Лекция 1. Понятие информационной безопасности. Введение

Цель лекции: Ознакомить студентов с понятием информационной безопасности и дать объяснения основным терминам в сфере ИБ.

План лекции:

1. Понятие информационной безопасности
2. Угрозы информационной безопасности
3. Средства защиты информации
4. Принципы обеспечения ИБ

Понятие информационной безопасности

Информационной безопасностью называют комплекс организационных, технических и технологических мер по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе.

Обеспечение информационной безопасности – непрерывный процесс, который заключается в развитии системы защиты, постоянном контроле, выявлении ее слабых мест, а также возможных каналов утечки информации. Воздействия любого характера могут привести к потере важных данных, их изменению или даже к овладению ими третьими лицами. Защита информационной безопасности предполагает комплексный подход. Применяемые меры по обеспечению ИБ направленны на защиту информации и ее основных элементов. Они бывают технические и правовые. Первые – это аппаратные, а также программные средства защиты от внешних сетевых атак, вредоносного ПО и пр. Вторые – законодательные акты, приказы и другие нормативные документы, с помощью которых регламентируются правила обращения с защищаемой информацией.

Информационная безопасность дает гарантию того, что достигаются следующие цели:

- *конфиденциальность* информации (свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц);
- *целостность* информации и связанных с ней процессов (неизменность информации в процессе ее передачи или хранения);
- *доступность* информации, когда она нужна (свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц);
- *учет* всех процессов, связанных с информацией.

Обеспечение безопасности информации складывается из трех составляющих:

- Конфиденциальности,
- Целостности,
- Доступности.

Конфиденциальность, доступность и целостность представляют собой три наиболее важных свойства информации в рамках обеспечения ее безопасности (в английской литературе эта триада обозначается как CIA - confidentiality, integrity и availability):

- конфиденциальность информации - состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;
- целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- доступность информации - состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Точками приложения процесса защиты информации к информационной системе являются:

- аппаратное обеспечение,
- программное обеспечение
- обеспечение связи (коммуникации).

Сами процедуры(механизмы) защиты разделяются на:

- защиту физического уровня,
- защиту персонала
- организационный уровень.

Угроза безопасности компьютерной системы – это потенциально возможное происшествие (преднамеренное или нет), которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.

Угрозы информационной безопасности:

1. Уничтожение информационных объектов
2. Утечка информации
3. Искажение информации
4. Блокирование объекта информации

Анализ угроз проведенных агентством национальной ассоциацией информационной безопасности (National Computer Security Association) в 1998 г. в США выявил следующую статистику:

Рисунок – 1 Показатели основных информационных угроз

Объект защиты информации - информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации. Объекты защиты информации:

- Владельцы и пользователи
- Носители и средства обработки
- Системы связи и информатизации
- Объекты органов управления

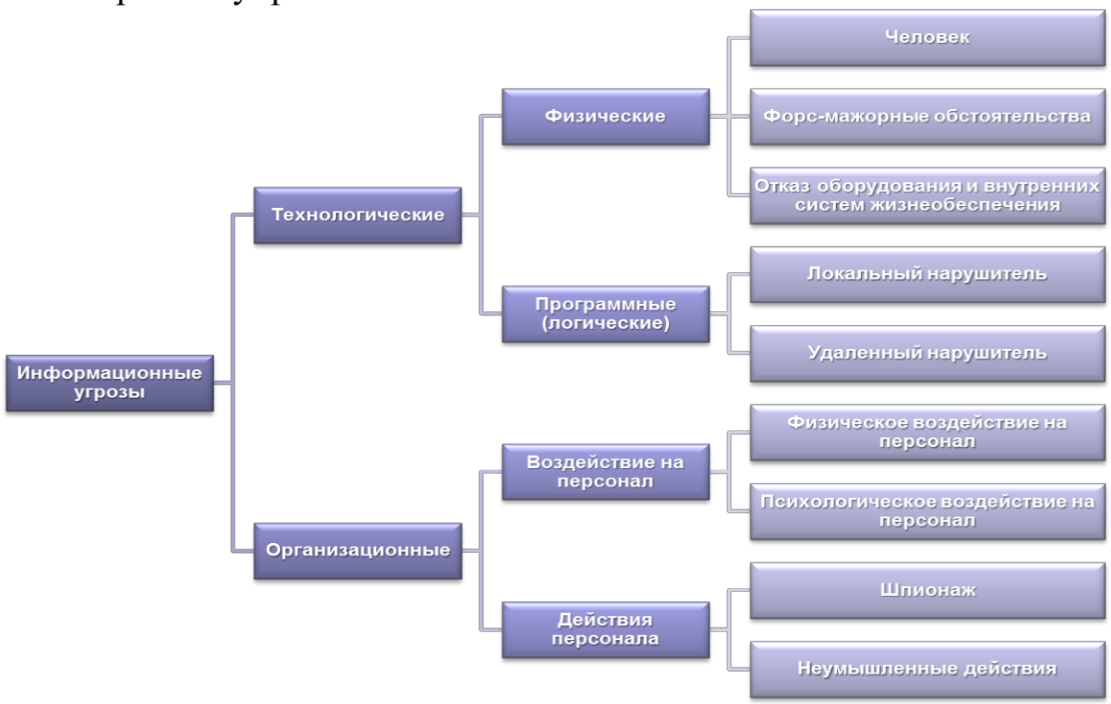

Рисунок – 2 Виды информационных угроз

Политика безопасности - это комплекс мер и активных действий по управлению и совершенствованию систем и технологий безопасности, включая информационную безопасность.

Организационная защита:

- *организация режима и охраны*.
- *организация работы с сотрудниками* (подбор и расстановка персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.)
- *организация работы с документами* и документированной информацией (разработка, использование, учет, исполнение, возврат, хранение и уничтожение документов и носителей конфиденциальной информации)
- *организация использования технических средств* сбора, обработки, накопления и хранения конфиденциальной информации;
- *организация работы по анализу внутренних и внешних угроз* конфиденциальной информации и выработке мер по обеспечению ее защиты;
- *организация работы по проведению систематического контроля за работой персонала* с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

Технические средства защиты информации

Для защиты периметра информационной системы создаются:

- системы охранной и пожарной сигнализации;
- системы цифрового видео наблюдения;
- системы контроля и управления доступом (СКУД).

Защита информации от ее утечки техническими каналами связи обеспечивается следующими средствами и мероприятиями:

- использованием экранированного кабеля и прокладка проводов и кабелей в экранированных конструкциях;
- установкой на линиях связи высокочастотных фильтров;
- построение экранированных помещений («капсул»);
- использование экранированного оборудования;
- установка активных систем зашумления;
- создание контролируемых зон.

Аппаратные средства защиты информации

- Специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
- Устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;

■ Схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.

■ Устройства для шифрования информации (криптографические методы).

■ Системы бесперебойного питания:

□ Источники бесперебойного питания;

□ Резервирование нагрузки;

□ Генераторы напряжения.

Программные средства защиты информации

■ Средства защиты от несанкционированного доступа (НСД):

□ Средства авторизации;

□ Мандатное управление доступом;

□ Избирательное управление доступом;

□ Управление доступом на основе ролей;

□ Журналирование (так же называется Аудит).

■ Системы анализа и моделирования информационных потоков (CASE-системы).

■ Системы мониторинга сетей:

□ Системы обнаружения и предотвращения вторжений (IDS/IPS).

□ Системы предотвращения утечек конфиденциальной информации (DLP-системы).

■ Анализаторы протоколов.

■ Антивирусные средства.

■ Межсетевые экраны.

■ Криптографические средства:

□ Шифрование;

□ Цифровая подпись.

■ Системы резервного копирования.

■ Системы аутентификации:

□ Пароль;

□ Ключ доступа (физический или электронный);

□ Сертификат;

□ Биометрия.

■ Инструментальные средства анализа систем защиты:

□ Мониторинговый программный продукт.

ВИДЫ АНТИВИРУСНЫХ ПРОГРАММ

■ Детекторы позволяют обнаруживать файлы, заражённые одним из нескольких известных вирусов. Некоторые программы-детекторы также выполняют эвристический анализ файлов и системных областей дисков, что

часто (но отнюдь не всегда) позволяет обнаруживать новые, не известные программе-детектору, вирусы.

■ Фильтры - это резидентные программы, которые оповещают пользователя о всех попытках какой-либо программы записаться на диск, а уж тем более отформатировать его, а также о других подозрительных действиях.

■ Программы-доктора или фаги не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние.

■ Ревизоры запоминают сведения о состоянии файлов и системных областей дисков, а при последующих запусках – сравнивают их состояние исходным. При выявлении несоответствий об этом сообщается пользователю.

■ Сторожа или фильтры располагаются резидентно в оперативной памяти компьютера и проверяют на наличие вирусов запускаемые файлы и вставляемые USB-накопители.

■ Программы-вакцины или иммунизаторы модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже заражёнными.

Недостатки антивирусных программ

■ Ни одна из существующих антивирусных технологий не может обеспечить полной защиты от вирусов.

■ Антивирусная программа забирает часть вычислительных ресурсов системы, нагружая центральный процессор и жёсткий диск. Особенно это может быть заметно на слабых компьютерах.

■ Антивирусные программы могут видеть угрозу там, где её нет (ложные срабатывания).

■ Антивирусные программы загружают обновления из Интернета, тем самым расходуя трафик.

■ Различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы не обнаруживаемыми антивирусным программным обеспечением. Для обнаружения этих «замаскированных» вирусов требуется мощный механизм распаковки, который может дешифровать файлы перед их проверкой. Однако во многих антивирусных программах эта возможность отсутствует и, в связи с этим, часто невозможно обнаружить зашифрованные вирусы.

Принципы обеспечения ИБ

- Системность
- Комплексность
- Непрерывность защиты
- Разумная достаточность

- Открытость алгоритмов защиты
- Простота применения защиты

Принцип системности. Учет всех элементов, условий, факторов при всех видах информационной деятельности, при всех режимах функционирования, на всех этапах функционального цикла,при всех видах взаимодействия с внешней средой.

Принцип комплексности. Согласование всех разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее элементов.

Принцип непрерывности. Принятие соответствующих мер защиты на всех этапах жизненного цикла ИС от разработки до завершения этапа функционирования.

Разумная достаточность. При достаточном времени и средствах преодолевается любая защита.Поэтому имеет смысл создавать только достаточный уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемы.

Гибкость системы защиты. Средства защиты должны варьироваться применительно к изменяющимся внешним условиям и требованиям к уровню защищенности ИС.

Открытость механизмов защиты. Знание алгоритмов защиты не должно давать средств и возможностей ее преодоления.Это не означает, что информация о системе защиты должна быть общедоступна-параметры системы должны быть также защищены.

Принцип простоты применения средств защиты. Механизмы защиты должны быть понятны и просты в использовании. Не должны использоваться специальные языки, малопонятные или трудоемкие для пользователя дополнительные действия.

Правильное сочетание и использование перечисленных выше мер является необходимым условием для обеспечения требуемого уровня защиты информации. Важно понимать, что ни одна из систем защиты информации не может обеспечить стопроцентную защиту. Построение системы защиты это всегда поиск компромисса между затратами на обеспечение информационной безопасности, требованиями регуляторов и уровнем риска, который обладатель информации готов принять.

Список использованной литературы

1. Adam Shostack. “Threat Modeling: Designing for Security”. Published by John Wiley & Sons, Inc., Canada 2014.- 626 p.

2. Richard Bejtlich. “The Practice of Network Security Monitoring”. Published by No Starch Press, Inc., USA 2013. – 380 p.

3. Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams and Abdul Aslam. “Enterprise Cybersecurity: how to build a successful Cyberdefense program against advanced threats”. Published by Apress, 2015. – 508 p.

4. Башлы П. Н. Информационная безопасность [Электронный учебник] : учебное пособие / Башлы П. Н.. - Евразийский открытый институт, 2012. - 311 c. - Режим доступа: http://iprbookshop.ru/10677