Информационная безопасность

Аппаратно-программные способы защиты

- Информационная безопасность компьютерных систем
- Криптосистемы
- Идентификация и аутентификация
- Электронная цифровая подпись
- Защита от удаленных атак через Internet

Не существует абсолютной защиты. Всякая защита измеряется временем взлома.

Информационная безопасность компьютерных систем

- доступность (возможность за разумное время получить требуемую информационную услугу);
- целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного прочтения).

Основные угрозы информационной безопасности. Несанкционированный доступ

- Через человека:
  - хищение носителей информации;
  - чтение информации с экрана или клавиатуры;
  - чтение информации из распечатки.
- Через программу:
  - перехват паролей;
  - дешифровка зашифрованной информации;
  - копирование информации с носителя.
- Через аппаратуру:
  - подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
  - перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т.д.

Меры обеспечение информационной безопасности

- законодательный
- административный
- физический
- аппаратно-программный

Принципы системы защиты. 1

- Стоимость средств защиты должна быть меньше, чем размеры возможного ущерба.
- Каждый пользователь должен иметь минимальный набор привилегий, необходимый для работы.
- Защита тем более эффективна, чем проще пользователю с ней работать.
- Возможность отключения в экстренных случаях.
- Специалисты, имеющие отношение к системе защиты должны полностью представлять себе принципы ее функционирования и в случае возникновения затруднительных ситуаций адекватно на них реагировать.
- Под защитой должна находиться вся система обработки информации.
- Разработчики системы защиты, не должны быть в числе тех, кого эта система будет контролировать.
- Система защиты должна предоставлять доказательства корректности своей работы.

Принципы системы защиты. 2

- Лица, занимающиеся обеспечением информационной безопасности, должны нести личную ответственность.
- Объекты защиты целесообразно разделять на группы так, чтобы нарушение защиты в одной из групп не влияло на безопасность других.
- Надежная система защиты должна быть полностью протестирована и согласована.
- Защита становится более эффективной и гибкой, если она допускает изменение своих параметров со стороны администратора.
- Система защиты должна разрабатываться, исходя из предположения, что пользователи будут совершать серьезные ошибки и, вообще, имеют наихудшие намерения.
- Наиболее важные и критические решения должны приниматься человеком.
- Существование механизмов защиты должно быть по возможности скрыто от пользователей, работа которых находится под контролем.

Аппаратно-программные средства защиты информации

- **Системы идентификации (распознавания) и аутентификации (проверки подлинности) пользователей.**
- **Системы шифрования дисковых данных.**
- **Системы шифрования данных, передаваемых по сетям.**
- **Системы аутентификации электронных данных.**
- **Средства управления**

Шифрование

- **Способ преобразования данных из одного представления в другое — из «открытого» представления в «закрытое».**

- **Под «открытым» представлением понимаются данные, содержащие информацию в том виде, в котором она, собственно, существует(например обычный текст), под «закрытым» — видоизмененные данные, которые не содержат изначальной информации сами по себе.**

Общий принцип и понятие «ключа»

x – исходное сообщение

f(x)—процесс шифрования сообщения

Пусть задан процесс шфирования вида:

y=x^n

Возведение в степень – это алгоритм шифрования

Показатель степени (n) — «ключ», т.е. параметр алгоритма

Криптосистема с открытым ключом «Асимметричное шифрование»

- Система шифрования и/или электронной цифровой подписи (ЭЦП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭЦП и для шифрования сообщения.
- Для генерации ЭЦП и для расшифровки сообщения используется секретный ключ

Имя пользователя	«Фактический» пароль	«Сохранённый» пароль
USER	PASS1	QWERTY123

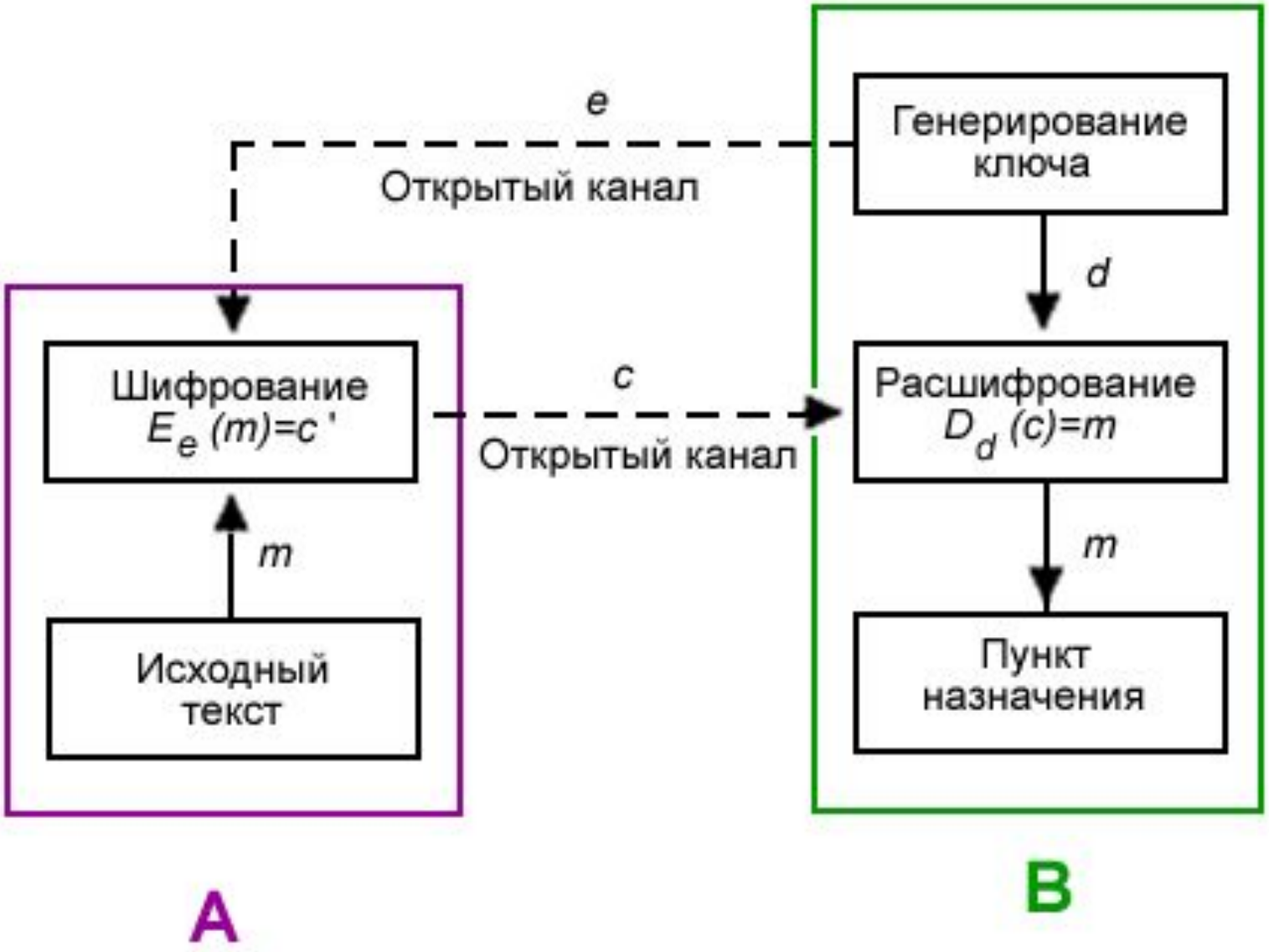
Краткая суть метода

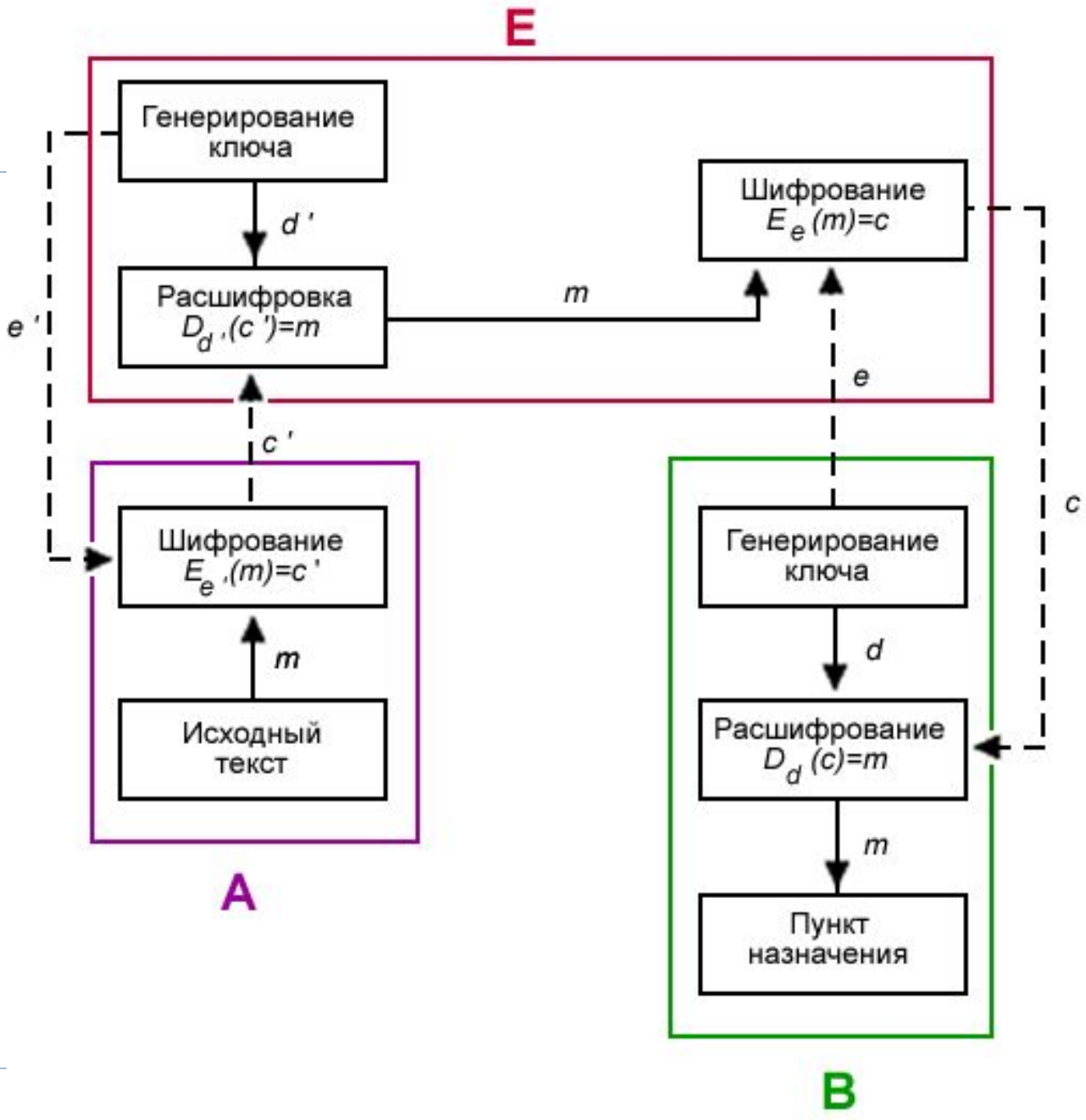
Часы —сообщение

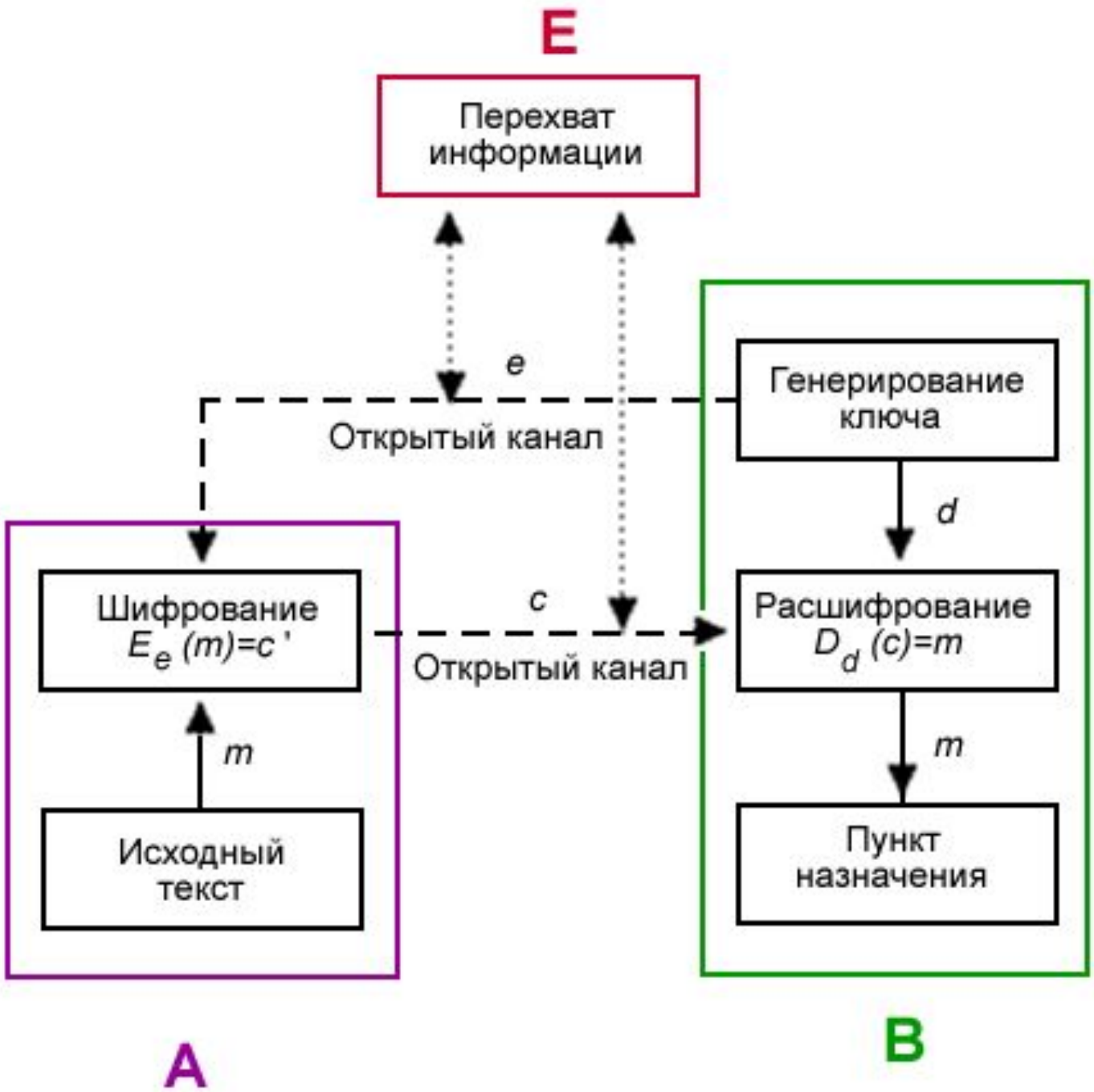
Отвёртка — «открытый» ключ

Инструкция по сборке — «закрытый» ключ

Общая схема работы системы




E
Генерирование ключа
d '
Расшифровка $D_{d'}(c')=m$
m
Шифрование $E_e(m)=c$
e '
e
c '
c
Шифрование $E_{e'}(m)=c'$
m
Исходный текст
A
Генерирование ключа
d
Расшифрование $D_d(c)=m$
m
Пункт назначения
B


E
Перехват информации
e
Открытый канал
Генерирование ключа
d
Шифрование $E_e(m)=c'$
c
Открытый канал
Расшифрование $D_d(c)=m$
m
m
Исходный текст
Пункт назначения
A
B

Аутентификация на основе сертификатов

Аутентификация с применением цифровых сертификатов является альтернативой использованию паролей и представляется естественным решением в условиях, когда число пользователей сети (пусть и потенциальных) измеряется миллионами.

Сертификат представляет собой электронную форму, в которой содержится следующая информация:

1. **открытый ключ владельца данного сертификата;**
2. **сведения о владельце сертификата**
3. **наименование сертифицирующей организации, выдавшей данный сертификат.**
4. **электронная подпись сертифицирующей организации — зашифрованные закрытым ключом этой организации данные, содержащиеся в сертификате.**

Симметричные криптосистемы «Симметричное шифрование»

- **Способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. До изобретения схемы асимметричного шифрования единственным существовавшим способом являлось симметричное шифрование.**
- **Ключ алгоритма должен сохраняться в секрете обеими сторонами.**
- **Алгоритм шифрования выбирается сторонами до начала обмена сообщениями**

Симметричные криптосистемы «Симметричное шифрование»

THIS_IS_A_SAMPLE_MESSAGE

T	_	L	A	_	_	_
H	A	E	G	_	_	_
I	_	_	E	_	_	_
S	S	M	_	_	_	_
_	I	E	_	_	_	_
I	M	S	_	_	_	_
S	P	S	_	_	_	_

Строка 1	T	_	L	A	_
Строка 2	_	_	H	A	E
Строка 3	G	_	_	_	I
Строка 4	_	_	E	_	_
Строка 5	_	S	S	M	_
Строка 6	_	_	_	_	I
Строка 7	E	_	_	_	_
Строка 8	I	M	S	_	_
Строка 9	_	_	S	P	S
Строка 10	_	_	_	_	

Вредоносная программа

- **Любое программное обеспечение, предназначенное для обеспечения получения несанкционированного доступа к информации, хранимой на ЭВМ, с целью причинения вреда (ущерба) владельцу информации и/или владельцу ЭВМ (сети ЭВМ).**

Diff types of…

- **Эксплойт**
- **Логическая бомба**
- **Троянская программа**
- **Компьютерный вирус**
- **Сетевой**

- Вредоносное ПО может образовывать цепочки: например, с помощью эксплойта (1) на компьютере жертвы развёртывается загрузчик (2), устанавливающий из интернета червя (3).

definition

- **разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (саморепликация).**

- **В дополнение к этому вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю и/или компьютеру. По этой причине вирусы относят к вредоносным программам.**

TYPES OF…

- **Вирусы распространяются, копируя свое тело и обеспечивая его последующее исполнение: внедряя себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск и другое.**
- **Вирусом или его носителем может быть не только программы, содержащие машинный код, но и любая информация, содержащая автоматически исполняемые команды — например, пакетные файлы и документы Microsoft Word и Excel, содержащие макросы.**

WAYs OF SPREADING

- **Флеш-накопители (флешки)**
- **Электронная почта**
- **Системы обмена мгновенными сообщениями**
- **Веб-страницы**
- **Интернет и локальные сети (черви)**

General calssification

- **Анти-антивирусный вирус (Anti-antivirus Virus, Retrovirus)**
- **Вариант вируса, штамм, модификация (Variant, modification)**
- **Вирусная программа-червь (Worm-virus)**
- **Вирусный мистификатор (Hoax)**
- **Вирусы-спутники, вирусы-компаньоны (Virus-companion)**
- **"Дроппер" (Dropper)**
- **Зоологический вирус (Zoo virus)**
- **Полиморфные вирусы (Polymorphic viruses)**
- **MtE вирусы (MtE viruses)**
- **Резидентный (в памяти) вирус (Memory resident virus)**
- **Скрипт-вирусы (Script virus**
- **Стелс-вирусы (Stealth virus**
- **Шифрованные вирусы (Encrypted viruses)**

Classification.2

- **Файловые вирусы (File viruses)**
- **Загрузочные (бутовые) вирусы (Boot viruses)**
- **Макрокомандные вирусы (макровирусы) (Macroviruses)**

Weapon of choice

- **Антивирусная программа (антивирус) —** программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще, и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом (например, с помощью вакцинации).

- **Антивирусное программное** обеспечение состоит из подпрограмм, которые пытаются обнаружить, предотвратить размножение и удалить компьютерные вирусы и другое вредоносное программное обеспечение.

classification

- **Продукты для домашних пользователей:**
  - **Собственно антивирусы;**
  - **Комбинированные продукты (например, к классическому антивирусу добавлен антиспам, файрвол, антируткит и т. д.);**
- **Корпоративные продукты:**
  - **Серверные антивирусы;**
  - **Антивирусы на рабочих станциях («endpoint»);**
  - **Антивирусы для почтовых серверов;**
  - **Антивирусы для шлюзов**

How it works

- **Сканирование файлов для поиска известных вирусов, соответствующих определению в антивирусных базах.**
- **Обнаружение подозрительного поведения любой из программ, похожего на поведение заражённой**

Обнаружение, основанное на сигнатурах

- **Удалить инфицированный файл.**
- **Заблокировать доступ к инфицированному файлу.**
- **Отправить файл в карантин**
- **Попытаться «вылечить» файл, удалив тело вируса из файла.**
- **В случае невозможности лечения/удаления, выполнить эту процедуру при следующей перезагрузке операционной системы.**

Обнаружение аномалий

- **Антивирусы, использующие метод обнаружения подозрительного поведения программ не пытаются идентифицировать известные вирусы, вместо этого они прослеживают поведение всех программ.**

Обнаружение, основанное на эмуляции

- **Некоторые программы-антивирусы пытаются имитировать начало выполнения кода каждой новой вызываемой на исполнение программы перед тем как передать ей управление.**

Метод «белого списка»

- **Общая технология по борьбе с вредоносными программами — это «белый список». Вместо того, чтобы искать только известные вредоносные программы, эта технология предотвращает выполнение всех компьютерных кодов за исключением тех, которые были ранее обозначены системным администратором как безопасные.**

Эвристический анализ

- **В целом термином «эвристический анализ» сегодня называют совокупность функций антивируса, нацеленных на обнаружение неизвестных вирусным базам вредоносных программ, но в то же время этот же термин обозначает один из конкретных способов.**

Why it sucks?

- **Ни одна из существующих антивирусных технологий не может обеспечить полной защиты от вирусов.**
- **Антивирусная программа забирает часть вычислительных ресурсов системы, нагружая центральный процессор и жёсткий диск. Особенно это может быть заметно на слабых компьютерах. Замедление в фоновом режиме работы может достигать 380 %.**
- **Антивирусные программы могут видеть угрозу там, где её нет (ложные срабатывания).**
- **Антивирусные программы загружают обновления из Интернета, тем самым расходуя трафик.**
- **Различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы не обнаруживаемыми антивирусным программным обеспечением.**

Main heroes

- ESET NOD32 Suite 4
- Kaspersky Internet Security
- Dr. WEB
- McAfee (now Intel division)

FIREWALL & Traffic filtering

WTF

- **Межсетевой экран или сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами.**

CLASSIFICATION.1

- **Сетевые экраны подразделяются на различные типы в зависимости от следующих характеристик:**
  - **обеспечивает ли экран соединение между одним узлом и сетью или между двумя или более различными сетями;**
  - **происходит ли контроль потока данных на сетевом уровне или более высоких уровнях модели OSI;**
  - **отслеживаются ли состояния активных соединений или нет.**

CLASSIFICATION.2

- **В зависимости от охвата контролируемых потоков данных сетевые экраны делятся на:**
  - **традиционный сетевой (или межсетевой) экран — программа (или неотъемлемая часть операционной системы) на шлюзе (сервере передающем трафик между сетями) или аппаратное решение, контролирующие входящие и исходящие потоки данных между подключенными сетями.**
  - **персональный сетевой экран — программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа только этого компьютера.**

Classification.3

- **В зависимости от уровня, на котором происходит контроль доступа, существует разделение на сетевые экраны, работающие на:**
  - **сетевом уровне**
  - **сеансовом уровне**
  - **уровне приложений**

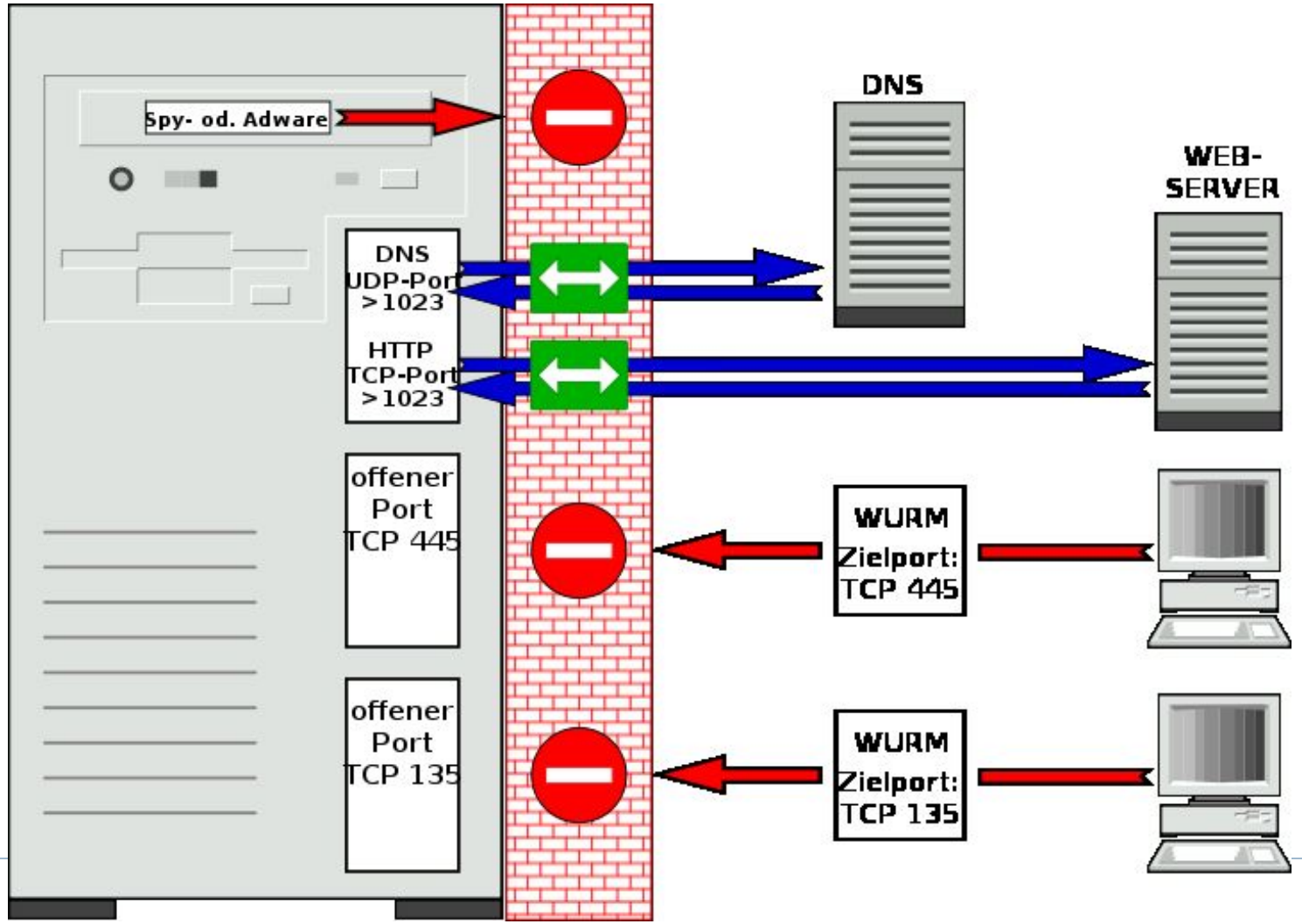
Classification.4

- В зависимости от отслеживания активных соединений сетевые экраны бывают:
  - **stateless (простая фильтрация)**
  - **stateful, stateful packet inspection (SPI)**

Personal firewall

- **Персональный файрвол— приложение, исполняющее роль межсетевого экрана для отдельного компьютера (обычно персонального), запущенное на этом же самом компьютере.**

SHEME OF WORK



Проблемы, не решаемые файрволом

- не защищает узлы сети от проникновения через «люки» (англ. back doors) или уязвимости ПО;
- не обеспечивает защиту от многих внутренних угроз, в первую очередь — утечки данных;
- не защищает от загрузки пользователями вредоносных программ, в том числе вирусов;