

Лекция №2 18.09.2020

18 сентября 2020 г. 17:25

Ценность актива - мера ущерба наносимого нарушения безопасности информации.

Важность актива при выборе мер защиты информации:

- Жизненно важная - та без которой система в принципе не может функционировать
- Важная - ущерб велик, но при этом система может функционировать
- Полезная (рабочая) -
- Несущественная -

Что учитывается при создании систем защиты информации:

- 1) Простота -
- 2) Полнота - например если какой-нибудь секретный, шифрующий сервер, находящийся в бункере, но при этом раз в неделю приезжает бабушка уборщица, которая протирает мониторы. Необходимо закрыть все подходы к информации.
- 3) Ответственность - когда вы проектируете систему защиты информации, необходимо обеспечить идентификацию всех тех, кто пользуется системой.
- 4) Обоснованность доступа (необходимые и достаточные полномочия) - когда вы создаете взрослую систему, необходимо разграничивать права доступа между сотрудниками.
- 5) Разграничение потоков информации
- 6) Чистота повторного использования - например уничтожать старые жесткие диски.
- 7) Целостность средств защиты

Методы защиты информации:

- 1) Системы аутентификации
 - Пароль
 - Ключ доступа
 - Сертификат
 - Биометрия
 - Одноразовые коды
 - Третья доверенная сторона (ЕСИА)
- 2) Средство авторизации
 - Модели доступа
 - Журналирование
- 3) Криптографические средства
 - Шифрование

- Электронная подпись
- 4) Системы анализа и моделирование системных потоков
 - Мониторинг
 - Моделирование (имитация)
 - Межсетевое экранирование
- 5) Антивирусы + регулярное обновление
- 6) Регулярное резервирование
- 7) Резервирование Hardware
 - Железо
 - Питание
- 8) Режимные меры

Допустимая потеря данных

Персональные данные

- Общедоступные источники персональные данные
- Специальные персональные данные
- Биометрические персональные данные
- Трансграничная передача персональных данных

Методы защиты от нелегального копирования

- Внутренняя самозащита
- Ограничение по сроку
- Аутентификация/авторизация
- Нарушение штатного функционала
- Вирусы
- Аппаратные средства
- Изменение формата хранения
- Собственная защита программной инженерии

ЛАБ №1:

Берите любую программу (не сдавайте скрипты), нужен *.exe. Нужно эту программу защитить. Должен быть инсталлятор, который привязывает программу к машине. Надо написать программу и инсталлятор.

Устанавливаем, все запускается. Берем флешку, скидываем на другой комп, переносим - не работает. Запускаем инсталлятор - все начинает работать.

Нужно привязаться к уникальным характеристикам компа.

Виды параметров:

- 1) Постоянные - +
- 2) Изменяемые - -

Критерии:

- 1) Уникальность

- 2) Неизменность
- 3) Доступность

Мак адрес - топ тема

1. WinAPI
 - Get current hardware profile() - не использовать
2. WMI - Windows Management Instrumentation - хранит всю информацию ОС
 - Win32_Processor
 - BIOS
 - DiskDrive
 - MSFT_NetAdapter

WMIC

```
Csproduct  
Getuuid
```

```
Cat /proc/cpuinfo  
      /diskstars  
      /partition
```

Sysctl hw - выводит параметры процессора

Ioreg - система вывода

dmidecode

Лекция №2 18.09.2020

18 сентября 2020 г. 17:25

Ценность актива - мера ущерба наносимого нарушения безопасности информации.

Важность актива при выборе мер защиты информации:

- Жизненно важная - та без которой система в принципе не может функционировать
- Важная - ущерб велик, но при этом система может функционировать
- Полезная (рабочая) -
- Несущественная -

Что учитывается при создании систем защиты информации:

- 1) Простота -
- 2) Полнота - например если какой-нибудь секретный, шифрующий сервер, находящийся в бункере, но при этом раз в неделю приезжает бабушка уборщица, которая протирает мониторы. Необходимо закрыть все подходы к информации.
- 3) Ответственность - когда вы проектируете систему защиты информации, необходимо обеспечить идентификацию всех тех, кто пользуется системой.
- 4) Обоснованность доступа (необходимые и достаточные полномочия) - когда вы создаете взрослую систему, необходимо разграничивать права доступа между сотрудниками.
- 5) Разграничение потоков информации
- 6) Чистота повторного использования - например уничтожать старые жесткие диски.
- 7) Целостность средств защиты

Методы защиты информации:

- 1) Системы аутентификации
 - Пароль
 - Ключ доступа
 - Сертификат
 - Биометрия

- Одноразовые коды
 - Третья доверенная сторона (ЕСИА)
- 2) Средство авторизации
- Модели доступа
 - Журналирование
- 3) Криптографические средства
- Шифрование
 - Электронная подпись
- 4) Системы анализа и моделирование системных потоков
- Мониторинг
 - Моделирование (имитация)
 - Межсетевое экранирование
- 5) Антивирусы + регулярное обновление
- 6) Регулярное резервирование
- 7) Резервирование Hardware
- Железо
 - Питание
- 8) Режимные меры

Допустимая потеря данных

Персональные данные

- Общедоступные источники персональные данные
- Специальные персональные данные
- Биометрические персональные данные
- Трансграничная передача персональных данных

Методы защиты от нелегального копирования

- Внутренняя самозащита
- Ограничение по сроку
- Аутентификация/авторизация
- Нарушение штатного функционала
- Вирусы
- Аппаратные средства
- Изменение формата хранения
- Собственная защита программной инженерии

ЛАБ №1:

Берите любую программу (не сдавайте скрипты), нужен *.exe.

Нужно эту программу защитить. Должен быть инсталлятор, который привязывает программу к машине. Надо написать программу и инсталлятор. Устанавливаем, все запускается. Берем флешку, скидываем на другой комп, переносим - не работает. Запускаем инсталлятор - все начинает работать. Нужно привязаться к уникальным характеристикам компа.

Виды параметров:

- 1) Постоянные - +
- 2) Изменяемые - -

Критерии:

- 1) Уникальность
- 2) Неизменность
- 3) Доступность

Мак адрес - топ тема

1. WinAPI
 - Get current hardware profile() - не использовать
2. WMI - Windows Management Instrumentation - хранит всю информацию ОС
 - Win32_Processor
 - BIOS
 - DiskDrive
 - MSFT_NetAdapter

WMIC

```
Csproduct  
    Getuuid
```

```
Cat /proc/cpuinfo  
        /diskstats  
        /partition
```

Sysctl hw - выводит параметры процессора
Ioreg - система вывода
dmidecode