

# **ЗАЩИТА И БЕЗОПАСНОСТЬ**

*Safety and Security*

*Компьютеры ненадежны,  
но люди ещё ненадежнее*

## Защита

- Защита – это управление доступом к ресурсам вычислительной системы и ресурсам пользователя со стороны программ, процессов и пользователей
- Защита через разграничение доступа повышает надежность
- Сбой в работе одной программы или ошибки программиста не должны нарушать работу других программ и приводить к краху всей системы
- Должна быть предусмотрена защита от неправильного использования некомпетентным пользователем или несанкционированного доступа
- Защита = мероприятия
- Безопасность = состояние
  - Безопасность – результат работы системы защиты

## Безопасность

- *Безопасность* - поддержание целостности данных и работоспособности вычислительной системы; предотвращение несанкционированного доступа, преступного/злонамеренного использования системы и изменения данных
- Безопасность = степень/уровень защищенности
- Защита – внутреннее дело вычислительной системы
- Безопасность требует не только системы защиты, но и учета внешней среды, в которой работает компьютер (люди, здания, ценности, угрозы)
- Защита относится к ОС, безопасность к менеджменту

## Необходимость защиты

- защита данных, прикладных программ, системного ПО, всей ИС
- по разным причинам требуется скрыть данные или защитить от других
- новые возможности несанкционированного доступа
  - глобальные сети
- работа нескольких пользователей в одной ИС потенциально опасна
  - один может помешать работе другого
- простейшие ошибки программирования, недочеты, наличие служебных функций могут повлиять на безопасность информационной системы

## Функции системы защиты

- управление средствами защиты и разграничение доступа
- распознавание разрешенного и запрещенного доступа к ресурсам
- ведение журнала (протокола) регистрации и действий пользователей и программ (*accounting*)
  - накопленная статистика нужна для оплаты услуг и для оптимизации работы вычислительной системы
- обнаружение ошибок (процессора, памяти, УВВ, программы, пользователя) и восстановление работоспособности вычислительной системы после сбоев

## Червь Морриса

- Первый червь в 80-е годы парализовал работу интернета
  - вывел из строя UNIX- машины типа Sun и Vax
- Червь не испортил данные, но нарушил нормальную работу
  - Продемонстрировал потенциальную уязвимость вычислительной системы
- Моррис (автор червя) получил 3 года условно, 400 часов общественных работ и штраф 10 тыс. долл. плюс расходы на судебный процесс

## Домашнее задание

- Срыв (переполнение) буфера
- Срыв стека
  - Механизм атаки
  - Источник уязвимости
  - Методика противодействия

## Механизм

- *Защита* - механизмы управления доступом пользователей к ресурсам компьютера (разграничение доступа)
- Необходима защита одного пользователя от другого, одного процесса от другого
- Механизмы ОС реализуют *политику* защиты - общие положения/требования/идеи об ограничении доступа к ресурсам для обеспечения надежной работы
- Политика определяет, *что* нужно делать, механизм - *как*.
- Изменение политики может привести только к изменению системных таблиц при тех же механизмах

## Объекты защиты

- Вычислительная система включает различные объекты
  - оборудование компьютера
    - процессор, секция памяти, принтер, диск, УВВ
  - программы
    - файлы, программы, абстрактные типы данных (флаги, семафоры)
  - данные
    - Результаты работы пользователей, клиентские данные, базы данных
- Каждый объект имеет имя; с объектом выполняют только заранее определенные операции
  - процессор только выполняет программы
  - память доступна на чтение и запись
  - компакт-диск - только чтение
- Функция защиты: гарантировать корректный доступ к объектам и только со стороны процессов, имеющих на это право
  - Процесс может обращаться только к своим внутренним переменным, а не к области памяти, занятой другим процессом

## Выбор системы защиты

- Выбор – компромисс
  - надежность – цена
  - затраты – отдача
- Экономические соображения
  - стоимость и сложность защиты
  - возможный ущерб от взлома
    - прямые потери
    - упущенная выгода
    - потеря доверия клиентов
  - возможности и интересы взломщика

## Принципы

### Принципы организации системы безопасности

1. баланс
  - путей взлома
  - цены охранных мероприятий
2. эшелонирование
  - многослойные системы защиты
3. человеческий фактор
  - сотрудничество системного администратора и отдела безопасности

## Требования к безопасности

- Конфиденциальность
  - Информация и ресурсы – только авторизованным лицам
- Целостность
  - Изменения вносят только авторизованные лица
- Доступность
  - Средства ОС – только авторизованным лицам
- Аутентичность
  - Возможность проверки личности пользователя

## Виды угроз

- Прерывание
  - Нарушение доступности ВС
    - Компоненты ВС недоступны или непригодны
- Перехват
  - Нарушение конфиденциальности
    - Несанкционированный доступ
- Изменение
  - Нарушение целостности
    - Изменение данных, программ, сообщений
- Подделка
  - Нарушение аутентичности
    - Поддельные объекты, сообщения, записи

## Характер угроз

- Пассивные угрозы
  - Чтение сообщений
  - Анализ трафика
- Активные угрозы
  - Имитация
  - Воспроизведение
  - Изменение сообщений
  - Отказ в обслуживании

## Выявление вторжений

- Своевременное обнаружение взломщика снижает возможный ущерб
  - Аудит (журнал, протокол)
  - Поведение взломщика отличается от поведения законного пользователя
    - Статистические отклонения
      - Пороговое обнаружение (частота событий)
      - Профильное обнаружение (закономерности поведения)
    - Выявление на основе правил
      - Выявление отклонений (от предыдущих характеристик)
      - Идентификация проникновения (подозрительное поведение)
- Предотвращение вторжений
- Статистика методов вторжений для совершенствования системы защиты

# Вредоносное ПО

- *malicious software (malware)*
- Использующие программу-носитель
  - Люки
    - Доступ к ВС в обход обычных процедур
  - Логические бомбы
    - Код активизируется по условию
  - Троянские кони
    - «Полезная» программа, содержащая вредоносный код
  - Вирусы
    - Программа, заражающая другие программы
- Независимые
  - Черви
    - Сетевые программы, переходящие из одной ВС в другую
    - Используют транспортные средства для самовоспроизведения
  - Зомби (боты, бот-сети)
    - Программа использует другой компьютер
    - DDOS или рассылка спама

Размножаются

**Возможны комбинации**

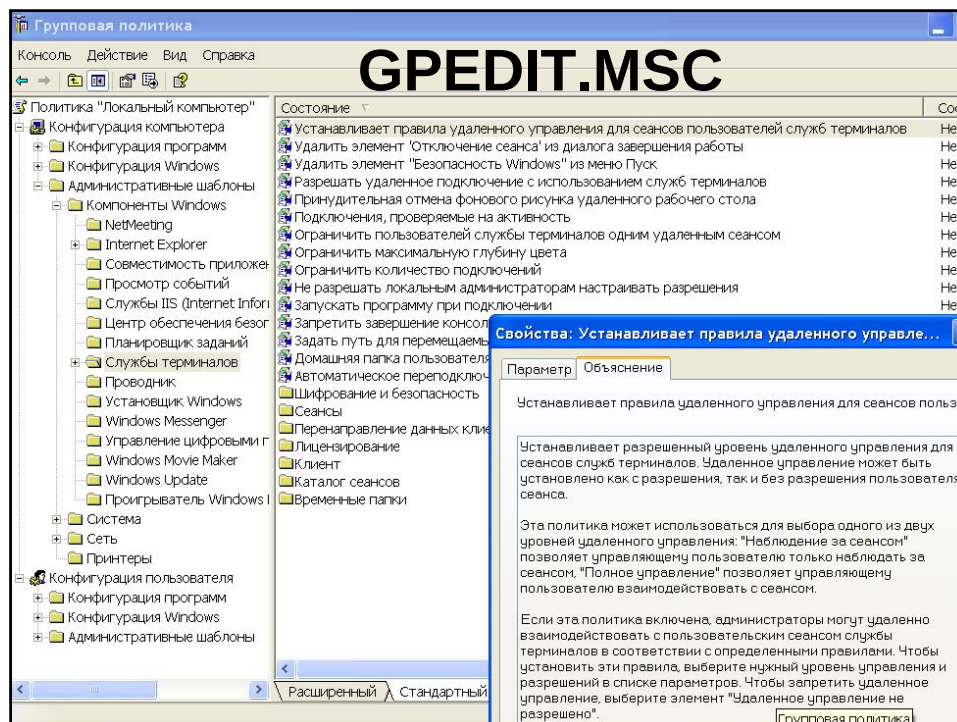
# Спам

- *spam*
- Анонимная/автоматическая массовая несанкционированная рассылка
  - Junk mail
  - Опасность потерять полезный email в почтовом ящике среди тысяч ненужных
  - Потери времени
  - Затраты на трафик
- Реклама
- Политика, агитация
- Мошенничество
  - Нигерийские письма
  - Фишинг (*Phishing*)
- Письма счастья
- Вирусные письма
- Фильтрация спама
  - Kaspersky Anti-Spam
- SPAM: spiced ham (Hormel Foods, 1930-е гг.)



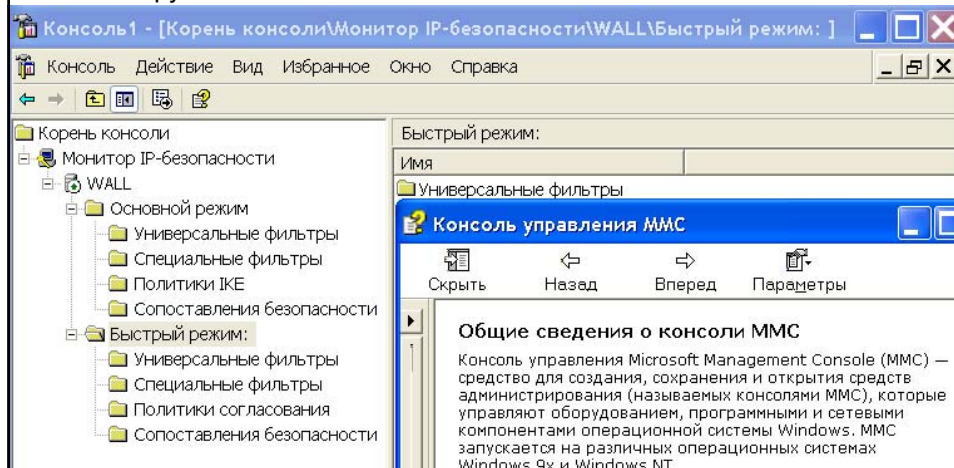
# Механизмы и политика

- Политика решает, ЧТО нужно делать
- Механизм определяет, КАК делать что-либо
- Один из принципов построения ОС –  
разделение механизма и политики
- Это дает максимальную гибкость, если  
потребуется изменение политики



# MS Management Console

- Консоль управления
- Групповая политика – средство администрирования для группы



## Этапы доступа

### *Два этапа управления доступа к данным*

- Аутентификация
    - личность пользователя
  - Авторизация
    - права доступа конкретного пользователя
- 
- *аутентичный* – подлинный, настоящий, достойный доверия
  - **Gr. authentikos** (тот, кто сам производит что-либо)  
*auto + hentes* (сам работник)
  - *авторизация* - согласие, одобрение, санкция, разрешение, предоставление прав
  - **E. author** - автор, создатель; *authority* – власть

## Сессия

- Принцип сессии (сеанс работы)
  - регистрация пользователя при входе в систему
    - login
  - завершение сессии по окончании работы
    - logout
- *Учетная запись* в системной БД
  - user account
    - [Fr. conter <- L. computare]
- *Контекст доступа* для каждой учетной записи
  - security context
  - далее присваивается каждой задаче

## Security context

- ***security*** – безопасность, охрана, защита
  - L. securus se (без) + cura (опека, забота) = свободный от опеки
- ***context*** – часть текста, окружающая слово и определяющая его смысл
  - условия и обстоятельства, относящиеся к событию
    - L. com (вместе) + text (плести, ткать) = переплетаться (ср. текстиль, текстура)
    - L. texere - создавать, сочинять

## Идентификатор

- UID (user identifier)
  - идентификатор пользователя
- UID может присваиваться сессии и отдельным заданиям
- PID (process identifier)
  - Идентификатор процесса
- Запуск отдельных задач без входа в систему и организации сессии
  - Win NT/2000/XP – системные службы

## Linux: PS и TOP

- Список процессов

```
knoppix@ttu00[knoppix]$ ps -F
```

| UID     | PID  | PPID | C | SZ   | RSS  | PSR | STIME | TTY   | TIME     | CMD       |
|---------|------|------|---|------|------|-----|-------|-------|----------|-----------|
| knoppix | 672  | 669  | 0 | 1404 | 2372 | 0   | 22:17 | ttty0 | 00:00:00 | /bin/bash |
| knoppix | 1077 | 672  | 0 | 707  | 832  | 0   | 22:22 | ttty0 | 00:00:00 | ps -F     |

```
top - 22:27:44 up 12 min, 0 users, load average: 0.00, 0.01, 0.00
Tasks: 33 total, 2 running, 31 sleeping, 0 stopped, 0 zombie
Cpu(s):  0.7% user, 24.3% system,  0.0% nice, 75.0% idle
Mem:  126792k total, 120448k used,  6344k free,  5300k buffers
Swap:   0k total,    0k used,    0k free,  62068k cached
```

| PID | USER    | PR | NI | UIRT  | RES  | SHR  | S | %CPU | %MEM | TIME+   | Command  |
|-----|---------|----|----|-------|------|------|---|------|------|---------|----------|
| 430 | knoppix | 15 | 0  | 17600 | 17m  | 14m  | S | 4.3  | 13.9 | 0:03.97 | kdeinit  |
| 245 | root    | 8  | 0  | 2200  | 2200 | 1176 | S | 0.0  | 1.7  | 0:00.16 | bash     |
| 296 | root    | 9  | 0  | 1552  | 1548 | 1420 | S | 0.0  | 1.2  | 0:00.03 | xsession |
| 303 | root    | 9  | 0  | 1548  | 1544 | 1420 | S | 0.0  | 1.2  | 0:00.00 | xsession |
| 305 | root    | 9  | 0  | 25452 | 16m  | 1284 | S | 0.0  | 13.3 | 0:08.40 | XFree86  |
| 313 | knoppix | 9  | 0  | 1556  | 1552 | 1076 | S | 0.0  | 1.2  | 0:00.16 | xinitrc  |

## Windows: PID

| Имя образа          | PID  | Имя пользователя | ЦП | Память    |
|---------------------|------|------------------|----|-----------|
| csrss.exe           | 532  |                  | 00 | 3 828 КБ  |
| explorer.exe        | 1660 |                  | 00 | 18 860 КБ |
| lsass.exe           | 624  |                  | 00 | 1 176 КБ  |
| POWERPNT.EXE        | 520  |                  | 00 | 12 232 КБ |
| ps.exe              | 1780 |                  | 00 | 4 840 КБ  |
| services.exe        | 608  |                  | 00 | 2 928 КБ  |
| smss.exe            | 480  |                  | 00 | 392 КБ    |
| spoolsv.exe         | 1008 |                  | 00 | 4 704 КБ  |
| svchost.exe         | 776  |                  | 00 | 3 220 КБ  |
| svchost.exe         | 844  |                  | 00 | 3 904 КБ  |
| svchost.exe         | 884  |                  | 00 | 15 448 КБ |
| svchost.exe         | 932  |                  | 00 | 2 528 КБ  |
| svchost.exe         | 964  |                  | 00 | 4 088 КБ  |
| svchost.exe         | 1140 |                  | 00 | 3 860 КБ  |
| System              | 4    |                  | 00 | 216 КБ    |
| taskmgr.exe         | 1352 |                  | 00 | 2 172 КБ  |
| TOTALCMD.EXE        | 1956 |                  | 00 | 8 180 КБ  |
| winlogon.exe        | 564  |                  | 00 | 1 296 КБ  |
| WINWORD.EXE         | 1864 |                  | 00 | 30 980 КБ |
| Бездействие системы | 0    | SYSTEM           | 99 | 16 КБ     |

## Аутентификация

## Аутентификация

- Знание
  - пароль с клавиатуры
- Собственность
  - механические ключи
  - магнитные карточки
- Атрибут человека (биометрические методы):
  - рисунок кожи руки/сетчатки глазного дна
  - звучание голоса
- Предположения
  - пользователь помнит пароль
  - пароль трудно подобрать
  - пользователь не разглашает пароль

## Словарная атака

- Компьютерный подбор пароля по стандартным словам
  - Словарная атака
    - Dictionary attack
  - Стандартные слова
  - Имя человека, членов семьи, домашних животных
- Длинные пароли из цифр и букв в верхнем и нижнем регистрах
  - Число вариантов для шестизначного пароля
  - Сложный пароль придется записать
- Мнемоника
  - Пароль по первым буквам слов в предложении
    - легко запомнить
    - тяжело подобрать

## Защита при аутентификации

- Квотирование
  - Ограничение числа попыток
- Комбинированный пароль
  - Комиссия из нескольких человек, каждый со своим паролем
- Визуальное или электронное подсматривание пароля
  - Смотреть на клавиатуру через плечо
  - Просматривать все сетевые пакеты, извлекать имя пользователя и пароль
  - Программная эмуляция запроса и ввода логина
- *аутентификация в сети* - ввод пароля с терминала, сессия "привязана" к терминалу (предполагается, что никто не вклинится в соединение и не пошлет поддельные пакеты)

## Хэширование пароля

- Хэш – одностороннее шифрование
  - Пароли хранятся в виде хэш-кодов
  - По хэшу узнать пароль нельзя
  - Введенный пароль преобразуется в хэш-код
  - Хэш введенного пароля сравнивается с хэш-кодом в системной БД
    - *E. hash* (накрошить, нарезать, перемешать)
    - *Fr. hacher* (изрубить, измельчить)
    - *Fr. hache* (топор)
    - *E. hatchet* (топор)

## Криптография

- *криптографические* методы аутентификации
  - криптография - тайное письмо, засекреченный язык сообщений
    - Gr. *kryptos* (тайный, скрытый)
    - *kryptein* (прятать, скрывать)
    - *gramma* (буква, написание, запись)
    - *graphein* (писать)
- Все пакеты информации передаются по сети в зашифрованном виде
  - адрес отправителя
  - адрес получателя
  - передаваемую информацию
  - контрольную сумму
  - др. служебную информацию

## Алгоритм RSA

- Шифрование с открытым ключом RSA
  - *Rivest – Shamir - Adleman*
- Алгоритм шифрования известен
  - Секретом является код (ключ)
- Сообщение можно прочитать, но нельзя подделать
- Создается два ключа (кодовая последовательность)
  - Целые числа в интервале от 0 до  $n - 1$
  - Шифрование: арифметические операции
- Private key
  - Закрытый ключ для шифрования
    - Пароль шифрования знает только отправитель
- Public key
  - Открытый ключ расшифровки
    - Пароль чтения доступен всем

# Авторизация

## Авторизация

- Авторизация – назначение полномочий
  - разрешение выполнять операцию над защищаемым объектом
- Матрица доступа (*access matrix*)
  - строки – учетные записи
  - столбцы – объекты
  - клетки – разрешенные операции (права доступа)

| ПОЛЬЗОВАТЕЛЬ | объект |         |       |
|--------------|--------|---------|-------|
|              | R1     | ...     | Rk    |
| U1           | read   |         |       |
| ...          |        | execute |       |
| Un           | write  |         | print |

## Матрица доступа

- Матрица определяет
  - какие права доступа к каждому ресурсу получает процесс, запущенный определенным пользователем
- Политика реализуется путем заполнения таблицы
- Механизм обеспечивает работу по правилам, заложенным в таблицу

## Два подхода к авторизации

- Два вида списков:
  - Access Control List, ACL (для пользователя)
    - Список управления доступом
    - в матрице нет пустых строк
  - Capability List (для ресурса)
    - Список полномочий
    - в матрице нет пустых столбцов
      - » *E. access* (доступ, вход)
      - » *L. ad* (направление к чему-л.) + *cedere* (идти) = подойти, войти
      - » *E. capability* (полномочия)
      - » *L. capere* (брать)

## Проблемы списков

- Таблица быстро растет
- Способы сокращения размеров
  - права *по умолчанию* (все остальные пользователи)
  - *группы объектов*
  - *группы пользователей* с одинаковыми правами - для выполнения одинаковых обязанностей (студент/преподаватель/лаборант или бухгалтер/инженер/программист)
  - *иерархия групп* – соответствует иерархии функций в организации

## Полномочия процессов

Два режима работы процессора

- Monitor mode
  - Системный режим, режим монитора
  - Программы, запускаемые ОС, получают полный (привилегированный) доступ
- User mode
  - Пользовательский режим
  - Программы, запускаемые пользователем, выполняются в пользовательском режиме
- Пользователь не имеет доступа в системное адресное пространство ОЗУ

# Администратор

- Три вида *администраторов* в вычислительной системе
  - Системный администратор
    - настройка системы
    - проект «СисАдмин»  
<http://sysadmin.mail.ru/>
  - Администратор учетных записей
    - вводит/удаляет пользователя и пароль
    - определяет квоты
  - Администратор данных
    - резервное копирование/ восстановление
    - целостность данных
- Эти **функции** выполняет (в зависимости от масштабов ВС)
  - Сам пользователь
  - Системный администратор, «системный программист»
  - Группа администраторов

# Виды атак

## Атаки на систему защиты

- Несанкционированный доступ к ресурсам системы
  - Подбор пароля
  - Открытые порты
  - Люки
- Отказ в обслуживании (DoS Denial of Service)
  - Вывод системы из строя без входа
  - Распределенный DoS (DDoS)
- Троянская программа
  - Помещение в систему программы, которую запустит другой человек (с его правами доступа)

## Защита системы

- внесение изменений - только системный администратор
- ограничение использования глобальных сетей
- отключение флоппи-дисководов и портов USB
- периодические проверки защиты
- квотирование ресурсов (против DoS)
- своевременная установка обновлений и заплаток patch
- установка и обновление антивирусов
- мониторинг подозрительных действий пользователя
  - анализ протокола регистрации пользователей (log file)
- регулярная смена паролей
- использование лицензионного и свободного ПО
- мониторинг изменения системных файлов - контрольные суммы

## Безопасность

- Нарушение безопасности
  - Намеренное
  - Случайное
    - Проще защититься от случайного.
- Злонамеренное нарушение:
  - чтение данных (кража информации)
  - изменение данных
  - удаление данных

## Абсолютная защита невозможна

- Цель защиты
  - сделать стоимость взлома достаточно высокой для преступника, чтобы предотвратить большинство или все попытки несанкционированного доступа
- Два уровня защиты:
  - Физический
  - Человеческий
    - Если компьютер выключен, его кабели убирают в сейф

## Уровень безопасности

- Безопасность системы определяется безопасностью самого дальнего соединения
  - Секретная локальная сеть должна находиться только в пределах секретного здания
    - Колонна движется со скоростью самой медленной машины
  - Удаленный доступ через Интернет: фактор риска