Лекция №1

1. **Розкрийте єдність та відміни у поняттях «дані» та «інформація».**

Термин данные происходит от слова data - факт, а информация (informatio) означает разъяснение, изложение, т.е. сведения или сообщение.

Данные - это совокупность сведений, зафиксированных на определенном носителе в форме, пригодной для постоянного хранения, передачи и обработки. Преобразование и обработка данных позволяет получить информацию.

Информация - это результат преобразования и анализа данных. Отличие информации от данных состоит в том, что данные - это фиксированные сведения о событиях и явлениях, которые хранятся на определенных носителях, а информация появляется в результате обработки данных при решении конкретных задач. Например, в базах данных хранятся различные данные, а по определенному запросу система управления базой данных выдает требуемую информацию.

2. **За якими признаками можна виконати класифікацію інформації (признаки информации)**
   - По объектам информационного взаимодействия:
   - По способу восприятия:
   - По форме представления:
   - По назначению
   - По значению
   - По истинности
3. **Назвіть основні властивості інформації (свойства информации)**

Объективность информации. Объективный — существующий вне и независимо от человеческого сознания. Информация — это отражение внешнего объективного мира. Информация объективна, если она не зависит от методов ее фиксации, чьего-либо мнения, суждения.

Достоверность информации. Информация достоверна, если она отражает истинное положение дел. Объективная информация всегда достоверна, но достоверная информация может быть как объективной, так и субъективной. Достоверная информация помогает принять нам правильное решение. Недостоверной информация может быть по следующим причинам:

a. преднамеренное искажение (дезинформация) или непреднамеренное искажение субъективного свойства;
b. искажение в результате воздействия помех («испорченный телефон») и недостаточно точных средств ее фиксации.

Полнота информации. Информацию можно назвать полной, если ее достаточно для понимания и принятия решений. Неполная информация может привести к ошибочному выводу или решению.

Точность информации определяется степенью ее близости к реальному состоянию объекта, процесса, явления и т. п.

Актуальность информации — важность для настоящего времени, злободневность, насущность. Только вовремя полученная информация может быть полезна.

Полезность (ценность) информации. Полезность может быть оценена применительно к нуждам конкретных ее потребителей и оценивается по тем задачам, которые можно решить с ее помощью.

4. **Розкрийте поняття «конфіденційна інформація»**

Конфиденциальная информация — информация, доступ к которой ограничен физическим или юридическим лицом, кроме субъектов властных полномочий, и которая может распространяться в определенном ими порядке по их желанию в соответствии с предусмотренными ими условиями. Не может быть отнесена к конфиденциальной информация, указанная в частях первой и второй статьи 13 настоящего Закона.

5. **Розкрийте поняття «службова інформація»**

Служебная информация - информация, которая содержится в документах субъектов властных полномочий, представляющих внутриведомственную служебную корреспонденцию, докладные записки, рекомендации, если они связаны с разработкой направления деятельности учреждения или осуществлением контрольных, надзорных функций органами государственной власти, процессом принятия решений и предшествуют публичному обсуждению и/или принятию решений;

6. **Розкрийте поняття «таємна інформація»**

   Секретная информация — информация, доступ к которой ограничивается, а разглашение которой может нанести вред лицу, обществу и государству. Секретной признается информация, содержащая государственную, профессиональную, банковскую тайну, тайну следствия и иную предусмотренную законом тайну.

7. **Дайте визначення поняттю «інформаційна безпека»**

   Информационная безопасность (англ. *information security*)[4] — все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчётности, аутентичности и достоверности информации или средств её обработки.

8. **Назвіть мету організації інформаційної безпеки**

   Целью организации информационной безопасности — исключение утечки информации и, таким образом, уменьшение или полное исключение возможности нанесения предприятию ущерба, к которому эта утечка может привести.

9. **Шо таке «захист інформації» та з чого це поняття складається**

   Защита информации — это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

   Объект защиты — информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

   Цель защиты информации — это желаемый результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

10. **Визначте основні проблеми захисту інформації**

    Основные проблемы защиты информации при работе в компьютерных сетях, можно условно разделить на три типа:

    - перехват информации (нарушение конфиденциальности информации),
    - модификация информации (искажение исходного сообщения или замена другой информацией),
    - подмена авторства (кража информации и нарушение авторского права).

11. **Назвіть й охарактеризуйте існуючі рівні інформаційної безпеки.**

    1. Программно-аппаратный уровень
    2. Процедурный уровень
    3. Административный уровень
    4. Законодательный уровень.

12. **Які методи забезпечення інформаційної безпеки є найбільш відомими?**

    - препятствие;
    - управление доступом
    - механизмы шифрования;
    - противодействие атакам вредоносных программ;
    - регламентация;
    - принуждение;
    - побуждение.

13. **Назвіть основні засоби захисту інформації**

Аппаратные средства – устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу.

Физические средства включают различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных действий. Примеры физических средств: замки на дверях, решетки на окнах, средства электронной охранной сигнализации и т.п.

Программные средства – это специальные программы и программные комплексы, предназначенные для защиты информации в ИС. Как отмечалось, многие из них слиты с ПО самой ИС.

Организационные средства осуществляют своим комплексом регламентацию производственной деятельности в ИС и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет проведения организационных мероприятий. Комплекс этих мер реализуется группой информационной безопасности, но должен находиться под контролем первого руководителя.

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические средства защиты включают всевозможные нормы поведения (которые традиционно сложились ранее), складываются по мере распространения ИС и ИТ в стране и в мире или специально разрабатываются.

Лекция №2

1.Перечислите Законодательные акты Украины в области ИБ

1) ЗУ «Про інформацію» від 2.10.1992
2) ЗУ «Про доступ до публічної інформації» від 13.01.2011
3) ЗУ «Про захист персональних даних» від 1 червня 2010 рок
4) ЗУ «Про державну таємницю» від 21 січня 1994 року
5) ЗУ «Про захист інформації в автоматизованих системах»,5.07.94 року N80/94-ВР
6) Положення про захист інформації в Національній системі масових електронних платежів N 119, 02.06.2008, Протокол, Національний банк України
7) «Про Доктрину інформаційної безпеки України»;Указ Президента України, 8 липня 2009 року 514
8) «Про положення про технічний захист інформації в Україні», Указ Президента України, 27.09.1999 № 1229/99

2.Укажите основу законодательных актов РФ в области ИБ

1) Конституция РФ непосредственно не регулирует отношения в области производства и применения новых информационных технологий, но создает предпосылки для такого регулирования, закрепляя права граждан (свободно искать, получать, передавать, производить и распространять информацию любым законным способом - ст. 29 ч. 4; на охрану личной тайны - ст. 24 ч. 1 и др.) и обязанности государства (ст. 24 ч. 2).
2) Доктрина информационной безопасности Российской Федерации утв. 9 сентября 2000 г
3) Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. N 149-ФЗ
4) Закон «Об информации, информатизации и защите информации» 1999 год
5) Закон «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.92 № 3523-1)
6) Закон «Об авторском праве и смежных правах» (от 09.07.93 № 5351-1)
7) Закон «О государственной тайне» (от 21.07.93 № 5485-1)
8) Федеральный закон «О связи» (от 16.02.95 № 15-ФЗ)
9) Федеральный закон «Об информации, информатизации и защите информации» (от 20.02.95 № 24-ФЗ)

3.Охарактеризуйте особенности Британского стандарта ИБ

[Документ "BS7799: Управление ИБ" состоит из двух частей.

В "Части 1: Практические рекомендации", 1995 г., определяются и рассматриваются следующие аспекты ИБ:

- *Политика безопасности.*
- *Организация защиты.*
- *Классификация и управление информационными ресурсами.*
- *Управление персоналом.*
- *Физическая безопасность.*
- *Администрирование компьютерных систем и сетей.*
- *Управление доступом к системам.*
- *Разработка и сопровождение систем.*
- *Планирование бесперебойной работы организации.*
- *Проверка системы на соответствие требованиям ИБ.*

"Часть 2: Спецификации системы", 1998 г. [9] , рассматривает эти же аспекты с точки зрения сертификации информационной системы на соответствие требованиям стандарта.] (Нагло сперто откуда-то)

BS 7799-1:2005 — Британский стандарт BS 7799 первая часть. BS 7799 Part 1 — Code of Practice for Information Security Management (Практические правила управления информационной безопасностью) описывает 127 механизмов контроля, необходимых для построения системы управления информационной безопасностью (СУИБ) организации, определённых на основе лучших примеров мирового опыта (best practices) в данной области. Этот документ служит практическим руководством по созданию СУИБ

BS 7799-2:2005 — Британский стандарт BS 7799 вторая часть стандарта. BS 7799 Part 2 — Information Security management — specification for information security management systems (Спецификация системы управления информационной безопасностью) определяет спецификацию

СУИБ. Вторая часть стандарта используется в качестве критериев при проведении официальной процедуры сертификации СУИБ организации.

BS 7799-3:2006 — Британский стандарт BS 7799 третья часть стандарта. Новый стандарт в области управления рисками информационной безопасности

4.Что такое «Оранжевая книга» и в чем заключаются ее основные особенности

«Оранжевая книга» - это критерии определения безопасности компьютерных систем содержащихся в компьютерной системе. Критерии используются для определения, классификации и выбора компьютерных систем, предназначенных для обработки, хранения и поиска важной или секретной информации. Оранжевая книга используется исключительно Министерством Обороны США.

Оранжевая книга, занимают центральное место среди публикаций «Радужной серии» Министерства обороны США.

5.Что такое классы безопасности? Охарактеризуйте их и укажите градацию

В Оранжевой книге критерии делятся на 4 раздела: D, C, B и A, из которых наивысшей безопасностью обладает раздел A. Каждый дивизион представляет собой значительные отличия в доверии индивидуальным пользователям или организациям. Разделы C, B и A иерархически разбиты на серии подразделов, называющиеся классами: C1, C2, B1, B2, B3 и A1. Каждый раздел и класс расширяет или дополняет требования указанные в предшествующем разделе или классе.

Уровни доверия

Классификация, введенная в «Оранжевой книге» (кратко):

- уровень C — произвольное управление доступом;
- уровень B — принудительное управление доступом;
- уровень A — верифицируемая безопасность.

Разделы безопасности:

D — Минимальная защита
C — Дискреционная защита
B — Мандатная защита
A — Проверенная защита

Подразделяются на классы. Классов безопасности всего шесть — C1, C2, B1, B2, B3, A1 (перечислены в порядке ужесточения требований).

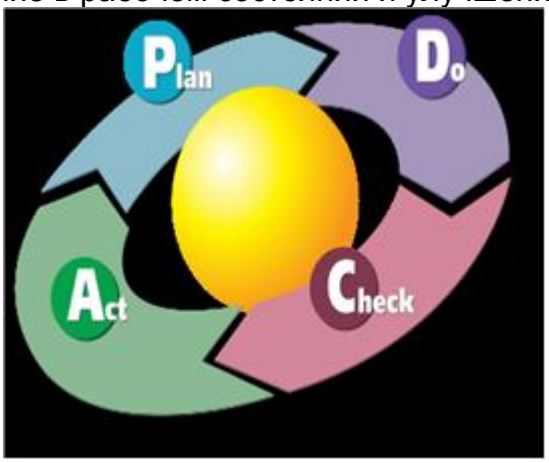
6. Стандарт 27000. Структура, содержание, назначение стандартов.

ISO/IEC 27000 *- Серия стандартов по менеджменту информационной безопасности Разрабатывается техническим комитетом* ***ISO/IEC JTC 1*** *подкомитетом* ***SC 27****.*

Содержит в себе требования по реализации и совершенствованию систем управления защитой информации и основывается на модели

PDCA(Plan-Do-Check-Act):

- планируй — идентификация активов, менеджмент рисков;
- делай — этап реализации соответствующих мер по управлению безопасностью;
- проверяй — мониторинг и анализ;
- действуй — поддержание в рабочем состоянии и улучшение.



включает в себя следующие документы:

ISO/IEC 27001:2013 Information security management systems. Requirements — Система менеджмента информационной безопасностью. Требования.

ISO/IEC 27000:2014 Information security management systems. Overview and vocabulary — Система менеджмента информационной безопасности. Обзор и терминология.

ISO/IEC 27002:2013 Code of practice for information security management — Практические правила по управлению информационной безопасностью.

ISO/IEC 27003:2010 Information Security Management Systems Implementation Guidance — Руководство по внедрению системы менеджмента информационной безопасностью.

ISO/IEC 27004:2009 Information security management. Measurement — Измерение эффективности системы менеджмента информационной безопасностью.

ISO/IEC 27005:2011 Information security risk management — Управление рисками информационной безопасности.

ISO/IEC 27006:2011 Requirements for bodies providing audit and certification of information security management systems — Требования к органам аудита и сертификации систем менеджмента информационной безопасностью.

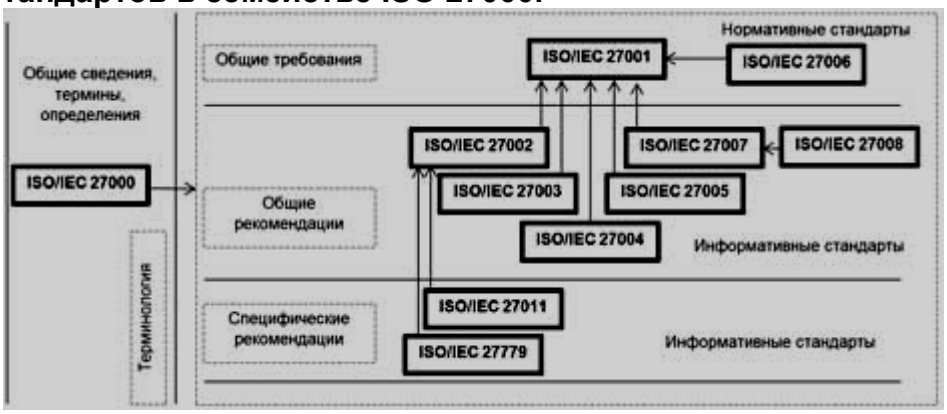
ISO/IEC 27007:2011 Guidelines for Information Security Management Systems auditing (FCD) — Руководство для аудита **СМИБ**.

ISO/IEC 27008:2011 Guidance for auditors on ISMS controls (DRAFT) — Руководство по аудиту механизмов контроля **СМИБ**.

ISO/IEC 27011:2008 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 — Руководство по управлению информационной безопасностью для телекоммуникаций на основе**ISO/IEC 27002**.

ISO/IEC 27799:2008 Information security management in health using ISO/IEC 27002 — Руководство по управлению информационной безопасностью для организаций здравоохранения на основе **ISO/IEC 27002**.

Взаимосвязь стандартов в семействе ISO 27000.



Выполнение требований стандарта I**SO/IEC 27001** главным образом позволяет минимизировать риски потерь активов предприятия/организации, а следовательно сократить финансовые потери.

Стандарт **ISO/IEC 27001** предназначен для сертификации систем информационной безопасности.

Сертификация системы менеджмента информационной безопасностью (сертификация СМИБ) — это эффективное управление бизнес-процессами предприятия/организации, информационными рисками, а также свидетельство о устойчивой, развивающийся и надежной компании, что в свою очередь дает позитивное отношение бизнес-партнеров.

СМИБ в соответствии со стандартом **ISO/IEC 27001** — это часть общей системы менеджмента компании.

Лекция № 3

1. Дайте определение и раскройте понятие «Угроза информационной безопасности»

Угроза информационной безопасности (ИБ) – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Цепочка:

источник угрозы - **фактор** (уязвимость) - **угроза** (действие) - **последствия** (атака).

Источник угрозы - это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

Угроза (действие) - это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и потери информации.

Фактор (уязвимость) - это присущие объекту информатизации причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации.

Последствия (атака) - это возможные последствия реализации угрозы (возможные действия) при взаимодействии источника угрозы через имеющиеся факторы (уязвимости).

2. Классификация угроз. Типы классификаций. Примеры

Угрозы информационной безопасности могут быть классифицированы по различным признакам:

- По аспекту информационной безопасности, на который направлены угрозы:
  - *Угрозы конфиденциальности* (неправомерный доступ к информации).
  - *Угрозы целостности* (неправомерное изменение данных).
  - *Угрозы доступности* (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы).
- По степени преднамеренности действий:
  - *Случайные* (неумышленные действия, например, сбои в работе систем, стихийные бедствия).
  - *Преднамеренные* (умышленные действия, например, шпионаж и диверсии).
- По расположению источника угроз:
  - *Внутренние* (источники угроз располагаются внутри системы).
  - *Внешние* (источники угроз находятся вне системы).
- По размерам наносимого ущерба:
  - *Общие* (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба).
  - *Локальные* (причинение вреда отдельным частям объекта безопасности).
  - *Частные* (причинение вреда отдельным свойствам элементов объекта безопасности).
- По степени воздействия на информационную систему:
  - *Пассивные* (структура и содержание системы не изменяются).
  - *Активные* (структура и содержание системы подвергается изменениям).

3. Угрозы доступности. Особенности, виды, примеры.

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**. Под пользователями в данном случае мы понимаем широкий круг персонала, работающего с системой: операторы, программисты, администраторы и т.д.
- **Непреднамеренные ошибки.** Непреднамеренная ошибка может вызвать непосредственно порчу данных или средств доступа либо создать условия для реализации другой угрозы, например вторжения злоумышленника.

- **Внутренний отказ информационной системой.** Причиной нежелания может, например, быть необходимость освоения новых возможностей системы или несоответствие системы запросам пользователей.
- **Невозможность работать с системой.** Причиной невозможности работать с системой может быть как отсутствие соответствующей подготовки персонала, так и отсутствие необходимой документации по системе.

4. Угрозы целостности. Особенности, виды, примеры

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.

5. Угрозы конфиденциальности. Особенности, виды, примеры

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.

Активное прослушивание - нарушение атомарности транзакций, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.).

6. Внешние и внутренние угрозы. Раскрыть суть понятия и привести примеры

Внешние угрозы возникают благодаря непосредственной деятельности недобросовестных конкурентов, преступных элементов, иностранных разведывательных служб, из-за неумелой постановки взаимоотношений с представителями государственных структур, общественных организаций, средств массовой информации. Действия извне могут быть направлены на пассивные носители информации следующими способами:

- похищение или снятие копий с различных носителей информации;
- снятие информации в процессе коммуникации;
- снятие информации в процессе её передачи по сети связи;
- уничтожение информации или повреждение ее носителей;
- случайное или преднамеренное доведение до сведения конкурентов документов и материалов, содержащих секретную информацию.

Действия извне могут быть также направлены на персонал компании и выражаться в формах:

- подкупа
- шантажа
- выведывания с целью получения информации
- переманивания ведущих специалистов на конкурирующую фирму и т. п.

Большинство инцидентов информационной безопасности связано с воздействием **внутренних угроз** – утечки и кражи информации, утечки коммерческой тайны и персональных данных клиентов организации, ущерб информационной системе связаны, как правило, с

действиями сотрудников этой организации. В классификации внутренних угроз в первую очередь можно выделить две большие группы – совершаемые из корыстных или других злонамеренных соображений, и совершаемые без злого умысла, по неосторожности или технической некомпетентности.

Преступления сотрудников, способных причинить вред сохранности интеллектуальной и коммерческой собственности организации (их принято называть «инсайдерами») можно разделить на категории злонамеренного инсайда и непредумышленного инсайда. Злоумышленным инсайдером могут стать:

- Сотрудники, затаившие злобу на компанию-работодателя («обиженные»). Такие инсайдеры действуют исходя из мотивов личной мести, причин для которой может быть масса – от увольнения/понижения в должности до отказа компании предоставить статусные атрибуты, например, ноутбук или расширенный соцпакет.
- Нечистые на руку сотрудники, стремящиеся подзаработать за счёт компании-работодателя. Такими инсайдерами становятся сотрудники, использующие секретные информационные ресурсы компании для собственной выгоды. Базы данных клиентов, интеллектуальная собственность компании, состав коммерческой тайны – такая информация может использоваться инсайдером в личных интересах, либо продаваться конкурентам.
- Внедрённые и завербованные инсайдеры. Самый опасный и самый трудно-идентифицируемый тип внутренних злоумышленников. Как правило, являются звеном преступной цепочки или членом организованной преступной группы. Такие сотрудники имеют достаточно высокий уровень доступа к конфиденциальной информации, ущерб от их действий может стать фатальным для компании.

Лекция № 4

1. **Раскрыть понятие Риски информационной безопасности. Дать определение.**

ISO 27005 конкретизирует понятие информационного риска , раскладывая его на активы, угрозы, уязвимости и ущерб. Согласно ISO 27005: “Риск ИБ - это потенциальная возможность использования уязвимостей актива или группы активов конкретной угрозой для причинения ущерба организации.”.

> Понятие риска, данное в ISO 27005, пожалуй, является наиболее полным. Однако можно оперировать и более простыми и легко запоминающимися определениями. Например, риск можно рассматривать просто как потенциальную проблему либо как вероятные потери организации в результате инцидентов. В стандарте Банка России СТО БР ИББС риск определяется как «неопределенность, предполагающая возможность потерь».
>
> Таким образом, риск является комплексной величиной, всегда определяемой через комбинацию ряда других величин. Это обусловливает ошибки в определении и описании конкретных рисков, нередко допускаемые даже специалистами, что вызывает трудности при оценке рисков.
>
> Описание факторов риска, таких как угрозы, инциденты, уязвимости и виды ущерба, по отдельности не является описанием риска. О риске можно говорить только в том случае, если все факторы риска рассматриваются в совокупности. Только комбинация оценочных значений для угроз, уязвимостей и ущерба позволяет получить оценку риска.

2. **Единство и различие понятий Риск и Угроза информационной безопасности**

Риск ИБ - это потенциальная возможность использования уязвимостей актива или группы активов конкретной угрозой для причинения ущерба организации.

Угроза ИБ — совокупность условий и факторов, создающих опасность нарушения ИБ. Под угрозой (в общем) понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.

В сценарном анализе «риск» отличают от «угрозы». Угроза — это неисследованное негативное событие, которое некоторые аналитики могут быть неспособными оценить при оценке риска, потому что это событие никогда не происходило, и для которого не доступна никакая информация о эффективных профилактических мерах (шаги, предпринимаемые, чтобы уменьшить вероятность или воздействие возможного будущего события). Это различие наиболее ясно иллюстрируется предупредительным принципом, который стремится уменьшить угрозу, требуя от неё быть сведённой к набору хорошо-определённых рисков, чтобы только затем перейти к действиям, проектам, новшествам или экспериментам. Примеры угрозы:

a. природные катастрофы: землетрясение, наводнение, цунами, извержение вулкана, лесные пожары;
b. антропогенные катастрофы: ядерная угроза, экологическая угроза.

Пример риска:

- природные катастрофы: цунами, по результатам анализа возможно произойдет с вероятностью не более 1 раз в 100 лет. Высота волны в зоне воздействия будет не более 10 баллов по шкале Рихтера, что приведет к разрушению забора предприятия по периметру на расстоянии 15 метров и края левого крыла склада хранения стройматериалов № 3 (см. прилагаемую схему). Общий ущерб, с учетом возможного загрязнения окружающей среды, составит не более 173 тыс. рублей в действующих ценах. Потери среди персонала возможны, только при грубом нарушении правил действия в условиях чрезвычайной ситуации. Идентификация чрезвычайной ситуации произойдет минимум за 15 минут, а оповещение персонала за 12 мин. 30 сек. Вероятность потерь личного состава на одного сотрудника H=1x10-12 … Приложение. План мероприятий по снижению уровня указанного риска и смета затрат.

- **Информационный риск**. В информационной безопасности риск определяется как функция трёх переменных:
  1. Вероятность существования угрозы.
  2. Вероятность существования незащищённости.
  3. Потенциальное воздействие.

Если любая из этих переменных приближается к нулю, полный риск приближается к нулю.

Схожесть понятий в том, что они оба отождествляют некий неблагоприятный исход для организации. Только угроза - это описание самой ситуации и исхода, а риск - ее качественная или количественная оценка.

3. **Способы оценки (измерения) риска. Механизмы оценивания.**

Количественный метод

Количественная оценка рисков применяется в ситуациях, когда исследуемые угрозы и связанные с ними риски можно сопоставить с конечными количественными значениями, выраженными в деньгах, процентах, времени, человекоресурсах и проч. Метод позволяет получить конкретные значения объектов оценки риска при реализации угроз информационной безопасности.

При количественном подходе всем элементам оценки рисков присваивают конкретные и реальные количественные значения. Алгоритм получения данных значений должен быть нагляден и понятен. Объектом оценки может являться ценность актива в денежном выражении, вероятность реализации угрозы, ущерб от реализации угрозы, стоимость защитных мер и прочее.

Как провести количественную оценку рисков?

1. Определить ценность информационных активов в денежном выражении.
2. Оценить в количественном выражении потенциальный ущерб от реализации каждой угрозы в отношении каждого информационного актива.
3. Определить вероятность реализации каждой из угроз ИБ.
4. Определить общий потенциальный ущерб от каждой угрозы в отношении каждого актива за контрольный период (за один год).
5. Провести анализ полученных данных по ущербу для каждой угрозы.

Принять риск — значит осознать его, смириться с его возможностью и продолжить действовать как прежде. Применимо для угроз с малым ущербом и малой вероятностью возникновения.

Снизить риск — значит ввести дополнительные меры и средства защиты, провести обучение персонала и т д. То есть провести намеренную работу по снижению риска. При этом необходимо произвести количественную оценку эффективности дополнительных мер и средств защиты. Все затраты, которые несет организация, начиная от закупки средств защиты до ввода в эксплуатацию (включая установку, настройку, обучение, сопровождение и проч.), не должны превышать размера ущерба от реализации угрозы.

Перенести риск — значит переложить последствия от реализации риска на третье лицо, например с помощью страхования.

В результате количественной оценки рисков должны быть определены:

- ценность активов в денежном выражении;
- полный список всех угроз ИБ с ущербом от разового инцидента по каждой угрозе;
- частота реализации каждой угрозы;
- потенциальный ущерб от каждой угрозы;
- рекомендуемые меры безопасности, контрмеры и действия по каждой угрозе.

Качественный метод

При качественном подходе не используются количественные или денежные выражения для объекта оценки. Вместо этого объекту оценки присваивается показатель, проранжированный по трехбалльной (низкий, средний, высокий), пятибалльной или десятибалльной шкале (0… 10). Для сбора данных при качественной оценке рисков применяются опросы целевых групп, интервьюирование, анкетирование, личные встречи.

Как провести качественную оценку рисков:

1. Определить ценность информационных активов.

Ценность актива можно определить по уровню критичности (последствиям) при нарушении характеристик безопасности (конфиденциальность, целостность, доступность) информационного актива.

2. Определить вероятность реализации угрозы по отношению к информационному активу.

Для оценки вероятности реализации угрозы может использоваться трехуровневая качественная шкала (низкая, средняя, высокая).

3. Определить уровень возможности успешной реализации угрозы с учетом текущего состояния ИБ, внедренных мер и средств защиты.

4. Сделать вывод об уровне риска на основании ценности информационного актива, вероятности реализации угрозы, возможности реализации угрозы.

5. Провести анализ полученных данных по каждой угрозе и полученному для нее уровню риска.

Часто группа анализа рисков оперирует понятием «приемлемый уровень риска». Это уровень риска, который компания готова принять (если угроза обладает уровнем риска меньшим или равным приемлемому, то она не считается актуальной). Глобальная задача при качественной оценке — снизить риски до приемлемого уровня.

6. Разработать меры безопасности, контрмеры и действия по каждой актуальной угрозе для снижения уровня риска.

Количественный метод дает наглядное представление в деньгах по объектам оценки (ущербу, затратам), однако он более трудоемок и в некоторых случаях неприменим.

Качественный метод позволяет выполнить оценку рисков быстрее, однако оценки и результаты носят более субъективный характер и не дают наглядного понимания ущерба, затрат и выгод от внедрения СЗИ.

Выбор метода следует делать исходя из специфики конкретной компании и задач, поставленных перед специалистом.

4. **Понятия допустимого, недопустимого и остаточного риска. Примеры.**

Приемлемый (допустимый) риск – это такая минимальная величина риска, которая достижима по техническим, экономическим и технологическим возможностям. Таким образом, приемлемый риск сочетает в себе технические, экономические, социальные и политические аспекты и представляет собой некоторый компромисс между уровнем безопасности и возможностями ее достижения.

Допустимый риск — это риск, потери по которому не превышают расчётной суммы прибыли по осуществляемой операции.

Пример: риск внутреннего мошенничества. Допустим, в некий банк было установлено новое ПО для обработки транзакций. ПО было с уязвимостями. Работники банка прознали об уязвимостях и редко стали из использовать. Воровать много они не станут, ибо их заметят и уволят. Такой риск существует во всех банках и его допускают до момента исправления, который наступает не в особо срочном порядке.

Недопустимый (неприемлемый) риск - уровень риска, установленный административными или регулирующими органами как максимальный, при достижении которого необходимо принять меры по его устранению.

Пример: ситуация та же, как и в прошлом примере. Произошла утечка информации об этой уязвимости. На этот раз с помощью выявленной бреши в ПО злоумышленники украли солидную сумму у банка. В таком случае риск переходит в категорию недопустимого.

Остаточный риск - риск, остающийся после обработки риска нарушения ИБ.

Пример: уязвимость из прошлого примера исправили, но все еще существует риск атаки на систему извне.

5. **Способы количественной оценки величины риска. Суммарный и интегральный риски.**

Количественная оценка рисков определяет вероятность возникновения рисков и влияние последствий рисков на проект, что помогает группе управления проектами верно принимать решения и избегать неопределенностей. Количественная оценка рисков позволяет определять:

- Вероятность достижения конечной цели проекта
- Степень воздействия риска на проект и объемы непредвиденных затрат и материалов, которые могут понадобиться.

- Риски, требующие скорейшего реагирования и большего внимания, а также влияние их последствий на проект.
- Фактические затраты, предполагаемые сроки окончания.

Количественная оценка рисков часто сопровождает качественную оценку и также требует процесс идентификации рисков. Количественная и количественная оценка рисков могут использоваться по отдельности или вместе, в зависимости от располагаемого времени и бюджета, необходимости в количественной или качественной оценке рисков.

Методология количественной оценки рисков основывается на вероятностях исходных событий, сценариях развития инцидентов с возможными последствиями и соответствующими вероятностями их реализации. В соответствии с этой методологией возможны следующие методы количественной оценки рисков.

1. Статистические методы — предполагается определение вероятности реализации угрозы для рассматриваемого информационного актива за интервал времени на основе выполнения следующих требований: — объекты, к анализу которых предполагается использовать статистику, и объекты, на которых собрана статистика, являются эквивалентными (требование эквивалентности объектов); — условия, при которых предполагается использовать статистику, и условия ее сбора являются эквивалентными (требование эквивалентности условий); — объемы выборок статистики являются достаточными, методы обработки — корректными, а источники сведений — заслуживающими доверия (требование убедительности). К недостаткам этой группы методов следует отнести критичность к исход- ным данным, которые, как правило, или отсутствуют, или их недостаточно для построения корректных выводов.

2. Вероятностно-статистические методы используют привлечение дополнительной информации о распределении ущербов в случае реализации угрозы безопасности информационного актива. Предполагается, что для рассматриваемых условий функционирования организационно-технической системы предприятия известна функция распределения ущерба инцидентов информационной безопасности. На ее основе определяется доля катастрофических событий от общего чис- ла негативных событий. Считая эту долю постоянной либо прогнозируя по временному ряду ее значение на заданный момент времени, можно определить вероятностные характеристики катастрофических событий. При этом точность и достоверность результатов, полученных с применением вероятностно-статистических методов, определяется качеством и объемом дополнительной информации о распределении ущербов. Количественная оценка рисков безопасности информации на основе пробит-анализа ISSN 1560-9189 Реєстрація, зберігання і обробка даних, 2010, Т. 12, № 3 87

3. Теоретико-вероятностные методы используются для определения частот или вероятностей реализации редких угроз безопасности информации со значительными последствиями, по которым статистика практически отсутствует. В основе этого метода лежат закономерности перерастания инициирующих событий в чрезвычайные, декомпозиция задачи, оценки частных показателей и определение частоты редких негативных событий с учетом взаимосвязи частных показателей. Теоретико-вероятностный метод достаточно трудоемок, имеет низкую точность и достоверность получаемых в процессе исследования результатов, но при отсутствии других оценок его применение оправдано.

4. Экспертные методы основываются на знаниях и опыте экспертов. Эти методы

целесообразно применять в том случае, когда отсутствуют статистические данные. При этом экспертам предлагается ответить на вопросы о состоянии или будущем поведении информационных активов, характеризующихся неопределенными параметрами или неизученными свойствами. Для интерпретации или математической обработки экспертных данных можно использовать математический аппарат теории нечетких множеств.

Сложность анализа рисков безопасности информации экспертным методом связана, прежде всего, с неопределенностью характеристик массивов данных, на базе которых сформирован опыт эксперта и, как следствие, с отсутствием гарантий получения достоверных результатов.

Таким образом, можно констатировать наличие существенных ограничений в применении известных методов количественной оценки рисков в сфере безопасности информации, в связи с чем поиск новых подходов, обеспечивающих решение задач определения характеристик вероятности (случайности) безопасности информации в условиях недостаточных статистик, представляет собой актуальную задачу.

Одним из важных показателей уровня безопасности информации в информационной системе (ИС) организации, позволяющем в совокупности учесть влияние всего множества актуальных для данной ИС угроз, является обобщенный риск R, называемый также **интегральным риском.** Нахождение обобщенного риска – завершающий этап процесса анализа и оценивания рисков (АОР), в ходе которого результаты АОР, представленные профилем рисков, отображаются в скалярный показатель R. Очевидно, что как структура обобщенного риска, так и процедура его вычисления должны обеспечивать объективность и корректность производимого отображения. Однако корректность именно этих аспектов оценивания рисков часто оказывается под вопросом. Рассмотрим проблемы, возникающие при применении одной из наиболее распространенных форм показателя обобщенного риска, называемой суммарным риском:

$$R_{\Sigma} = \sum_{i=1}^{n} r_i = \sum_{i=1}^{n} p_i q_i,$$

где:

r – значение риска, обусловленное возможным влиянием некоторого негативного фактора v, вероятность реализации которого – p

q - потери организации, возникающие в случае реализации воздействия этого фактора на объект риска, в данном случае – на ИС организации.

Логику возникновения и развития негативных воздействий на ИС в общем случае можно описать следующей схемой:

опасности среды функционирования ИС ⇒ воздействие опасных явлений и процессов на элементы ИС ⇒ угрозы информационным активам ИС ⇒ атаки уязвимостей ИС ⇒ потери организации, обусловленные реализацией угроз.

При этом в ходе АОР рассчитывается три вида рисков: риски атак, реализующие или иную угрозу, риски отдельных угроз и обобщенный риск R, обусловленный опасностями среды функционирования ИС (т.е. совместными действиями всей совокупности угроз, генерируемых средой функционирования ИС). Если воспользоваться формулой (1) для расчета риска, связанного с влиянием некоторой угрозы t, которая может быть реализована любой успешной атакой из множества , получим следующее выражение:

$$\mathbf{A}=\{\alpha_j\}, \quad j=\overline{1,k_i},$$

$$r_i = \sum_{j=1}^{k_i} \rho_j = \sum_{j=1}^{k_i} p_{aj} q_i = q_i \sum_{j=1}^{k_i} p_{aj}, \qquad (2)$$

где $\rho_j = p_{aj} q_i$ – частный риск, обусловленный успехом атаки α_j, позволяющей реализовать угрозу t_i, используя уязвимость v_j, p_{aj} – вероятность успешного завершения атаки α_j. Соотношение (2) выведено в предположении, что реализация угрозы t_i посредством любой из атак $\{\alpha_j\}$, $j = \overline{1, k_i}$, ведет к одной и той же величине потерь q_i. При этом, учитывая, что для произвольной вероятности p_{aj} справедливо неравенство $0 \le p_{aj} \le 1$, очевидно утверждение:

$$0 \le \sum_{j=1}^{k_i} p_{aj} \le k_i. \qquad (3)$$

С другой стороны, т.к. риск, обусловленный возможной реализацией угрозы t_i, определяется формулой:

$$r_i = q_i p_{ti}, \qquad (4)$$

из сопоставления выражений (2) и (4) вытекает равенство:

$$p_{ti} = \sum_{j=1}^{k_i} p_{aj}, \qquad (5)$$

из которого, принимая во внимание, что значение вероятностного параметра p_{ti} не может превышать 1, следует ошибочность правого неравенства в утверждении (3). Причину возникновения этого противоречия можно выяснить, описав ситуацию <угроза t_i / атаки > с позиций теории вероятностей.

Лекция №5

1. Сущность мероприятий по управлению рисками

Использование информационных систем связано с определенной совокупностью рисков. Когда риск (возможный ущерб) неприемлемо велик, необходимо принять экономически оправданные защитные меры. Периодическая (пере)оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

С количественной точки зрения размер риска является функцией вероятности реализации определенной угрозы (использующей некоторые уязвимости), а также величины возможного ущерба.

Таким образом, суть работы по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры по уменьшению этого размера и затем убедиться, что риски заключены в приемлемые рамки (и остаются таковыми). Следовательно, управление рисками включает в себя два вида деятельности, которые чередуются циклически:

- (пере)оценку (измерение) рисков;
- выбор эффективных и экономичных защитных средств (нейтрализация рисков).

По отношению к выявленным рискам возможны следующие действия:

- ликвидация риска (например, за счет устранения причины);
- уменьшение риска (например, за счет использования дополнительных защитных средств);
- принятие риска (и выработка плана действия в соответствующих условиях);
- переадресация риска (например, путем заключения страхового соглашения).

2. Этапы управления рисками

Процесс управления рисками можно подразделить на следующие этапы:

1) выбор анализируемых объектов и уровня детализации их рассмотрения;
2) выбор методики оценки рисков;
3) идентификация активов;
4) анализ угроз и их последствий, определение уязвимостей в защите;
5) оценка рисков;
6) выбор защитных мер;
7) реализация и проверка выбранных мер;
8) оценка остаточного риска.

Этапы (6) и (7) относятся к выбору защитных средств (нейтрализации рисков), остальные — к оценке рисков.

Уже перечисление этапов показывает, что управление рисками — процесс циклический. По существу, последний этап — это оператор конца цикла, предписывающий вернуться к началу. Риски нужно контролировать постоянно, периодически проводя их переоценку. Отметим, что добросовестно выполненная и тщательно документированная первая оценка может существенно упростить последующую деятельность.

Первые три этапа процесса управления рисками можно считать подготовительными. Их суть состоит в следующем.

Выбор анализируемых объектов и уровня детализации их рассмотрения — первый шаг в оценке рисков. Для небольшой организации допустимо рассматривать всю информационную инфраструктуру; однако, если организация крупная, всеобъемлющая оценка может потребовать неприемлемых затрат времени и сил. В таком случае следует сосредоточиться на наиболее важных сервисах, заранее соглашаясь с приблизительностью итоговой оценки. Если важных сервисов все еще много, выбираются те из них, риски для которых заведомо велики или неизвестны.

По многим причинам целесообразно создать карту информационной системы организации. Для управления рисками подобная карта особенно важна, поскольку она наглядно показывает, какие сервисы выбраны для анализа, а какими было решено пренебречь. Если ИС меняется, а карта поддерживается в актуальном состоянии, то при переоценке рисков сразу станет ясно, какие новые или существенно изменившиеся сервисы нуждаются в рассмотрении.

Вообще говоря, уязвимым является каждый компонент информационной системы — от куска сетевого кабеля, который могут прогрызть мыши, до базы данных, которая может быть разрушена из-за неумелых действий администратора. Как правило, в сферу анализа невозможно включить каждый винтик и каждый байт. Приходится останавливаться на некотором уровне детализации, отдавая себе отчет в приблизительности оценки. Для новых систем предпочтителен детальный

анализ; старая система, подвергшаяся небольшим модификациям, может быть проанализирована более поверхностно.

Управление рисками — процесс далеко не линейный. Практически все его этапы связаны между собой, и по завершении почти любого из них может выявиться необходимость возврата к предыдущему. Так, при идентификации активов может появиться понимание, что выбранные границы анализа следует расширить, а степень детализации — увеличить. Особенно труден первичный анализ, когда многократные возвраты к началу неизбежны.

3. Управление рисками и жизненный цикл информационной системы

Управление рисками, как и любую другую деятельность в области информационной безопасности, необходимо интегрировать в жизненный цикл ИС. Тогда эффект оказывается наибольшим, а затраты — минимальными. Можно выделить пять основных этапов жизненного цикла ИС:

- инициация;
- закупка (разработка);
- установка;
- эксплуатация;
- выведение из эксплуатации.

Кратко опишем, что может дать управление рисками на каждом из перечисленных этапов.

На этапе инициации известные риски следует учесть при выработке требований к системе вообще и средствам безопасности в частности.

На этапе закупки (разработки) выявленные риски способны помочь при выборе архитектурных решений, играющих ключевую роль в обеспечении безопасности.

На этапе установки выявленные риски следует учитывать при конфигурации, тестировании и проверке ранее сформулированных требований, а полный цикл управления рисками должен предшествовать внедрению системы в эксплуатацию.

На этапе эксплуатации управление рисками должно сопровождать все существенные изменения в системе.

При выведении системы из эксплуатации управление рисками помогает убедиться в том, что миграция данных происходит безопасным образом.

Лекция №6

1. Особенности анализа и управления рисками информационных систем компаний с помощью метода CRAMM.

Текущая версия CRAMM 5 , соответствует стандарту BS 7799 (ISO 17799).

Целью разработки метода являлось создание формализованной процедуры, позволяющей:

- убедиться, что требования, связанные с безопасностью, полностью проанализированы и документированы;
- избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков;
- оказывать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем;
- обеспечить проведение работ в сжатые сроки;
- автоматизировать процесс анализа требований безопасности;
- представить обоснование для мер противодействия;
- оценивать эффективность контрмер, сравнивать различные их варианты;
- генерировать отчеты.

Концепция, положенная в основу метода

Анализ рисков включает идентификацию и вычисление уровней (мер) рисков на основе оценок, присвоенных ресурсам, угрозам и уязвимостям ресурсов.

Контроль рисков состоит в идентификации и выборе контрмер, благодаря которым удается снизить риски до приемлемого уровня.

Формальный метод, основанный на этой концепции, позволяет убедиться, что защита охватывает всю систему и существует уверенность в том, что:

- все возможные риски идентифицированы;
- уязвимости ресурсов идентифицированы и их уровни оценены;
- угрозы идентифицированы и их уровни оценены;
- контрмеры эффективны;
- расходы, связанные с ИБ, оправданы.

Исследование ИБ системы с помощью CRAMM проводится в несколько этапов.

На первой стадии, Initiation, производится формализованное описание границ информационной системы, ее основных функций, категорий пользователей, а также персонала, принимающего участие в обследовании.

Риск определяется как – возможность потерь в результате какого-либо действия или события, способного нанести ущерб.

На стадии идентификации и оценки ресурсов, Identification and Valuation of Assets, описывается и анализируется все, что касается идентификации и определения ценности ресурсов системы. В конце этой стадии заказчик исследования будет знать, удовлетворит ли его существующая традиционная практика или он нуждается в проведении полного анализа рисков. В последнем случае будет построена модель информационной системы с позиции информационной безопасности.

Критерии оценки ценности ресурсов:

- Ущерб для репутации организации
- Безопасность персонала
- Разглашение персональных сведений
- Разглашение коммерческих сведений
- Неприятности со стороны правоохранительных органов
- Финансовые потери
- Невозможность нормальной работы организации

Стадия оценивания угроз и уязвимостей, Threat and Vulnerability Assessment, не является обязательной, если заказчика удовлетворит базовый уровень информационной безопасности. Эта стадия выполняется при проведении полного анализа рисков. Принимается во внимание все, что относится к идентификации и оценке уровней угроз для групп ресурсов и их уязвимостей. В конце стадии заказчик получает идентифицированные и оцененные уровни угроз и уязвимостей для своей системы.

Основные шаги:

- Идентификация угроз ресурсов и возможных уязвимостей.
- Группировка по угрозам или воздействиям с целью минимизации объема работы по анализу рисков.
- Измерение рисков.
- Получение отчета и обсуждение результатов с заказчиками.
- Коррекция по результатам обсуждения.

Оценка риска выполняется по двум факторам: вероятность реализации и размер ущерба.

$$Риск = P_{реализации} \cdot Ущерб$$

Дальнейшая детализация вероятности реализации

$$P_{реализации} = P_{угрозы} \cdot P_{уязвимости}$$

Угроза – действие или событие, способное нанести ущерб безопасности.

Уязвимость – слабость в защите ресурса или группы ресурсов, допускающая возможность реализации угрозы.

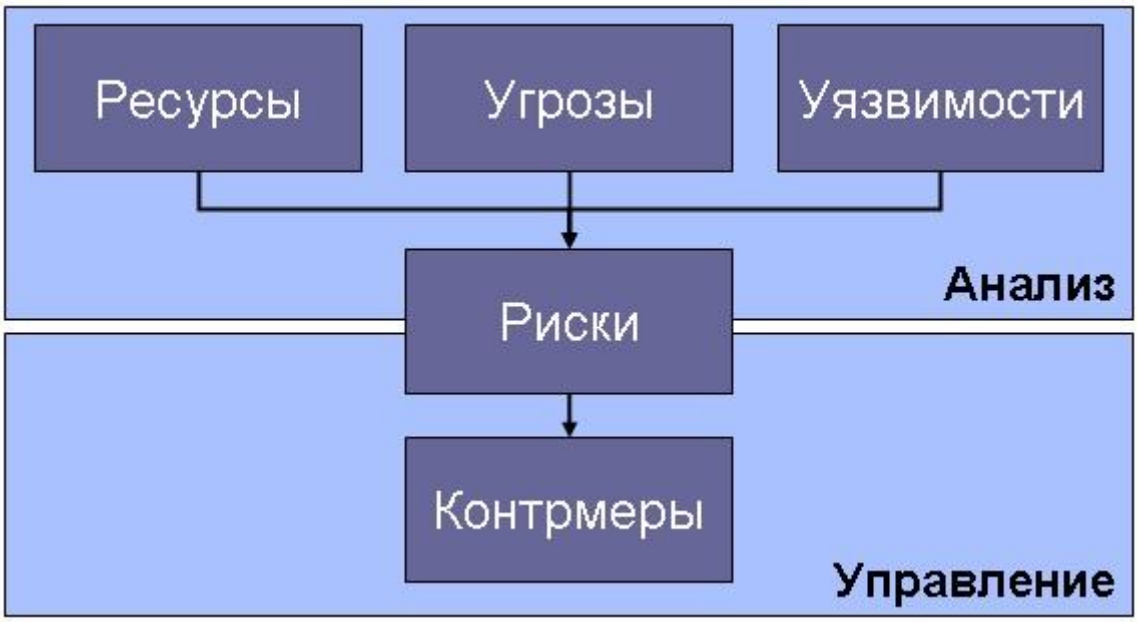
Стадия анализа рисков, Risk Analysis, позволяет оценить риски либо на основе сделанных оценок угроз и уязвимостей при проведении полного анализа рисков, либо путем использования упрощенных методик для базового уровня безопасности.

На стадии управления рисками, Risk Management, производится поиск адекватных контрмер. По существу речь идет о нахождении варианта системы безопасности, наилучшим образом удовлетворяющей требованиям заказчика. В конце стадии он будет знать, как модифицировать систему в терминах мер уклонения от риска, а также путем выбора специальных мер противодействия, ведущих к снижению или минимизации оставшихся рисков.

Выбор контрмер. Основные шаги:

- Генерация вариантов контрмер.
- Выбор подходящих вариантов и анализ их эффективности.
- Сравнительный анализ различных вариантов (What if)
- Получение отчета и обсуждение результатов с заказчиками.
- Коррекция по результатам обсуждения.

Каждая стадия объявляется законченной после детального обсуждения и согласования результатов с заказчиком.

- 

2. Недостатки и преимущества метода CRAMM

Достоинства и недостатки метода CRAMM

Достоинства:

- хорошо апробированный метод
- удачная система моделирования ИТ

- обширная БД для оценки рисков и выбора контрмер
- возможность использования как средства аудита

Недостатки:

- большой объем отчетов
- сравнительно высокая трудоемкость

3. Особенности анализа и управления рисками информационных систем компаний с помощью программного обеспечения RiskWatch

Программное обеспечение RiskWatch является мощным средством анализа и управления рисками. В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности.

В методе RiskWatch в качестве критериев для оценки и управления рисками используются предсказание годовых потерь (Annual Loss Expectancy, ALE) и оценка возврата от инвестиций (Return on Investment, ROI).

В отличие от CRAMM, программа RiskWatch более ориентирована на точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. Надо также отметить, что в этом продукте риски в сфере информационной и физической безопасности компьютерной сети предприятия рассматриваются совместно.

4. Преимущества и недостатки программного обеспечения RiskWatch

Семейство программных продуктов RiskWatch имеет массу достоинств. RiskWatch помогает провести анализ рисков и сделать обоснованный выбор мер и средств защиты.

К недостаткам RiskWatch можно отнести:

- Такой метод подходит, если требуется провести анализ рисков на программно-техническом уровне защиты, без учета организационных и административных факторов.
- Полученные оценки рисков (математическое ожидание потерь) далеко не исчерпывает понимание риска с системных позиций - метод не учитывает комплексный подход к информационной безопасности.
- Программное обеспечение RiskWatch существует только на английском языке.
- Высокая стоимость лицензии (от 10 000 долл. за одно рабочее место для небольшой компании).

5. Основные этапы метода анализа рисков RiskWatch

Первый этап - определение предмета исследования. Здесь описываются такие параметры, как тип организации, состав исследуемой системы (в общих чертах), базовые требования в области безопасности. Для облегчения работы аналитика, в шаблонах, соответствующих типу организации ("коммерческая информационная система", "государственная/военная информационная система" и т.д.), есть списки категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты. Из них нужно выбрать те, что реально присутствуют в организации.

Например, категории потерь:

- Задержки и отказ в обслуживании;
- Раскрытие информации;
- Прямые потери (например, от уничтожения оборудования огнем);
- Жизнь и здоровье (персонала, заказчиков и т.д.);
- Изменение данных;
- Косвенные потери (например, затраты на восстановление);
- Репутация.

Определение категорий защищаемых ресурсов.

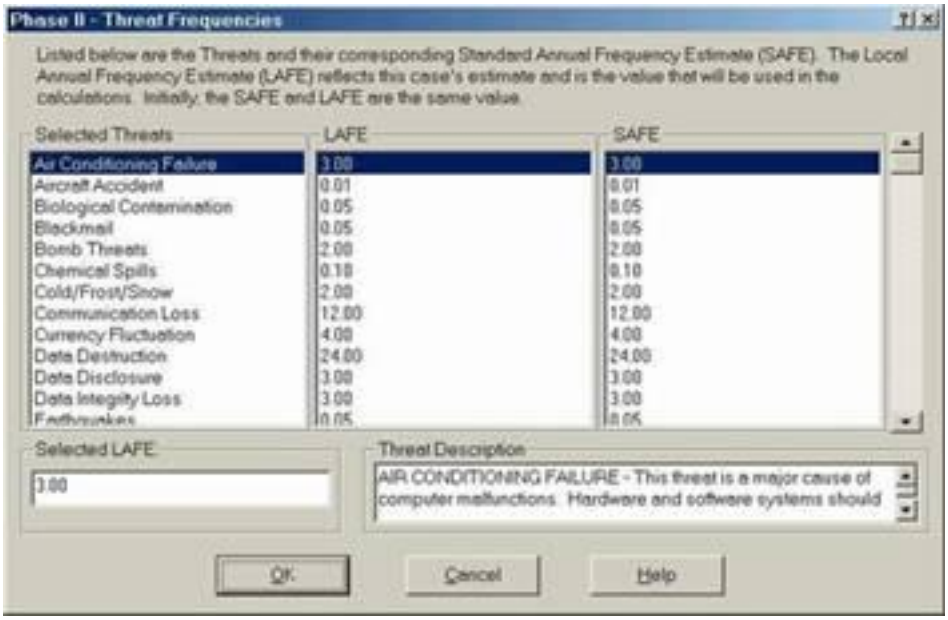
Второй этап - ввод данных, описывающих конкретные характеристики системы. Данные могут вводиться вручную или импортироваться из отчетов, созданных инструментальными средствами исследования уязвимости компьютерных сетей.

На этом этапе:

Подробно описываются ресурсы, потери и классы инцидентов. Классы инцидентов получаются путем сопоставления категории потерь и категории ресурсов.

Для выявления возможных уязвимостей используется опросник, база которого содержит более 600 вопросов. Вопросы связаны с категориями ресурсов.

Задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов. Все это используется в дальнейшем для расчета эффекта от внедрения средств защиты.



Пример оценок LAFE и SAFE для одной из угроз.

Третий и, наверное, самый важный этап - количественная оценка. На этом этапе рассчитывается профиль рисков, и выбираются меры обеспечения безопасности.

Сначала устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих шагах исследования (риск описывается совокупностью этих четырех параметров).

Фактически, риск оценивается с помощью математического ожидания потерь за год. Например, если стоимость сервера $150000, а вероятность того, что он будет уничтожен пожаром в течение года равна 0.01, то ожидаемые потери составят $1500.

Общеизвестная формула (m=p*v , где m-математическое ожидание, p - вероятность возникновения угрозы, v - стоимость ресурса) претерпела некоторые изменения, в связи с тем, что RiskWatch использует определенные американским институтом стандартов NIST оценки, называемые LAFE и SAFE. LAFE (Local Annual Frequency Estimate) - показывает, сколько раз в год в среднем данная угроза реализуется в данном месте (например, в городе). SAFE (Standard Annual Frequency Estimate) - показывает, сколько раз в год в среднем данная угроза реализуется в этой "части мира" (например, в Северной Америке). Вводится также поправочный коэффициент, который позволяет учесть, что в результате реализации угрозы защищаемый ресурс может быть уничтожен не полностью, а только частично.

Дополнительно рассматриваются сценарии "что если:", которые позволяют описать аналогичные ситуации при условии внедрения средств защиты. Сравнивая ожидаемые потери при условии внедрения защитных мер и без них можно оценить эффект от таких мероприятий.

RiskWatch включает в себя базы с оценками LAFE и SAFE, а также с обобщенным описанием различных типов средств защиты.

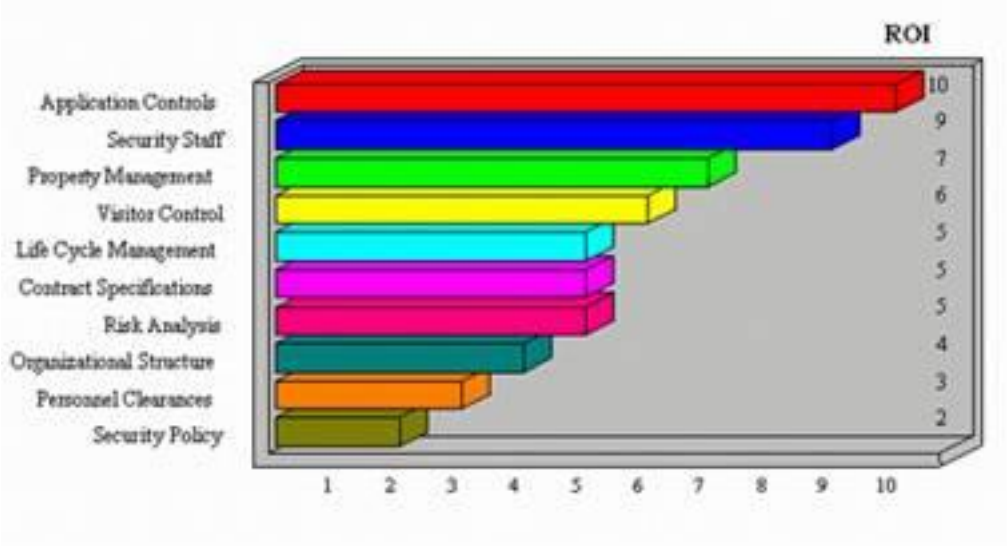
Эффект от внедрения средств защиты количественно описывается с помощью показателя ROI (Return on Investment - отдача от инвестиций), который показывает отдачу от сделанных инвестиций за определенный период времени. Рассчитывается он по формуле:

$$ROI = \sum_i NVP(Benefits_i) - \sum_i NVP(Costs_i)$$

где Costsi - затраты на внедрение и поддержание i-меры защиты; Benefitsi - оценка той пользы (т.е. ожидаемого снижения потерь), которую приносит внедрение данной меры защиты; NPV (Net Present Value) - дает поправку на инфляцию.

Четвертый этап - генерация отчетов. Типы отчетов:

- Краткие итоги.
- Полные и краткие отчеты об элементах, описанных на стадиях 1 и 2.
- Отчет от стоимости защищаемых ресурсов и ожидаемых потерях от реализации угроз.
- Отчет об угрозах и мерах противодействия.
- Отчет о ROI.
- Отчет о результатах аудита безопасности.



Пример графика показателя ROI для различных мер защиты.