Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра радиоэлектронных средств

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Методические указания и контрольные вопросы
для студентов специальностей «Техническое обеспечение безопасности»
и «Моделирование и компьютерное проектирование
радиоэлектронных средств»
заочной формы обучения

Минск 2005

УДК 004.056 (075.8)
ББК 32.97 я 73
О-75

С о с т а в и т е л ь:
В.М. Алефиренко

О-75 **Основы** защиты информации: Метод. указания и контр. вопр. для студ. спец. «Техническое обеспечение безопасности» и «Моделирование и компьютерное проектирование радиоэлектронных средств» заоч. формы обуч./ Сост. В.М.Алефиренко. – Мн.: БГУИР, 2005. – 20 с.

Приводится программа, методические указания к изучению учебной дисциплины «Основы защиты информации» и перечень контрольных вопросов к каждому разделу.

УДК 004.056 (075.8)
ББК 32.97 я 73

ЦЕЛЬ И ЗАДАЧИ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью изучения дисциплины является получение студентами базовых знаний по общим вопросам организации защиты информации на объекте, методам и средствам ее защиты в устройствах и каналах передачи.

Основными задачами изучения дисциплины являются:

- получение знаний о принципах организации и построения системы защиты информации на объекте;
- изучение основных каналов утечки информации и причин их образования;
- изучение методов и средств скрытого съема информации;
- изучение методов и средств защиты, обнаружения и противодействия в различных каналах передачи информации;
- изучение методов и средств защиты информации в персональных компьютерах и сетях ЭВМ, включая криптографические и стеганографические методы.

В результате изучения дисциплины студент должен:

- **знать**:
- основные направления обеспечения информационной безопасности;
- основные каналы утечки информации и причины их образования;
- методы и средства, используемые для скрытого съема информации;
- методы и средства защиты, используемые для защиты, обнаружения и противодействия в акустических, телефонных, электромагнитных и оптических каналах передачи информации;
- методы и средства, используемые для защиты информации в персональных компьютерах и сетях ЭВМ;
- общие принципы организации и построения системы защиты информации на объекте;
- **уметь:**
- проводить анализ возможных каналов утечки информации и выбирать соответствующие методы и средства ее защиты;
- **иметь представление:**
- о физических принципах, используемых при несанкционированном съеме информации;
- о физических принципах, используемых при защите, обнаружении и противодействии в каналах передачи информации;
- об основных принципах защиты информации с помощью методов компьютерной криптографии и стеганографии.

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, МЕТОДИЧЕСКИЕ УКАЗАНИЯ И КОНТРОЛЬНЫЕ ВОПРОСЫ

РАЗДЕЛ 1. Общие вопросы защиты информации

Тема 1.1. Информация и ее защита

Понятие информации. Информация и информатика. Виды представления информации. Действия над информацией. Оборот информации. Классификация информации. Информация открытая и с ограниченным доступом. Секретная информация. Конфиденциальная информация. Виды конфиденциальной информации. Личная тайна. Судебно-следственная тайна. Служебная тайна. Профессиональная тайна. Коммерческая тайна. Производственная тайна. Основные термины и определения защиты информации.

Тема 1.2. Концепция информационной безопасности

Понятие безопасности. Обеспечение безопасности. Система безопасности. Фрагментарный и системный подход к защите информации. Цели защиты информации. Требования к защите информации. Виды обеспечения системы защиты информации. Концептуальная модель информационной безопасности и ее компоненты. Модель построения системы информационной безопасности предприятия. Угрозы конфиденциальной информации и их классификация. Действия, приводящие к неправомерному овладению конфиденциальной информацией. Разглашение, утечка, несанкционированный доступ.

Тема 1.3. Обеспечение информационной безопасности

Направления обеспечения информационной безопасности. Правовая защита. Международное и внутригосударственное право. Государственное и ведомственное право. Виды правовых документов, регламентирующих информационную безопасность. Организационная защита. Организация режима и охраны. Организация работы с сотрудниками. Организация работы с документами. Организация использования технических средств. Организация работы по анализу угроз. Организация работы по проведению контроля за работой персонала. Инженерно-техническая защита. Классификация инженерно-технической защиты. Физические средства. Аппаратные средства. Программные средства. Криптографические и стеганографические средства.

Методические указания

При изучении данного раздела необходимо в первую очередь правильно уяснить понятие информации, виды ее представления, действия над ней и способы передачи.

Понятие «информация» является сложным и имеет ряд аспектов. Важнейшими из них являются семантический (смысловой) и математический (операционный), базирующийся на определении количественных мер.

В смысловом (семантическом) аспекте понятие «информация» является одним из первичных и соответствует терминам «сведения», «знания». Для передачи информации используется тот или иной язык, который характеризуется знаками и правилами их применения. Совокупность знаков, содержащих некоторую информацию, подлежащую передаче, называется сообщением. Сообщения могут принимать различные формы (звук, текст, изображения). Различия в форме сообщений определяют выбор средств для их передачи (телефон, телевидение).

Научное определение термина «информация» основано на вероятностных свойствах полученных сведений. Чем менее вероятно событие, о котором сообщается, тем больше информации несет сообщение о нем. В теории передачи информации имеется в виду вероятностный характер информации, а для ее количественной оценки используется понятие энтропии, которая обозначает меру степени неопределенности ситуации (случайного события) и может быть вычислена по соответствующей формуле.

Следует знать, что с понятием информации тесно связано понятие информатики – научной дисциплины, изучающей структуру и общие свойства информации, а также закономерности процессов коммуникации (передачи, обмена информацией).

Информация может быть открытой и с ограниченным доступом, которая делится на секретную и конфиденциальную. Следует уяснить, что для защиты информации необходимо использовать системный подход, который предполагает создание единой защищенной среды обработки, хранения и передачи информации, объединяющий разнообразные методы и средства ее защиты. Система защиты информации должна обеспечить сохранение основных ее свойств: конфиденциальности, достоверности, целостности и доступности.

Необходимо также понимать, что информация может подвергаться угрозам, которые проявляются в нарушении ее основных свойств. Угроза – это потенциальные или реальные действия, приводящие к моральному или материальному ущербу. Действиями, приводящими к неправомерному овладению информацией, являются разглашение, утечка и несанкционированный доступ. Для обеспечения безопасности информации используется правовая, организационная и инженерно-техническая защита.

Для изучения вопросов данного раздела достаточно ознакомиться с литературой [1, 2, 11]. Можно также ознакомиться с материалами, опубликованными в журнале «Конфидент» № 2 и № 3 за 2002 г.

Контрольные вопросы

1. Что такое информация?
2. В чем отличие информации от информатики?

3. В каком виде может представляться информация?
4. В чем заключается системный подход к защите информации?
5. Сохранение каких основных свойств информации должна обеспечить система ее защиты?
6. Назовите компоненты концептуальной модели безопасности информации.
7. Что такое угрозы информации и как они классифицируются?
8. Какие действия приводят к неправомерному овладению информацией?
9. Назовите основные направления обеспечения информационной безопасности.
10. В чем состоит правовая защита информации?
11. В чем состоит организационная защита информации?
12. В чем состоит инженерно-техническая защита информации?
13. Назовите инженерно-технические средства защиты информации.

РАЗДЕЛ 2. Каналы утечки и методы скрытого съема информации

Тема 2.1. Каналы утечки информации

Причины и условия утечки информации. Средства переноса информации. Понятие канала утечки. Классификация и общая характеристика каналов утечки. Визуально-оптические каналы. Акустические каналы. Электромагнитные каналы. Материально-вещественные каналы. Технические каналы утечки. Причины возникновения технических каналов утечки. Источники образования технических каналов утечки. Преобразователи физических величин. Излучатели электромагнитных колебаний. Паразитные связи и наводки. Физические явления образования технических каналов утечки.

Тема 2.2. Каналы утечки речевой информации

Классификация и характеристика каналов утечки речевой информации. Акустический канал. Вибрационный канал. Проводной канал. Электромагнитный канал. Оптический канал. Канал речевого общения. Анализ технических каналов утечки речевой информации и методов ее съема. Воздушные технические каналы утечки. Вибрационные технические каналы утечки. Электроакустические технические каналы утечки. Оптоэлектронные технические каналы утечки. Параметрические технические каналы утечки.

Тема 2.3. Методы и средства скрытого съема аудио- и видеоинформации

Методы дистанционного проникновения в помещение для скрытого съема аудио- и видеоинформации. Технические средства съема аудиоинформации. Малогабаритные проводные и радиомикрофоны. Микрофоны-стетоскопы. На-

правленные микрофоны. Лазерные микрофоны. Микрофоны инфракрасного излучения. СВЧ-микрофоны. Вторичные микрофоны. Устройства ВЧ-навязывания. Устройства с перемодуляцией радиоизлучений на нелинейных элементах. Устройства с двойной модуляцией. Устройства с питанием и передачей информации по сети. Диктофоны. Методы съема информации в телефонных линиях связи. Технические средства съема видеоинформации. Микрообъективы и видеокамеры. Камкодеры. Эндоскопы. Оптические системы. Рентгеновские телевизионные системы.

Тема 2.4. Методы и средства скрытого съема информации в электромагнитных и оптических каналах передачи

Виды электромагнитных излучений. Методы и средства съема информации по радиоканалу. Электромагнитные излучения средств телевизионной и вычислительной техники. Восстановление информации по электромагнитному излучению дисплея. Электромагнитные излучения и съем информации в высокочастотных кабелях. Оптические излучения и съем информации в волоконно-оптических кабелях. Взаимосвязь способов несанкционированного доступа к информации и каналов утечки информации.

Методические указания

При изучении данного раздела необходимо прежде всего уяснить, какие причины и условия приводят к утечке информации, по каким каналам может происходить утечка информации, а также причины возникновения и источники образования технических каналов утечки информации.

Утечка информации – это бесконтрольный выход охраняемых сведений за пределы организации или круга лиц, которым они были доверены. Следует понимать, что в основе утечки лежит неконтролируемый перенос конфиденциальной информации посредством акустических, оптических, электромагнитных и других полей и материальных объектов. Причины утечки связаны, как правило, с несовершенством норм по сохранению информации, а также нарушением этих норм. Условия утечки включают различные факторы и обстоятельства, которые складываются в процессе деятельности организации и создают предпосылки для утечки информации.

Необходимо знать, что под каналом утечки информации понимается физический путь от источника конфиденциальной информации к злоумышленнику. Он включает в себя источник сигнала, среду, по которой передается сигнал, и приемник сигнала. С учетом физической природы образования каналы утечки информации могут быть визуально-оптические, акустические, электромагнитные и материально-вещественные.

Следует также понимать, что широкое использование различных технических средств для обработки, хранения и передачи информации привело к появлению технических каналов утечки. Переносчиками неконтролируемой инфор-

мации в них выступают побочные электромагнитные излучения и наводки различного происхождения (акустопреобразовательные, излучательные, паразитные связи и наводки). Надо знать, что побочные электромагнитные излучения и наводки присущи любым радиоэлектронным устройствам и системам по самой природе их проявления. Физические явления, лежащие в основе появления опасных излучений, имеют различный характер, тем не менее в общем виде утечка информации может рассматриваться как непреднамеренная передача охраняемой информации по некоторой «побочной» системе связи. Следует также понимать, что радиоэлектронные средства и системы могут не только непосредственно излучать сигналы, содержащие информацию, но и улавливать за счет своих микрофонных или антенных свойств акустические и электромагнитные сигналы, преобразовывать их в электрические сигналы и передавать по своим линиям связи бесконтрольно, что в еще большей степени повышает опасность утечки информации.

Следует знать, что причинами возникновения технических каналов утечки информации являются несовершенство схемных решений технических средств обработки, хранения и передачи информации и эксплуатационный износ элементов, приводящий к изменению их параметров, а основными источниками образования технических каналов являются преобразователи физических величин, излучатели электромагнитных колебаний, входящие в состав технических средств, а также паразитные связи и наводки.

Далее при изучении учебного материала этого раздела необходимо уяснить, что многообразие различных технических каналов утечки информации и физических явлений их образования породило и многообразие различных методов и средств скрытого съема информации. При изучении этих методов и средств необходимо знать и понимать основные физические явления, на основе которых они работают.

Материал этого раздела в достаточном объеме изложен в литературе [1-3]. Для более глубокого изучения вопросов и понимания принципов работы различных средств скрытого съема информации можно также ознакомиться с литературой [4].

Контрольные вопросы

1. Назовите причины и условия возникновения утечки информации.
2. Назовите средства переноса информации.
3. Дайте определение каналов утечки информации.
4. Какие существуют виды каналов утечки информации?
5. Дайте краткую характеристику каждого вида канала утечки информации.
6. Что такое технический канал утечки информации?
7. Укажите причины возникновения технических каналов утечки информации.
8. Что является источниками образования технических каналов?

9. За счет каких явлений могут образоваться технические каналы утечки информации?

10. Какие существуют виды каналов утечки речевой информации?

11. Назовите и дайте краткую характеристику методов и средств скрытого съема аудиоинформации.

12. Назовите и дайте краткую характеристику методов и средств скрытого съема видеоинформации.

13. Назовите и дайте краткую характеристику методов и средств скрытого съема информации в электромагнитных и оптических каналах передачи.

РАЗДЕЛ 3. Методы и средства защиты информации

Тема 3.1. Методы и средства защиты, обнаружения и противодействия в акустических каналах передачи информации

Методы защиты речевой информации. Пассивные и активные методы. Защита речевой информации с помощью маскирующих сигналов. Системы виброакустического зашумления. Подавители диктофонов. Блокираторы сотовых телефонов. Защита от узконаправленных микрофонов. Защита от лазерного съема информации. Методы и средства обнаружения радиозакладок. Общая характеристика радиозакладок. Классификация и общая характеристика радиоприемных устройств обнаружения. Индикаторы поля. Панорамные сканирующие радиоприемники. Аппаратно-программные комплексы. Обнаружители диктофонов. Нелинейные радиолокаторы.

Тема 3.2. Методы и средства защиты, обнаружения и противодействия в телефонных линиях связи

Общие принципы защиты телефонных линий связи. Методы и средства пассивной защиты. Фильтры и блокираторы. Методы и средства активной защиты. Методы подавления телефонных закладок. Маскираторы. Средства постановки активных помех. Скремблеры и вокодеры. Методы и средства обнаружения и противодействия. Физические принципы возможности обнаружения средств несанкционированного подключения. Анализаторы телефонных линий. Нейтрализаторы средств несанкционированного подключения. Защита информации в IP-телефонии. Основные способы выявления и противодействия подслушиванию телефонных разговоров.

Тема 3.3. Методы и средства защиты, обнаружения и противодействия в электромагнитных и оптических каналах передачи информации

Защита информации от утечки по электромагнитным каналам. Общая характеристика методов защиты. Защита от утечки за счет микрофонного эффек-

та. Защита от утечки за счет электромагнитного излучения. Защита от утечки за счет паразитной генерации. Защита от утечки по цепям питания. Защита от утечки по цепям заземления. Защита от утечки за счет взаимного влияния проводов и линий связи. Защита от утечки за счет высокочастотного навязывания. Защита от утечки в волоконно-оптических линиях связи. Защита линий связи. Экранирование технических средств и помещений. Применение радиоэлектронных помех.

Тема 3.4. Защита информации в персональных компьютерах и сетях ЭВМ

Основные направления защиты. Программные методы защиты. Аппаратно-программные методы защиты. Криптографические и стеганографические методы защиты. Защита от компьютерных вирусов. Классификация вирусов. Профилактика против заражения вирусами. Обнаружение заражения вирусом. Действия при заражении вирусом. Виды антивирусных программ защиты. Защита информации от перехвата по электромагнитному каналу. Обеспечение безопасности информации в сетях ЭВМ.

Тема 3.5. Криптографические методы защиты информации

Основные понятия, термины и определения криптографии. Методы криптографии. Классификация методов. Методы криптографии с секретными (закрытыми) ключами. Методы замены (подстановки). Моноалфавитная замена. Шифр Вижинера. Шифры Бофора. Гомофоническая замена. Полиалфавитная замена. Полиграммная замена. Шифр Плэйфера. Метод замены с использованием датчика псевдослучайных чисел. Методы перестановки. Простая и усложненная перестановка. Перестановка с использованием графа. Объемная (многомерная) перестановка. Метод перемешивания. Методы криптографии с открытыми ключами.

Тема 3.6. Стеганографические методы защиты информации

Основные понятия, термины и определения стеганографии. Компьютерная стеганография. Виды контейнеров и стегосистем. Методы компьютерной стеганографии. Классификация методов. Методы, основанные на избыточности визуальной и аудиоинформации. Метод замены младших битов. Методы, основанные на использовании специальных свойств компьютерных форматов. Метод замены цветовой палитры. Метод сортировки цветовой палитры. Метод компьютерной стеганографии в JPEG-файлах. Компьютерная стеганография в PRN-файлах. Компьютерная стеганофония. Основные направления использования компьютерной стеганографии и стеганофонии.

Тема 3.7. Электронная цифровая подпись

Аутентификация электронных документов. Модель аутентификации. Виды злоумышленных действий. Активный перехват. Маскарад. Ренегатство. Переделка. Подмена. Повтор. Архитектура системы электронной цифровой подписи. Постановка и проверка электронной цифровой подписи. Генерация ключей. Подписание документа. Проверка подписи. Пользовательские критерии электронной цифровой подписи. Виды нападений на электронную цифровую подпись.

Методические указания

Приступая к изучению материала данного самого большого и важного раздела, необходимо вспомнить или повторить разделы физики, связанные с явлениями, возникающими при прохождении через различные среды акустических, электромагнитных, оптических, тепловых и радиационных волн и излучений, а также явления, на основе которых работают средства скрытого съема информации в различных каналах утечки.

Следует понимать, что средства (методы) защиты информации делятся на средства обнаружения устройств несанкционированного съема информации, средства их подавления (противодействия) и собственно средства защиты.

При изучении методов и средств защиты речевой (акустической) информации необходимо различать защиту по акустическому и вибрационному каналу.

При изучении вопросов защиты речевой информации с помощью маскирующих сигналов необходимо иметь в виду, что важным фактором здесь является не столько уровень самого сигнала, сколько вид его спектра. Подбирая соответствующий вид спектра, можно значительно уменьшить уровень сигнала, что повысит комфортность речевого общения и позволит использовать аппаратуру с более низкими энергетическими показателями.

Для обнаружения радиозакладных устройств используется широкий набор приемных устройств различного вида, от достаточно простых индикаторов поля до специальных аппаратно-программных комплексов, позволяющих проводить локализацию и полный анализ характеристик всех видов сигналов.

Особое внимание необходимо уделить изучению и пониманию принципа работы нелинейного радиолакатора, особенностью которого является то, что он позволяет обнаруживать неработающие (пассивные) устройств несанкционированного съема информации.

Определенное внимание необходимо также уделить вопросам защиты телефонных линий связи, которые в настоящее время широко используются не только для телефонных разговоров, но и для передачи факсимильных сообщений и сообщений по сети Интернет. Здесь надо различать методы пассивной и активной защиты. Необходимо понимать, что применение для защиты актив-

ных помех не приводит к ухудшению качества разговора, так как перед подачей на приемный аппарат они компенсируются.

При изучении методов и средств обнаружения и противодействия в телефонных линиях связи необходимо четко уяснить, какие физические принципы используются для этого.

Необходимо также знать, что скремблеры и вокодеры предназначены для защиты речевой информации, передаваемой по телефонным и другим каналам связи путем соответствующего преобразования аналогового речевого сигнала. Однако необходимо различать принципы их работы. Принцип работы скремблера основан на изменении характеристик речевого сигнала таким образом, чтобы полученный модулированный сигнал, обладая свойствами неразборчивости и неузнаваемости, занимал такую же полосу частот пропускания, что и исходный открытый сигнал. Речевой сигнал при этом может подвергаться частотной инверсии, частотной и временной перестановкам и их комбинациям. Принципы же работы вокодера основаны на оцифровке речевого сигнала и дальнейшем его кодировании. Для повышения стойкости передаваемой информации дополнительно могут использоваться устройства криптографического преобразования цифрового потока.

Для защиты речевой информации, передаваемой по сети Интернет (IP-сети), применяются криптографические алгоритмы шифрования исходных пакетов и сообщений, что позволяет обеспечить гарантированную стойкость информации.

Начиная изучение вопросов, связанных с методами и средствами защиты, обнаружения и противодействия в электромагнитных и оптических каналах передачи информации, необходимо знать, что радиоэлектронные средства обладают основным и нежелательным электромагнитным излучением. Нежелательные излучения подразделяют на побочные, внеполосные и шумовые. Наиболее опасными с точки зрения утечки информации являются побочные излучения. Необходимо также различать ближнее электромагнитное поле (внутри помещения) и дальнее электромагнитное поле (за пределами помещения). В зависимости от этого применяется тот или иной метод защиты. Наиболее эффективным методом защиты в электромагнитных каналах является полное экранирование помещения, где находятся технические средства, а также экранирование линий связи. Однако большие затраты, трудоемкость и внесение определенного дискомфорта для обслуживающего персонала являются существенным препятствием для его широкого применения. Поэтому в большинстве случаев используются методы и средства, предназначенные для защиты конкретных каналов утечки информации.

При изучении вопросов защиты информации в персональных компьютерах и сетях ЭВМ необходимо знать, что основными методами защиты являются программные и аппаратно-программные методы. Особое внимание при этом необходимо обратить на защиту от вирусов. Необходимо знать основные признаки заражения вирусом, действия при заражении вирусом, виды вирусов и антивирусных программ и их возможности. Надо также знать, как проводится

защита информации в персональных компьютерах от перехвата по электромагнитному каналу.

С широким применением вычислительной техники и ее возможностями стали применяться такие методы защиты в персональных компьютерах и сетях ЭВМ, как компьютерная криптография и стеганография. При этом необходимо понимать разницу между криптографией и стеганографией.

Криптография оперирует шифрами, с помощью которых зашифрованные данные становятся доступными только тому, кто знает, как их расшифровать. Методы криптографии делятся на методы с секретными (закрытыми) ключами (симметричное шифрование) и методы с открытыми ключами (несимметричное шифрование). Методы с открытыми ключами обладают большей стойкостью к дешифрованию, но они и более трудоемки. Эти методы используются также и для создания электронной подписи.

В отличие от криптографии, когда противник точно может определить, является ли передаваемая информация зашифрованным текстом, методы стеганографии позволяют встраивать секретную информацию в открытую таким образом, чтобы было невозможным заподозрить существование самой встроенной информации.

Таким образом, если цель криптографии состоит в блокировании несанкционированного доступа к информации путем ее шифрования, то цель стеганографии – в скрытии самого факта существования секретной информации.

Следует знать, что компьютерная стеганография базируется на двух основных принципах. Первый принцип заключается в том, что файлы, содержащие цифровое изображение или звук, могут быть до некоторой степени видоизменены без потери их функциональности. Второй принцип заключается в неспособности органов чувств человека различать незначительные изменения в цвете изображения или качестве звука. Необходимо также знать, что методы компьютерной стеганографии делятся на два вида: методы, основанные на избыточности визуальной и аудиоинформации, и методы, основанные на использовании специальных свойств компьютерных форматов.

Следует понимать, что для повышения эффективности зашиты информации методы криптографии и стеганографии могут быть объединены.

При изучении вопросов, связанных с электронной цифровой подписью, необходимо уяснить, что цифровая подпись является средством защиты электронных документов от подделки и ее применение основано на использовании методов криптографии с открытыми ключами, а также методов компьютерной стеганографии.

Материал этого раздела в достаточном объеме изложен в литературе [1-3, 7, 12, 13]. Для более глубокого изучения вопросов, связанных с защитой информации в различных каналах утечки, можно ознакомиться с литературой [4, 5, 14]. По защите информации в персональных компьютерах и сетях ЭВМ рекомендуется дополнительная литература [6, 8]. Для более детального изучения методов криптографии и стеганографии рекомендуется воспользоваться

литературой [9, 10]. Полезным также будет ознакомиться с некоторыми материалами, опубликованными в журнале «Конфидент» за 1998-2003 гг.

Контрольные вопросы

1. Дайте характеристику пассивных и активных методов защиты речевой информации.
2. Для каких целей используются акустические и вибрационные излучатели при защите речевой информации?
3. На каких принципах работают подавители диктофонов?
4. Назовите меры, которые необходимо принимать для защиты от узконаправленных микрофонов.
5. Какие методы и средства используются для защиты от лазерных микрофонов?
6. Дайте характеристику средств обнаружения радиозакладных устройств.
7. В чем отличие индикаторов поля, панорамных сканирующих радиоприемников и аппаратно-программных комплексов?
8. На каком принципе работают обнаружители диктофонов?
9. На каком принципе работают нелинейные радиолокаторы?
10. Что является помехой для нелинейного радиолокатора и как отличить полезный сигнал от помехового?
11. Дайте характеристику пассивных и активных методов защиты телефонных линий связи.
12. Как работают маскираторы и средства постановки активных помех в телефонных линиях связи?
13. Как работают аналоговые и цифровые скремблеры и в чем их отличие?
14. Что такое вокодеры и для чего они используются?
15. На каких принципах работают анализаторы телефонных линий?
16. На каком принципе работают нейтрализаторы средств несанкционированного подключения?
17. Как осуществляется защита информации в IP-телефонии?
18. Какие методы и средства используются для защиты информации в электромагнитных каналах передачи?
19. Как осуществляется защита от утечки за счет микрофонного эффекта?
20. Как осуществляется защита от утечки за счет электромагнитного излучения?
21. Как осуществляется защита от утечки за счет паразитной генерации?
22. Как осуществляется защита от утечки по цепям питания и заземления?
23. Как осуществляется защита от утечки за счет взаимного влияния проводов и линий связи?
24. Как осуществляется защита от утечки за счет высокочастотного навязывания?
25. Как осуществляется защита от утечки в волоконно-оптических линиях связи?

26. Назовите основные методы защиты, применяемые в линиях связи.

27. Для каких целей используется экранирование технических средств и помещений?

28. Какие виды радиоэлектронных помех используются для защиты информации в электромагнитных каналах передачи?

29. Какие методы и средства используются для защиты информации в персональных компьютерах и сетях ЭВМ?

30. Дайте характеристику видов компьютерных вирусов и антивирусных программ.

31. Назовите признаки заражения компьютера вирусом и необходимые действия при этом.

32. В чем заключается профилактика против компьютерных вирусов?

33. Назовите методы криптографии, используемые для защиты информации.

34. В чем различие методов криптографии с секретными (закрытыми) и открытыми ключами?

35. Что такое компьютерная стеганография?

36. В чем отличие стеганографических методов защиты информации от криптографических?

37. На каких принципах базируется компьютерная стеганография?

38. Назовите методы компьютерной стеганографии, используемые для защиты информации.

39. Для чего используется цифровая подпись?

40. Какие принципы (методы) криптографии и стеганографии используются для реализации цифровой подписи?

РАЗДЕЛ 4. Организация защиты информации на объекте

Тема 4.1. Построение систем охраны и защиты информации на объекте

Классификация способов и средств защиты информации. Способы защиты. Препятствие. Управление. Маскировка. Регламентация. Принуждение. Побуждение. Физические, аппаратные, программные, организационные, законодательные, морально-этические средства защиты. Построение системы охраны и защиты объекта. Зоны безопасности объекта. Схема охраны и защиты объекта. Виды технических средств охраны и защиты объекта. Технические средства обнаружения, отражения и ликвидации угроз. Основные и дополнительные технические средства защиты. Охранно-пожарная сигнализация. Охранное телевидение. Охранное освещение.

Тема 4.2. Поиск устройств несанкционированного съема информации

Подготовка поискового мероприятия. Этапы работ поискового мероприятия. Проведение поискового мероприятия. Осмотр окружающей территории и помещения. Исследование электромагнитных сигналов. Исследование телефонных систем. Исследование механической (виброакустической) энергии. Исследование электромагнитных излучений оптического диапазона. Исследование ядерного излучения. Радиомониторинг.

Методические указания

Данный раздел является заключительным и его изучение базируется на знании материала предыдущих разделов.

Прежде всего необходимо уяснить, что использование методов и средств защиты информации, рассмотренных в предыдущем разделе, может быть эффективным только в том случае, если правильно построена система охраны и защиты информации на объекте. Необходимо вспомнить также материал первого раздела, в котором говорится о комплексном подходе к защите информации.

Рассматривая систему охраны и защиты объекта, необходимо уяснить, что она строится из нескольких зон безопасности, каждая из которых имеет свои методы и средства защиты. При этом основу построения каждой зоны безопасности составляет принцип равнопрочности ее границ.

Необходимо также знать, какие составляющие входят в общую систему охраны и защиты объекта и какими конкретно техническими средствами они реализуются, включая средства, рассмотренные в предыдущем разделе, и средства, рассматриваемые в данном разделе.

При рассмотрении вопросов, связанных с организацией, подготовкой и проведением поисковых мероприятий на объекте, необходимо в первую очередь определить, какие каналы утечки информации могут иметь место на объекте, знать, какими методами и средствами может быть снята информация с этих каналов, а также какими методами и средствами можно осуществить защиту информации в этих каналах. Для этого необходимо вспомнить материал, изложенный во втором и третьем разделах.

Следует также знать, что само поисковое мероприятие состоит из нескольких этапов, каждый из которых имеет свои особенности.

Для изучения вопросов данного раздела достаточно ознакомиться с литературой [1, 3]. Дополнительные знания могут быть получены при ознакомлении с материалами, опубликованными в журнале «Конфидент» № 4-5 за 2000 г., № 3 за 2003 г. и № 1 за 2004 г.

В заключение следует отметить, что достаточно большое количество материала, связанного с защитой информации и необходимого для изучения данной дисциплины, может быть найдено в сети Интернет с использованием известных поисковых систем и соответствующих ключевых слов, а также названий фирм,

связанных с защитой информации. Однако следует иметь в виду, что некоторые материалы носят рекламный характер и имеют ряд неточностей и ошибок. Поэтому пользоваться ими необходимо с определенной осторожностью.

Контрольные вопросы

1. Какие способы и средства защиты используются при построении системы охраны и защиты информации на объекте?
2. Назовите зоны безопасности объекта.
3. Какие средства обнаружения угроз используются при построении системы охраны и защиты объекта?
4. Какие средства отражения и ликвидации угроз используются при построении системы охраны и защиты объекта?
5. Какие технические средства используются для защиты информации при построении системы охраны и защиты объекта?
6. Из каких этапов состоит поисковое мероприятие?
7. Какие действия осуществляются при осмотре окружающей территории?
8. Какие действия осуществляются при осмотре помещения?
9. Какие действия осуществляются при исследовании электромагнитных сигналов?
10. Какие действия осуществляются при исследовании телефонных систем?
11. Какие действия осуществляются при исследовании механической (виброакустической) энергии?
12. Какие действия осуществляются при исследовании электромагнитных излучений оптического диапазона?
13. Какие действия осуществляются при исследовании ядерного излучения.
14. Что такое радиомониторинг и для чего он проводится?

ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ

1. Определение уровня качества технических средств защиты информации.

Изучаются методы определения показателей качества технических средств защиты информации и практически определяется их уровень качества с использованием комплексных показателей.

2. Исследование разборчивости речи методом артикуляционных измерений при защите речевой информации различными видами маскирующих сигналов.

Изучается метод определения разборчивости речи с помощью артикуляционных измерений, который практически используется для исследования защиты речевой информации маскирующими сигналами различных видов.

3. Изучение криптографических методов защиты информации.

Изучаются методы защиты информации с помощью различных видов шифров, используемых в криптографии.

4. Исследование метода компьютерной стеганографии для защиты информации.

Изучается метод замены младших битов, используемый в компьютерной стеганографии для защиты информации.

Все практические работы проводятся в лабораториях кафедры, оборудованных электронно-вычислительной техникой. Для проведения практических работ используются оригинальные программные средства, разработанные на кафедре и позволяющие проводить как контроль теоретических знаний студентов с допуском их к выполнению работы, так и выполнение самой работы с контролем правильности выполнения задания. Практические работы могут выполняться как в индивидуальном режиме (при достаточном количестве вычислительной техники), так и в групповом (бригадами по 2-4 студента).

Для более эффективного проведения практических работ каждая работа выполняется в течение двух 2-часовых занятий, следующих одно за другим.

ЛАБОРАТОРНАЯ РАБОТА

Выполняется лабораторная работа на тему *Изучение технических характеристик и выбор технических средств защиты, обнаружения и противодействия в каналах передачи информации.*

Изучаются различные виды технических средств защиты информации, их характеристики и возможности. На основе знаний, полученных на практических занятиях, проводится обоснование и выбор технического средства, обладающего более высоким уровнем качества, для решения конкретной задачи по защите, обнаружению или противодействию в каналах передачи информации.

Лабораторная работа, как и практические работы, проводится в лабораториях кафедры, оборудованных электронно-вычислительной техникой.

При необходимости вместо лабораторной работы могут выполняться практические работы № 2 и № 4.

КОНТРОЛЬНАЯ РАБОТА И ЕЕ КРАТКАЯ ХАРАКТЕРИСТИКА

Контрольная работа состоит из двух заданий.

Первое задание посвящено определению уровня качества технических средств защиты информации и тематически связано с практической работой № 1. В задании приводятся исходные данные для трех различных типов устройств защиты информации одного вида. Перед проведением расчетов необходимо предварительно подготовить или преобразовать некоторые исходные данные с подробным обоснованием принятых значений. Краткие методические указания, необходимые формулы для расчета и литература приведены в самом задании.

Второе задание посвящено изучению вопросов защиты информации с помощью методов криптографии и тематически связано с практической работой № 3. Оно состоит из пяти отдельных заданий по зашифрованию и расшифрова-

нию небольших отрезков связного текста (пословиц и поговорок) различными методами криптографии. Необходимая литература приведена в конце задания.

Подробные пояснения при выполнении заданий являются обязательными. Оформление контрольной работы в электронном виде является желательным и приветствуется.

Всего разработано 30 вариантов заданий, каждый из которых компактно размещен на двух сторонах одного листа. Варианты заданий можно также получить и в электронном виде.

При выполнении контрольной работы рекомендуется использовать литературу [12] для первого задания и [1, 13] для второго задания.

Литературу [12, 13] также можно получить в электронном виде.

ПЕРЕЧЕНЬ КОМПЬЮТЕРНЫХ ПРОГРАММ, ИСПОЛЬЗУЕМЫХ ПРИ ПОДГОТОВКЕ

1. Программа «LEVEL».
2. Программа «SPEECH».
3. Программа «CRYPT».
4. Программа «STEGAN».
5. Программа «SYSCONTR».
6. Программа ADV Stego Plugin.
7. Программа Advanced Viewer.

ЛИТЕРАТУРА

Основная

1. Петраков А.В. Основы практической защиты информации. - М.: Радио и связь, 2000. - 368 с.
2. Ярочкин В.И. Информационная безопасность. - М.: Международные отношения, 2000. - 400 с.

Дополнительная

3. Петраков А.В., Лагутин В.С. Защита абонентского телетрафика. - М.: Радио и связь, 2001. - 504 с.
4. Рудометов Е.А., Рудометов В.Е. Электронные средства коммерческой разведки и защиты информации. – СПб.: Полигон, 2000. – 224 с.
5. Андрианов В.И., Соколов А.В. Устройства для защиты объектов и информации. – СПб.: Полигон, 2000. – 256 с.
6. Соколов А.В., Степанюк О.М. Методы информационной защиты объектов и компьютерных сетей. – СПб.: Полигон, 2000. – 272 с.
7. Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. - СПб.: БХВ - Петербург, 2002. - 496 с.

8. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ – Петербург, 2000. – 384 с.
9. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ – ОБРАЗ, 2001. –368 с.
10. Грибунин В.Г., Оков И.Н., Турничев И.В. Цифровая стеганография. – М.: СОЛОН – Пресс, 2002. – 272 с.
11. ГОСТ 50922-96. Защита информации. Основные термины и определения. - М.: Госстандарт России, 1996. - 7 с.

Методические пособия и разработки

12. Алефиренко В.М., Шамгин Ю.В. Основы защиты информации: Практикум для студ. спец. "Техническое обеспечение безопасности" и "Моделирование и компьютерное проектирование радиоэлектронных средств" дневной, вечерней и заочной форм обучения: В 2ч. Ч.1. - Мн.: БГУИР, 2004. - 43 с.
13. Алефиренко В.М. Основы защиты информации: Практикум для студ. спец. "Техническое обеспечение безопасности" и "Моделирование и компьютерное проектирование радиоэлектронных средств" дневной, вечерней и заочной форм обучения: В 2ч. Ч.2. - Мн.: БГУИР, 2004. - 44 с.
14. Алефиренко В.М., Давыдов Г.В., Шамгин Ю.В. Расчет и измерение разборчивости речи для акустических устройств РЭС: Метод. указания к практическим занятиям по курсу "Конструирование РЭС" для студ. спец. "Проектирование и производство РЭС". - Мн.: БГУИР, 1998. - 32 с.

Св. план 2005, поз. 6

Учебное издание

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Методические указания и контрольные вопросы
для студентов специальностей
«Техническое обеспечение безопасности» и
«Моделирование и компьютерное проектирование
радиоэлектронных средств»
заочной формы обучения

Составитель
Алефиренко Виктор Михайлович

Редактор Т.Н. Крюкова
Корректор Е.Н. Батурчик

Подписано в печать 13.05.2005. Формат 60x84 1/16. Бумага офсетная.
Гарнитура «Таймс». Печать ризографическая. Усл. печ. л. 1,4.
Уч.-изд. л. 1,0. Тираж 100 экз. Заказ 167.

Издатель и полиграфическое исполнение: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
Лицензия на осуществление издательской деятельности № 02330/0131518 от 01.04.2004.
Лицензия на осуществление полиграфической деятельности № 02330/0133108 от 30.04.2004.
220013, Минск, П. Бровки, 6