Медведев Владимир Арсентьевич

E – mail: krat29@rambler.ru

Информационная безопасность организации

Лекция 9. Техническое обеспечение ИБ

Санкт – Петербург, 2015 г.

Информационная безопасность в транспортной логистике

Средства КСИБ

- сканеры безопасности
- резервное копирование
- мониторинг
- системы антивирусной защиты
- защита информации от НСД
- криптография
- сетевая защита
- фильтрация содержимого
- идентификация и аутентификация пользователей

Информационная безопасность

Средства анализа защищенности

сканеры безопасности

- инвентаризация ресурсов
- идентификация и анализ уязвимостей
- патчинг новых уязвимостей
- формирование отчетов

задачи

Сканеры

- Сетевые
- Хостовые
- Web-приложений
- Специализированые БД
- беспроводных (Wi-Fi) сетей

Патчинг – автоматизированная отдельно поставленная программа необходимая для устранения проблем в ПО или изменением его функционала

Детектор поля

Детектор «жучков» Spider SX-08 предназначен для обнаружения прослушивающих устройств.

Оперативно реагирует, и тем самым обнаруживает подслушивающие устройства практически любого типа (радиопередающих и передающих по gsm каналу). Содержат новейшие микропроцессоры.

Широкий диапазон охватываемых частот, делает доступным обнаружение цифровых и аналоговых подслушивающих устройств, а также скрытые камеры беспроводного типа передающие информацию посредством радиосигнала, мобильные телефоны, рации, радио микрофоны , скрытые жучки и т.д.

Детектор поля - Spider SX-08

Цена 9900 руб.
на 1.01.2013 г

Частотные разбежки, а также устройства работающие в этих диапазонах:

- 1 MHz-470 MHz микрофоны, наушники скрытого типа;
- 50 MHz-460 MHz прослушивание телефона, радиопрослушка;
- 500 MHz-2500 MHz gsm «жучки», DECT закладки и др.;
- 900 MHz-1900 MHz цифровые устройства слежения, GPS-трекеры автомобильного и персонального типа;
- 700 MHz-580 0MHz мини-камеры (радиосигнал);
- 2400 MHz-5800 MHz камеры наблюдения беспроводные;
- 4000 MHz-8000 MHz другие «жучки» и устройства

Сканирование телефонных разговоров

Характерные ситуаций, когда требуются сканеры телефонных разговоров:

1) контроль за деятельностью сотрудников, работающих непосредственно с клиентами – для оперативного реагирования на их жалобы о невежественности, неисполнительности или грубости, и для обеспечения пропорционального использования рабочего времени персоналом;

2) нахождение решений в конфликтных ситуациях - для принятия решений, когда две стороны (например, клиент - менеджер) утверждают разные взаимоисключающие вещи или для контроля выполнения данных поручений и заданий;

Сканирование телефонных разговоров

Характерные ситуаций, когда требуются сканеры телефонных разговоров:

3) контроль за передаваемой информацией – для выявления источника утечки конфиденциальной информации, а также для обнаружения хищений и нарушений режима работы организации;

4) устранение несанкционированных платных звонков (междугородных или международных) - для снижения расходов компании на телефонную связь и выявления нарушителей;

5) организация приоритета служб экстренного реагирования, диспетчерских служб и правоохранительных органов - для оперативной работы скорой помощи, милиции и других служб.

Информационная безопасность

Средства КСИБ

мониторинг

Обнаружение инцидентов в режиме реального времени

Определение приоритетов событий и инцидентов

Автоматизация процесса реакции на инциденты

Централизованный сбор, анализ и хранение событий безопасности

функции

Symantec SIM

Создание отчетов о сетевой и пользовательской активности, инцидентах, соблюдении нормативных требований информационной безопасности

Сервер

Агент сбора

Анализатор

Основной сервер, осуществляет управление системой

Собирает события с объектов (syslog, файлы, журналы и др.) и передает их на анализатор

Производит обработку, корреляцию событий, обнаружение инцидентов по заданным правилам и политикам

Symantec Security Information Manager

Symantec Security Information Manager

- обеспечивает сбор данных о событиях в масштабе предприятия, управление данными и их хранением, что позволяет централизованно хранить и анализировать большие объемы разнотипных данных журналов.

Модуль корреляции объединяет организационные данные, информацию о событиях безопасности и результаты анализа угроз, что позволяет классифицировать действия по обработке инцидентов безопасности по степени риска для бизнеса.

При таком превентивном подходе обеспечивается более эффективная защита предприятия от угроз и соблюдение требований отраслевых стандартов.

Symantec Security Information Manager

Symantec O3 представляет собой платформу для защиты информации *в облаке*, обеспечивающую контроль доступа с учетом контекста, безопасность и управление информацией в виде «услуги» для пользователей *облачных приложений* и служб.

Платформа поддерживает любые конечные точки, включая мобильные. Она предоставляет информацию о попытках доступа и событиях безопасности, применяемую в целях аудита и анализа в соответствии с нормативами

http://www.symantec.com/products-solutions/products/videos-lightbox.jsp?cid=symantec-o3

Информационная безопасность

Средства КСИБ

резервное копирование

Резервирование **– это один из необходимых методов обеспечения непрерывности, а в ряде случаев обязательной подсистемой для соответствия стандартам в области ИБ.**

Система резервного копирования и защиты данных позволяет произвести резервное копирование и защиту данных:

- **На платформах Windows, Linux, UNIX средах;**
- **В средах виртуализации Hyper-V, VMWare**
- **На серверах и рабочих станциях;**

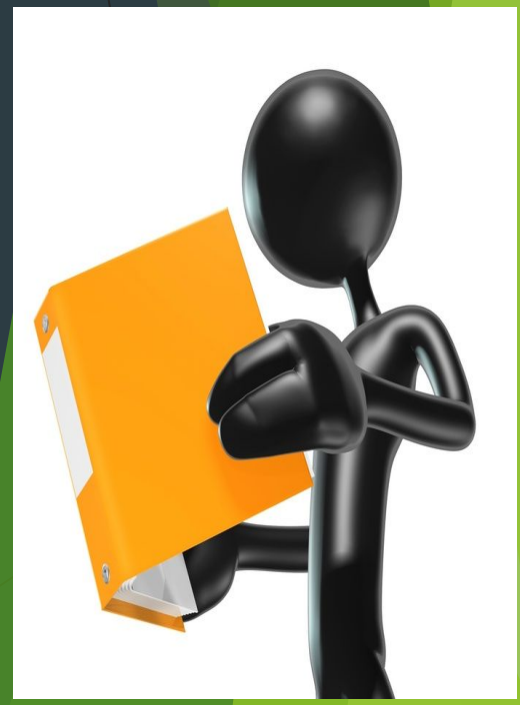
Резервное копирование

Лучшая системная конфигурация ничего не стоит, если резервирование выполняется неправильно, если стратегия не соответствует требованиям, или если восстановление не происходит.

Если данные представляют большую ценность, то имеет смысл либо поместить все важные файлы в зашифрованный контейнер (например, в TrueCrypt) и включить этот зашифрованный файл в резервную копию, либо можно использовать функцию шифрования программы резервирования.

Резервирование и восстановление данных: обзор трёх решений для Windows 7

Решение 1: резервирование встроенными средствами - *может резервировать отдельные файлы и создать образ своего системного раздела и восстановить его через загрузку с установочного диска.*



Решение 2: Acronis True Image Home 2010

- это утилита Acronis True Image, которая изначально предназначалась для создания образов:

- *резервирование диска и его разделов;*
- *онлайновое резервирование (Online backup), при котором требуется наличие учётной записи;*
- *резервирование файлов;*
- *непрерывное резервирование (Nonstop backup).*

Резервирование и восстановление данных: обзор трёх решений для Windows 7

Решение 3: Rebit

- программа постоянно клонирует и архивирует данные на специальный резервный накопитель.
Данная утилита поставляется с накопителем Seagate Replica, но её можно купить отдельно с другими накопителями.

Нередко от чашки кофе "умирает" внешний жёсткий диск - поэтому лучше один раз переплатить за герметичное решение, чем потом восстанавливать данные с пластин.

Информационная безопасность

Средства КСИБ

защита информации от НСД

- идентификация пользователей по паролям и по аппаратным идентификаторам;
- ограничение доступа пользователей к ПК по дате и времени;
- ранжирование доступа с помощью мандатного или дискреционного контроля;
- контроль целостности параметров компьютера;
- очистка остаточной информации, освобождаемой памяти и др.;
- контроль печати на принтерах;
- автоматическое ведение различных видов электронных журналов;
- создание замкнутой программной среды;
- функция преобразования данных на локальных дисках;
- централизованное администрирование системы защиты.

Zecurion Zlock

-предназначен для защиты от утечек конфиденциальной информации на конечных точках сети.
Zecurion Zlock позволяет контролировать использование устройств, подключаемых к портам USB, LPT, COM, IrDA, IEEE 1394, слоту PCMCIA, внутренних устройств — в том числе встроенных сетевых карт, модемов, Bluetooth, Wi-Fi, CD/DVD-дисководов, а также локальных и сетевых принтеров.

Zecurion Zlock

Решаемые задачи:

- разграничение доступа к любым устройствам и портам на основе гибкой настройки политик доступа;
- контроль всей информации, которая копируется на съемные устройства и распечатывается на принтерах;
- анализ содержимого файлов на предмет наличия в них конфиденциальных данных;
- блокирование печати, чтения и записи на устройства при выявлении нарушений политик безопасности;
- архивирование всех записанных и распечатанных документов;
- своевременное предотвращение утечек информации.

Информационная безопасность

Средства КСИБ

идентификация и аутентификация

В качестве критерия идентификации пользователя при использовании электронных USB-ключей и смарт-карт eToken могут использоваться:

- **цифровые сертификаты стандарта X.509 (PKI);**
- **пользовательские пароли, коды доступа.**

Электронные ключи eToken **– персональное средство аутентификации и защищённого хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и ЭЦП**

Информационная безопасность

Средства КСИБ

криптография

1. Прозрачное шифрование в реальном времени, позволяет работать с документами в обычном режиме;
2. Информация хранится в контейнере в виде зашифрованного файла на диске или внешнем носителе и защищается файл-ключом или электронным ключом;
3. При подключении контейнер отображается в системе как обычный диск;
4. В программе существуют режимы экстренного отключения контейнеров и выхода из программы, а также режим экстренного уничтожения доступа к информации для всех пользователей программы.

Криптография

Средства защиты периметра сети и антивирусы не смогут предотвратить утечки информации, если злоумышленник получит физический доступ к носителю информации.

Варианты утечки информации:

- размещение серверов в стороннем дата-центре (collocation);
- отправка серверов или жестких дисков в ремонт;
- перевозка компьютеров из одного офиса в другой;
- утилизация компьютеров, серверов, жестких дисков и лент;
- перевозка и хранение магнитных лент в специальном депозитарии (off-site storage);
- кража или потеря жестких дисков или лент.

Информационная безопасность

Средства КСИБ

сетевая защита

- идентифицирует, классифицирует и блокирует вредоносный трафик и предотвращает нарушения работы приложений;
- обеспечивает высокоэффективное интеллектуальное обнаружение угроз и защиту при различных вариантах развертывания;
- использует фильтрацию на основании репутации и глобальные проверки;
- поддерживает непрерывность деятельности и помогает предприятиям обеспечивать соответствие требованиям стандартов и нормативов.

Информационная безопасность

Средства КСИБ

фильтрация содержимого

- **мониторинг и анализ данных, отправляемых за пределы корпоративной сети через почтовые системы, web, системы обмена сообщениями, распечатываемых или копируемых на различные устройства ввода-вывода;**
- **предотвращение утечки конфиденциальных данных путем блокирования процесса передачи в случае обнаружения нарушения политики безопасности;**
- **анализ и хранение данных для проведения расследований;**

Информационная безопасность

Средства КСИБ

фильтрация содержимого

- анализирует содержание, контекст и направление передачи данных, позволяя администраторам управлять транзакциями;
- проводит мониторинг всех типов данных в сети и на конечных компьютерах, защищая данные от утечек, независимо от их формата и местоположения;
- централизованная система управления и отчетности предоставляет мощные инструменты анализа, выявления и устранения инцидентов, а также генерации отчетов.

Процесс адаптации системы контроля

Актуальные условия

Изменившиеся условия

Разработка

Модификация

Система контроля 1

Система контроля 2

ИТС

АТАКА

Информационная безопасность

Защита от умышленных попыток манипуляции со стороны «хакеров»

- применения защищённых от НСД специальных АС;
- постоянная модификация АС при обнаружении новых видов мошенничества;
- мониторинг активности черного рынка;
- обеспечение высокого уровня контроля за работой АС;
- создание системы слежения за работой самих контролеров.

Арсений Григорьевич Головко

(1906 – 1962 лучевая болезнь)

— советский флотоводец, адмирал (1944). Бессменный командующий Северным морским флотом во время Великой Отечественной войны.

Под его руководством флот участвовал в обороне Мурманска и всего Советского Заполярья, в обеспечении проводки северных морских конвоев союзников и внутренних конвоев, в борьбе на коммуникациях германских войск у Северной Норвегии, в Петсамо - Киркинесской операции.