым: длина не менее **12 знаков**, использование **прописных и строчных букв** кириллического и латинского алфавитов, а также задействование **цифр и спецсимволов**

Альтернативой являются мнемонические способы запоминания сложных многокомпонентных цифробуквенных комбинаций. **Обновлять пароли необходимо в среднем один раз в полгода**



Резервные  
копии важных  
данных

Атака вируса-шифровальщика может лишить пользователя всей информации, содержащейся на устройстве

ОБЯЗАТЕЛЬНО  
РЕЗЕРВИРУЙТЕ важную  
информацию. Лучше всего  
делать это **методом 3-2-1**