Презентация к выпускной квалификационной работе учащегося: Васильева Анатолия Евгеньевича ГРУППА 34 НК

На тему: Создание и отладка комплекса мероприятий по защите персональных данных

Система защиты персональных данных

Стадии построения системы защиты персональных данных

- Предпроектная стадия по обследованию ИСПДн
- Стадия проектирования и реализации ИСПДн
- Стадия ввода в действие СЗПДн

Выбор средств защиты персональных данных

Федеральный закон «О персональных данных»

Обеспечение безопасности персональных данных достигается, в частности … применением прошедших в установленном порядке **процедуру оценки соответствия** средств защиты информации.

Постановление Правительства РФ от 01.11.2012 № 1119

Выбор средств защиты информации для системы защиты персональных данных **осуществляется оператором в соответствии с нормативными правовыми актами, принятыми** ФСБ России и ФСТЭК России во исполнение части 4 статьи 19 Федерального закона «О персональных данных».

Постановление Правительства РФ от 01.11.2012 № 1119

Требования к защите персональных данных при их обработке в информационных системах персональных данных

1. Настоящий документ устанавливает **требования к защите** персональных данных при их обработке в информационных системах персональных данных (далее - информационные системы) и **уровни защищенности** таких данных.

2. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью **системы защиты** персональных данных, **нейтрализующей актуальные угрозы**, определенные в соответствии **с частью 5 статьи 19**

Защита информации

- **Защита данных, защита информации [data protection]** - совокупность мер, обеспечивающих защиту прав собственности владельцев информационной продукции, в первую очередь - программ, баз и банков данных от несанкционированного доступа, использования, разрушения или нанесения ущерба в какой-либо иной форме.

Виды и методы защиты информации

Вид защиты	Метод защиты
От преднамеренного искажения, вандализма (компьютерных вирусов)	•Общие методы защиты информации; • профилактические меры; • использование антивирусных программ
От несанкционированного (нелегального) доступа к информации (её использования, изменения, распространения)	• Шифрование; • паролирование; • «электронные замки»; • совокупность административных и правоохранительных мер

Компьютерные преступления

- **Компьютерные преступления** — это предусмотренные уголовным законодательством общественно опасные действия, в которых объектом или средством преступного посягательства является машинная информация.
- Другими словами, в качестве предмета или орудия такого преступления выступает машинная информация, компьютер, компьютерная система или сеть.
- Причины возникновения
  1. Расширение сфер использования технических средств
  2. Появление различных форм собственности
  3. Промышленный и финансовый шпионаж
  4. Прозрачность территориальных границ

Основные виды компьютерных преступлений

- Компьютерные преступления условно можно подразделить на две большие категории:
  1. Вмешательство в работу компьютеров
  2. Использование компьютеров в качестве необходимых технических средств.
- К основным видам преступлений, связанных с вмешательством в работу компьютеров, относятся:

1. несанкционированный доступ к данным и их перехват;
2. несанкционированное изменение компьютерных данных;
3. компьютерное мошенничество;
4. незаконное копирование машинной информации;
5. компьютерный саботаж.

Основные виды компьютерных преступлений

Несанкционированный доступ к данным и их перехват осуществляется, как правило:

- с помощью чужого сетевого имени
- изменения физических адресов технических устройств
- использования информации, оставшейся после решения задач
- модификации программного и информационного обеспечения
- хищения носителей информации
- установки аппаратуры прослушивания, подключаемой к каналам передачи данных

Хакер – лицо, совершающее систематические несанкционированные доступы в компьютерные системы и сети с целью развлечения, мошенничества или нанесения ущерба (в том числе и путем распространения компьютерных вирусов).

Их можно условно разделить на четыре группы.

1) романтики-одиночки, взламывающие компьютерные системы просто ради собственного удовольствия.

2) - пираты. Они взламывают защиту компьютеров для похищения информации.

3) – разведчики, взламывают сети конкурентов и крадут оттуда информацию

4) - кибергангстеры, которые охотятся за секретной информацией по чьим-либо заказам.

- **Компьютерные данные подвержены трем типам опасностей,** к которым относятся:
  - нарушение конфиденциальности
  - нарушение целостности
  - нарушение доступности
- Опасности делят на
  - случайные угрозы
  - умышленные угрозы

Умышленные угрозы

- Основные угрозы:
  - внедрение в систему вредоносного программного обеспечения.
  - несанкционированный доступ к сетевым ресурсам;
  - раскрытие и модификация данных и программ, их копирование
  - раскрытие, модификация или подмена трафика вычислительной сети
  - фальсификация сообщений,
  - перехват и ознакомление с информацией, передаваемой по каналам связи

Уязвимость – это еще одно важное понятие в теории защиты информации. **Под уязвимостью понимают** такое свойство системы, которое позволяет реализовать соответствующую угрозу.

Случайные угрозы

- Основная причина всех неприятных случайностей – это недостаточно бережное отношение владельца к компьютеру вообще и к компьютерным данным в частности. Иначе говоря, недостаточный уровень компьютерной грамотности.
- Итак, перечислим наиболее вероятные угрозы случайного характера:
  - ошибки обслуживающего персонала и пользователей;
  - потеря информации, обусловленная неправильным хранением данных;
  - случайное уничтожение или изменение данных;
  - сбои и отказы аппаратной части компьютера;
  - перебои электропитания;
  - некорректная работа программного обеспечения;
  - непреднамеренное заражение системы компьютерными вирусами или другими видами вредоносного программного обеспечения.

Основные виды компьютерных преступлений

Несанкционированное изменение компьютерных данных

- Разработка и распространение компьютерных вирусов
- Ввод в программное обеспечение «логических бомб»
- Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов
- Подделка компьютерной информации
- Хищение компьютерной информации

Основные виды компьютерных преступлений

- Использование компьютеров в качестве необходимых технических средств.
  - Разработка математических моделей
  - Создание компьютера-шпиона

Программы-шпионы

- На такие программы обычно возлагаются следующие функции:
  - сбор сведений о программном обеспечении, установленном на компьютере (в том числе тип и версия используемой операционной системы);
  - перехват клавиатурного ввода (в частности, отслеживание вводимых паролей, сетевых имен и т. д.);
  - поиск на жестком диске (дисках) персональных данных;
  - выявление адресов посещаемых Web-сайтов, адресов электронной почты и т. п.;
  - создание снимков экрана или окон конкретных активных приложений (некоторые шпионы способны также записывать целые видеоклипы о работе владельца компьютера).

70% сотрудников присваивают корпоративную информацию

Около 70% сотрудников компаний выносят корпоративную информацию из внутренней компьютерной сети компании. 68% пользуются на работе социальными сетями, а более половины респондентов (56%) унесли бы не просто корпоративную, а строго конфиденциальную информацию с собой на флешке.

Системы защиты от утечек данных за последнее время стали самым быстрорастущим направлением среди всех защитных продуктов. Объёмы утечек данных в компаниях увеличиваются год от года. Из-за действий инсайдеров (умышленных или совершенно невинных) конфиденциальные данные компаний беспрепятственно покидают корпоративные сети и утекают во внешний мир.

Интернет стал основным криминальным инструментом

- В 2011г. Интернет стал главным инструментом противозаконной деятельности для европейской организованной преступности.
- Просторы Всемирной паутины используются для торговли наркотиками и людьми, отмывания денег и кибератак.
- Посредством интернета ведется торговля живыми людьми, развивается незаконная иммиграция и происходит продажа контрафактной продукции.
- Преступники уверены в безопасности налаживания каналов поставок через интернет.
- Кроме того, интернет является местом обналичивания украденных кредитных карт. Оборот денег от такого рода преступлений в Европе превышает 1,5 млр долларов.

ПРЕДУПРЕЖДЕНИЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

- Базовые принципы информационной безопасности:
  - целостность данных (защита от сбоев, ведущих к потере информации, а также от неавторизованного создания или уничтожения данных)
  - конфиденциальность информации (обеспечения ее доступности только для авторизованных пользователей)
- Основные методы предупреждение компьютерных преступлений:
  - правовые
  - программно-технические
  - организационно-экономические