МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«11» 04 2023 г.

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Методические указания по выполнению самостоятельной работы
для студентов направления подготовки
10.03.01«Информационная безопасность» и специальности 10.05.02 «Информационная безопасность телекоммуникационных систем»

Курск 2023

УДК 004

Составители: Кулешова Е.А.

Рецензент

Кандидат технических наук, доцент кафедры «Вычислиельная техника» А.В. Киселев

Техническая защита информации: методические указания по выполнению самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 23 с.: Библиогр.: с. 22.

Содержатся сведения о темах для самостоятельного изучения по дисциплине «Техническая защита информации», необходимые для успешного освоения дисциплины. Указывается порядок выполнения самостоятельной работы всех предусмотренных учебным планом видов, приводятся рекомендации по оформлению результатов работы.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов направления подготовки 10.03.01«Информационная безопасность» и специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 1,34. Уч.-изд. л. 1,21. Тираж 100 экз. Заказ. Бесплатно. 243
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Введение

Самостоятельная работа - это индивидуальная или коллективная учебная деятельность, осуществляемая без непосредственного руководства преподавателя, но по его заданиям и под его контролем.

Самостоятельная работа студентов включает:

- изучение лекционного материала по конспекту с использованием рекомендованной литературы;
- отработку изучаемого материала по печатным и электронным источникам, конспектам лекций;
- подготовку к выполнению лабораторных работ;
- выполнение отчетов по лабораторным работам и подготовку к их защите;
- индивидуальные задания (решение задач, подготовка сообщений, докладов, исследовательские работы и т.п.);
- работу над творческими заданиями;
- подготовку кратких сообщений, докладов, рефератов, самостоятельное составление задач по изучаемой теме (по указанию преподавателя).

Назначение самостоятельной работы студентов.

- ***Овладение знаниями***, что достигается:

чтением текста (учебника, первоисточника, дополнительной литературы), составлением плана текста, графическим структурированием текста, конспектированием текста, выписками из текста, работой со словарями и справочниками, поиском информации в сети Интернет и т.п.;

- ***закрепление знаний,*** что достигается:

работой с конспектом лекций, обработкой текста, повторной работой над учебным материалом (учебником, первоисточником, дополнительной литературой), составлением плана, составлением таблиц для систематизации учебного материала, ответами на контрольные вопросы, заполнением рабочей тетради, аналитической обработкой текста (аннотирование, рецензирование,

реферирование, конспект-анализ и др), составлением библиографии и т.п.;

- ***формирование навыков и умений***, что достигается:

решением задач и упражнений по образцу, решением вариативных задач, выполнением схем, выполнением расчетов, решением ситуационных задач, подготовкой к дискуссиям, проектированием и моделированием разных видов и компонентов профессиональной деятельности, математическим описанием опытно экспериментальной работой и т.п.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от поставленной цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Контроль результатов внеаудиторной самостоятельной работы студентов может осуществляться в пределах времени, отведенного на обязательные учебные занятия по дисциплине и внеаудиторную самостоятельную работу студентов по дисциплине, может проходить в письменной, устной или смешанной форме.

Текущий контроль качества выполнения самостоятельной работы может осуществляться с помощью:

- контрольного опроса;
- собеседования;
- автоматизированного программированного контроля (машинного контроля, тестирования с применением ЭВМ).

Контроль выполнения индивидуальных заданий осуществляется поэтапно в соответствии с разработанным преподавателем графиком.

Самостоятельная работа по темам 3 и 10. Оптическая разведка. Противодействие видовой разведке.

Цель работы - ознакомится со способами формирования оптического канала утечки и способами предотвращения утечки информации по техническим каналам. Провести анализ технических средств перехвата информации в оптическом диапазоне.

Задание. Провести анализ технических средств перехвата информации в оптическом диапазоне волн, используя каталог технических средств защиты информации, представленный на сайте **http://bnti.ru/** (Техника для спецслужб. Бюро научно-технической информации.).

Для выполнения данной работы необходимо использовать следующие каталоги:

1) «Оборудование для оперативно-розыскной деятельности» / «Средства скрытого видеонаблюдения»
2) «Оборудование для оперативно-розыскной деятельности» / «Средства скрытого фотографирования»
3) «Оборудование для оперативно-розыскной деятельности» / «Системы перехвата каналов связи» / «Системы контроля оптических линий связи»
4) «Тепловизионные и оптические системы».

Проведите подробный анализ 8-10 средств технической защиты из перечисленных выше каталогов и занесите данные в таблицу.

	Наименование	Изображение	Технические характеристики
1			
…	…	…	…
10			

Контрольные вопросы:

1) Перечислите характеристики технического канала утечки информации.
2) Перечислите показатели, характеризующие оптический прибор перехвата.

3) Перечислите принципы выявления закладных устройств оптического перехвата.

4) Каковы основные способом борьбы с утечкой информации по оптическим каналам?

5) Какие мероприятия должны быть предусмотрены при построении системы защиты оптических каналов?

6) Перечислите характеристики средств наблюдения.

Самостоятельная работа по темам 1, 2 и 8. Технические средства разведки. Общие сведения. Радиоэлектронная разведка. Радиоэлектронное противодействие и радиомаскировка.

Цель работы - ознакомится со способами формирования канала утечки и способами предотвращения утечки информации по техническим каналам. Провести анализ технических средств перехвата информации в радиоэлектронном и электромагнитном диапазонах.

Задание. Провести анализ технических средств перехвата информации радиоэлектронном и электромагнитном диапазонах, используя каталог технических средств защиты информации, представленный на сайте **http://bnti.ru/** (Техника для спецслужб. Бюро научно-технической информации.).

Для выполнения данной работы необходимо использовать следующие каталоги:

1) «Оборудование для оперативно-розыскной деятельности» / «Системы перехвата каналов связи» / «Системы перехвата сотовой связи»

2) «Оборудование для оперативно-розыскной деятельности» / «Системы перехвата каналов связи» / «Системы перехвата спутниковой связи»

3) «Оборудование для оперативно-розыскной деятельности» / «Системы перехвата каналов связи» / «Системы перехвата пейджинговой связи»

4) «Оборудование для оперативно-розыскной деятельности» / «Системы перехвата каналов связи» / «Системы перехвата факсов»

Проведите подробный анализ 8-10 средств технической защиты из перечисленных выше каталогов и занесите данные в таблицу.

	Наименование	Изображение	Технические характеристики
1			
…	…	…	…
10			

Контрольные вопросы:

1. Какие задачи выполняют органы радиотехнической разведки?
2. Из чего состоит типовой комплекс перехвата радиосигналов?
3. Что такое антенна?
4. Что такое радиоприёмник?
5. Функции радиоприёмника
6. Виды радиоприёмников

Самостоятельная работа по темам 4 и 9. Акустическая разведка. Противодействие акустической разведке.

Цель работы - ознакомится со способами формирования канала утечки и способами предотвращения утечки информации по акустическим каналам. Провести анализ технических средств перехвата информации в акустическом диапазоне.

Задание. Провести анализ технических средств перехвата информации в акустическом диапазоне волн, используя каталог технических средств защиты информации, представленный на сайте **http://bnti.ru/** (Техника для спецслужб. Бюро научно-технической информации.).

Для выполнения данной работы необходимо использовать следующие каталоги:

1) «Средства многоканальной видео-, аудиозаписи и оповещения» / «Средства многоканальной записи телефонных переговоров»

2) «Средства многоканальной видео-, аудиозаписи и оповещения» / «Средства многоканальной записи переговоров»

3) «Оборудование для оперативно-розыскной деятельности» / «Средства акустического контроля»

4) «Оборудование для оперативно-розыскной деятельности» / «Средства контроля телефонных переговоров»

Проведите подробный анализ 8-10 средств технической защиты из перечисленных выше каталогов и занесите данные в таблицу.

	Наименование	Изображение	Технические характеристики
1			
…	…	…	…
10			

Контрольные вопросы

1 Область применения параболического микрофона?
2 Перечислите акустические закладные устройства.

3 Перечислите акустические закладки использующие телефонные линии.

4 Перечислите методы обработки речевых сигналов.

5 Назовите основные характеристики направленных микрофонов.

Самостоятельная работа по темам 5-7. Компьютерная разведка. Средства технической разведки. Противодействие техническим разведкам.

Цель работы - ознакомится со способами формирования канала утечки и способами предотвращения утечки информации. Провести анализ технических средств перехвата информации в каналах, образованных средствами вычислительной техники.

Задание.

1) Изучить технические средства перехвата информации в каналах, образованных средствами вычислительной техники, используя каталог технических средств защиты информации, представленный на сайте **http://bnti.ru/** (Техника для спецслужб. Бюро научно-технической информации.). Для выполнения данной работы необходимо использовать следующие каталоги: «Оборудование для оперативно-розыскной деятельности / Системы контроля электронной информации / Системы контроля электронной информации в компьютерных сетях»

2) Изучить состав «кейлоггеров», представленных на сайте **https://www.keyloggers.com/ru/**

3) Провести подробный анализ 8-10 средств технической защиты из перечисленных выше каталогов и занести данные в таблицу.

	Наименование	Изображение	Технические характеристики
1			
…	…	…	…
10			

Контрольные вопросы

1) Что такое технические средства приема, обработки, хранения и передачи информации (ТСПИ)?

2) Перечислите технические каналы утечки информации, как они классифицируются в зависимости от физической природы возникновения

информационных сигналов, а также среды их распространения и способов перехвата?

3) Что такое ВТСС?
4) Что такое случайная антенна?
5) Что такое электромагнитные каналы утечки информации?
6) Что такое параметрические каналы утечки информации?

Самостоятельная работа по темам 11-12. Защита от внедряемых на объекты разведывательных устройств. Технические средства защиты информации.

Цель работы - ознакомится со способами формирования канала утечки и способами предотвращения утечки информации. Провести анализ технических средств перехвата информации в материально-вещественном канале утечки.

Задание. Провести анализ технических средств перехвата информации в материально-вещественном канале утечки, используя каталог технических средств защиты информации, представленный на сайте **http://bnti.ru/** (Техника для спецслужб. Бюро научно-технической информации.).

Для выполнения данной работы необходимо использовать следующие каталоги:

1) «Антитеррористическое оборудование» / «Средства обнаружения и идентификации веществ»
2) «Досмотровое оборудование» / «Средства обнаружения радиации»

Проведите подробный анализ 8-10 средств технической защиты из перечисленных выше каталогов и занесите данные в таблицу.

	Наименование	Изображение	Технические характеристики
1			
…	…	…	…
10			

Контрольные вопросы

1) Особенность материально-вещественного канала утечки информации.
2) Основные источники информации в материально-вещественном канале.
3) Утечка какого вида информации возможна в материально-вещественном канале?

4) Приемники информации в материально-вещественном канале утечки информации
5) Средства обнаружения утечки информации о радиоактивных веществах.

Рекомендации по выполнению самостоятельной работы

Изучение теоретических основ дисциплин

Изучение теоретической части дисциплин способствует углублению и закреплению знаний, полученных на аудиторных занятиях, а также развивает у студентов творческие навыки, инициативу и умение рационально организовать свое время.

Самостоятельная работа при изучении дисциплины включает:

- работу над конспектом лекций;
- изучение рекомендованной литературы;
- поиск и ознакомление с информацией в сети Интернет;
- подготовку к различным формам контроля (контрольный опрос, собеседование, тесты);
- подготовку ответов на вопросы по различным темам дисциплины, в том числе заданным преподавателем по результатам контроля знаний.

Материал, законспектированный в течение лекций, необходимо регулярно прорабатывать и дополнять сведениями из других источников и литературы.

При освоении дисциплины сначала необходимо по каждой теме изучить рекомендованную литературу и составить краткий конспект основных положений, терминов, сведений, требующих запоминания и являющихся основополагающими в этой теме для освоения последующих тем курса. После этого следует разобраться с обоснованием утверждений. Для расширения знаний по дисциплине рекомендуется использовать Интернет-ресурсы; проводить поиски в различных системах и использовать материалы сайтов, рекомендованных преподавателем.

По требованию преподавателя конспект лекций предоставляется ему для проверки. Замеченные недостатки и внесенные замечания и предложения следует отработать в приемлемые сроки.

Практические задания

При подготовке и защите практических заданий необходимо обращать особое внимание на полноту и грамотность выполнения отчета по работе, наличие в них кратких обоснований принимаемых решений и выводов по результатам работы. При несоответствии отчета этим требованиям преподаватель может возвращать его на доработку. При опросе студентов основное внимание обращается на усвоение ими основных теоретических положений, на которых базируется данная работа, и понимание того, как эти положения применяются на практике. Для освоения дисциплины в полном объеме студенту необходимо посещать все аудиторные занятия и самостоятельно прорабатывать полученный материал.

Контроль результатов самостоятельной работы студентов осуществляется перед выполнением практических заданий, в процессе защиты отчета по работе, а так же на зачете.

При самостоятельном изучении дисциплины, подготовке к аудиторным занятиям и выполнении домашних заданий студенты должны использовать рекомендованную учебную литературу и учебно-методические указания. Источники информации доступны на сайте кафедры.

Самостоятельная работа осуществляется при подготовке к работе в соответствии с заданными темами, подготовке ответов к вопросам для самоконтроля и контрольным вопросам.

Отчет по практическим заданиям выполняется индивидуально или один на бригаду по решению преподавателя.

Отчет должен содержать все предусмотренные методическими указаниями разделы, включая задания и краткое изложение необходимого теоретического материала.

Темы рефератов по курсу

1.Методы борьбы с фишинговыми атаками.

2.Законодательство о персональных данных.

3.Защита авторских прав.

4.Назначение, функции и типы систем видеозащиты.

5.Как подписывать с помощью ЭЦП электронные документы различных форматов.

6.Обзор угроз и технологий защиты Wi-Fi-сетей.

7.Проблемы внедрения дискового шифрования.

8.Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.

9.Особенности процессов аутентификации в корпоративной среде.

10.Квантовая криптография.

11.Утечки информации: как избежать. Безопасность смартфонов.

12.Безопасность применения пластиковых карт - законодательство и практика.

13.Защита CD- и DVD-дисков от копирования.

14.Современные угрозы и защита электронной почты.

15.Программные средства анализа локальных сетей на предмет уязвимостей.

16.Безопасность применения платежных систем - законодательство и практика.

17.Аудит программного кода по требованиям безопасности.

18.Антишпионское ПО (antispyware).

19.Обеспечение безопасности Web-сервисов.

20.Защита от внутренних угроз.

21.Технологии RFID.

22.Уничтожение информации на магнитных носителях.

23.Ботнеты - плацдарм современных кибератак.

24.Цифровые водяные знаки в изображениях.

25.Электронный документооборот. Модели нарушителя.

26.Идентификация по голосу. Скрытые возможности.

27.Безопасность океанских портов.

28.Безопасность связи.

29.Безопасность розничной торговли.

30.Банковская безопасность.

31.Информатизация управления транспортной безопасностью.

32.Биопаспорт.

33.Обзор современных платформ архивации данных.

34.Что такое консалтинг в области ИБ.

35.Бухгалтерская отчетность как источник рассекречивания информации.

36.Управление рисками: обзор употребительных подходов.

37.Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности.

38.Распределенные атаки на распределенные системы.

39.Оценка безопасности автоматизированных систем.

40.Windows и Linux: что безопаснее?

41.Функциональная безопасность программных средств.

42.Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств.

43.Информационная безопасность: экономические аспекты.

Контрольные вопросы для самоконтроля

Тема 1. Технические разведки. Общие сведения.

1. Элементы, содержащиеся в любой системе технической разведки.
2. Реализация обнаружения и анализа демаскирующих признаков в системе технической разведки.
3. Операции выполнения ДП по физической сути.
4. Прямые и побочные каналы утечки информации.
5. Специальные технические средства и решения, формирующие каналы утечки информации.
6. Достоинства и недостатки технической разведки.
7. Классификация технических разведок по видам носителей аппаратуры разведки.
8. Классификация технических разведок по способу добывания информации и типу аппаратуры разведки.

Тема 2. Радиоэлектронная разведка.

1. Этапы разделение радиоэлектронной разведки.
2. Критерии выбора стратегий разведки и маскировки
3. Способы определения частоты сигналов РЭС.
4. Назовите основные способы пеленгации радиоэлектронных средств.
5. Принципы работы доплеровского пеленгатора.
6. Назначение радиолокационная разведка.
7. Сущность теплового радиоизлучения.
8. Разведка побочных электромагнитных излучений и наводок.

Тема 3. Оптическая разведки.

1. Основные сведения об оптических линзовых системах.
2. Основные этапы визуально-оптическая разведка.
3. Фотографическая и фототелевизионная разведка.
4. Диагностические тепловые системы с охлаждаемыми и неохлаждаемыми приемниками излучения.
5. Назначение теплопеленгационной станции.
6. В чем заключается оптическая локация ?
7. Структурная схема дальномерного канала.

Тема 4. Акустическая разведка.

1. Область применения параболического микрофона.
2. Акустические закладные устройства.
3. Использование закладных устройств.
4. Классификация радиозакладок по используемому диапазону.
5. Скрытая запись на диктофон как способ документирования информации.
6. Акустические закладки использующие телефонные линии.

7. Использование диапазона радиоволн.
8. Методы обработки речевых сигналов.
9. Назовите основные характеристики направленных микрофонов.
10. Использование адаптивного фильтра.

Тема 5. Компьютерная разведка.

1. Методы взлома компьютерных систем.
2. Программы шпионы.
3. Классификация программных закладок.
4. Основные группы деструктивных действий, осуществляемые программными закладками.
5. Модели воздействия программных закладок на компьютеры.
6. Статистическое и динамическое искажения.
7. Клавиатурные шпионы.
8. В чем заключается метод криптоаналитических закладок ?

Тема 6. Средства технической разведки.

1. Сделайте выборку средств космической разведки.
2. Назовите основные средства воздушной разведки.
3. Какие средства контроля классификаций морская разведка бывают ?
4. Автоматические устройства технической разведки кабельных линий.
5. Портативная техника для разведслужб.
6. Скрыто устанавливаемые микрофоны.
7. Классификация радиопередатчиков телефонных линий.

Тема 7. Противодействия техническим разведкам.

1. Роль противодействия техническим средствам разведки.
2. Этапы управления сложными системами.
3. Методы борьбы с системами и средствами управления противника.
4. Способы достижения противодействия распознаванию типа объекта.
5. Основные направления противодействия ТСР. Сравнение скрытия информации и технической дезинформации.

Тема 8. Радиоэлектронная противодействие и радиомаскировка.

1. Назовите цель пассивной радиомаскировки.
2. Цель применения экранирования.
3. Основное назначение фильтров. Типы фильтров.
4. Требования к заземлению технических средств.
5. Что представляют собой специальные помещения и с какой целью они используются?
6. Способы маскировки от средств радиолокационной разведки.

7. Назовите цель активной радиомаскировки.
8. Перечислите способы активного подавления РЛС.
9. Какие особенности противодействия радио- и радиотехнической разведке?
10. Какие существуют методы криптографической защиты информации?

Тема 9. Противодействие акустической разведки.

1. В чём заключается метод слухового контроля? Цель его применения.
2. Какие существуют пассивные методы акустической защиты?
3. Эффективность применения экранных глушителей звука.
4. Характеристика прозрачных переговорных кабин.
5. Как осуществляется оценка звукоизоляции объекта?
6. Какие существуют активные методы акустической защиты?
7. Технические защитные устройства.

Тема 10. Противодействие видовой разведки.

1. Как осуществляется защита от оптической и оптикоэлектронной разведок?
2. Назовите способы достижения нарушения контакта при противодействии средствам оптической и радиолокационной разведке (РЛР).
3. Что представляет собой защита от видовой РЛР?
4. Способы снижения уровня сигнала на входе приёмника РЛС.

Тема 11. Защита от внедряемых на объекты разведывательных устройств.

1. Этапы защиты от внедряемых на объекты разведывательных устройств.
2. Содержание поисковых мероприятий.
3. Назовите цель применения рентгеновского контроля.
4. Сравнительная характеристика поисковых приборов.
5. Основная задача обследования помещений.
6. Цель проведения проверки электроустановок и коммуникаций.

Тема 12. Технические средства защиты информации.

1. Область применения нелинейных локаторов.
2. Какие существуют методы защиты информации от утечки по электромагнитному каналу?
3. Предназначение отсекающего линейного фильтра.
4. Способ предотвращения несанкционированного использования сотовых телефонов.
5. Сравните отечественные и зарубежные помехоподавляющие фильтры.

Список литературы

1. Котенко В. В. Теория информации: учебное пособие / В.В. Котенко. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 240 с. // Режим доступа - https://biblioclub.ru/index.php?page=book&id=561095. – Текст: электронный.
2. Горбунов, А. В. Проектирование защищённых оптических телекоммуникационных систем : учебное пособие : [16+] / А. В. Горбунов, Ю. В. Зачиняев, А. П. Плёнкин. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. – 128 с. :– URL: https://biblioclub.ru/index.php?page=book&id=598665 (дата обращения: 20.08.2021). Режим доступа: по подписке. – Текст : электронный.
3. Зайцев А.П. Технические средства и методы защиты информации [Текст]: учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. – М.: ООО «Издательство Машиностроение», 2009. – 508 с.
4. Титов А.А. Инженерно-техническая защита информации [Электронный ресурс]: учебное пособие / А.А. Титов. - Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. - 195 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=208567
5. Меньшаков Ю.К. Основы защиты от технических разведок[Текст]: учебное пособие / Ю.К. Меньшаков. – М.: Издательство МГТУ им. Н.Э. Баумана, 2011. – 478 с.
6. Меньшаков Ю.К. Виды и средства иностранных технических средств разведок[Текст]: учебное пособие Ю.К. Меньшаков. – М.: Издательство МГТУ им. Н.Э. Баумана, 2009. – 656 с.
7. Креопалов В.В. Технические средства и методы защиты информации [Электронный ресурс]: учебно-практическое пособие / В.В. Креопалов. - М. : Евразийский открытый институт, 2011. - 278 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=90753
8. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник. - 2-е изд., испр. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. // Режим доступа - http://biblioclub.ru/index.php?page=book&id=429070
9. Информационная безопасность и защита информации [Текст]: учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. - 384 с.

10. Грибунин В. Г. Комплексная система защиты информации на предприятии [Текст] : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. - 416 с.