Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования «Томский государственный университет систем управления и радиоэлектроники»

Кафедра безопасности информационных систем

С.Ю. Исхаков

Информационная безопасность телекоммуникационных систем

Методические указания для выполнения практических, самостоятельных и лабораторных работ

для студентов специальности *10.05.02*

Томск 2017

Содержание

1 Описание дисциплины

Изучение дисциплины «Информационная безопасность телекоммуникационных систем» направлено на достижение следующих основных целей:

1) заложить терминологический фундамент;
2) рассмотреть особенности построения телекоммуникационных систем;
3) приобрести навыки аудита телекоммуникационных систем;
4) научить правильно проводить оценку рисков информационной безопасности для телекоммуникационных систем;
5) изучить методы и средства обеспечения информационной безопасности телекоммуникационных систем;
6) рассмотреть основные общеметодологические принципы построения системы защиты информации для телекоммуникационных систем.

Содержание дисциплины раскрыто в таблице 1.

Таблица 1 — Содержание курса «Информационная безопасность телекоммуникационных систем»

Название раздела	Содержание раздела
Введение	Обзор содержания курса, правовые аспекты защиты информации, краткий обзор по развитию систем защиты информации, методические указания по изучению курса.
Основы построения и функционирования современных телекоммуникационных систем	Этапы построения телекоммуникационных систем. Эталонная модель взаимодействия открытых систем. Основные протоколы телекоммуникационных систем.
Основные понятия и цели обеспечения безопасности телекоммуникационных систем	Понятие безопасности телекоммуникационных систем. Основные цели защиты информации. Основные направления защиты телекоммуникационных систем.

Угрозы информационной безопасности телекоммуникационных систем	Понятие угрозы. Виды угроз и характер их происхождения. Источники и предпосылки появления угроз. Классы каналов несанкционированного получения информации. Потенциально возможные действия нарушителя. Построение модели угроз.
Методы анализа уязвимостей телекоммуникационных систем	Понятие риска в информационной безопасности. Выбор параметров для количественного анализа рисков в телекоммуникационных системах. Определение видов ущерба. Технологии обнаружения вторжений. Технические и программные средства анализа защищенности телекоммуникационных систем. Сертификационные и аттестационные испытания.
Методы, способы и средства защиты информации в телекоммуникационных системах	Виды побочных каналов, оценка возможности утечки информации, основные методы защиты информации от утечки по побочным каналам. Понятия субъекта и объекта доступа, их взаимодействие в информационном обмене. Идентификация, аутентификация, авторизация в телекоммуникационных системах. Математическая модель систем шифрования. Основные категории стойкости. Совершенная криптосистема. Понятие о расстоянии единственности. Классификация шифров. Блоковые шифры, потоковые

	шифры, шифрование речевых сигналов. Криптосистемы с открытым ключом. Гибридные шифры. Технические и программные средства сбора информации о состоянии объектов телекоммуникационных систем. Работа с данными: агрегация, поиск общих атрибутов (корреляция). Средства оповещения и отображения. Средства экспертного анализа.

Дисциплина «Информационная безопасность телекоммуникационных систем» включает следующие виды занятий:

1) лекции
2) практические занятия;
3) лабораторные занятия;
4) самостоятельная работа студентов.

На лекциях излагаются основные теоретические положения, составляющие дисциплину, и разбираются примеры практических задач. Практические занятия направлены на закрепление лекционного материала. Лабораторные занятия направлены на приобретение практических навыков по работе с телекоммуникационными системами и средствами обеспечения информационной безопасности телекоммуникационных систем. Самостоятельная работа студентов заключается в подготовке к лекционным, практическим и лабораторным занятиям и выполнении домашних заданий, выдаваемых преподавателем по каждому из разделов дисциплины. Для подготовки к практическим занятиям рекомендуется самостоятельный разбор представленных в разделе 3 заданий.

Для проверки усвоения студентами изучаемого материала в течение учебного семестра должны быть проведены две контрольные работы по разным разделам курса. По времени каждая из работ рассчитана на одно занятие. Для получения студентами зачета либо допуска к экзамену все контрольные работы должны быть выполнены не менее чем на удовлетворительную оценку. По итогам проверки контрольных работ должны быть проведены практические занятия, посвященные разбору заданий и типичных ошибок, допущенных при их выполнении.

2 Задания для практических занятий

1. Практические занятия по разделу «Основы построения и функционирования современных телекоммуникационных систем».

Содержание раздела: примеры построения телекоммуникационных систем; рассмотрение модели взаимодействия открытых систем на практике; изучение основных протоколов, используемых в телекоммуникационных системах.

Задание: используя лекционный материал, а также материал для самостоятельной подготовки, подготовить доклад (презентацию) с описанием выбранной для исследования телекоммуникационной системы. Описание должно содержать в себе принципиальную схему объекта исследования (основные блоки, модули, сегменты и их назначение), схему сетевых соединений с указанием используемого оборудования (тип, используемые функции). Для каждого из сегментов системы, а также для указанного оборудования перечислить используемые протоколы и кратко рассказать об их назначении.

2. Практические занятия по разделу «Основные понятия и цели обеспечения безопасности телекоммуникационных систем».

Содержание раздела: систематизация знаний об основных направлениях защиты телекоммуникационных систем; формирование целей и составления технических заданий на разработку систем защиты.

Задание: используя лекционный материал, а также материал для самостоятельной подготовки, подготовить отчет по занятию в форме технического задания на разработку системы защиты для выбранной телекоммуникационной системы (допускается продолжение работы с объектом исследований, выбранным для предыдущего занятия). Необходимо сформировать цели и подробно описать все требуемые направления защиты для исследуемого объекта. Задание должно подробно отражать все этапы и формы отчетности исполнителя.

3. Практические занятия по разделу «Угрозы информационной безопасности телекоммуникационных систем»

Содержание раздела. Исследование объекта: определение потенциальных угроз, характера их происхождения, источников и предпосылок. Анализ потенциально возможных действий нарушителя. Построение модели угроз.

Задание: используя лекционный материал, а также материал для самостоятельной подготовки, подготовить доклад (презентацию) в форме отчета о предпроектном обследовании телекоммуникационной системы (допускается продолжение работы с объектом исследований, выбранным для предыдущих занятий). Отчет должен отражать все потенциальные угрозы,

характер их происхождения, источники и предпосылки. Кроме того, необходимо проанализировать потенциальные действия нарушителя и представить модель угроз.

4. Практические занятия по разделу «Методы анализа уязвимостей телекоммуникационных систем»

Содержание раздела: анализ рисков в телекоммуникационных системах, изучение современных аппаратных и программных средствами анализа уязвимостей.

Задание: подготовить реферат по методикам анализа рисков в телекоммуникационных системах, либо по обзору средств анализа уязвимостей (примерный список тем рефератов будет предоставлен преподавателем, допускается самостоятельный выбор темы по согласованию с преподавателем).

5. Практические занятия по разделу «Методы, способы и средства защиты информации в телекоммуникационных системах»

Содержание раздела: защита информации от утечки по побочным каналам; взаимодействие субъекта и объекта доступа в информационном обмене; применение современных методов криптозащиты в телекоммуникационных системах; современные средства сбора и анализа информации о состоянии телекоммуникационных систем.

Задание 1: используя лекционный материал, а также материал для самостоятельной подготовки, подготовить доклад (презентацию) по выявлению побочных каналов утечки информации в выбранном на предыдущих занятиях объекте исследований (допускается обмен объектами исследований для развития профессиональных навыков). Кроме того, доклад должен содержать информацию о возможном применении современных методов криптозащиты в исследуемом объекте.

Задание 2: используя лекционный материал, а также материал для самостоятельной подготовки, подготовить реферат по современным средствам сбора и анализа информации (примерный список тем рефератов будет предоставлен преподавателем, допускается самостоятельный выбор темы по согласованию с преподавателем).

3 Вопросы для самоконтроля

1. Что стандартизирует модель OSI?
2. Можно ли представить еще один вариант модели взаимодействия открытых систем с другим количеством уровней, например, 8 или 5?
3. Ниже перечислены оригинальные (англоязычные) названия семи уровней модели OSI. Отметьте, какие из названий уровней не

соответствуют стандарту? Physical layer, data-link layer, network layer, transport layer, seances layer, presentation layer, application layer.

4. Какие из приведенных утверждений вы считаете ошибочными:
   - протокол — это программный модуль, решающий задачу взаимодействия систем;
   - протокол — это формализованное описание правил взаимодействия, включающих последовательность обмена сообщениями и их форматы;
   - термины «интерфейс» и «протокол», в сущности, являются синонимами.
5. На каком уровне модели OSI работает прикладная программа?
6. Как вы считаете, протоколы транспортного уровня устанавливаются только на конечных узлах, только на промежуточном коммуникационном оборудовании (маршрутизаторах) или и там, и там?
7. На каком уровне модели OSI работают сетевые службы?
8. Ниже перечислены некоторые сетевые устройства:
   - маршрутизатор;
   - коммутатор;
   - мост;
   - повторитель;
   - сетевой адаптер;
   - концентратор.

   В каком из этих устройств реализуются функции физического уровня модели OSI? Канального уровня? Сетевого уровня?
9. Какое название традиционно используется для единицы передаваемых данных на каждом из уровней OSI?
10. Дайте определение открытой системы.
11. Пусть малоизвестная небольшая компания предлагает нужный вам продукт с характеристиками, превосходящими характеристики аналогичных продуктов известных фирм. В каком из перечисленных вариантов ваши действия можно считать согласующимися с принципом открытых систем:
    - приму предложение, проверив прилагаемую документацию и убедившись, что в ней указаны характеристики, превосходящие известные аналоги;
    - приму предложение только после того, как проведу тестирование и удостоверюсь, что характеристики действительно лучше;
    - в любом случае откажусь в пользу продукта известной фирмы, так как последняя наверняка следует стандартам, а значит, будет меньше проблем с совместимостью;

- откажусь от продукта неизвестной компании, так как есть риск ее исчезновения, а значит, могут быть проблемы с поддержкой.

12. Какая организация разработала стандарты сетей Ethernet?
13. Какое из административных подразделений Интернета непосредственно занимается стандартизацией?
14. Какие из перечисленных терминов являются синонимами:
    - стандарт;
    - спецификация;
    - RFC;
    - Никакие.
15. К какому типу стандартов могут относиться современные документы RFC:
    - к стандартам отдельных фирм;
    - к государственным стандартам;
    - к национальным стандартам;
    - к международным стандартам.
16. Какая организация стояла у истоков создания и стандартизации стека TCP/IP?
17. Определите основные особенности стека TCP/IP.
18. Сравните функции самых нижних уровней моделей TCP/IP и OSI.
19. Дайте определение транспортных и информационных услуг.
20. Какие протоколы относятся к слою управления (control plane)? А к слою менеджмента (management plane)?
21. Должны ли маршрутизаторами поддерживаться протоколы транспортного уровня?
22. Пусть на двух компьютерах установлено идентичное программное и аппаратное обеспечение за исключением того, что драйверы сетевых адаптеров Ethernet поддерживают отличающиеся интерфейсы с протоколом сетевого уровня IP. Будут ли эти компьютеры нормально взаимодействовать, если их соединить в сеть?
23. Как организовать взаимодействие двух компьютеров, если у них отличаются протоколы:
    - физического и канального уровней;
    - сетевого уровня;
    - прикладного уровня.
24. Опишите ваши действия в случае, если вам необходимо проверить, на каком этапе находится процесс стандартизации технологии MPLS?

4 Лабораторный практикум

Лабораторная № 1. Исследование телекоммуникационной системы как объекта защиты

Угроза информации – возможность возникновения на каком-либо этапе жизнедеятельности системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию.

Виды угроз. Основные нарушения:

1. Физической целостности (уничтожение, разрушение элементов).
2. Логической целостности (разрушение логических связей).
3. Содержания (изменение блоков информации, внешнее навязывание ложной информации).
4. Конфиденциальности (разрушение защиты, уменьшение степени защищенности информации).
5. Прав собственности на информацию (несанкционированное копирование, использование).

Три наиболее выраженные угрозы:

1) подверженность физическому искажению или уничтожению;
2) возможность несанкционированной (случайной или злоумышленной) модификации;
3) опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.

Характер происхождения угроз

1. Умышленные факторы:
1.1. хищение носителей информации;
1.2. подключение к каналам связи;
1.3. перехват ЭМИ;
1.4. несанкционированный доступ;
1.5. разглашение информации;
1.6. копирование данных.
2. Естественные факторы:
2.1. несчастные случаи (пожары, аварии, взрывы);
2.2. стихийные бедствия (ураганы, наводнения, землетрясения);
2.3. ошибки в процессе обработки информации (ошибки пользователя, оператора, сбои аппаратуры).

Источники угроз

Понимается непосредственный исполнитель угрозы в плане ее негативного воздействия на информацию.

- люди;
- технические устройства;
- модели, алгоритмы, программы;
- технологические схемы обработки;
- внешняя среда.

Предпосылки появления угроз

- объективные (количественная или качественная недостаточность элементов системы) — причины, не связанные непосредственно с деятельностью людей и вызывающие случайные по характеру происхождения угрозы;

- субъективные — причины, непосредственно связанные с деятельностью человека и вызывающие как преднамеренные (деятельность разведок иностранных государств, промышленный шпионаж, деятельность уголовных элементов и недобросовестных сотрудников), так и непреднамеренные (плохое психофизиологическое состояние, недостаточная подготовка, низкий уровень знаний) угрозы информации.

Несанкционированный доступ — получение лицами в обход системы защиты с помощью программных, технических и других средств, а также в силу случайных обстоятельств доступа к обрабатываемой и хранимой на объекте информации.

Разглашение информации ее обладателем есть умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшие к не вызванному служебной необходимостью оглашению охраняемых сведений, в также передача таких сведений по открытым техническим каналам или обработка на не категорированных ЭВМ.

Утечку информации в общем плане можно рассматривать как бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена.

Система защиты информации — совокупность взаимосвязанных средств, методов и мероприятий, направленных на предотвращение уничтожения, искажения, несанкционированного получения конфиденциальных сведений, отображенных полями, электромагнитными, световыми и звуковыми волнами или вещественно-материальными носителями в виде сигналов, образов, символов, технических решений и процессов.

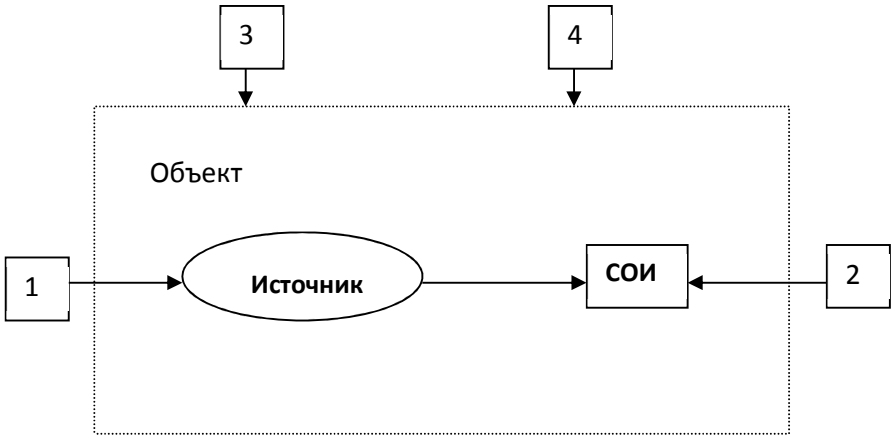

Рисунок 1 — Классы каналов несанкционированного получения информации

1.1. Хищение носителей информации.

1.2. Копирование информации с носителей (материально-вещественных, магнитных и т.д.).

1.3. Подслушивание разговоров (в том числе аудиозапись).

1.4. Установка закладных устройств в помещение и съем информации с их помощью.

1.5. Выведывание информации обслуживающего персонала на объекте.

1.6. Фотографирование или видеосъемка носителей информации внутри помещения.

2.1. Снятие информации с устройств электронной памяти.

2.2. Установка закладных устройств в СОИ.

2.3. Ввод программных продуктов, позволяющих злоумышленнику получать информацию.

2.4. Копирование информации с технических устройств отображения (фотографирование с мониторов и др.)

3.1.Получение информации по акустическим каналам (в системах вентиляции, теплоснабжения, а также с помощью направленных микрофонов).

3.2. Получение информации по виброакустическим каналам (с использованием акустических датчиков, лазерных устройств).

3.3. Использование технических средств оптической разведки (биноклей, подзорных труб и т.д.).

3.4. Использование технических средств оптико-электронной разведки (внешних телекамер, приборов ночного видения и т.д.).

3.5. Осмотр отходов и мусора.

3.6. Выведывание информации у обслуживающего персонала за пределами объекта.

3.7. Изучение выходящей за пределы объекта открытой информации (публикаций, рекламных проспектов и т.д.).

1.1. Электромагнитные излучения СОИ (ПЭМИ, паразитная генерация усилительных каскадов, паразитная модуляция высокочастотных генераторов низкочастотным сигналом, содержащим конфиденциальную информацию).

1.2. Электромагнитные излучения линий связи.

1.3. Подключения к линиям связи.

1.4. Снятие наводок электрических сигналов с линий связи.

1.5. Снятие наводок с системы питания.

1.6. Снятие наводок с системы заземления.

1.7. Снятие наводок с системы теплоснабжения.

1.8. Использование высокочастотного навязывания.

1.9. Снятие с линий, выходящих за пределы объекта сигналов образованных на технических средствах за счет акустоэлектрических преобразований.

1.10.Снятие излучений оптоволоконных линий связи.

1.11.Подключение к базам данных и ПЭВМ по компьютерным сетям.

Причины нарушения целостности информации

1.1. Субъективные преднамеренные.

1.1.1. Диверсия (организация пожаров, взрывов, повреждений электропитания и др.).

1.1.2. Непосредственные действия над носителем (хищение, подмена носителей, уничтожение информации).

1.1.3. Информационное воздействие (электромагнитное облучение, ввод в компьютерные системы разрушающих программных средств, воздействие на психику личности психотропным оружием).

1.2. Субъективные непреднамеренные.

1.2.1. Отказы обслуживающего персонала (гибель, длительный выход из строя).

1.2.2. Сбои людей (временный выход из строя).

1.2.3. Ошибки людей.

2.1. Объективные непреднамеренные.

2.1.1. Отказы (полный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения.

2.1.2. Сбои (кратковременный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения.

2.1.3. Стихийные бедствия (наводнения, землетрясения, ураганы).

2.1.4. Несчастные случаи (пожары, взрывы, аварии).

2.1.5. Электромагнитная несовместимость.

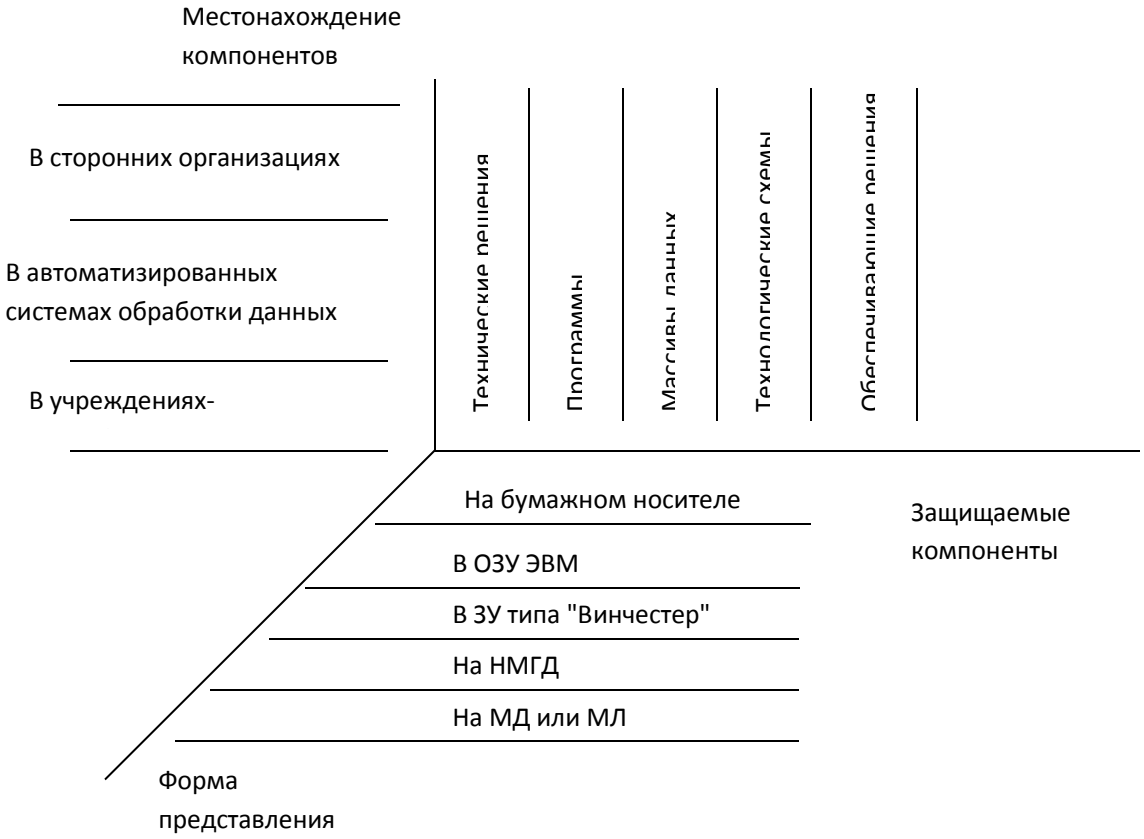

Рисунок 2 — Методы и модели оценки уязвимости информации

Уязвимость информации есть событие, возникающее как результат такого стечения обстоятельств, когда в силу каких-то причин используемые в автоматизированных системах обработки данных средства защиты не в состоянии оказать достаточного противодействия проявлению

дестабилизирующих факторам и нежелательного их воздействия на защищаемую информацию. Модель уязвимости информации в автоматизированных системах обработки данных в общем виде показано на рисунке 3.

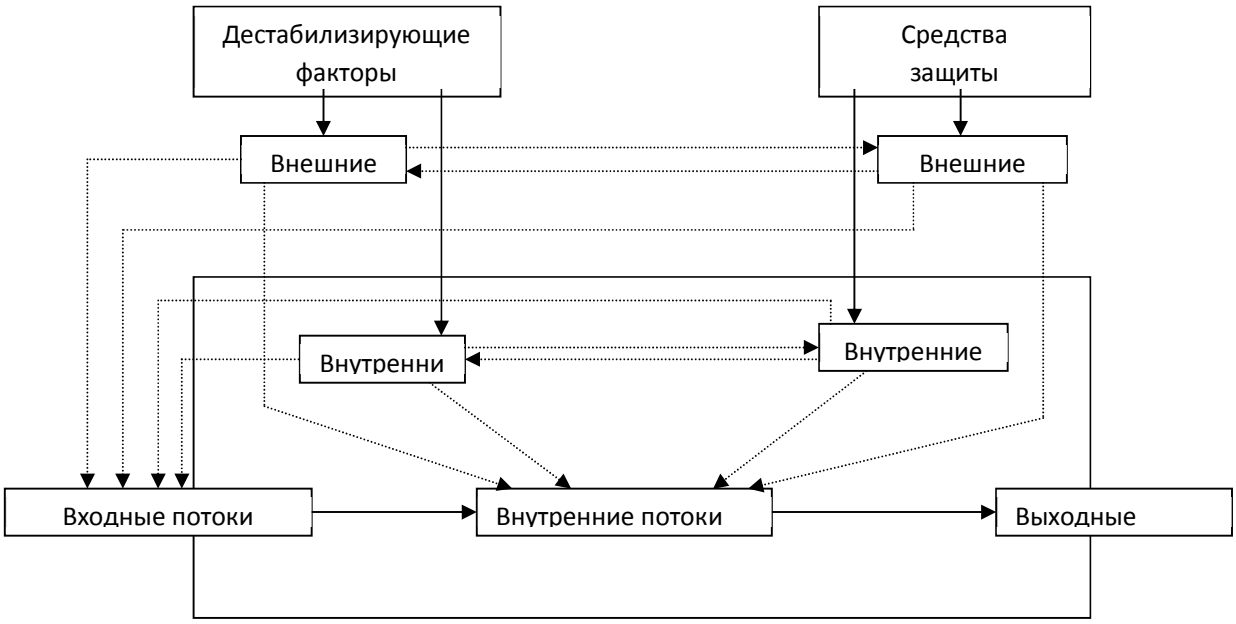

Рисунок 3 — Общая модель воздействия на информацию

Данная модель детализируется при изучении конкретных видов уязвимости информации: нарушения физической или логической целостности, несанкционированной модификации, несанкционированного получения, несанкционированного размножения.

При детализации общей модели основное внимание акцентируется на том, что подавляющее большинство нарушений физической целостности информации имеет место в процессе ее обработки на различных участках технологических маршрутов. При этом целостность информации зависит не только от процессов, происходящих на объекте, но и от целостности информации, поступающей на его вход. Основную опасность представляют случайные дестабилизирующие факторы (отказы, сбои и ошибки компонентов автоматизированных систем обработки данных), которые потенциально могут проявиться в любое время, и в этом отношении можно говорить о регулярном потоке этих факторов. Из стихийных бедствий наибольшую опасность представляют пожары, опасность которых в большей или меньшей степени также является постоянной. Опасность побочных явлений практически может быть сведена к нулю путем надлежащего выбора места для помещений автоматизированной системы обработки данных и их оборудования. Что касается злоумышленных действий, то они связаны, главным образом, с несанкционированным доступом к ресурсам автоматизированной системы обработки данных. При этом наибольшую опасность представляет занесение вирусов.

В соответствии с изложенным общая модель процесса нарушения физической целостности информации на объекте автоматизированной системы обработки данных может быть представлена в виде, показанном на рисунке 4.

Рисунок 4 — Общая модель процесса нарушения физической целостности информации

С точки зрения несанкционированного получения информации принципиально важным является то обстоятельство, что в современных автоматизированных системах обработки данных оно возможно не только путем непосредственного доступа к базам данных, но и многими путями, не требующими такого доступа. При этом основную опасность представляют злоумышленные действия людей. Воздействие случайных факторов непосредственно не ведет к несанкционированному получению информации, оно лишь способствует появлению каналов несанкционированного получения информации, которыми может воспользоваться злоумышленник. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных для самого общего случаю представлена на рисунке 5.

Выделенные зоны определяются следующим образом:

1) внешняя неконтролируемая зона — территория вокруг автоматизированной системы обработки данных, на которой персоналом и средствами автоматизированной системой обработки данных не применяются

никакие средства и не осуществляется никакие мероприятия для защиты информации;

2) зона контролируемой территории — территория вокруг помещений автоматизированной системы обработки данных, которая непрерывно контролируется персоналом или средствами автоматизированной системы обработки данных;

3) зона помещений автоматизированной системы обработки данных — внутренне пространство тех помещений, в которых расположена система;

4) зона ресурсов автоматизированной системы обработки данных — та часть помещений, откуда возможен непосредственный доступ к ресурсам системы;

5) зона баз данных — та часть ресурсов системы, с которых возможен непосредственный доступ к защищаемым данным.

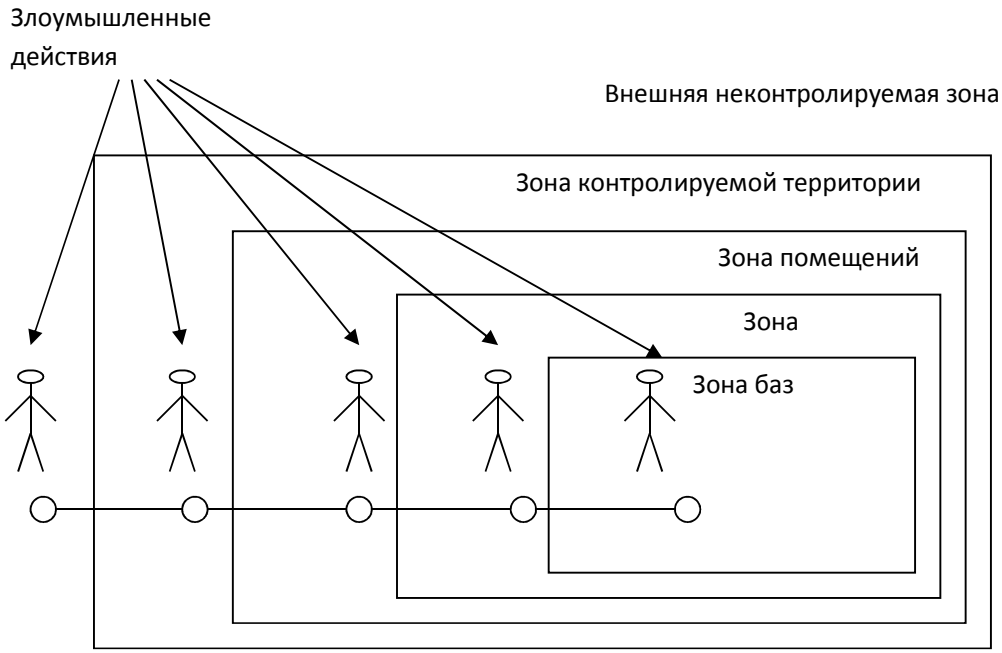

Рисунок 5 — Схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных

Злоумышленные действия с целью несанкционированного получения информации в общем случае возможны в каждой из перечисленных зон. При этом для несанкционированного получения информации необходимо одновременное наступление следующих событий: нарушитель должен получить доступ в соответствующую зону; во время нахождения нарушителя в зоне в ней должен проявиться (иметь место) соответствующий канал несанкционированного получения информации; соответствующий канал несанкционированного получения информации должен быть доступен нарушителю соответствующей категории; в канале несанкционированного получения информации в момент доступа к нему нарушителя должна находиться защищаемая информации.

Рассмотрим далее трансформацию общей модели уязвимости с точки зрения несанкционированного размножения информации. Принципиальными особенностями этого процесса являются:

1) любое несанкционированное размножение есть злоумышленное действие;

2) несанкционированное размножение может осуществляться в организациях-разработчиках компонентов автоматизированной системы обработки данных, непосредственно в автоматизированной системе обработки данных и сторонних организациях, причем последние могут получать носитель, с которого делается попытка снять копию как законным, так и незаконным путем.

Попытки несанкционированного размножения информации у разработчика и в автоматизированной системе обработки данных есть один из видов злоумышленных действий с целью несанкционированного ее получения и поэтому имитируются приведенной моделью. Если же носитель с защищаемой информацией каким-либо путем (законным или незаконным) попал в стороннюю организацию, то для его несанкционированного копирования могут использоваться любые средства и методы, включая и такие, которые носят характер научных исследований и опытно-конструкторских разработок.

В процессе развития теории и практики защиты информации сформировалось три методологических подхода к оценке уязвимости информации: *эмпирический, теоретический и теоретико-эмпирический*.

Эмпирический подход к оценке уязвимости информации.

Сущность эмпирического подхода заключается в том, что на основе длительного сбора и обработки данных о реальных проявлениях угроз информации и о размерах того ущерба, который при этом имел место, чисто эмпирическим путем устанавливаются зависимости между потенциально возможным ущербом и коэффициентами, характеризующими частоту проявления соответствующей угрозы и значения имевшего при ее проявлении размера ущерба. Наиболее характерным примером моделей рассматриваемой разновидности являются модели, разработанные специалистами американской фирмы IBM. Рассмотрим развиваемые этих моделях подходы.

Исходной посылкой при разработке моделей является почти очевидное предположение: с одной стороны, при нарушении защищенности информации наносит некоторый ущерб, с другой, обеспечение защиты информации сопряжено с расходованием средств. Полная ожидаемая стоимость защиты может быть выражена суммой расходов на защиту и на потерь от ее нарушения. Совершенно очевидно, что оптимальным решением было бы выделение на защиту информации средств в размере $C_{опт}$, поскольку при этом обеспечивается минимизация общей стоимости защиты информации. Для того, чтобы воспользоваться данным подходом к решению проблемы, необходимо, во-первых, знать (или уметь определять) ожидаемые потери при нарушении защищенности информации, а во-вторых, в зависимость между уровнем защищенности и средствами, затрачиваемыми на защиту информации. Решение первого вопроса, т.е. оценки ожидаемых потерь при

нарушении защищенности информации, принципиально может быть получено лишь тогда, когда речь идет о защите промышленной, коммерческой и им подобной тайны, хотя и здесь встречаются весьма серьезные трудности. Что касается оценки уровня потерь при нарушении статуса защищенности информации, содержащей государственную, военную и им подобную тайну, то здесь до настоящего времени строгие подходы к их получению не найдены. Данное обстоятельство существенно сужает возможную область использования моделей, основанных на рассматриваемых подходах.

Для определения уровня затрат, обеспечивающих требуемый уровень защищенности информации, необходимо по крайней мере знать, во-первых, полный перечень угроз информации, во-вторых, потенциальную опасность для информации для каждой из угроз и, в третьих, размеры затрат, необходимых для нейтрализации каждой из угроз.

$$R_i = 10^{(S_i + V_i - 4)}$$

Поскольку оптимальное решение вопроса о целесообразном уровне затрат на защиту состоит в том, что этот уровень должен быть равен уровню ожидаемых потерь при нарушении защищенности, достаточно определить только уровень потерь. Специалистами фирмы IBM предложена следующая эмпирическая зависимость ожидаемых потерь от i-й угрозы информации:

Где Si — коэффициент, характеризующий возможную частоту возникновения соответствующей угрозы; Vi — коэффициент, характеризующий значение возможного ущерба при ее возникновении. Предложенные специалистами значения коэффициентов:

Значения коэффициента Si

Ожидаемая (возможная) частота появления угрозы	Предполагаемое значение Si
Почти никогда	0
1 раз в 1000 лет	1
1 раз в 100 лет	2
1 раз в 10 лет	3
1 раз в год	4
1 раз в месяц (примерно, 10 раз в год)	5
12 раза в неделю (примерно 100 раз в год)	6
3 раза в день (1000 раз в год)	7

Возможные значения коэффициента Vi

Значение возможного ущерба при проявлении угрозы (доллары США)	Предполагаемое значение Vi
1	0
10	1
100	2
1 000	3
10 000	4
100 000	5
1 000 000	6
10 000 000	7

Суммарная стоимость потерь определяется формулой

$$R = \sum_{\forall i} R_i$$

Таким образом, если бы удалось собрать достаточное количество фактических данных о проявлениях угроз и их последствиях, то рассмотренную модель можно было бы использовать для решения достаточно широкого круга задач защиты информации, причем, нетрудно видеть, что модель позволяет не только находить нужные решения, но и оценивать их точность.

Задание на лабораторную работу

Для выполнения лабораторной работы необходимо для выбранной телекоммуникационной системы необходимо составить ее описание как объекта защиты, провести анализ защищенности информации по следующим разделам: 1. виды угроз; 2. характер происхождения угроз; 3. источники появления угроз; 4. классы каналов несанкционированного получения информации; 5. причины нарушения целостности информации; 6. потенциально возможные злоумышленные действия. На основании полученных данных необходимо построить модель угроз с использованием эмпирического подхода.

Лабораторная № 2. Выявление уязвимостей телекоммуникационной системы

Лабораторная работа посвящена практическому применению методов выявления уязвимостей телекоммуникационных систем. Обзор современных аппаратных и программных средств (в том числе дистрибутивов) для проведения разведки и сбора информации об исследуемой телекоммуникационной системе: сканирование сети, анализ защищенности сетевой инфраструктуры, анализ методов обход проактивных систем защиты. Введение в социальную инженерию.

Задание на лабораторную работу

Лабораторная работа состоит из трех разделов: моделирование инфраструктуры, поиск и анализ уязвимостей, эксплуатация уязвимостей и их устранение.

Раздел 1. Моделирование инфраструктуры.

Для выполнения лабораторной работы необходимо составить проект телекоммуникационной системы (не менее 2 активных устройств) и реализовать его с помощью средств виртуализации. Допускается использовать собственные аппаратно-программные средства для построения виртуального объекта исследований при учете возможности демонстрации преподавателю созданной виртуальной инфраструктуры.

Возможно выполнение работы в группах по 2-3 человека. После завершения раздела 1 группы обмениваются данными о расположении

построенных моделях и выполняют разделы 2 и 3 применительно к «чужим» объектам.

Пример.

Раздел 1. Создание стенда виртуального объекта исследований.

1. Создать на базе VMware Player лабораторный стенд согласно рисунка 6.

2. Установить источник событий, в качестве которого будет выступать Cisco CSR1000V

3. Установить сервер приёма событий на базе ОС Debian 8.

4. Запустить на сервере приёма событий простой Syslog север(python3)

5. Сконфигурировать CSR100V на отправку событий на данный сервер и собрать следующие события:

a) События входа пользователя

b) Событие изменения конфигурации

c) Событие срабатывания правила фильтрации (рекомендуется использовать правило закрывающие доступ по Telnet на базе стандартных ACL)

d) Событие загрузки IOS

e) Событие программного отключения/включения интерфейса

f) Событие аппаратного отключения/включения интерфейса (через консоль гипервизора перевести интерфейс в состояние not connected) g) Изменение параметров интерфейса

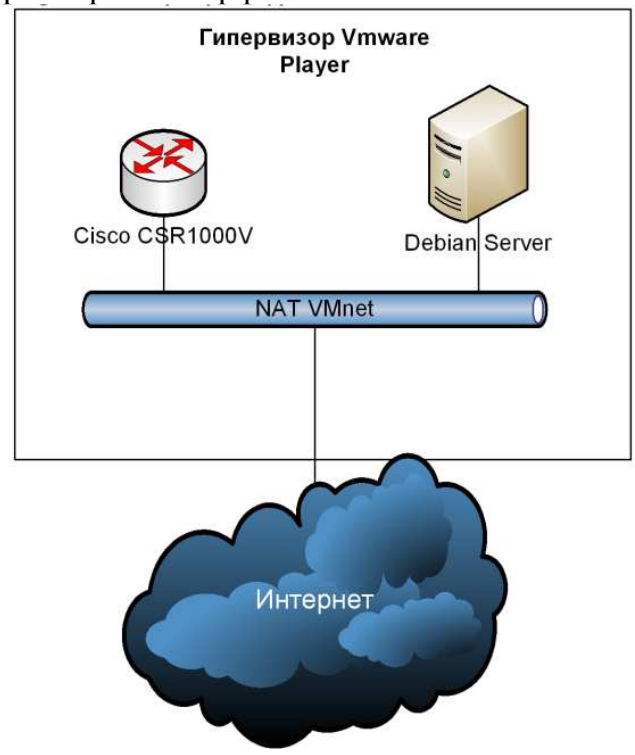

Рисунок 6 — Схема стенда

Раздел 2. Поиск и анализ уязвимостей.

Для выполнения данного этапа лабораторной работы необходимо ознакомиться и установить один из дистрибутивов (например, Kali Linux), обеспечив подключение к виртуальному стенду со стороны Интернет (согласно рисунку 6).

С помощью имеющегося инструментария провести разведку и сбор информации об исследуемой телекоммуникационной системе на предмет открытых портов и получение информации об инфраструктуре объекта, а также существующих уязвимостях.

Раздел 3. Эксплуатация уязвимостей и их устранение.

Используя полученные в предыдущих разделах данные, оценить возможность и постараться эксплуатировать выявленные уязвимости. Составить подробный отчет с описанием выявленных уязвимостей и рекомендуемыми методами их устранения.