Информационная безопасность

Лекция 1

Основные понятия курса

Понятие информационной безопасности

- Под **информационной безопасностью** понимается 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.
- **Защита информации** – комплекс мероприятий, направленных на обеспечение информационной безопасности.

Проблемы информационной безопасности

- Информационная безопасность является одним из важнейших аспектов интегральной безопасности.
- Иллюстрациями являются следующие факты:
  - В Доктрине информационной безопасности РФ защита от НСД к информационным ресурсам, обеспечение безопасности информационных и телекоммуникационных систем выделены в качестве важных составляющих национальных интересов;
  - В период 1994-1996 гг. были предприняты почти 500 попыток проникновения в компьютерную сеть ЦБ РФ. В 1995 году было похищено 250 миллиардов рублей.
  - По сведениям ФБР ущерб от компьютерных преступлений в США в 1997 г. составил 136 миллионов долларов.

Проблемы информационной безопасности

- По данным отчета «Компьютерная преступность и безопасность – 1999: проблемы и тенденции»
  - 32% респондентов – обращались в правоохранительные органы по поводу компьютерных преступлений
  - 30% респондентов – сообщили, что их ИС были взломаны злоумышленниками;
  - 57% - подверглись атакам через Интернет;
  - 55% - отметили случаи нарушений ИБ со стороны собственных сотрудников;
  - 33 % - не смогли ответить не вопрос «были ли взломаны Ваши веб-серверы и системы электронной коммерции?».

Проблемы информационной безопасности

- Глобальное исследование по информационной безопасности 2004 г., проведенное консалтинговой фирмой Ernst&Young выявило следующие основные аспекты:
  - Лишь 20% опрошенных убеждены в том, что их организации рассматривают вопросы информационной безопасности на уровне высшего руководства;
  - По мнению респондентов «недостаточная осведомленность в вопросах ИБ» является главным препятствием для создания эффективной системы ИБ. Лишь 28% отметили в качестве приоритетных задач «повышение уровня обучения сотрудников в области ИБ»;
  - «Неправомерные действия сотрудников при работе с ИС» были поставлены на второе место по распространенности угроз ИБ, после вирусов, «троянов» и Интернет-червей.
  - Менее 50% респондентов проводят обучения сотрудников в области ИБ;
  - Лишь 24% опрошенных считают, что их отделы ИБ заслуживают наивысшей оценки за удовлетворение бизнес потребностей своих организаций своих организаций;
  - Лишь 11% респондентов считают, что принятые государственными органами нормативные акты в области безопасности позволили существенно улучшить состояние их информационной безопасности.

Угрозы информационной безопасности

- **Угроза информационной безопасности** (ИБ) – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.
- Попытка реализации угрозы называется **атакой**.
- Классификация угроз ИБ можно выполнить по нескольким критериям:
  - **по аспекту ИБ** (доступность, целостность, конфиденциальность);
  - **по компонентам ИС**, на которые угрозы нацелены (данные, программа, аппаратура, поддерживающая инфраструктура);
  - **по способу осуществления** (случайные или преднамеренные действия природного или техногенного характера);
  - **по расположению источника угроз** (внутри или вне рассматриваемой ИС).

Свойства информации

- Вне зависимости от конкретных видов угроз информационная система должна обеспечивать базовые свойства информации и систем ее обработки:
  - **доступность** – возможность получения информации или информационной услуги за приемлемое время;
  - **целостность** – свойство актуальности и непротиворечивости информации, ее защищенность от разрушения и несанкционированного изменения;
  - **конфиденциальность** – защита от несанкционированного доступа к информации.

Примеры реализации угрозы нарушения конфиденциальности

- Часть информации, хранящейся и обрабатываемой в ИС, должна быть сокрыта от посторонних. Передача данной информации может нанести ущерб как организации, так и самой информационной системе.
- Конфиденциальная информация может быть разделена на **предметную** и **служебную**. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, однако ее раскрытие может привести к несанкционированному доступу ко всей информации.
- Предметная информация содержит информацию, раскрытие которой может привести к ущербу (экономическому, моральному) организации или лица.
- Средствами атаки могут служить различные технические средства (подслушивание разговоров, сети), другие способы (несанкционированная передача паролей доступа и т.п.).
- Важный аспект – непрерывность защиты данных на всем жизненном цикле ее хранения и обработки. Пример нарушения – доступное хранение резервных копий данных.

Примеры реализации угрозы нарушения целостности данных

- Одними из наиболее часто реализуемых угроз ИБ являются кражи и подлоги. В информационных системах несанкционированное изменение информации может привести к потерям.
- Целостность информации может быть разделена на **статическую** и **динамическую.**
- Примерами нарушения статической целостности являются:
  - ввод неверных данных;
  - несанкционированное изменение данных;
  - изменение программного модуля вирусом;
- Примеры нарушения динамической целостности:
  - нарушение атомарности транзакций;
  - дублирование данных;
  - внесение дополнительных пакетов в сетевой трафик.

Вредоносное программное обеспечение

- Одним из способов проведения атаки является внедрение в системы вредоносного ПО. Данный вид программного обеспечения используется злоумышленниками для:
  - внедрения иного вредоносного ПО;
  - получения контроля над атакуемой системой;
  - агрессивного потребления ресурсов;
  - изменение или разрушение программ и/или данных.
- По механизму распространения различают:
  - вирусы – код, обладающий способностью к распространению путем внедрения в другие программы;
  - черви – код, способный самостоятельно вызывать распространение своих копий по ИС и их выполнение.

Вредоносное программное обеспечение

- В ГОСТ Р 51272-99 «Защита информации. Объект информатизации. Факторы воздействующие на информацию. Общие положение» вводится следующее понятие вируса:
  - **Программный вирус** – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.

Примеры реализации угрозы отказа в доступе

- Отказ служб (отказа в доступе к ИС) относится к одним из наиболее часто реализуемых угроз ИБ. Относительно компонент ИС данный класс угроз может быть разбит на следующие типы:
  - отказ пользователей (нежелание, неумение работать с ИС);
  - внутренний отказ информационной системы (ошибки при переконфигурировании системы, отказы программного и аппаратного обеспечения, разрушение данных);
  - отказ поддерживающей инфраструктуры (нарушение работы систем связи, электропитания, разрушение и повреждение помещений).

Понятие атаки на информационную систему

- **Атака** – любое действие или последовательность действий, использующих уязвимости информационной системы и приводящих к нарушению политики безопасности.
- **Механизм безопасности** – программное и/или аппаратное средство, которое определяет и/или предотвращает атаку.
- **Сервис безопасности** - сервис, который обеспечивает задаваемую политикой безопасность систем и/или передаваемых данных, либо определяет осуществление *атаки*. *Сервис* использует один или более механизмов безопасности.

Классификация атак

- Классификация атак на информационную систему может быть выполнена по нескольким признакам:
  - По месту возникновения:
    - Локальные атаки (источником данного вида атак являются пользователи и/или программы локальной системы);
    - Удаленные атаки (источником атаки выступают удаленные пользователи, сервисы или приложения);
  - По воздействию на информационную систему
    - Активные атаки (результатом воздействия которых является нарушение деятельности информационной системы);
    - Пассивные атаки (ориентированные на получение информации из системы, не нарушая функционирование информационной системы);

Классификация сетевых атак

- При описании сетевых атак в общем случае используется следующее представление:
  - существует информационный поток от отправителя (файл, пользователь, компьютер) к получателю (файл, пользователь, компьютер):

Сетевые атаки

- **I. Пассивная атака**
- Пассивной называется такая *атака*, при которой *противник* не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения. Целью *пассивной атаки* может быть только прослушивание передаваемых сообщений и анализ трафика.

Сетевые атаки

- Активной называется такая *атака*, при которой *противник* имеет возможность модифицировать передаваемые сообщения и вставлять свои сообщения. Различают следующие типы *активных атак*:
- **Отказ в обслуживании** - *DoS-атака (Denial of Service)*
  - Отказ в обслуживании нарушает нормальное функционирование сетевых сервисов. *Противник* может перехватывать все сообщения, направляемые определенному адресату. Другим примером подобной *атаки* является создание значительного трафика, в результате чего сетевой сервис не сможет обрабатывать запросы законных клиентов.
  - Классическим примером такой *атаки* в сетях TCP/IP является SYN-атака, при которой нарушитель посылает пакеты, инициирующие установление TCP-соединения, но не посылает пакеты, завершающие установление этого соединения.
  - В результате может произойти переполнение памяти на сервере, и серверу не удастся установить соединение с законными пользователями.

Сетевые атаки

- **Модификация потока данных** - *атака "man in the middle"*
- Модификация потока данных означает либо изменение содержимого пересылаемого сообщения, либо изменение порядка сообщений.

Сетевые атаки

- **Создание ложного потока (фальсификация)**
- *Фальсификация* (нарушение аутентичности) означает попытку одного субъекта выдать себя за другого

Сетевые атаки

- **Повторное использование**
- Повторное использование означает пассивный захват данных с последующей их пересылкой для получения несанкционированного доступа - это так называемая *replay-атака*.
- На самом деле *replay-атаки* являются одним из вариантов фальсификации, но в силу того, что это один из наиболее распространенных вариантов *атаки* для получения несанкционированного доступа, его часто рассматривают как отдельный тип *атаки*.

Подходы к обеспечению информационной безопасности

- Для защиты АИС могут быть сформулированы следующие положения:
  - Информационная безопасность основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов;
  - Информационная безопасность АИС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мероприятий;
  - Информационная безопасность АИС должна обеспечиваться на всех этапах технологической обработки данных и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ;

Подходы к обеспечению информационной безопасности

- Для защиты АИС могут быть сформулированы следующие положения:
  - Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АИС;
  - Неотъемлемой частью работ по информационной безопасности является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию;
  - Защита АИС должна предусматривать контроль эффективности средств защиты. Этот контроль может быть периодическим или инициируемым по мере необходимости пользователем АИС.

Принципы обеспечения информационной безопасности

- Системность;
- Комплексность;
- Непрерывность защиты;
- Разумная достаточность;
- Гибкость управления и применения;
- Открытость алгоритмов и механизмом защиты;
- Простота применения защитных мер и средств.

Системность средств защиты информации

- Системность при выработке и реализации систем защиты информации предполагает определение возможных угроз информационной безопасности и выбор методов и средств, направленных на противодействие данного комплексу угроз.
- Решения должны иметь системный характер, то есть включать набор мероприятий противодействующий всему комплексу угроз.

Комплексность систем защиты

- При решение вопросов обеспечения информационной безопасности необходимо ориентироваться на весь набор средств защиты данных – программные, технические, правовые, организационные и т.д.

Непрерывность защиты

- Непрерывность защиты предполагает, что комплекс мероприятий по обеспечению информационной безопасности должен быть непрерывен во времени и пространстве.
- Защита информационных объектов должна обеспечиваться и при выполнении регламентных и ремонтных работ, во время настройки и конфигурирования информационных систем и сервисов.

Разумная достаточность

- Построение и обслуживание систем информационной безопасности требует определенных, подчас значительных, средств. Вместе с тем невозможно создание все объемлемой системы защиты.
- При выборе системы защиты необходимо найти компромисс между затратами на защиту информационных объектов и возможными потерями при реализации информационных угроз.

Гибкость управления и применения

- Угрозы информационной безопасности многогранны и заранее не определены. Для успешного противодействия необходимо наличие возможности изменения применяемых средств, оперативного включения или исключения используемых средств защиты данных, добавления новых механизмов защиты.

Открытость алгоритмов и механизмов защиты

- Средства информационной безопасности сами могут представлять собой угрозу информационной системе или объекту. Для предотвращения такого класса угроз требуют, чтобы алгоритмы и механизмы защиты допускали независимую проверку на безопасность и следование стандартов, а также на возможность их применение в совокупности с другими средствами защиты данных.

Простота применения защитных мер и средств

- При проектировании систем защиты информации необходимо помнить, что реализация предлагаемых мер и средств будет проводится пользователями (часто не являющихся специалистами в области ИБ).
- Поэтому для повышения эффективности мер защиты необходимо, чтобы алгоритм работы с ними был понятен пользователю. Кроме того, используемые средства и механизмы информационной безопасности не должны нарушать нормальную работу пользователя с автоматизированной системой (резко снижать производительность, повышать сложность работы и т. п.).

Методы обеспечения ИБ

- Рассмотрим пример классификации методов, используемых для обеспечения информационной безопасности:
  - **препятствие** – метод физического преграждения пути злоумышленнику к информации;
  - **управление доступом** – метод защиты с помощью регулирования использования информационных ресурсов системы;
  - **маскировка** – метод защиты информации путем ее криптографического преобразования;
  - **регламентация** – метод защиты информации, создающий условия автоматизированной обработки, при которых возможности несанкционированного доступа сводится к минимуму;
  - **принуждение** – метод защиты, при котором персонал вынужден соблюдать правила обработки, передачи и использования информации;
  - **побуждение** – метод защиты, при котором пользователь побуждается не нарушать режимы обработки, передачи и использования информации за счет соблюдения этических и моральных норм.

Средства защиты информационных систем

- Такие средства могут быть классифицированы по следующим признакам:
  - **технические средства** – различные электрические, электронные и компьютерные устройства;
  - **физические средства** – реализуются в виде автономных устройств и систем;
  - **программные средства** – программное обеспечение, предназначенное для выполнения функций защиты информации;
  - **криптографические средства** – математические алгоритмы, обеспечивающие преобразования данных для решения задач информационной безопасности;
  - **организационные средства** – совокупность организационно-технических и организационно-правовых мероприятий;
  - **морально-этические средства** – реализуются в виде норм, сложившихся по мере распространения ЭВМ и информационных технологий;
  - **законодательные средства** – совокупность законодательных актов, регламентирующих правила пользования ИС, обработку и передачу информации.