«Московский государственный технический университет имени Н.Э. Баумана»
(МГТУ им. Н.Э. Баумана)

Факультет: Информатика и системы управления

Кафедра: ИУ7

Защита информации

Студент группы ИУ7-73,

Степанов Александр

Преподаватель:

Григорьев Александр Сергеевич

2020 г.

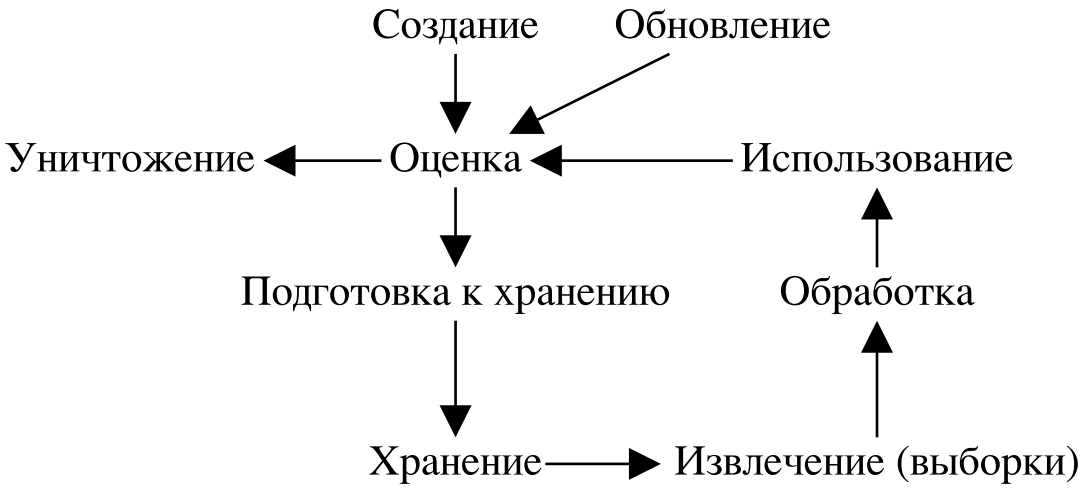
Содержание

§1 Информация

149 ФЗ об информации, информационных законах и защите информации

Информация – сведения, независимые от формы представления.

1.1 Стадия жизни информаиции



Документ – информация, зафиксированная на материальном носителе, она снабжена реквизитами

Электронный документ – документированная иформация, представленная в электронной форме.

Защита информации – принятие мер:

— правовые (законы)

— организационно-структурные (внутренние правила)

— технические (что используется)

направленные на:

1. предотвращение неправомерных действий

- доступ
- копирование
- модификация
- блокирование
- предоставление
- распространение
- уничтожение

2. соблюдение конфиденциальности (информация ограниченного доступа)
3. реализация права доступа к информации

1.2 Стандарт банка России – СТО БР ИББС

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

Информационная сфера:

- информация
- информационная структура
- субъекты
- процедуры

Система регулирования – контролирующая, чтобы все было безопасно.

Угроза – опасность, предполагающая возможность потерь или ущерба.

Безопасность – состояние защищенности в условиях угроз.

Информационная безопасность – безопасность в условиях угроз в информационной сфере.

Обеспечивает

- доступность

— целостность

— конфиденциальность

— ответственность

— подотчетность

— аутентичность

— достоверность

Индентификация – присвоение уникального имени.

Аутентификация – установление подлинности идентификатора.

Авторизация – предоставление прав доступа.

1.3 Активы

Ценность актива – меры ущерба, наносимые нарушением безопасности этого актива.

Важность актива бывает:

— жизненно важная – та, без которой система не может функционировать;

— важная – ущерб велик, но система может функционировать без нее;

— полезная (рабочая) – рабочая информация для функционирования, баботать плохо, но можно;

— несущественная – вспомогательные файлы, архивы.

Что учитывать

1. Простота – чем проще, тем меньше непротестированных моментов;
2. Полнота – закрыть все возможные подходы для нарушения безопасности;

3. Ответственность – авторизация, аутентификация, идентификация, если что сделал не так, то имеет ответственность за произошедшее;
4. Обоснованность доступа – необходимое и достаточное;
5. Разграничение потоков информации – разделять разные уровни секретности (важности) информации;
6. Чистота повторного использования;
7. Целостность средств защиты – сертификаты удостоверяются, что ничего не поменялось.

1.4 Методы защиты информации

1. **Системы аутентификации**
   - пароль;
   - ключ доступа;
   - сертификат;
   - биометрия;
   - одноразовые коды;
   - третья доверенная сторона.
2. **Средства авторизации**
   - модели доступа;
   - журналирование.
3. **Криптографические средства**
   - алгоритм шифроваия;
   - электронная подпись.
4. **Системы анализа и моделирования инфо потоков**

- средста мониторинга;
- моделирование с имитацией;
- межсетевое экранирование.

5. **Антивирусы + регулярное обновления**
6. **Регулярное резервное копирование**
7. **Резервирование HW**
   - железо;
   - питание.
8. **Режимные меры, физическая защита**

§2 Персональные данные

152 ФЗ регламентирует доступ к персоналным данным

— Общедоступные источники персональных данных (ПДн) – все сведения, которые мы храним, они взяты из открытых источников.

— Специальные ПДн – расовые, религиозные, медицинские.

— Биометрические ПДн.

— Трансграничкая передача ПДн.

2.1 Методы защиты от нелегального копирования

— внутренняя самозащита;

— ограничения по сроку;

— аутентификация / авторизация;

— нарушение штатного функционала;

— вирусы;

— аппаратные средства;

— изменение формата записи (хранения);

— собственная защита программного обеспечения.

Виды параметров

— постоянные;

— изменяемые.

Критерии выбора параметра

— уникаьность;

— неизменность;

— доступность.

ЛР1 защита информации от копирования

— Написать программу, она не может запуститься на компьютере;

— После запуска инсталлера, программа привязывается к компьютеру с помощью уникальных параметров и может запуститься;

— На другом компьютере не может запуститься, пока не запустить инсталлер.

1. Win API (get current hardware profile)
2. WMI (Windows Management Instrumentation) -> WQL
   - Win32_Processor
   - Win32_BIOS
   - Win32_DiskDrive
   - Win32_LogicalDisk
3. wmic
4. cat /proc/cpuinfo, /diskstats, /partiton
5. sysctl – MAC
6. stsctl conf
7. sysctl hw
8. ioreg
9. dmidocode

§3 Моделирования угроз и нарушителей

Уязвимость – это свойство системы, допускающее или способствующее реализации угрозы.

Цель моделирования угроз заставить разработчика конструктивно (на основе формального описания) мыслить при проектировании системы с точки зрения информационной безопасности.

3.1 Стандарт моделирвоания угроз

1 этап. Определение активов (что?)

2 этап. Описание архитектуры (где?)

- границы системы
- функциональность
- технологии

3 этап. Декомпозиция системы

- области защиты
- политики безопасности

4 этап. Определение угроз

- природные источники
- техногенные источники
- антропогенные источники
  - случайные
  - умышленные

5 этап. Документирование угроз

- цель угрозы
- категория по STRIDE

  - spoofing (подлинность)
  - tampering (целостность)
  - repudation (потеря ответственности)
  - information disclousure (нарушение конфиденциальности)
  - denial of service (отказ доступа)
  - elevation of privilege (поднятие полномочий)

6 этап. оценка / метод защиты

- DREAD
  - damage potential (что сломается)
  - reproducibility (воспроизводимость)
  - exploitability (используемость)
  - affected users (пострадавшие пользователи)
  - discoverability (возможность обнаружения)

3.2 Модель нарушителя

- низкий (может запускать разрешенные ему средства)
- средний (могжет запускать собственные средства, которые он должен протащить)
- высокий (может управлять системой)
- абсолютный (создатель системы)

1. Увлеченные (мотивы: развлечение, слава, недооцененность на работе, доступ)
2. Профессионалы (мотив: деньги)

3.3 Модели доступа

- HRU (дискретный доступ)

Таблица 1: Матрица доступа. Объект-субъект.

	O1	O2	O3
S1	RW		
S2		R	RWEX

Таблица 2: Матрица доступа. Ролевая модель. Роли.

	R1	R2
S1	X	
S2	X	X

Таблица 3: Матрица доступа. Ролевая модель. Права ролей.

	O1	O2	O3
R1	RW		
R2		R	RWEX

— Мандатная модель

  – ССОВ – совершенно секретно особой важности
  – СС – совершенно секретно
  – С – секретно
  – ДСП – для служебного пользования

Таблица 4: Матрица доступа

	ССОВ	СС	С	ДСП
ССОВ	■	■	■	■
СС		■	■	■
С			■	■
ДСП				■