Защита информации.

Григорьев Александр Сергеевич

grigoriev@bmstu.ru

Лабораторные:

1. Привязка к ПК
2. Эмуляция энигмы
3. Шифрование с открытым ключом
4. Симметричное шифрование
5. Подписание цифровой подписью

Информация – сведения, сообщения или данные независимо от формы их представления. Накопленный опыт человечества.

Жизненный цикл информации:

1. Создание
2. Оценивание
3. Подготовка к хранению
4. Хранение
5. Выборка
6. Обработка
7. Использование
8. Отчеты
9. Оценка (2)
10. Обновления -> Оценка

Документ – информация, зафиксированная на материальном носителе.

Электронный документ – документированная информация, представленная в электронной форме.

Защита информации. Включает в себя три группы мер.

1. Организационно-правовые. Некие правила, предписания
2. Структурные. Те правила, по которым организованы участники процесса
3. Программно-технические. Средства для осуществления процесса

Эти группы направлены на решение следующих задач

1. Противодействия неправомерным действиям в отношении информации (доступ, уничтожение, чтение, модификация, группировка, распространение и предоставление)
2. Соблюдение конфиденциальности информации (ограниченного доступа)
3. Реализация права на доступ к информации

Серия стандартов банка России по защите информации.

Актив – все, что имеет ценность для субъекта и находится в его распоряжении.

Информационная сфера включает в себя информацию, информационную инфраструктуру, субъектов, процедуры и систему регулирования отношений.

Угроза – опасность, предполагающая возможность потерь (ущерба).

Безопасность – состояние защищенности интересов и/или целей в условиях угроз.

Информационная безопасность – безопасность в условиях угроз в информационной сфере.

ИБ обеспечивает доступность, целостность, конфиденциальность, неотказуемость (невозможность отказаться от авторства), подотчетность, аутентичность (подлинность), достоверность.

Идентификация – присвоение и проверка уникального имени объекта.

Аутентификация – установление и подтверждение подлинности предъявленного пользователем идентификатора.

Авторизация – определение и предоставление прав доступа к каким-то ресурсам.

Ценность информации – мера ущерба, наносимого нарушением безопасности информации.

Информация может оцениваться по важности для бизнеса: жизненно-важная, важная, полезная, несущественная.

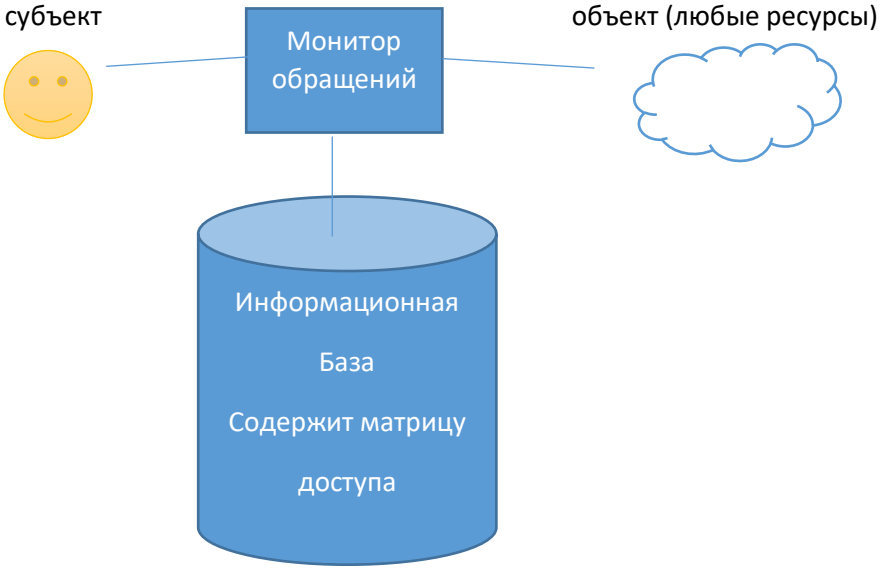
Требования к системам защиты информации.

1. Простоты
2. Полноты
3. Изоляции
4. Ответственности
5. Психологической привлекательности

Принципы защиты информации:

1. Обоснованность доступа
2. Достаточная глубина контроля доступа
3. Разграничение потоков информации
4. Частота повторного использования
5. Персональная ответственность
6. Целостность средств защитной информации

Схема контроля доступа



Пароли. Одноразовые пароли, отпечатки пальцев, арбитраж.

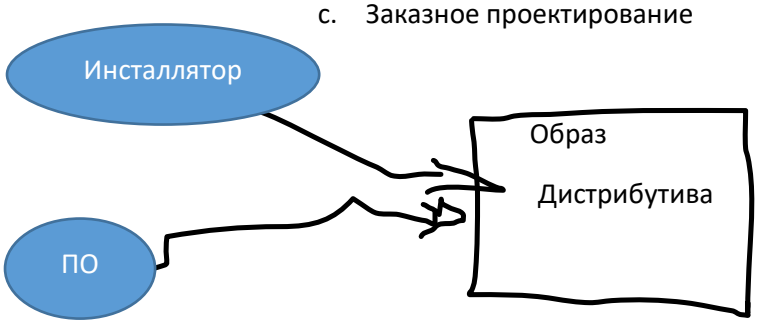
Лекция №2. 26.09.2014

Лабораторная 1. Защита программ от нелегального копирования.

Написать инсталлятор, который установит программу только на 1 компьютер.

Меры защиты

1. По виду воздействия:
    a. Активные
    b. Пассивные
2. По методу реализации
    a. Внутренние
    b. Видимые
    c. Идентификация
    d. Информационные средства (водяные знаки, метки, публикации)
3. Защита отдельных составляющих в составе вычислительных систем
    a. Защита носителей информации (изменение формата записи, специальные метки
    b. Специальная аппаратура
    c. Серийные номера
    d. Ключи
    e. Аппаратная защита от считывания (токены)
    f. Изменение функций (изменение прерываний)
    g. Переименовывание устройств
4. Защита запросом информации
    a. Запрос кодов (паролей, персональных данных)
    b. Шифрование
    c. Проверка сигнатур
5. Собственная защита ПО
    a. Документирование кода
    b. Услуги по сопровождению ПО
    c. Заказное проектирование



Виды параметров, к которым можно привязаться

- Постоянные (аппаратные)
- Переменные

Критерии:

- Неизменность
- Доступность
- Уникальность

Способы:

1. Получение уникальных характеристик устройства ASM
2. WinAPI, группы (GetWindowsDirectory, GetName, GetVolumeInfo, GetCurrentHWProfile)
3. WMI
4. proc -> LS/PROC/; cat /proc/cpuinfo

Моделирование угроз.

Цель: заставить разработчика конструктивно (на основе формального описания) мыслить при проектировании систем с точки зрения безопасности.

Моделирование угроз включает в себя шесть этапов:

1. Определение активов (ресурсы, секретная информация, средства контроля доступа).
    - Обязательно участвует заказчик.
2. Описание архитектуры. Необходимо зафиксировать границы системы, возможности, используемые технологии)
    - Архитектор, безопасник
3. Декомпозиция системы.
    - инфраструктура
    - разработчик
        a) Выделяются области защиты
        b) Политики безопасности (проверки ввода данных)
        c) Предопределить проверяемые важные события (зафиксировать потоки данных, определить точки входа, зафиксировать границы доверия, проверить права, с которыми выполняется код)
4. Определение угроз
    - Природные
    - Техногенные
    - Антропогенные
        i. Умышленные (целенаправленные)
            1. Атаки
            2. Изменение поведения
            3. Социальная инженерия
        ii. Случайные
5. Документирование угроз. Зафиксировать цель, категорию, величину риска (вероятность) и метод борьбы.
6. Оценка серьезности угроз. Определить потенциальный ущерб, воспроизводимость угроз, доступность начала атаки, активы, легкость обнаружения.

Методы защиты от рисков:

1. Защищаться
2. Передать риск
3. Принять риск

Модель нарушителя.

По уровню возможностей:

- Низкий (предопределенные функции
- Средний (новые функции)
- Высокий (управляют функционированием системы и могут воздействовать на базовое ПО и аппаратуру)
- Абсолютный (проектирование, реализация, обслуживание)

Хакеры:

- Любители
- Профессионалы
    - Вербовка служащих
    - Изучение открытой информации
    - Перехват информации (электронная почта)
    - Анализ распечаток
    - Кража докуметов

Классификация автоматизированных систем с точки зрения безопасности

3 Группа (1 пользователь, 1 уровень информации) 3А, 3Б

2 Группа (несколько пользователей, разные уровни информации, один уровень доступа) 2А, 2Б

1 Группа (Многопользовательская, разные права, разные уровни доступа) 1А-1Д

Матрица доступа

Объекты

С
У
Б
Ъ
Е
К
Т
Ы

Мандатная модель. Уровни доступа. Уровень доступа субъекта должен быть не ниже, уровня объекта.
O1 – 1
S1 – 1
S2 – 2

Ролевая модель. Развитие матрицы доступа. Вводятся роли.

Журналирование позволяет

- выявить частоиспользуемые ресурсы для улучшения работы системы
- выявить частоошибающихся пользователей
- восстановление утраченных ресурсов по последовательности действий
- психологическое воздействие

Лекция №3. 03.10.2014

Криптография	Шифрование информации
Криптоанализ	Дешифровка

Стеганография – сокрытие информации.

Шифрование (encryption) – преобразование открытого текста (plain text) в зашифрованный (ciphertext).

Inciphering, deciphering.

Рассеивание – влияние одного знака открытого текста на множество знаков зашифрованных текстов.

Огюст Керхоф.

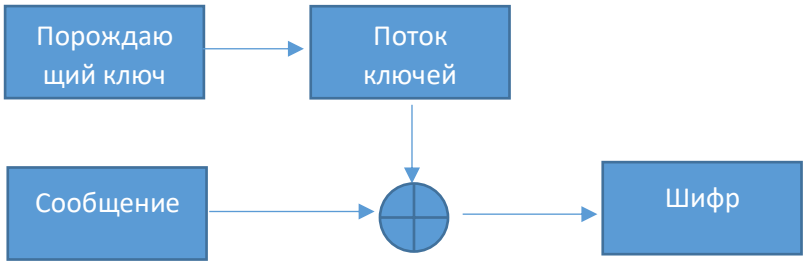
Первое правило Керхофа: стойкость алгоритма определяется только секретностью ключа.

Симметричные алгоритмы. Используется один ключ для шифрования и расшифровки.

Асимметричные алгоритмы – алгоритмы с открытым ключом. Открытый ключ/секретный ключ.

Блочные – ориентированы на конкретные блоки определенного размера, составляющие несколько байт.

Поточные – нацелены на шифрование непрерывного потока.

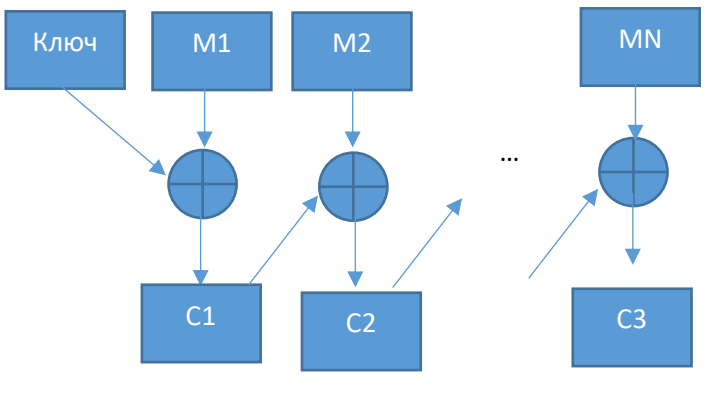


Современные алгоритмы шифрования включают в себя две основные операции:

1. Перестановки (Permutation)
2. Подстановки (Substitution)
    1. Моноалфавитные подстановки – один алфавит
    2. Полиалфавиттные подстановки – много алфавитов
3. Составные (P+S)

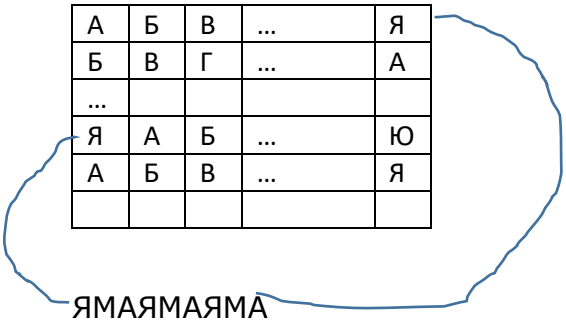
Примеры алгоритмов:

1. Отрывные блокноты
2. Сцепление блоков шифра.



Шифр Виженера.

А	Б	В	…	Я
Б	В	Г	…	А
…				
Я	А	Б	…	Ю
А	Б	В	…	Я



ЯМАЯМАЯМА
СООБЩЕНИЕ

Скитала.

На веревке писали буквы, потом ее разматывали.

Использование правила. Правило 321: ООСЕЩБЕИН. Перестановка букв.

Квадрат Полибия. Буквы записываются в квадрат, и каждая буква заменяется на стоящую над ней. Размер квадрата является ключом.

Многоалфавитные подстановки. Маскируют естественную частоту символов в языке.

Энигма.

После каждого символа первое колесо сдвигается на 1 элемент. После возвращения колеса в исходное состояние, поворачивается второе колесо.

Расшифровка: колеса возвращаются в исходное состояние и зашифрованное сообщение прогоняется еще раз.

Основные требования к алгоритмам шифрования.

1. Сложность расшифровки и модификации.

2. Малое изменение исходного текста или ключа влечет значительное изменение шифра текста.

3. Область значений ключа должна исключать его перебор.

4. Стоимость дешифрации сообщения превышает стоимость информации.

Лекция №4.

Случайные числа.

- Физические процессы
- Действия пользователя

Псевдослучайные числа. На основе математического закона. Алгоритмы:

- Алгоритм Фон-Неймана
- На числах Фибоначчи

- Линейный конгруэнтный генератор
  Xn+1 = (a * Xn + c) mod m
  a, c, m
  a = 106 или 84589, c = 1283 или 45989, m = 6075 или 217728

Новая лаба: на выбор DES или AES

Симметричные алгоритмы.

1. Алгоритм DES (Data Encryption Standard)
   К – 64 (56) бит – длина ключа, блоки шифрования – 64 бита.
   1. Расширение ключа.
      К(64) -> Нач. перестановка В (для того, чтобы убрать каждый восьмой бит)
      -> две половинки: C0(28) и D0(28) -> пропускаются через сдвиг S-1,2,9,16 = 1, для остальных = 2 -> объединяются – в р-те i-тый ключ -> переход к сдвигу половинок для получения следующего ключа -> 16 ключей
   2. Функция Фейстеля.
      Вход – R(32 разряда) -> расширяется до 48 бит перестановкой Е (расширяющая перестановка дублирует некоторые биты) -> xor с ключом Ki -> 48 бит делятся на 8 блоков по 6 бит, 4 бита для столбца в таблице, крайние – строки, таблица 4*16, в ней хранятся 4-битные элементы -> при объединении блоков получается 32 бита.
   3. Алгоритмы шифрования и расшифровки.
      Данные (64 бита) -> Начальная перестановка P(64) –> Блок делится на две части по 32 бита L0 и R0 ->16 раундов (столько же, сколько ключей), преобразуются левые и правые части, L1 = R0, R0 идет в функцию шифрования Фейстеля xor L0, т.е. R1 = Ф(R0, Ki+1) xor L0 (первый шаг, потом повторяется с новыми ключами и полученными блоками), на последнем шаге не выполняется перемещение L16 = L15, R16 = R15 + F(L15, K15) -> половинки объединяются -> конечная перестановка P-1(64b)
      При расшифровке ключи используются в обратном порядке.

2. AES (вырос из Rijndale) Data – 128b, Key – 128b, 192b, 256b

Лекция №5. 17.10.2014

Алгоритм AES.

Алгоритм RSA.

Лекция №6. 24.10.2014.

Теорема Рабина для получения простых чисел.

Цифровая подпись. Для подписи используется закрытый ключ, для проверки подписи – открытый ключ.

Хэш-функция:

- Применимость к блоку любой длины
- Длина результата фиксированная
- Лёгкость вычисления данных для любой длины

- Невозможность вычисления исходных данных по хэшу
- Невозможность найти два различных блока с одинаковым хэшем.

Хэш-функция – средство аутентификации данных.

Два семейства: MD (Message Digest, MD4, MD5), SHA (Secure Hash Algorithm, SHA0, SHA1, SHA2).

MD5 использует блоки 128 бит для входа и выхода.

SHA0 –вход – 512 бит, выход – 160 бит.

SHA1 – 512, 160.

SHA2 – SHA224, SHA256, SHA384, SHA512 – размеры выходных данных

Электронная подпись

- Добровольное согласие
- Аутентичность
- Непереносимость
- Целостность
- Неотказуемость

M – H(M) – RSA(H(M)) – M + C

Электронный сертификат (Сертификат открытого ключа) (владелец, полномочия)

Центр сертификации (Certification Authority, CA), УЦ

Протокол X509 задает форму хранения электронных сертификатов.

Процедура получения сертификата.

1. Certificate Signing Request (CSR)
2. Генерация сертификата
3. Certificate Revocation List
4. Проверка срока действия, принадлежности CRL

31.10.2014

Алгоритмы архивации. LZW, Haffman

14.11.2014

Квантовая криптография.

Секретная информация: преобразование; сокрытие.

Сокрытие: стеганография, разрушение информации при несанкционированном доступе.

Для передачи одного бита информации должна использоваться одна (в худшем случае две) частицы. Фотон можно поляризовать в ортогональном и диагональном базисе. Если не знать нужного базиса, то произойдет ошибка. На этом основан первый алгоритм квантового шифрования – BB84.

Кодирование бита:

0	↑	↗
1	→	↘

Квантовый канал. Используется только для передачи секретных данных.

Открытый канал. Все остальные коммуникации.

Отправитель:

1	x	x	x	x	+	+	+	+
2	0	1	0	1	0	1	0	1

Шифр.	↗	↘	↗	↘	↑	→	↑	→

Получатель:

1	x	+	x	+	x	+	x	+
2	↗		↗			→		→

Договориться о том, какие поляризаторы использовались для обмена. Понять, какие из битов были расшифрованы правильно. Обмен данными о поляризаторах происходит в открытом канале.

Если данные были перехвачены, информация с вероятностью 50% может быть искажена. Чтобы проверить сохранность данных, можно подсчитать контрольную сумму.

Этапы сжатия:

1. Построение модели.
2. Кодирование.

Простейший алгоритм.
___Здравствуйте
Решение – три пробела заменяются на количество повторов/блок данных

Хаффмен (62 г.)
1. Таблица частот символов алфавита.

Криптология: Криптография и криптоанализ

Стеганография.

Криптоаналитик – лицо или группа лиц, целью которых является прочтение или подделка защищенных криптографическими методами сообщениями.

Возможности нарушителя:

1. Знает алгоритм шифрования.
2. Имеет доступ к зашифрованным текстам.
3. Есть доступ к открытым тестам (всем или некоторым).
4. Есть достаточные вычислительные возможности и прочие ресурсы: человеческие, временные, но не превышающие стоимость информации.

Уровень возможностей:

1. Доступ только к зашифрованной информации
2. Известны открытые тексты.
3. Подобранный открытый текст.
4. Выбор открытого текста.

Частотный анализ.

1. Количество повторов Na, Nb, Nz.
2. Вероятность появления символа в тексте Pa, Pb, …
3. Полученные значения сравниваются с таблицей вероятности языка.
4. Полные совпадения (замена шифр на текст из табл.)
5. Перестановка букв с близкой частотой.
6. Заполнение символов.

КА шифра Виженера.

1. Пары одинаковых строк L>=3;
2. Вычисляется R между этими строчками
3. L1,l2,l3
4. Обычный частотный анализ

«Бандитский» анализ. (Нацелен на человеческий фактор)

1. Обман
2. Угрозы
3. Насилие
4. Шантаж
5. Подкуп

Методы защиты

1. Защита с открытым ключом
2. Двусмысленное шифрование

Атаки: пассивные и активные; агрессивные, умеренно-агрессивные и неагрессивные.

Алгебраический криптоанализ.

Дифференциальный анализ.

Линейный анализ.

Грубая сила.

Внедрение кода.

Man in the middle.

DownGrade – понижение уровня защиты.

Побочные каналы.

- Потребление электричества
- Зондирование
- Атаки по времени
- Электромагнитное излучение.
- Акустические атаки.
- Видимое излучение.

12.12.2014

Криптология: криптоанализ, криптография.

Стеганография:

- Использование нетрадиционного носителя
- Кодирование одной информации в другой

Стегосистема

Сообщение (секретное)

Контейнер – информация, используемая для сокрытия секретного сообщения. Может быть пустой и заполненный.

Стегоканал – канал передачи контейнера.

Ключ: закрытый и открытый, симметричный.

Требования:

- Сложность выявления
- Устойчивость к искажению
- Наличие средств исправления ошибок
- Повторение сообщения для того, чтобы его можно было воспроизвести

Методы цифровой стеганографии.

- LSB – least significant bit
- JPEG
- Использование зарезервированных полей различных форматов
- Особенности файловых систем
- LACK – IP-телефония
- Фазовые преобразования. Преобразование Фурье для сигналов

Применение стеганографии.

- Сокрытие информации
- Водяные знаки. Для определения авторства.
- Идентификация