

Безопасная работа на компьютере



Виды угроз

- Вредоносное ПО
- Неправильные действия пользователей
- Действия злоумышленников
- Ошибки программ или техники



Компьютерная гигиена

- Будьте внимательны
- Делайте резервные копии
- Обновляйтесь
- Контролируйте работу ПК
- Защищайтесь



Вирусы (virus)

Вредоносное ПО способное к самостоятельному распространению различными способами.

Может содержать деструктивные функции или просто тратить системные ресурсы



Черви (worm)

Вредоносное ПО
использующие для
распространения сетевые
каналы.

Может предоставлять
доступ злоумышленнику к
зараженному
компьютеру, вести
незаметную деятельность
по атаке на другие
ресурсы или шпионить за
владельцем ПК



Блокировщики (blocker)

Блокируют работу ПК с целью вымогательства денежных средств.

Прописываются в автозагрузку и поражают файлы ОС, требуя перечислить деньги в обмен на получение кода разблокировки

КОМПЬЮТЕР ЗАБЛОКИРОВАН!

Ваш компьютер заблокирован за просмотр, копирование и тиражирование видеоматериалов содержащих элементы педофилии и насилия над детьми. Для снятия блокировки Вам необходимо оплатить штраф в размере 400 рублей на номер телефона МТС 8-911-757-25-04, после снятия блокировки удалить все материалы содержащие элементы насилия и педофилии. В противном случае, через 12 часов все данные будут безвозвратно удалены с Вашего ПК, а дело передано для разбирательства в Управление К МВД РФ, по статье 242 ч.1 УК РФ. Код разблокировки будет напечатан на фискальном чеке терминала в случае оплаты суммы равной штрафу либо превышающей ее.

Разблокировать

Статья 242.1. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних.

Изготовление, хранение или перемещение через Государственную границу Российской Федерации в целях распространения, публичной демонстрации или рекламирования либо распространение, публичная демонстрация или рекламирование материалов или предметов с порнографическими изображениями несовершеннолетних, а равно привлечение несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера лицом, достигшим восемнадцатилетнего возраста, - наказываются лишением свободы на срок от двух до восьми лет с ограничением свободы на срок до одного года либо без такового.

Мусорное ПО

Вредоносное ПО, показывающее рекламу или уведомления, маскируется под обычное ПО и требует от пользователя совершить какие-либо действия, которые и приведут к нарушениям.



Троянские программы

Вредоносное ПО, которое распространяется злоумышленниками с целью незаметного управления компьютером или для шпионажа. Часто служат для загрузки вирусов или червей



Фишинговые сайты

Имитируют дизайн и частично структуру известных сайтов с целью получить доступ к аккаунту пользователя, когда тот введет свои данные.

Часто имеют похожие на настоящие адреса
Например, yamdex.ru
yandex.zloyhaker.ru



Защитное ПО



TrustPort, a.s.
[Подробнее](#)



MYSecurityCenter
[Подробнее](#)



G Data
[Подробнее](#)



Norton by Symantec
[Подробнее](#)



Emsisoft
[Подробнее](#)



Microsoft Security Essentials
[Подробнее](#)



Лаборатория Касперского
[Подробнее](#)



CharityAntivirus
[Подробнее](#)



Panda Security
[Подробнее](#)



eScan
[Подробнее](#)



Ad-Aware
[Подробнее](#)



ESET
[Подробнее](#)



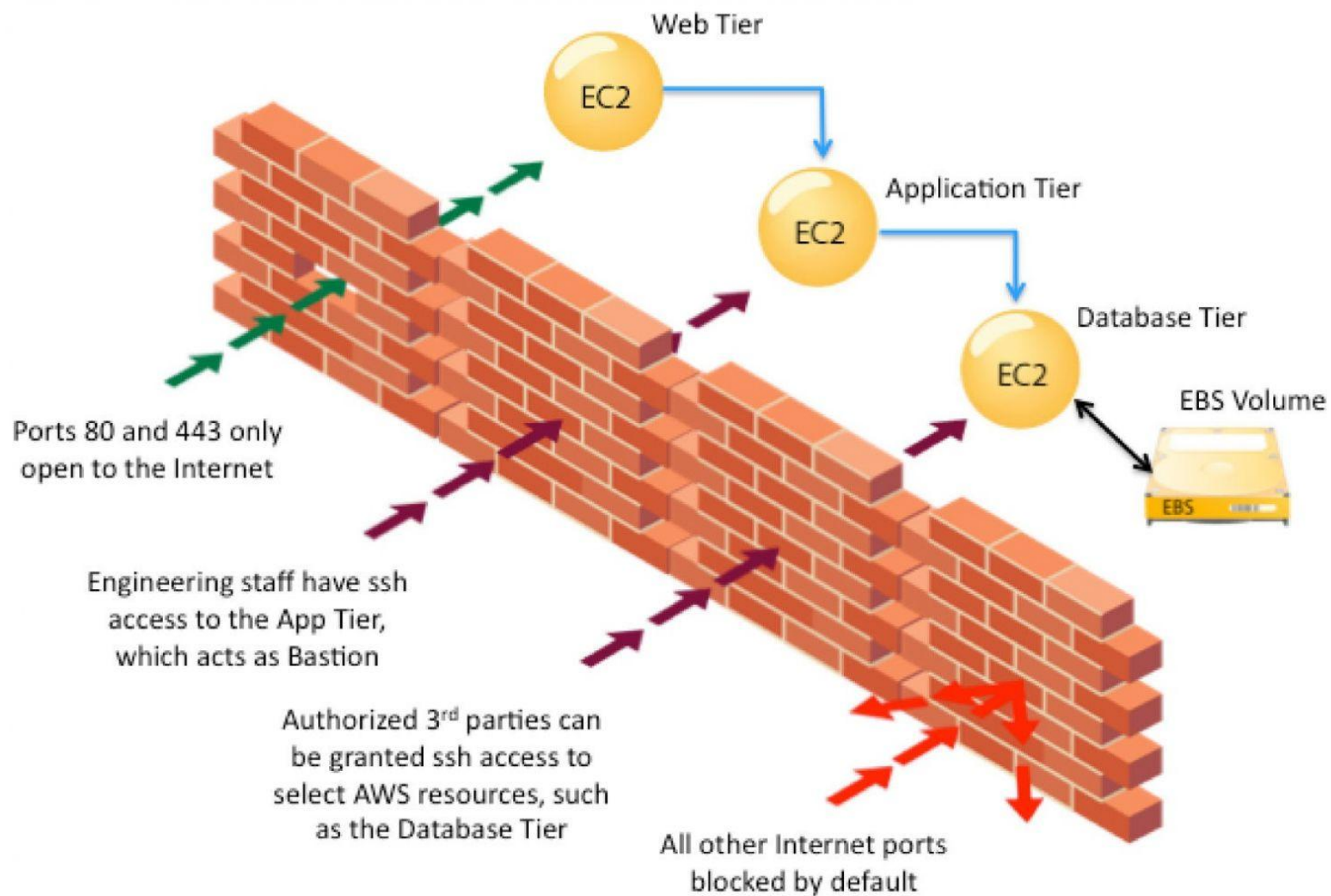
Антивирус

Сравнение кода программы с сигнатурами или эвристический анализ поведения программы с целью поиска вредоносных действий похожих на действия вирусов



Файервол

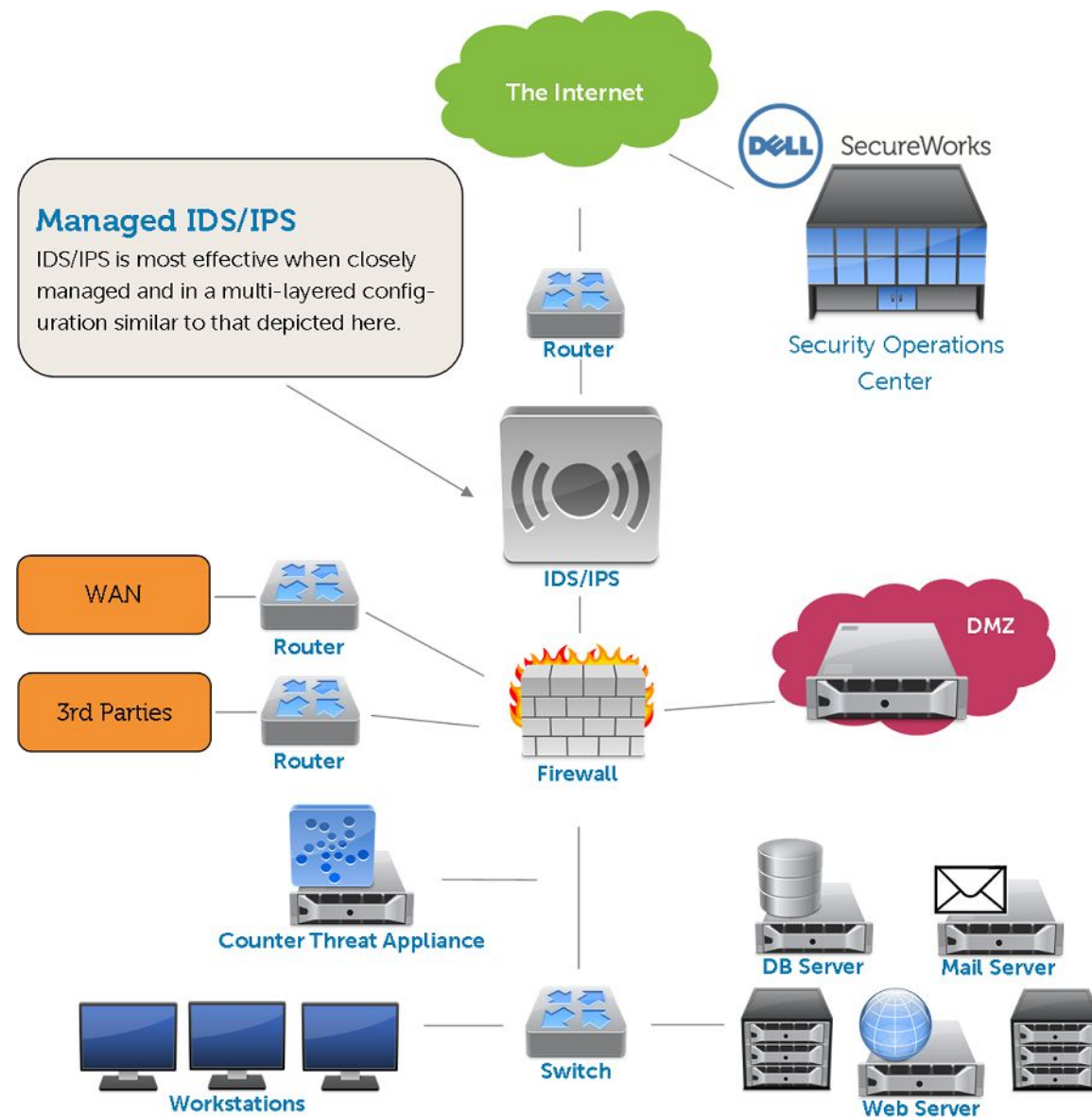
(брандмауэр,
межсетевой экран)
Сканирует сетевой
трафик с целью
поиска
подозрительной
сетевой активности
и позволяет
подавлять эту
активность



Системы обнаружения вторжений

IDS

Автоматический анализ программ и сети с целью выявления несанкционированных действий



Практика

Устанавливаем и
настраиваем
антивирус

