Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД.

Выполнил студент 332 группы
Климов Данил Сергеевич

Основные принципы защиты от НСД (1 из 4)

1 **Принцип обоснованности доступа**

- **Пользователь должен иметь достаточную «форму допуска» для доступа к информации данного уровня конфиденциальности**

- **Пользователю необходим доступ к данной информации для выполнения его производственных функций**

Основные принципы защиты от НСД (2 из 4)

2 **Принцип достаточной глубины контроля доступа**

Средства защиты информации должны включать механизмы контроля доступа ко всем видам информационных и программных ресурсов, которые в соответствии с принципом обоснованности доступа следует разделять между

пользователями

Основные принципы защиты от НСД (3 из 4)

3 **Принцип персональной ответственности**

- **Идентификация пользователей и процессов**
- **Аутентификация пользователей и процессов**
- **Регистрация работы механизмов контроля доступа к ресурсам системы с указанием даты и времени, идентификаторов запрашивающего и запрашиваемого ресурсов, включая запрещенные попытки доступа**

Основные принципы защиты от НСД (4 из 4)

4 **Принцип целостности средств защиты**

Система защиты информации должна точно выполнять свои функции в соответствии с основными принципами и быть изолированной от пользователей

(построение средств защиты проводится в рамках отдельного монитора обращений, контролирующего любые запросы на доступ к данным или программам со стороны пользователей)

Способы несанкционированного доступа

Основными способами несанкционированного доступа являются: инициативное сотрудничество, подслушивание, наблюдение, хищение, копирование, подделка, уничтожение, незаконное подключение, перехват.

Инициативное сотрудничество

Подслушивание

Наблюдение

Хищение

Копирование

Подделка

Уничтожение

Незаконное подключение

Перехват

Основные направления обеспечения защиты от НСД

Методы защиты компьютеров от несанкционированного доступа делятся на программно-аппаратные и технические. Создавая систему защиты информации (СЗИ) в организации, следует учитывать, насколько велика ценность внутренних данных в глазах злоумышленников.

Идентификация и аутентификация пользователей

Для выполнения этих процедур необходимы технические средства, с помощью которых производится двухступенчатое определение личности и подлинности полномочий пользователя.

После этого следует аутентификация.

Протоколы секретности для бумажной документации

Несмотря на повсеместную цифровизацию, традиционные бумажные документы по-прежнему используются в организациях. Они содержат массу информации – бухгалтерские сведения, маркетинговую информацию, финансовые показатели и прочие критические данные. Хранение, перемещение и копирование таких файлов производится по специальным правилам, исключающим возможность контакта с посторонними лицами.

Защита данных на ПК

Для защиты информации, хранящейся на жестких дисках компьютеров, используются многоступенчатые средства шифрования и авторизации.

Для особо важных устройств следует использовать модуль доверенной загрузки.

Предотвращение сетевых атак

Компьютеры, подключенные к Интернету, постоянно подвергаются риску заражения вредоносным программным обеспечением.

Для защиты системы от вредоносных программ, необходимо использовать антивирусные приложения, ограничить доступ в Сеть на определенные сайты.

Большинство пользователей хранит информацию в отдельных папках, которые названы «Пароли», «Мои карты» и т. п.

СПАСИБО ЗА ВНИМАНИЕ!