Федеральное государственное бюджетное образовательное учреждение высшего образования
«Алтайский государственный технический университет им. И.И. Ползунова»

**СОГЛАСОВАНО**

Декан ФИТ А.С. Авдеев

# Рабочая программа дисциплины

Код и наименование дисциплины: **Б1.Б.18 «Техническая защита информации»**

Код и наименование направления подготовки (специальности): **10.03.01 Информационная безопасность**

Направленность (профиль, специализация): **Организация и технология защиты информации**

Статус дисциплины: **обязательная часть (базовая)**

Форма обучения: **очная**

| Статус | Должность | И.О. Фамилия |
|---|---|---|
| Разработал | заведующий кафедрой | А.Г. Якунин |
| Согласовал | Зав. кафедрой «ИВТиИБ» | А.Г. Якунин |
| | руководитель направленности (профиля) программы | Е.В. Шарлаев |

г. Барнаул

## 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

| Код компетенции из УП и этап её формирования | Содержание компетенции | В результате изучения дисциплины обучающиеся должны: | | |
|---|---|---|---|---|
| | | знать | уметь | владеть |
| ОПК-1 | способностью анализировать физические явления и процессы для решения профессиональных задач | основные понятия, законы и модели разделов физики, особенности физических эффектов и явлений, используемых для обеспечения защиты информации с применением технических средств | применять основные законы физики при решении практических задач, в том числе связанных с технической защитой информации | навыками анализа физических явлений и процессов для решения задач в области защиты информации, в том числе технической защиты |
| ОПК-7 | способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты | основные угрозы безопасности информации, а также методы технической защиты и обнаружения этих угроз; | выявлять уязвимости информационно-технологических ресурсов информационных систем с применением средств технической защиты | методами выявления угроз и уязвимостей информационной безопасности информационных систем, основанных на применении технических средств защиты информации |
| ПК-1 | способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации | разновидности, характеристики, принципы работы, правила настройки и обслуживания технических средств защиты информации, в том числе коммерческой и конфиденциальной | выполнять работы по установке, настройке и обслуживанию технических средств защиты информации, основанных на различных физических эффектах и явлениях | навыками установки, настройки и обслуживания средств защиты информации, включая средства технической защиты |
| ПК-6 | способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств | методы и средства контроля эффективности различных видов средств защиты информации, в том числе средств технической защиты | проверять работоспособность и эффективность применения средств защиты информации, в том числе средств технической защиты | навыками проведения проверок работоспособности средств защиты информации, в том числе средств технической защиты |

| Код компетенции из УП и этап её формирования | Содержание компетенции | В результате изучения дисциплины обучающиеся должны: | | |
|---|---|---|---|---|
| | | знать | уметь | владеть |
| | защиты информации | | | |

## 2. Место дисциплины в структуре образовательной программы

| | |
|---|---|
| Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины. | Аппаратные средства вычислительной техники, Информатика, Основы информационной безопасности, Физика, Электроника и схемотехника |
| Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения. | Выпускная квалификационная работа, Измерительная аппаратура анализа защищенности объектов и электрорадиоизмерения, Микроконтроллерные системы в информационной безопасности, Организационное и правовое обеспечение информационной безопасности, Организация системы обеспечения информационной безопасности, Преддипломная практика, Программно-аппаратные средства защиты информации, Технические средства охраны и видеонаблюдения, Технологическая практика |

## 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося

Общий объем дисциплины в з.е. /час: 4 / 144
Форма промежуточной аттестации: Экзамен

| Форма обучения | Виды занятий, их трудоемкость (час.) | | | | Объем контактной работы обучающегося с преподавателем (час) |
|---|---|---|---|---|---|
| | Лекции | Лабораторные работы | Практические занятия | Самостоятельная работа | |
| очная | 34 | 34 | 0 | 76 | 74 |

## 4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

**Форма обучения: очная**
***Семестр: 5***

**Лекционные занятия (34ч.)**

**1. Общее представление о технической защите информации {беседа} (6ч.)[2,3,4]** Общее представление о технической защите информации

Введение (2 часа). Цели и задачи курса. Предмет дисциплины, связь курса с другими дисциплинами. Важность умения анализировать физические явления и процессы для решения профессиональных задач, связанных с технической защитой информации. Структура курса. Рекомендуемая литература.

Технические системы добывания информации (2). Назначение и функции видов разведки. Характеристика каналов утечки информации. Технические средства добывания информации.

Способы и средства защиты конфиденциальной информации техническими средствами (2). Задачи и требования к способам и средствам защиты конфиденциальной информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты.

**2. Виды разведок и их описание {беседа} (8ч.)[2,3,4,8]** Радиоэлектронная разведка (2ч). Общая характеристика радиоэлектронной разведки; основные показатели технических средств радио-, радиотехнической, радиолокационной и радиотепловой разведки и каналов утечки информации.

Оптическая разведка (2ч). Принципы оптической разведки; основные показатели средств визуальной, фотографической, телевизионной, инфракрасной и лазерной разведки и каналов информации.

Технические средства акустической разведки (2ч). Технические средства акустической разведки, их классификация. Лазерные системы. Системы с радиоканалом. Стетоскопы. Направленные микрофоны. Современные тенденции в средствах акустической разведки.

Дистанционные способы добывания информации (2ч). Способы доступа к источникам конфиденциальной информации без нарушения государственной границы, без проникновения на объект защиты. Компьютерная разведка. Аналитическая разведка.

**3. Методы и средства технической защиты информации и физические основы их работы (часть1) {беседа} (8ч.)[2,3,4,5,6,7,8,9]** Защита объектов от наблюдения в оптическом и тепловом диапазоне электромагнитных волн(2).

Пространственные, временные и энергетические условия наблюдения объектов. Факторы, снижающие возможность обнаружения и распознавания объектов, измерения их параметров. Защита объектов от радиолокационного и радиотеплолокационного наблюдения. Противорадиолокационные покрытия и экраны. Технические средства противорадиолокационной маскировки. Уголковые, дипольные, линзовые переотражатели, переизлучающие антенные

решетки.
Защита информации от утечек по техническим каналам (2 часа).
Способы защиты линий связи учреждений и предприятий государственных и коммерческих структур от утечки конфиденциальной информации. Принципы и средства закрытия речевой, буквенно-цифровой, телевизионной информации. Защита от утечек, обусловленных ПЭМИН Способы устранения утечки информации за счет побочных электромагнитных излучений и наводок. Средства защиты вспомогательных технических средств и систем, их типы, назначение, принципы действия.
Пассивные средства защиты от утечек по техническим каналам (2 часа). Пассивные и активные технические средства защиты, их принципы действия и возможности. Архитектурно-планировочные, акустотехнические и организационно-технические способы. Экранирование, фильтрация, заземление.
Средства обнаружения устройств и систем несанкционированного съема информации (2 часа).
Классификация средств радиоконтроля. Способы и средства обнаружения и локализации закладок. Индикаторы поля, сканирующие приёмники, интерсепторы, частотомеры. Комплексы радиоконтроля. Универсальные поисковые приборы.
**4. Методы и средства технической защиты информации и физические основы их работы (часть 2) {беседа} (8ч.)[2,3,4,5,6,7,8,9]** Нелинейная локация и вспомогательные поисковые средства (2 часа). Принципы нелинейной локации. Особенности использования нелинейных локаторов для обнаружения закладных устройств. Анализ тепловых полей тепловизорами. Металлодетекторы. Индикаторы неоднородностей. Рентгеновские установки.
Активные средства защиты (2 часа). Активное радиоэлектронное противодействие средствам радиотехнической разведки. Классификация помех. Основные способы и средства радиомаскировки и шумоподавления.
Средства электромагнитного зашумления (2 часа). Принципы и средства подавления излучения радиозакладок. Средства линейного зашумления. Способы противодействия лазерным средствам прослушивания. Рекомендации по оценке эффективности защиты информации от подслушивания.
Защита объектов от утечки акустической информации (2 часа). Основные способы и средства защиты акустической информации, меры по скрытию объектов от акустической разведки. Организационные меры по предотвращению утечек акустической информации. Временные, пространственные и территориальные ограничения. Технические ограничения. Способы и средства маскировки. Мероприятия и технические средства по дезинформации и созданию помех.
**5. Организационно-нормативные вопросы технической защиты информации {лекция с разбором конкретных ситуаций} (4ч.)[2,2,4,5,6,8]** Защита информации техническими средствами в учреждениях и на предприятиях (2 часа). Организация работ по инженерно-технической защите на предприятиях и в учреждениях государственных и коммерческих структур. Порядок и правила выполнения работ по установке, настройке и обслуживанию технических средств

защиты информации. Основные нормативные документы по защите предприятий и учреждений от технической разведки. Нормы допустимых уровней излучения. Аттестация помещений. Организационные и технические мероприятия по защите информации в учреждениях и на предприятиях. Основные руководящие документы по защите предприятий и учреждений от иностранной технической разведки.

Организация системы защиты информации объекта (2 часа).

Методы организации системы защиты информации на предприятиях и в учреждениях. Способы определения информационных ресурсов, подлежащих защите, угроз безопасности информации и путей реализации технической защиты от этих угроз на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты. Модели системы защиты. Выбор оптимальных вариантов защиты и технических средств. Контроль эффективности мер по защите информации техническими средствами Технический контроль эффективности принимаемых мер защиты. Назначение, содержание, вид и методы технического контроля. Порядок участия в организации и проведении контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации. Вопросы технико-экономического обоснования технической системы защиты информации объекта. Показатели эффективности. Стоимость защиты.

**Лабораторные работы (34ч.)**

**1. Выявление каналов утечки информации в радиочастотном диапазоне. {творческое задание} (6ч.)[1]**

**2. Выявление каналов утечки информации по проводным линиям. {творческое задание} (6ч.)[1]**

**3. Выявление каналов утечки информации в инфракрасном диапазоне. {творческое задание} (6ч.)[1]**

**4. Выявление каналов утечки информации по НЧ магнитным полям. {творческое задание} (6ч.)[1]**

**5. Оценка эффективности виброакустической защиты помещения. {творческое задание} (6ч.)[1]**

**6. Оценка эффективности звукоизоляции помещения {творческое задание} (4ч.)[1]**

**Самостоятельная работа (76ч.)**

**1. Подготовка к текущим занятиям, самостоятельное изучение материала {тренинг} (12ч.)[1,2,3,4]**

**3. Оформление отчетов по лабораторным работам(16ч.)[1]**

**4. Подготовка к текущему контролю успеваемости {тренинг} (12ч.)[1,2,3,4]**

**5. Подготовка к промежуточной аттестации (экзаемну) {тренинг} (36ч.)[2,3,4]**

## 5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Для каждого обучающегося обеспечен индивидуальный неограниченный доступ к электронно-библиотечным системам: Лань, Университетская библиотека он-лайн, электронной библиотеке АлтГТУ и к электронной информационно-образовательной среде:

1. Техническая защита информации. Методические указания к лабораторным работам по дисциплине «Техническая защита информации» /В.А.Кемпф, 2014.- Алт. гос. тех. ун-т им. И.И. Ползунова. – Барнаул: АлтГТУ. – 2015. -74 с. [электронный ресурс]: - режим доступа: http://new.elib.altstu.ru/eum/download/vsib/Kempf-tzi.pdf

## 6. Перечень учебной литературы

6.1. Основная литература

2. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - Прямая ссылка: Режим доступа: http://biblioclub.ru/index.php?page=book_red&id=429070&sr=1 (17.04.2019)

3. Зайцев, А.П. Технические средства и методы защиты информации [Электронный ресурс] : учебник / А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов. — Электрон. дан. — Москва: Горячая линия-Телеком, 2018. — 442 с. — Режим доступа: https://e.lanbook.com/book/111057. — Загл. с экрана. (17.04.2019)

4. Технические средства и методы защиты информации [Электронный ресурс] : учебное пособие / А.П. Зайцев [и др.]. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 616 с. — Режим доступа: https://e.lanbook.com/book/5154. — Загл. с экрана. (17.04.2019)

6.2. Дополнительная литература

5. Креопалов, В.В. Технические средства и методы защиты информации : учебно-практическое пособие / В.В. Креопалов. - М. : Евразийский открытый институт, 2011. - 278 с. - ISBN 978-5-374-00507-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=90753

6. Титов, А.А. Технические средства защиты информации : учебное пособие / А.А. Титов. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. - 194 с. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=208661 (22.04.2019).

7. Иванов, А.В. Защита речевой информации от утечки по акустоэлектрическим каналам : учебное пособие / А.В. Иванов, В.А. Трушин ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск : НГТУ, 2012. - 43 с. :

ил.,табл., схем. - ISBN 978-5-7782-1888-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=228846 (17.04.2019)

## 7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

8. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК) России [электронный ресурс]:- режим доступа: http:// www.fstec.ru

9. Официальный сайт федерального агентства по техническому регулированию и метрологии [электронный ресурс]: режим доступа: http://protect.gost.ru

## 8. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации

Содержание промежуточной аттестации раскрывается в комплекте контролирующих материалов, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС, которые хранятся на кафедре-разработчике РПД в печатном виде и в ЭИОС.

Фонд оценочных материалов (ФОМ) по дисциплине представлен в приложении А.

## 9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Для успешного освоения дисциплины используются ресурсы электронной информационно-образовательной среды, образовательные интернет-порталы, глобальная компьютерная сеть Интернет. В процессе изучения дисциплины происходит интерактивное взаимодействие обучающегося с преподавателем через личный кабинет студента.

| №пп | Используемое программное обеспечение |
|---|---|
| 1 | Windows |
| 2 | Acrobat Reader |
| 3 | LibreOffice |
| 4 | Chrome |
| 5 | Антивирус Kaspersky |

| №пп | Используемые профессиональные базы данных и информационные справочные системы |
|---|---|
| 1 | Бесплатная электронная библиотека онлайн "Единое окно к образовательным ресурсам" для студентов и преподавателей; каталог ссылок на образовательные интернет-ресурсы (http://Window.edu.ru) |
| 2 | Национальная электронная библиотека (НЭБ) — свободный доступ читателей к фондам российских библиотек. Содержит коллекции оцифрованных документов (как открытого доступа, так и ограниченных авторским правом), а также каталог |

| №пп | Используемые профессиональные базы данных и информационные справочные системы |
|---|---|
| | изданий, хранящихся в библиотеках России. (http://нэб.рф/) |

## 10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

| Наименование специальных помещений и помещений для самостоятельной работы |
|---|
| учебные аудитории для проведения занятий лекционного типа |
| учебные аудитории для проведения групповых и индивидуальных консультаций |
| учебные аудитории для проведения текущего контроля и промежуточной аттестации |
| помещения для самостоятельной работы |
| лаборатории в области технической защиты информации |
| специально оборудованный кабинет (класс, аудиторию) в области информатики, технологий и методов программирования |

Материально-техническое обеспечение и организация образовательного процесса по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья осуществляется в соответствии с «Положением об обучении инвалидов и лиц с ограниченными возможностями здоровья».