Технологии защиты информации

Информационная безопасность –защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Интегральная безопасность - необходимости обеспечить такое состояние условий функционирования человека, объектов и информации, при котором они надежно защищены от всех реальных видов угроз в ходе непрерывного производственного процесса и жизнедеятельности.

Цель интегральной защиты информации:

Создание таких условий, при которых будет невозможен как перехват, так и видоизменение и уничтожение информации, причем действие защиты должно быть непрерывно как во времени, так и в пространстве. В процессе интегральной защиты информации используются все необходимые средства защиты, а не только средства информационной безопасности.

ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ.

1.Технологии контроля и управления доступом к информации:

а) Технологии биометрической идентификации пользователя.

б) Технологии парольной защиты.

2.Технологии закрытой связи:

а) Скремблеры.

б) Маскираторы.

3.Технология обнаружения угроз:

а) Индикаторы поля, частотамеры.

б) Нелинейные локаторы.

в) Технологии радиоконтроля.

Технологии контроля и управления доступом к информации:

<u>Технологии биометрической идентификации пользователя</u> - это область науки, изучающую методы измерения физических характеристик и поведенческих черт человека для последующей идентификации и аутентификации личности.

BioLink U-Match 3.5 - Офисный оптический USB-сканер отпечатков пальцев. Сканеры отпечатков пальцев BioLink U-Match 3.5 пользуются особой популярностью у заказчиков. Количество выпущенных сканеров данной модели уже составляет десятки тысяч штук, эти сканеры применяются сотрудниками сотен коммерческих компаний и государственных структур более чем в 50 странах мира.

ТЕХНОЛОГИИ ПАРОЛЬНОЙ ЗАЩИТЫ - это аутентификация пользователей, т.е. подтверждение их подлинности, обеспечивается в первую очередь путем использования парольной защиты.

Программно-аппаратный комплекс «Мастер Паролей» предназначен для авторизации пользователей и разграничения прав доступа в среде Windows. Однопользовательская версия комплекса предназначена для индивидуальных пользователей или небольших организаций.

Технологии закрытой связи

Скремблер – это шифровальное устройство речи, используемое в системах телефонной связи.

Изменители голоса «Bluetooth voice changer» для мобильных телефонов – это устройства небольшого размера, которые работают совместно с сотовыми телефонами и изменяют Ваш голос таким образом, что абонент на другом конце линии не может определить, кто именно с ним разговаривает.

Скремблер GUARD-Bluetooth - это прибор высоким уровнем скремблирования. Он предназначен для шифрования разговоров, ведущихся по сотовой связи. Защита информации передаваемая по каналам сотовой связи обеспечивается за счет первоначального разрушения спектра речи .

Маскираторы – это устройства, снижающее вероятность перехвата голосовой информации.

Модули Icom ic- v8000 являются аналого-цифровыми скремблерами и предназначены для обеспечения среднего уровня закрытия переговоров по радиосвязи от прослушивания.

Технология обнаружения угроз

Индикаторы поля, частотамеры – устройства предназначенные для обнаружения и локализации всех видов радиозакладок, в том числе цифровых передатчиков.

BUG HUNTER - индикатор поля предназначенный для обнаружения и локализации миниатюрных радиопередатчиков, использующихся для несанкционированного получения информации, а также для беспроводных видеокамер (работающих по радиоканалу), сотовых телефонов и стационарных радиотелефонов.

Нелинейные локаторы

NR-900EMS- профессиональный детектор нелинейных переходов предназначен для обследования элементов строительных конструкций и предметов интерьера.

Применяется для выявления и локализации скрыто установленных средств негласного съема информации, в том числе диктофонов и другой аппаратуры, содержащей полупроводниковые радио-элементы.

Технологии радиоконтроля

Комплекс радиоконтроля, предназначен для поиска и локализации незаконно действующих источников излучений, использующих сложные алгоритмы маскировки во времени и по частотной шкале.

Кассандра М -комплекс радиомониторинга

- Уникальный по качеству и возможностям пользовательский интерфейс, который предоставляет оператору практически неограниченные возможности по отображению информации и обработке изображений для анализа сигналов.
- Широкие возможности задания порогов обнаружения сигналов, учтены практически любые варианты.

Средства сетевой защиты

Межсетевые экраны – обеспечивают реализацию механизмов защиты от атак в современных сетях.

Пандора (Gaumtlet) компании TIS: Gauntlet представляет собой наиболее эффективный с точки зрения защиты вариант firewall - фильтр на уровне приложений, при этом обеспечивает максимальную прозрачность при использовании, возможность создания VPN и простое управление всем этим.
HP-UX, IRIX и других UNIX-систем.

Продукт доступен в предустановленном виде на Pentium машинах, а также как отдельный пакет для BSD/OS, HP-UX, IRIX и других UNIX-систем

Застава - межсетевой экран.

Главные задачи этого межсетевого экрана это создание комплексных систем защиты распределенных сетей федеральных агентств и ведомств, обеспечение "жесткой" и быстрой фильтрации, а также реализация эффективного proxy-модуля для обработки трафика электронной почты, представляющей в современных условиях серьезную потенциальную угрозу безопасности сети - по сравнению с прочими "внешними" сервисами.