Безопасность ОС и сетей

Лекция 13.

Операционные системы. Linux

Безопасность (Security)

- **Проблема безопасности**
- **Аутентификация**
- **Программные угрозы (атаки)**
- **Системные угрозы (атаки)**
- **Защита систем**
- **Обнаружение взлома**
- **Криптография**
- **Windows NT, 2000, XP, 2003, Vista**
- **Инциатива Trustworthy Computing Initiative корпорации Microsoft**

Безопасность (Security)

Безопасность (security) – это защита от внешних атак.

Проблема безопасности

- **Подсистема безопасности должна проверять внешнее окружение системы и защищать ее от:**
  - Несанкционированного доступа.
  - Злонамеренной модификации или разрушения
  - Случайного ввода неверной информации.

- **Легче защитить от случайной, чем от злонамеренной порчи информации.**

Аутентификация

- **Идентификация пользователей наиболее часто реализуется через *пароли*.**

  Пароли должны сохраняться в секрете.
  - Частая смена паролей.
  - Использование “не угадываемых” паролей.
  - Сохранение всех неверных попыток доступа.

- **Пароли также могут быть закриптованы или разрешены для доступа лишь один**

Программные угрозы (атаки)

- **Троянский конь, троян (Trojan Horse)**
  - **Сегмент кода, который неверно использует свое окружение.**
  - **Использует механизмы для того, чтобы программы, написанные одними пользователями, могли исполняться другими пользователями.**
- **Вход в ловушку (Trap Door)**
  - **Указывается идентификатор пользователя или пароль, который позволяет избежать обычных проверок, связанных с безопасностью.**
- **Переполнение стека и буфера (Stack and Buffer Overflow)**
  - **Использует ошибку в программе**

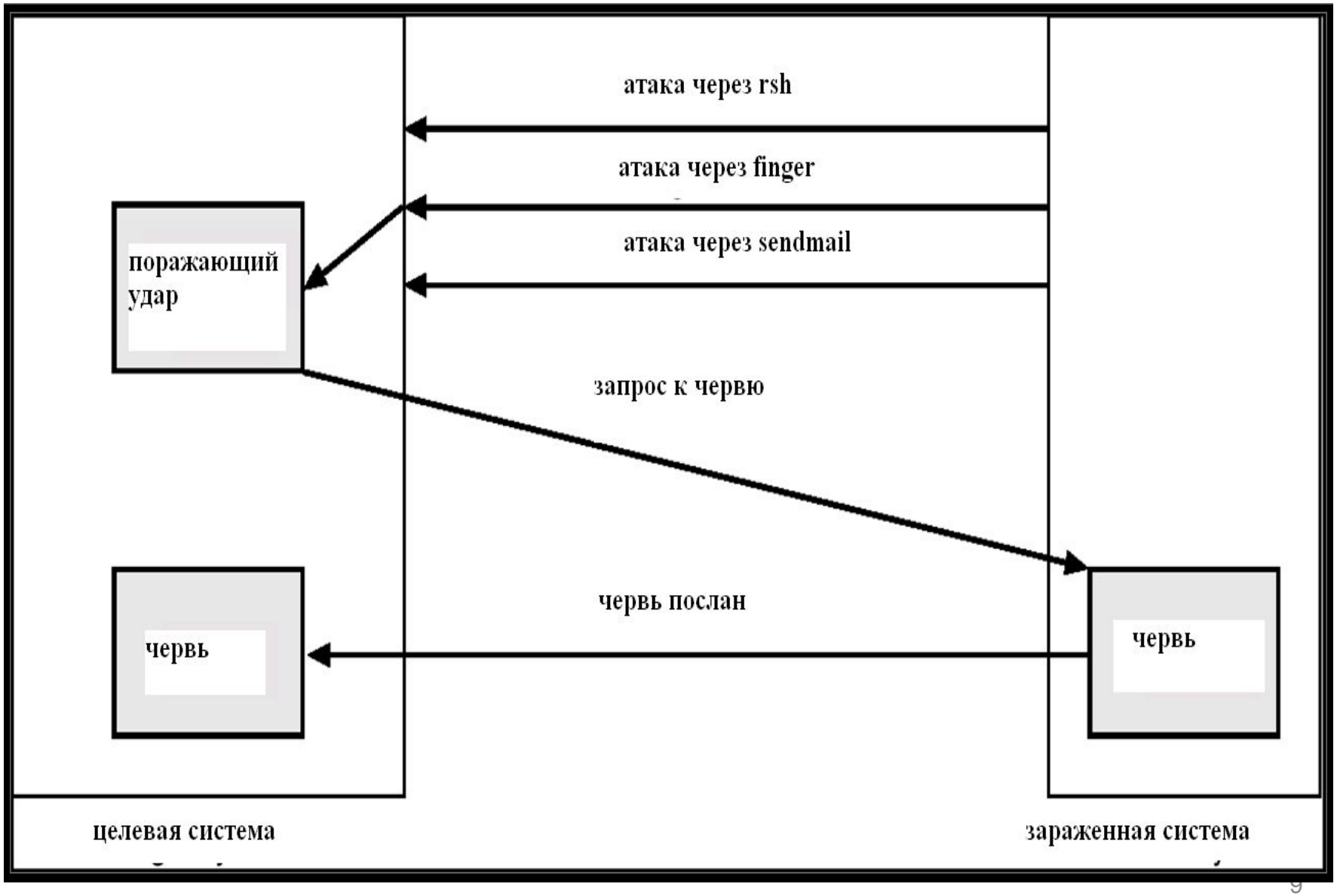
Системные угрозы (атаки)

- **Черви (Worms) – используют механизмы самовоспроизведения (размножения); отдельные программы**
- **Internet - червь**
  - **Использует сетевые возможности UNIX (удаленный доступ) и ошибки в программах finger и *sendmail*.**
  - **Постоянно используемая в сети программа распространяет главную программу червя.**
- **Вирусы – фрагменты кода, встраивающиеся в обычные программы.**
  - **В основном действуют на микрокомпьютерные системы.**
  - **Вирусы скачиваются из публично доступных BBS или с дискет, содержащих “инфекцию”.**
  - ***Соблюдайте принципы безопасности при использовании компьютеров (Safe computing) – антивирусы, guards – программы, постоянно находящиеся в памяти и проверяющие на вирусы каждый открываемый файл - .exe, doc, и т.д.***
- **Отказ в обслуживании (Denial of Service – DoS)**
  - **Создание искусственной перегрузки сервера с целью препятствовать его нормальной работе (например, искусственно сгенерировать миллион запросов “GET” для Web-сервера).**

Типы сетевых атак

- ***Phishing*** – попытка украсть login и пароль пользователя, номер его банковского счета и т. д.
- ***Pharming*** – перенаправление на злонамеренный Web-сайт (обычно с целью phishing)
- ***Tampering with data*** – злонамеренное искажение или порча данных
- ***Spoofing*** – “подделка” под определенного пользователя (злонамеренное применение его login, пароля и полномочий)
- ***Elevation of privilege*** – попытка расширить полномочия (например, до полномочий системного администратора) с целью

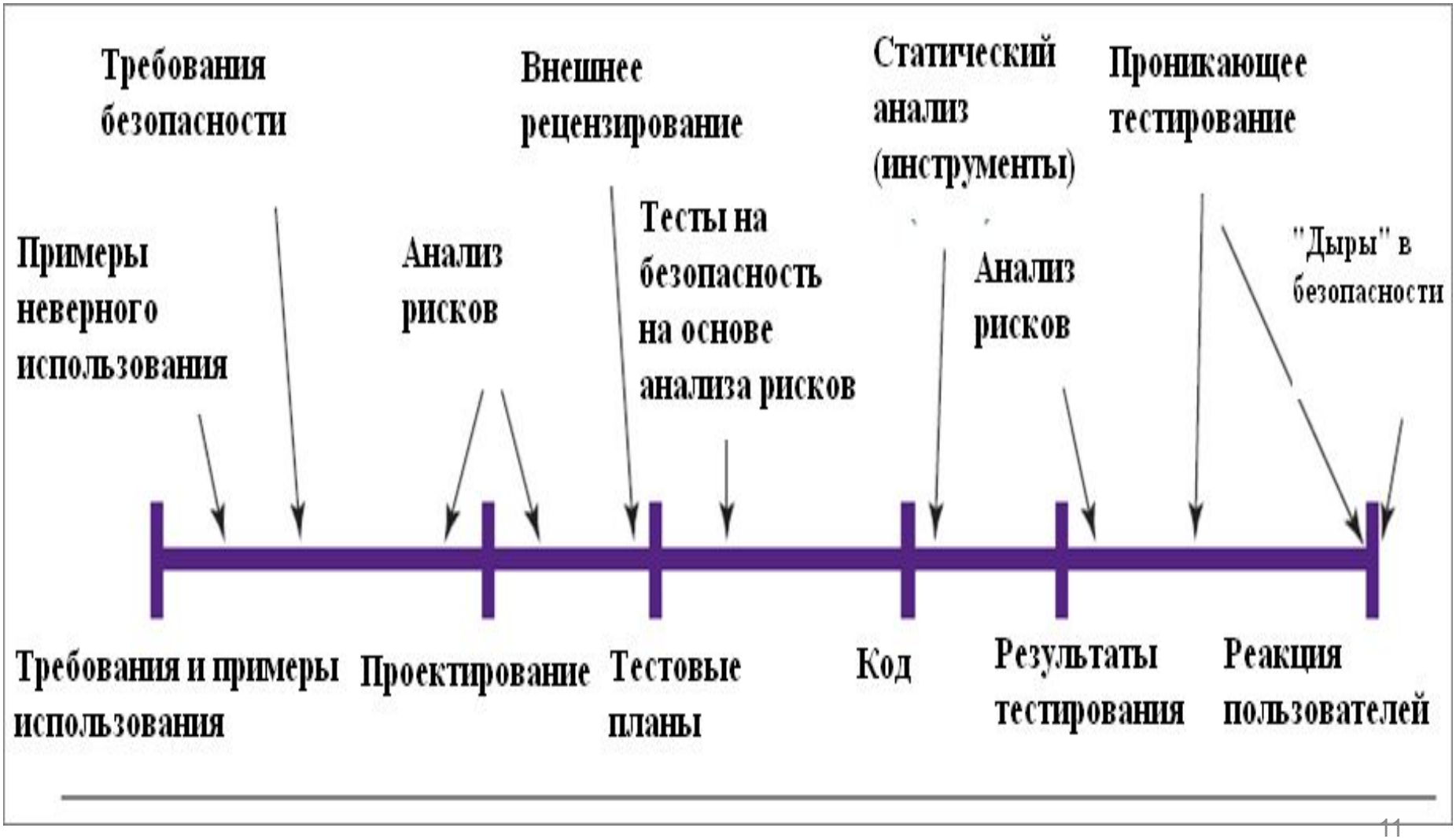
Интернет-червь Morris



Trustworthy Computing Initiative (Microsoft)

- **Объявлена в 2002 г. (email Билла Гейтса)**
- **Основные принципы: *Security, Privacy, Reliability, Business Integrity***
- **Microsoft полностью реорганизовала бизнес-процессы разработки программного обеспечения**
- **Принципы TWC воплощены во всех новых версиях продуктов Microsoft: Internet Explorer 7 и 8, Windows Vista и др.**
- **Обучение TWC в мире только начинается**
- **На мат-мехе: курс В.О. Сафонова “Архитектуры и модели программ и знаний” (4 курс) и элементы TWC во всех других курсах**
- **Кроме аспектов IT, очень важны социальные аспекты и “человеческий фактор” (в частности, корректность бизнеса)**

Жизненный цикл разработки безопасных программных продуктов (Security Development Life Cycle –SDLC): Microsoft



Основные идеи и принципы TWC и SDLC

- В течение всего цикла разработки ПО, начиная с самых ранних этапов (требования, спецификации, проектирование), необходимо постоянно предусматривать меры надежности и безопасности ПО, чтобы впоследствии не пришлось их встраивать в систему в “авральном порядке”, что значительно увеличит затраты
- Необходимо заранее анализировать и *моделировать возможные угрозы и атаки* на ПО и разрабатывать меры их отражения
- Необходимы инструменты количественной оценки рисков, с точки зрения надежности и безопасности
- Необходимы специальные виды тестирования ПО – security testing, fuzzy testing (fuzzing)
- Необходимы эксперты по безопасности ПО (security buddies), участвующие в разработке в течение всего цикла

Принципы безопасной разработки и использования программ: *SD3C* (Microsoft)

- ***Secure in Design*** – применение принципов безопасного проектирования; учет возможных атак; реализация способов их отражения
- ***Secure by Default*** – включение установок безопасности по умолчанию
- ***Secure in Deployment*** – безопасное развертывание и инсталляция программного обеспечения
- ***Communication*** – постоянное взаимодействие группы сопровождения продукта с пользователями, выпуск security patches; рекомендации по настройке безопасности
- ***Secure Development Lifecycle (SDLC)*** – процесс разработки безопасного программного обеспечения

STRIDE – классификация угроз

Spoofing – букв.: *пародирование, розыгрыш*

Например, воспроизведение транзакции, выполняющей аутентификацию пользователя.

Tampering – *Несанкционированное изменение*

Изменение данных с целью атаки. Например, модификация аутентификационных файлов с целью добавления нового пользователя

Repudiation – букв.: *категорическое несогласие, отрицание, отказ*

Пример из повседневной жизни: отрицание того, что Вы купили товары, которые Вы

на самом деле купили.

Драйвер может быть подвержен repudiation-угрозе, если он не выполняет журнали рование (logging) действий, которые могут привести к нарушению безопасности.

Например, драйвер видеоустройства, который не фиксирует запросы на изменение фокуса и уменьшение размеров изображения (который могут привести к его искажению

Information disclosure – Несанкционированный доступ к конфиденциальной информации

Например: Получение списка номеров кредитных карт клиентов банка

Denial of service – *Отказ в обслуживании*

Например: сознательное достижение эффекта излишней загрузки процессора, используя недостатки хеш-алгоритма

Elevation of privilege – *Увеличение привилегий*

Например: Запуск привилегированной программы для выполнения Ваших команд

Оценка атак на программное обеспечение: Схема *DREAD*

- ***Damage*** - Ущерб
- ***Reproducibility*** - Воспроизводимость

  Как часто происходит и может ли быть воспроизведена (смоделирована)
- ***Exploitability*** – здесь: Квалификация (уровень)

  Опыт и квалификация (хакера), необходимые для атаки
- ***Affected users*** – Против каких пользователей направлена
- ***Discoverability*** – Может ли быть обнаружена

Борьба с атаками

- Проверка на подозрительные примеры активности – например, несколько подряд попыток ввести неверный пароль могут означать попытку его угадать.
- Журнал аудита (Audit log) – в него записывается время, пользователь и тип каждой попытки доступа к объекту; используется для восстановления при нарушении защиты и для выработки более действенных мер безопасности.
- Периодическое сканирование системы на предмет “дыр” в системе безопасности; выполняется в моменты, когда компьютер практически не используется (пример: сканирование на вирусы).

Борьба с атаками (прод.)

- **Проверки на:**

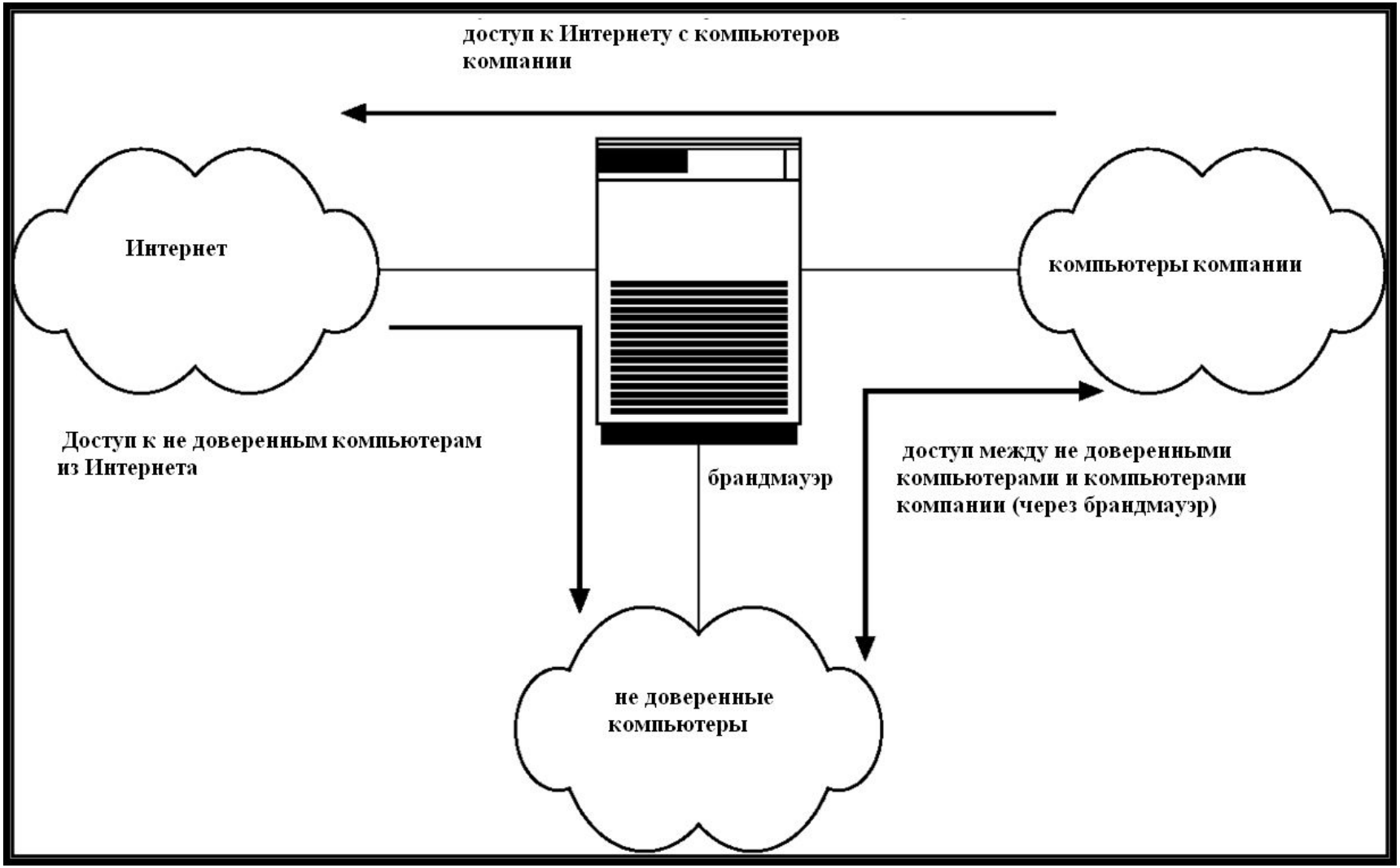
– Короткие или простые для угадывания пароли,
– Несанкционированные программы, устанавливаю-щие другие имена пользователей,
– Несанкционированные программы в системных директориях,
– Неожиданно долгие по времени процессы,
– Неверную защиту директорий,
– Неверную защиту системных файлов данных,
– Опасные элементы в путях для поиска программ (Троянские кони),
– Изменения в системных программах: проверки контрольных сумм.

Брандмауэр (FireWall)

- Брандмауэр помещается между “доверенными” и “не доверенными” компьютерами – например, компьютерами данной локальной сети и всеми остальными.

- Брандмауэр ограничивает сетевой доступ между двумя различными доменами безопасности.

Обеспечение сетевой безопасности с помощью разделения доменов брандмауэром



Обнаружение попыток взлома

- Обнаруживать попытки входа в компьютерные системы.

- Методы обнаружения:
  - Аудит и ведение журнала.
  - Tripwire (программы для UNIX , которые проверяют, не изменялись ли некоторые файлы и директории, например, файлы, содержащие пароли)

- Слежение за системными вызовами

Таблица слежения за последовательностью системных вызовов

системный вызов	расстояние = 1	расстояние = 2	расстояние = 3
open	read getrlimit	mmap	mmap close
read	mmap	mmap	open
mmap	mmap open close	open getrlimit	getrlimit mmap
getrlimit	mmap	close	
close			

Криптография

Криптография - преобразование понятного текста в зашифрованный текст.

- **Свойства хороших методов криптования:**
  - Относительно простой для авторизованных пользователей способ криптования и декриптования данных.
  - Схема криптования должна зависеть не от секретного алгоритма, а от секретного параметра алгоритма, называемого ключом криптования (encryption key).
  - Для несанкционированного пользователя должно быть крайне сложно определить ключ.
- ***Data Encryption Standard (DES)*** основана на подстановке символов и изменении их порядка на основе ключа, предоставляемого авторизованным пользователям через защищенный механизм. Такая схема лишь настолько безопасна, насколько безопасен сам механизм получения ключа.

Криптография (прод.)

- Криптование на основе публичного (открытого) ключа основано на принципе, при котором пользователю известны два ключа:
  - public key – публичный ключ для криптования данных.
  - private key – ключ, известный только пользователю и применяемый для декриптования данных.
- Должно быть основано на схеме криптования, которая может быть публично доступна, но это не будет облегчать разгадывание схемы декриптования.

Пример криптования - SSL

- SSL – Secure Socket Layer
- Семейство криптографических протоколов, предназначенное для обмена криптованными сообщениями через сокет.
- Используется для защищенного взаимодействия между Web-серверами и браузерами (например, ввода номеров кредитных карт)
- Сервер проверяется с помощью сертификата.
- Взаимодействие между компьютерами использует криптографию на основе симметричного ключа

Классификация уровней безопасности компьютеров

- Министерство обороны США классифицирует безопасность компьютеров по уровням: A, B, C, D.
- D – минимальная безопасность.
- C – Обеспечиваются периодические проверки с помощью аудита. Подразделяется на C1 и C2. C1 обозначает взаимодействие пользователей с одинаковым уровнем безопасности. C2 допускает управление доступом на уровне пользователей.
- B – Имеет все свойства C, однако каждый объект может иметь уникальные метки чувствительности (sensitivity labels). Подразделяется на B1, B2, B3.
- A – Используются формальные методы спецификации и проектирования для обеспечения безопасности

Пример: Windows NT

- Конфигурируемое обеспечение безопасности допускает политики уровней от D до C2.
- Безопасность основана на учетных записях пользователей, причем каждый пользователь имеет свой security ID.
- Используется субъектная модель для обеспечения безопасности доступа. Субъект отслеживает полномочия и управляет полномочиями для каждой программы, которую запускает пользователь.
- Каждый объект в Windows NT имеет свой атрибут безопасности, определяемый дескриптором безопасности (security descriptor). Например, файл имеет дескриптор безопасности, который задает полномочия доступа для всех пользователей.

Пример: Microsoft.NET

- Механизмы безопасности наиболее развиты
- Code Access Security
- Evidence-Based Security (evidence – информация о сборке – assembly)
- Role-Based Security
- Атрибуты безопасности
- Декларативное и императивное управление безопасностью