


| | | |
|---|---|-------------------------------|
|  | Балтийская государственная академия рыбопромыслового флота | |
| | Рабочая программа дисциплины «Техническая защита информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем» | |
| | Версия: I | Дата выпуска версии: 21.05.18 |

стр. 1 из 17

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Калининградский государственный технический университет»
Балтийская государственная академия рыбопромыслового флота
ФГБОУ ВО «КГТУ»
БГАРФ

УТВЕРЖДАЮ

И.О. декана РТФ



В.А. Баженов

27.06 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

(наименование дисциплины)

базовой части образовательной программы по специальности
10.05.03 «Информационная безопасность автоматизированных систем»

Специализация программы

Обеспечение информационной безопасности распределенных
информационных систем

(наименование специализации программы)

Факультет – РАДИОТЕХНИЧЕСКИЙ

Кафедра – «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Калининград 2018



Визирование РПД для исполнения в очередном учебном году


УТВЕРЖДАЮ:

и.о. декана РТФ  В.А.Баженов

«27» 06 2018 г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 2018 – 2019 учебном году на заседании кафедры «Информационная безопасность».

Протокол от «14» июня 2018 г. № 9

Заведующий кафедрой «Информационная безопасность»  /Великите Н.Я./

УТВЕРЖДАЮ:


и.о. декана РТФ _____ В.А.Баженов

«___» _____ 2019 г.

Рабочая программа рассмотрена, обсуждена и одобрена для исполнения в 2019 – 2020 учебном году на заседании кафедры «Информационная безопасность».

Протокол от «___» _____ 2019 г. №

Заведующий кафедрой «Информационная безопасность» _____ /Великите Н.Я./

| | | |
|---|---|-------------------------------|
|  | Балтийская государственная академия рыбопромыслового флота | |
| | Рабочая программа дисциплины «Техническая защита информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем» | |
| | Версия: 1 | Дата выпуска версии: 21.05.18 |

1. Цель освоения дисциплины.

1.1. Цели дисциплины

Целью дисциплины «Техническая защита информации» является теоретическая и практическая подготовка студентов по вопросам защиты информации от утечки по техническим каналам (технической защиты информации) на объектах информатизации и в выделенных помещениях.

1.2. Задачи дисциплины – изучение:

- технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
- технических каналов утечки акустической (речевой) информации;
- способов и средств защиты информации, обрабатываемой техническими средствами;
- способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;
- методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
- основ организации технической защиты информации на объектах информатизации.


1.3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий;
- ПК-1 способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке;
- ПК-3 способностью проводить анализ защищенности автоматизированных систем;
- ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
- ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации;
- ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации.

В результате изучения дисциплины студенты должны:


- знать технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам.
- уметь анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем, пользоваться нормативными документами по защите информации.
- владеть методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации.

| | | |
|---|---|-------------------------------|
|  | Балтийская государственная академия рыбопромыслового флота | |
| | Рабочая программа дисциплины «Техническая защита информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем» | |
| | Версия: 1 | Дата выпуска версии: 21.05.18 |


2. Результаты освоения дисциплины

Таблица 1 - Компетенции, формируемые в результате освоения дисциплины


| Компетенции выпускника ОП ВО и этапы их формирования в результате изучения дисциплины | Этапы формирования компетенции | Знания, умения и навыки, характеризующие этапы формирования компетенций |
|---|--------------------------------|--|
| 1 | | 2 |
| ОПК-8 - способность к освоению новых образцов программных, технических средств и информационных технологий | Знать | |
| | Уровень 1 | способы получения новых знаний в предметной области и областях, непосредственно связанных с будущей профессиональной деятельностью |
| | Уровень 2 | методы и средства получения знаний в предметной области: использовать периодические издания, научные и учебно-познавательные сайты в сети Internet; выбирать и применять для решения прикладных задач анализа и синтеза технических средств защиты информации |
| | Уровень 3 | предметы и объекты в областях науки и техники, непосредственно примыкающих к теории и практики технических средств защиты информации: процесс преобразования сигнала из формы, удобной для непосредственного использования информации, в форму, удобную для передачи, хранения или автоматической переработки |
| | Уметь | |
| | Уровень 1 | самостоятельно получать новые знания по предметной области и в областях, непосредственно примыкающих к объектам будущей профессиональной деятельности |
| | Уровень 2 | самостоятельно получать знания из смежных областей науки и техники: углублять знания, уточнять по признакам понятий, отделять существенные признаки от несущественных; уточнять границы использования знаний |
| | Уровень 3 | самостоятельно получать знания для решения исследовательских задач, задач повышенной сложности; использовать методы анализа и синтеза технических средств защиты информации для решения прикладных задач проектирования |
| | Владеть | |
| | Уровень 1 | технологиями систематизации и накопления научных знаний в предметной области |
| | | <p>Знать: принципы построения и функционирования, теории электрических цепей; принципы работы элементов функциональных узлов электронной аппаратуры; типовые схмотехнические решения основных узлов и блоков электронной аппаратуры</p> <p>Уметь: применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска); проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы; применять на практике методы анализа электрических цепей; работать с современной элементной базой электронной аппаратуры</p> <p>Владеть: навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов); навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов,</p> |

| | | |
|---|---|-------------------------------|
|  | Балтийская государственная академия рыбопромыслового флота | |
| | Рабочая программа дисциплины «Техническая защита информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем» | |
| | Версия: 1 | Дата выпуска версии: 21.05.18 |


| | | | |
|---|---|---|--|
| | Уровень 2 | методиками выполнения научно-исследовательских работ | архиваторов, стандартных сетевых средств обмена информацией); навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации; навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы |
| | Уровень 3 | методологией прикладных научных исследований в предметной области | |
| ПК-1 - способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке | Знать | | Знать: основные информационные технологии, используемые в автоматизированных системах; показатели качества программного обеспечения; язык программирования высокого уровня (объектно-ориентированное программирование); Уметь: применять действующую законодательную базу в области обеспечения информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации Владеть: навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках |
| | Уровень 1 | классификацию и характеристики информационных баз и хранилищ | |
| | Уровень 2 | информационные базы и хранилища, порядок обращения к ним и поиска информации | |
| | Уровень 3 | порядок обработки патентной информации, информации по интеллектуальной собственности | |
| | Уметь | | |
| | Уровень 1 | определить пути получения научно-технической информации, обобщать и систематизировать информацию | |
| | Уровень 2 | использовать ресурсы информационных баз и хранилищ для поиска, систематизации и обобщения материала в предметной области дисциплины | |
| | Уровень 3 | проводить патентный поиск по ключевым словам, выявлять аналоги и прототипы, обобщать и систематизировать научную информацию | |
| | Владеть | | |
| | Уровень 1 | навыками систематизации, обобщения справочной, нормативно-технической информации | |
| Уровень 2 | навыками поиска, обобщения, систематизации научно-технической информации, составления кратких отчетов, рефератов | | |
| Уровень 3 | навыками обобщения и систематизации научно-технической информации из предметной области исследований и других областей науки и техники, непосредственно примыкающих к проведенным исследованиям | | |
| ПК-3 - способностью проводить анализ защищенности автоматизированных систем | Знать | | Знать: технические каналы утечки информации; возможности технических средств перехвата информации; организа |
| | Уровень 1 | классификацию АС и перечень требований по защите информации к каждому классу автоматизированных систем | |

| | | |
|---|---|-------------------------------|
|  | Балтийская государственная академия рыбопромыслового флота | |
| | Рабочая программа дисциплины «Техническая защита информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем» | |
| | Версия: 1 | Дата выпуска версии: 21.05.18 |

| | | | |
|---|----------------|---|---|
| | Уровень 2 | требования стандарта ISO по номенклатуре услуг, предоставляемых системой безопасности | <p>цию защиты информации от утечки по техническим каналам на объектах информатизации</p> <p>Уметь: применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска); проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы; Владеть: навыками организации и обеспечения режим секретности</p> |
| | Уровень 3 | основные положения концепции защиты и показатели защищенности АС от несанкционированного доступа к информации | |
| | Уметь | | |
| | Уровень 1 | определять цель, объект и место проведения анализа АС, уточнять вид проводимого инструментального контроля, составлять перечень исследуемых систем | |
| | Уровень 2 | применять существующую методическую базу проведения оценки защищенности технических средств от утечки информации | |
| | Уровень 3 | проводить патентный поиск по ключевым словам, выявлять аналоги и прототипы, обобщать и систематизировать научную информацию | |
| | Владеть | | |
| | Уровень 1 | технологиями систематизации и накопления научных знаний в предметной области | |
| | Уровень 2 | методиками выполнения научно-исследовательских работ | |
| | Уровень 3 | методологией прикладных научных исследований в предметной области | |
| ПК-14 - способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации | Знать | | <p>Знать: основные информационные технологии, используемые в автоматизированных системах</p> <p>Уметь: контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем</p> |
| | Уровень 1 | цели и задачи технического контроля эффективности мер защиты информации | |
| | Уровень 2 | порядок проведения технического контроля выполнения норм защиты информации от утечки за счет ПЭМИН | |
| | Уровень 3 | порядок проведения проверки эффективности реально установленных механизмов защиты информации требованиям соответствующего класса защиты информации от НСД | |
| | Уметь | | |
| | Уровень 1 | определить пути получения научно-технической информации, обобщать и систематизировать информацию | |
| | Уровень 2 | использовать ресурсы информационных баз и хранилищ для поиска, систематизации и обобщения материала в предметной области дисциплины | |
| | Уровень 3 | проводить патентный поиск по ключевым словам, выявлять аналоги и прототипы, обобщать и систематизировать научную информацию | |

| | | |
|---|---|-------------------------------|
|  | Балтийская государственная академия рыбопромыслового флота | |
| | Рабочая программа дисциплины «Техническая защита информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем» | |
| | Версия: 1 | Дата выпуска версии: 21.05.18 |

| | | | |
|---|---|---|--|
| | Владеть | | Владеть: навыками участия в экспертизе состояния защищенности информации на объекте защиты; методами расчета и инструментального контроля показателей технической защиты информации; навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем. |
| | Уровень 1 | методами расчета и инструментального контроля показателей технической защиты информации | |
| | Уровень 2 | методиками выполнения научно-исследовательских работ | |
| | Уровень 3 | методологией прикладных научных исследований в предметной области | |
| ПК-16 - способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации | Знать | | Знать: возможности технических средств перехвата информации; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам. Уметь: анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. Владеть: методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации. |
| | Уровень 1 | цели и задачи технического контроля эффективности мер защиты информации | |
| | Уровень 2 | порядок проведения технического контроля выполнения норм защиты информации от утечки за счет ПЭМИН | |
| | Уровень 3 | порядок проведения проверки эффективности реально установленных механизмов защиты информации требованиям соответствующего класса защиты информации от НСД | |
| | Уметь | | |
| | Уровень 1 | определить пути получения научно-технической информации, обобщать и систематизировать информацию | |
| | Уровень 2 | использовать ресурсы информационных баз и хранилищ для поиска, систематизации и обобщения материала в предметной области дисциплины | |
| | Уровень 3 | проводить патентный поиск по ключевым словам, выявлять аналоги и прототипы, обобщать и систематизировать научную информацию | |
| | Владеть | | |
| | Уровень 1 | методами расчета и инструментального контроля показателей технической защиты информации | |
| Уровень 2 | методиками выполнения научно-исследовательских работ | | |
| Уровень 3 | методологией прикладных научных исследований в предметной области | | |
| ПК-17 - способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации | Знать | | Знать: технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам. |
| | Уровень 1 | характеристики каналов ПЭМИН в высокочастотной области спектра | |
| | Уровень 2 | порядок проведения работ при мониторинге защищенности АС | |
| | Уровень 3 | схемы проведения инструментального мониторинга характеристик каналов ПЭМИН, порядок оценки степени защищенности | |

| | | | |
|---|---|-------------------------------|--------------|
|  | Балтийская государственная академия рыбопромыслового флота | | |
| | Рабочая программа дисциплины «Техническая защита информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем» | | |
| | Версия: 1 | Дата выпуска версии: 21.05.18 | стр. 8 из 17 |

| | | | |
|--|----------------|--|---|
| | | автоматизированных систем по каналам утечки информации | |
| | Уметь | | Уметь: анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области безопасности для проектирования, разработки и оценки защищенности автоматизированных систем. Пользоваться нормативными документами по защите информации. Владеть: методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации |
| | Уровень 1 | моделировать параметры каналов ПЭМИН | |
| | Уровень 2 | выбирать средства измерений, проводить измерения характеристик каналов ПЭМИН при мониторинге защищенности АС | |
| | Уровень 3 | проводить оценку защищенности АС по каналам ПЭМИН при их инструментальном мониторинге, давать рекомендации по повышению уровня защиты информации | |
| | Владеть | | |
| | Уровень 1 | методиками расчета характеристик каналов ПЭМИН | |
| | Уровень 2 | способами проведения экспериментальных работ при инструментальном мониторинге АИС | |
| | Уровень 3 | методами проведения экспериментально-исследовательских работ при инструментальном мониторинге защищенности автоматизированных систем | |

3. Место дисциплины в структуре образовательной программы

Дисциплина Б1.Б.27 «Техническая защита информации» относится к числу дисциплин базовой части модуля Блок 1.

Изучение её базируется на следующих дисциплинах: «Математический анализ», «Физика», «Теория вероятностей и математическая статистика», «Электроника и схемотехника», «Основы информационной безопасности».

Обеспечивает чтение дисциплин «Программно-аппаратные средства обеспечения информационной безопасности» и «Разработка и эксплуатация защищённых автоматизированных систем», а также подготовку выпускной квалификационной работы.

| | | |
|--|---|-------------------------------|
| | Балтийская государственная академия рыбопромыслового флота | |
| | Рабочая программа дисциплины «Техническая защита информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем» | |
| | Версия: 1 | Дата выпуска версии: 21.05.18 |
| | | стр. 9 из 17 |

4. Содержание дисциплины

| Индекс, наименование дисциплины | Содержание дисциплины (дидактические единицы) | Всего часов |
|---------------------------------|---|-------------|
| Б1.Б.27 | Виды, источники и носители защищаемой информации; демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники; побочные электромагнитные излучения и наводки; структура, классификация и основные характеристики технических каналов утечки информации; классификация технической разведки; основные этапы и процедуры добывания информации технической разведкой; возможности видов технической разведки; концепция и методы инженерно-технической защиты информации; методы и средства инженерной защиты и технической охраны объектов; скрывание объектов наблюдения; скрывание речевой информации в каналах связи; энергетическое скрывание акустических информативных сигналов; обнаружение и локализации закладных устройств, подавление их сигналов; подавление опасных сигналов акустоэлектрических преобразователей; экранирование и компенсация информативных полей; подавление информативных сигналов в цепях заземления и электропитания; подавление опасных сигналов; характеристика государственной системы противодействия технической разведке; нормативные документы по противодействию технической разведке; виды контроля эффективности защиты информации; основные положения методологии инженерно-технической защиты информации; методы расчета и инструментального контроля показателей защиты информации | 180 |

РАЗДЕЛ 1. Концепция инженерно-технической защиты информации.

1.1. Системный подход к защите информации.

1.2. Основные направления инженерно-технической защиты информации.

РАЗДЕЛ 2. Теоретические основы инженерно-технической защиты информации.

2.1. Информация как предмет защиты.

2.2. Источники опасных сигналов.

2.3. Характеристика технической разведки.

2.4. Технические каналы утечки информации.

2.5. Методы инженерно-технической защиты информации.

2.6. Методы инженерной защиты и технической охраны объектов.

2.7. Методы скрывания информации и ее носителей.

2.8. Процессы подавления опасных сигналов.

РАЗДЕЛ 3. Технические средства добывания и инженерно-технической защиты информации.

3.1. Средства технической разведки.

3.2. Средства инженерной защиты и технической охраны.

3.3. Средства предотвращения утечки информации по техническим каналам.

РАЗДЕЛ 4. Организационные основы инженерно-технической защиты информации.

4.1. Государственная система защиты информации.

4.2. Контроль эффективности инженерно-технической защиты информации.

4.3. Методические рекомендации по оценке эффективности защиты информации.

| | | | |
|--|---|-------------------------------|---------------|
| | Балтийская государственная академия рыбопромыслового флота | | |
| | Рабочая программа дисциплины «Техническая защита информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем» | | |
| | Версия: 1 | Дата выпуска версии: 21.05.18 | стр. 10 из 17 |

5. Объем (трудоемкость освоения) и структура дисциплины, формы аттестации по ней

Таблица 2 - Структура дисциплины по очной форме обучения

| Номер и наименование раздела, темы | Объем учебной работы (час.) | | | | | |
|--|-----------------------------|-----------|----|-----------|-----------|------------|
| | Лекции | ЛЗ | ПЗ | СР | контроль | Всего |
| Семестр – 7 (5 ЗЕТ, 180 час.) | | | | | | |
| РАЗДЕЛ 1. Концепция инженерно-технической защиты информации. | 4 | - | - | - | 2 | 6 |
| 1.1. Системный подход к защите информации. | 2 | - | - | - | - | 2 |
| 1.2. Основные направления инженерно-технической защиты информации. | 2 | - | - | - | 2 | 4 |
| РАЗДЕЛ 2. Теоретические основы инженерно-технической защиты информации. | 17 | 6 | - | 16 | 8 | 47 |
| 2.1. Информация как предмет защиты. | 1 | - | - | - | - | 1 |
| 2.2. Источники опасных сигналов. | 2 | - | - | 8 | 1 | 11 |
| 2.3. Характеристика технической разведки. | 2 | - | - | - | 1 | 3 |
| 2.4. Технические каналы утечки информации. | 4 | 6 | - | - | 1 | 11 |
| 2.5. Методы инженерно-технической защиты информации. | 2 | - | - | 4 | 1 | 7 |
| 2.6. Методы инженерной защиты и технической охраны объектов. | 2 | - | - | - | 1 | 3 |
| 2.7. Методы скрытия информации и ее носителей. | 2 | - | - | 4 | 1 | 7 |
| 2.8. Процессы подавления опасных сигналов. | 2 | - | - | - | 2 | 4 |
| РАЗДЕЛ 3. Технические средства добывания и инженерно-технической защиты информации. | 18 | 39 | - | 16 | 8 | 81 |
| 3.1. Средства технической разведки. | 6 | 6 | - | 8 | 2 | 22 |
| 3.2. Средства инженерной защиты и технической охраны. | 6 | 21 | - | 4 | 2 | 33 |
| 3.3. Средства предотвращения утечки информации по техническим каналам. | 6 | 12 | - | 4 | 4 | 26 |
| РАЗДЕЛ 4. Организационные основы инженерно-технической защиты информации. | 12 | 6 | - | 10 | 8 | 36 |
| 4.1. Государственная система защиты информации. | 2 | - | - | - | - | 2 |
| 4.2. Контроль эффективности инженерно-технической защиты информации. | 4 | - | - | 4 | 4 | 12 |
| 4.3. Методические рекомендации по оценке эффективности защиты информации. | 6 | 6 | - | 6 | 4 | 22 |
| Всего | 51 | 51 | - | 42 | 26 | 170 |
| Подготовка к сдаче и сдача экзамена | - | - | - | - | 10 | 10 |
| Итого по дисциплине | 51 | 51 | - | 42 | 36 | 180 |
| | 102 | | | | | |

ЛЗ – лабораторные занятия,
ПЗ – практические занятия,
СР – самостоятельная работа студента

| | | |
|--|---|-------------------------------|
| | Балтийская государственная академия рыбопромыслового флота | |
| | Рабочая программа дисциплины «Техническая защита информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем» | |
| | Версия: 1 | Дата выпуска версии: 21.05.18 |

стр. 11 из 17

6. Лабораторные занятия (работы)

Таблица 3 - Лабораторные занятия по очной форме обучения

| № ПЗ | Тема дисциплины | Тема и содержание ЛЗ | Количество часов ЛЗ |
|------------------------------|-----------------|---|---------------------|
| Семестр – 7 (51 час.) | | | |
| 1. | 3.2 | Охрана выделенных помещений. Пожарная сигнализация. | 4 |
| 2. | 3.2 | Охрана выделенных помещений. Охранная сигнализация. | 5 |
| 3. | 3.2 | Ограничение доступа в выделенное помещение. Система контроля и управления доступом. | 6 |
| 4. | 3.2 | Охрана выделенных помещений. Система видеонаблюдения. | 6 |
| 5. | 2.3 | Электромагнитные наводки от средств вычислительной техники в линейных коммуникациях | 6 |
| 6. | 3.3 | Технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации | 6 |
| 7. | 3.1 | Средства нелинейно-локационного контроля | 6 |
| 8. | 3.3 | Пассивные и активные методы защиты от наводки средств вычислительной техники в линейных коммуникациях | 6 |
| 9. | 4.3 | Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки. | 6 |
| Всего за семестр: | | | 51 |
| Итого по дисциплине | | | 51 |

7. Практические занятия


Практические занятия по дисциплине учебным планом не предусмотрены.

| | | | |
|--|---|-------------------------------|---------------|
| | Балтийская государственная академия рыбопромыслового флота | | |
| | Рабочая программа дисциплины «Техническая защита информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем» | | |
| | Версия: 1 | Дата выпуска версии: 21.05.18 | стр. 12 из 17 |

8. Самостоятельная работа студента

Таблица 4 - Самостоятельная работа студента по очной форме обучения

| № | Вид (содержание) СР | Количество часов СР | Форма контроля, аттестации |
|----------------------------|---|---------------------|---|
| Семестр – 7 | | | |
| 1. | Распространение сигналов в технических каналах утечки информации. Физические процессы подавления опасных сигналов | 4 | опрос на занятиях, конспект лекций, реферат |
| 2. | Защита информации от фотографической и оптико-электронной, радиотехнической разведки | 2 | опрос на занятиях, конспект лекций |
| 3. | Электромагнитные каналы утечки информации | 4 | опрос на занятиях, конспект лекций, реферат |
| 4. | Сканерные приемники | 4 | опрос на занятиях, конспект лекций |
| 5. | Программно-аппаратные комплексы радио- и радиотехнической разведки | 4 | опрос на занятиях, конспект лекций, реферат |
| 6. | Средства компьютерного шпионажа | 4 | опрос на занятиях, конспект лекций |
| 7. | Особенности инструментального контроля эффективности инженерно-технической защиты информации | 4 | опрос на занятиях, конспект лекций |
| 8. | Технические средства для тестирования и контроля систем обеспечения безопасности информации | 4 | опрос на занятиях, конспект лекций, реферат |
| 9. | Технические средства радиомониторинга и обнаружения закладных устройств | 4 | опрос на занятиях, конспект лекций |
| 10. | Системы слежения за транспортными средствами | 4 | опрос на занятиях, конспект лекций |
| 11. | Портативные средства видовой разведки | 4 | опрос на занятиях, конспект лекций |
| Всего за семестр: | | 42 | |
| Итого по дисциплине | | 42 | |

| | | |
|---|---|-------------------------------|
|  | Балтийская государственная академия рыбопромыслового флота | |
| | Рабочая программа дисциплины «Техническая защита информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем» | |
| | Версия: 1 | Дата выпуска версии: 21.05.18 |

9. Учебная литература и учебно-методическое обеспечение самостоятельной работы студента

9.1. Основная учебная литература

1. Зайцев, А.П. Техническая защита информации : учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М. : Горячая линия-Телеком, 2009. – 616 с. (наличие в библиотеке БГАРФ - 17 экз.)
2. Ворона, В. А. Технические системы охранной и пожарной сигнализации : учеб. пособие / В. А. Ворона М.В., В. А. Тихонов. – М. : Горячая линия-Телеком, 2012. – 376 с. (наличие в библиотеке БГАРФ - 15 экз.)

9.2. Дополнительная учебная литература

1. Системы охранной, пожарной и охранно-пожарной сигнализации : учебник / В. Г. Синилов. - 4-е изд., стер. - М. : Академия, 2008. - 352 с. (наличие в библиотеке БГАРФ - 20 экз.)
2. Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью. / учеб. пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой – М.: Горячая линия-Телеком, 2012. – 214 с. (наличие в библиотеке БГАРФ - 20 экз.)

9.3. Периодические издания

1. Парамонов, И. Б. Способ защиты информации от утечки по цепи вторичного электропитания / И. Б. Парамонов, А. В. Мазин, А. А. Филимонов. // Вопросы радиоэлектроники. – 2017. – №11. - С.52-55.
2. Егошин, Н. С. Формирование модели нарушителя / Н. С. Егошин, А. А. Конев, А. А. Шелупанов. // Безопасность информационных технологий. – 2017. – №4.- С.21-29.
3. Козлачков, С. Б. Некоторые особенности формирования акустоэлектрического канала утечки речевой акустической информации / С. Б. Козлачков [и др.]. //Безопасность информационных технологий. – 2017. – №4 - С.64-76.
4. Паньчев, С. Н. Защита акустической информации методом интермодуляционного зашумления с помощью нелинейных случайных антенн / С. Н. Паньчев [и др.]. //Радиотехника. – 2017. – №6 - С.136-140

10. Информационные технологии, программное обеспечение и Интернет-ресурсы дисциплины.

Электронная информационная образовательная среда БГАРФ ФГБОУ ВО «КГТУ»: <http://83.171.112.16/login/index.php>

Ресурсы информационно-телекоммуникационной сети «Интернет»:

- «Консультант Плюс» (www.consultant.ru);
- «Гарант» (www.garant.ru);
- <http://www.rg.ru/dok/> [On-line] – опубликованные нормативные-правовые акты РФ;
- <http://fstec.ru>;
- <http://www.confident.ru>;
- <http://bgarf.ru/academy/biblioteka/elektronnyj-katalog/>;
- <http://www.iqlib.ru> - электронная интернет библиотека;
- <http://www.biblioclub.ru> - полнотекстовая электронная библиотека;
- <http://www.elibrary.ru> - научная электронная библиотека.

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем: программное обеспечение Microsoft Desktop Education.

| | | |
|--|---|-------------------------------|
| | Балтийская государственная академия рыбопромыслового флота | |
| | Рабочая программа дисциплины «Техническая защита информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем» | |
| | Версия: 1 | Дата выпуска версии: 21.05.18 |

11. Материально-техническое обеспечение дисциплины

11.1. Общие требования к материально-техническому обеспечению дисциплины

11.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения лекционных занятий используется учебная аудитория № 441.

Состав оборудования: столы учебные – 15 шт., стол преподавательский – 1 шт., стулья учебные – 30 шт., стул преподавательский – 1 шт., трибуна – 1 шт., экран раздвижной PROJEC-TA – 1 шт.; доска магнитно-маркерная – 1 шт.; мультимедийный проектор TOSHIBA – 1 шт.; ноутбук Acer Extensa – 1 шт.

Стенды: «Комплекс средств автоматизации деятельности оперативного персонала пункта централизованной охраны», «Требования и нормы проектирования по защите объектов от преступных посягательств». Специализированные стенды: СКУД «Стилпост»; «СИНЕРГЕТ» (цифровая система видеонаблюдения и аудиорегистрации).

Используется лицензионное программное обеспечение Microsoft Desktop Education, Microsoft Office 2016, Kaspersky Total Space Security Russian Edition.

11.1.2. Материально-техническое обеспечение для лабораторных, практических занятий

Для проведения лабораторных занятий используется лаборатория технической защиты информации № 440.

Состав оборудования: столы учебные – 10 шт., стол преподавательский – 1 шт., стулья учебные – 20 шт., стул преподавательский – 1 шт., доска маркерная – 1 шт.; мультимедийный проектор TOSHIBA – 1 шт.; ноутбук Acer Extensa – 1 шт.

Стенды охранно-пожарной сигнализации – 3 шт.

Стенды со специализированным оборудованием по защите информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок и контроля эффективности защиты (подавитель микрофонов «Шаман», детектор поля ST 007, портативный измеритель частоты и мощности MPF-8000).

Для проведения лабораторных занятий используются компьютерный класс № 248.

Состав оборудования: столы учебные – 19 шт., стол преподавательский – 1 шт., стулья учебные – 23 шт., стул преподавательский – 1 шт., шкаф для учебных пособий – 1 шт., доска маркерная – 1 шт.; мультимедийный проектор ViewSonic – 1 шт.; ноутбук Acer Extensa – 1 шт.; проекционный экран Redleaf – 1 шт.

Компьютер MUSTIFF (системный блок, монитор ASUS, мышка, клавиатура), с установленным лицензионным программным обеспечением: Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription, Kaspersky Total Space Security Russian Edition.

11.1.3. Материально-техническое обеспечение для самостоятельной работы


Для организации самостоятельной работы обучающихся используется библиотечный фонд вуза, библиотека.

Помещение для самостоятельной работы – читальный зал, оснащенный компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду вуза.

11.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов с нарушениями слуха предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной

| | | |
|---|---|-------------------------------|
|  | Балтийская государственная академия рыбопромыслового флота | |
| | Рабочая программа дисциплины «Техническая защита информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем» | |
| | Версия: 1 | Дата выпуска версии: 21.05.18 |
| | | стр. 15 из 17 |

системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов с нарушениями зрения предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеомониторов для удаленного просмотра.

При обучении студентов с нарушениями опорно-двигательного аппарата используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

12. Фонд оценочных средств для проведения аттестации по дисциплине

Аттестация по дисциплине (итоговая аттестация по дисциплине является промежуточной аттестацией по образовательной программе). Для рабочей программы разработано и утверждено приложение «Фонд оценочных средств» для аттестации по дисциплине «Техническая защита информации».

13. Особенности преподавания и освоения дисциплины

В ходе изучения дисциплины предусматривается применение эффективных методик обучения, которые предполагают постановку вопросов проблемного характера с разрешением их, как непосредственно в ходе занятий, так и в ходе самостоятельной работы. Реализация программы предполагает использование интерактивных форм проведения лабораторных занятий. Проведение лабораторных занятий подразумевает обучение, построенное на групповой совместной деятельности студентов, в том числе с использованием персонального компьютера.

Перед началом занятий преподаватель проводит инструктаж по технике электробезопасности и пожарной безопасности. Контроль знаний в ходе изучения дисциплины осуществляется в виде текущих контролей, а также итоговой аттестации в форме экзамена по итогам учебного семестра.

Текущие контроли предназначены для проверки хода и качества усвоения обучающимися учебного материала и стимулирования учебной работы студентов. Они могут осуществляться в ходе всех видов занятий в форме, избранной преподавателем или предусмотренной рабочей программой дисциплины. Текущие контроли предполагают постоянный контроль преподавателем качества усвоения учебного материала, активизацию учебной деятельности студентов на занятиях, побуждение их к самостоятельной систематической работе. Он необходим обучающимся для самоконтроля на разных этапах обучения. Их результаты учитываются выставлением оценок в журнале учета успеваемости.


К экзамену допускаются студенты, имеющие по всем текущим контролям положительные оценки.

14. Методические указания по освоению дисциплины

Планирование и организация времени, необходимого на изучение дисциплины, предусматривается ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем» и рабочим учебным планом подготовки специалистов. Объем часов и формы работы по изучению дисциплины распределены в рабочей программе соответствующей дисциплины.

14.1 Общие сведения о дисциплине

Цель дисциплины «Техническая защита информации» — заложить терминологический фундамент, научить правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, приобрести навыки анализа угроз информационной безопасности, рассмотреть основные

| | | |
|---|---|-------------------------------|
|  | Балтийская государственная академия рыбопромыслового флота | |
| | Рабочая программа дисциплины «Техническая защита информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем» | |
| | Версия: 1 | Дата выпуска версии: 21.05.18 |

общеметодологические принципы теории информационной безопасности; изучение методов и средств обеспечения информационной безопасности, методов нарушения конфиденциальности, целостности и доступности информации.

14.2. Виды занятий и способы контроля

В соответствии с рабочим учебным планом дисциплина «Техническая защита информации» включает следующие виды занятий: лекции, лабораторные занятия, самостоятельная работа студентов.

На лекциях излагаются основные теоретические положения, составляющие дисциплину, и разбираются примеры практических задач. Преподавателю, ведущему курс, рекомендуется на вводной лекции определить структуру курса, пояснить цели и задачи изучения дисциплины, сформулировать основные вопросы и требования к результатам освоения.

При рассмотрении темы важно выделить основные понятия и определения, желательна их визуализация. При подготовке и проведении занятий по данному курсу преподаватель должен руководствоваться как общими учебно-методическими принципами (научность, системность, доступность, последовательность, преемственность, наличие единой внутренней логики курса, его связь с другими предметами), так и специфическими особенностями дисциплины, которые находят выражение в агрегированности и комбинации подходов. В подборе материала к занятиям следует руководствоваться рабочей программой учебной дисциплины, обращая внимание на компетенции, указанные в федеральном государственном образовательном стандарте высшего образования.

На первом занятии преподаватель обязан довести до обучающихся порядок работы в аудитории и нацелить их на проведение самостоятельной работы с учетом количества часов, отведенных на нее учебным планом. Рекомендую литературу для самостоятельного изучения, преподаватель должен максимально использовать возможности, предлагаемые библиотекой академии, в том числе ее электронными ресурсами.

Во время лекционных занятий рекомендуется вести конспектирование учебного материала, обращать внимание на формулировки и категории, раскрывающие суть того или иного явления или процессов, научные выводы и практические рекомендации.

В конце лекции необходимо делать выводы и ставить задачи на самостоятельную работу. Лабораторные занятия направлены на закрепление лекционного материала. При подготовке к лабораторным занятиям руководствоваться «Методическими указаниями по выполнению лабораторных работ по дисциплине «Техническая защита информации»

Самостоятельная работа студентов заключается в подготовке к практическим и лекционным занятиям и выполнении домашних заданий, выдаваемых преподавателем по каждому из разделов дисциплины. В целях лучшего понимания сути представления и обработки информации при защите рекомендуется использовать гипотетическую модель информации, что позволит использовать архитектурные особенности, свойственные конкретным моделям анализа. Примеры следует выбирать так, чтобы вычисления были не слишком громоздкими. Следует рассматривать задачи, возникающие в самых различных отраслях и показать динамику решения задач: как подойти к решению конкретной проблемы, какие ограничения возникают в рамках данного решения и какие результаты получаются в конечном счете.

В самостоятельную работу входит выполнение индивидуальных заданий. Преподаватель принимает решение о допуске студента к практической работе по результатам собеседования. Студенты знакомятся с общими сведениями, порядком выполнения работы, ищут необходимые пояснения в соответствии с полученным вариантом задания. При защите работы студент отвечает преподавателю на контрольные вопросы, представляет теоретическую часть решения задачи, практический расчет.

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обуче -

| | | | |
|--|---|-------------------------------|---------------|
| | Балтийская государственная академия рыбопромыслового флота | | |
| | Рабочая программа дисциплины «Техническая защита информации» по специальности 10.05.03 «Информационная безопасность автоматизированных систем» | | |
| | Версия: 1 | Дата выпуска версии: 21.05.18 | стр. 17 из 17 |

ния, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

При самостоятельной работе руководствоваться «Методические указания по организации и контролю самостоятельной работы студентов по дисциплине «Техническая защита информации».

15. Сведения о рабочей программе и ее согласовании

Рабочая программа дисциплины представляет собой компонент образовательной программы по специальности 10.05.03 «Информационная безопасность автоматизированных систем» и соответствует учебному плану, утвержденному «31» января 2018 г. и действующему для студентов, принятых на первый курс, начиная с 2014 года.

Автор программы – доцент кафедры «Информационная безопасность» Жестовский А.Г.

Программа рассмотрена и одобрена на заседании кафедры «Информационная безопасность» (протокол № 9 от 14 июня 2018 г.)

Заведующий кафедрой «Информационная безопасность» /Великите Н.Я./

Программа рассмотрена и одобрена на заседании методической комиссии радиотехнического факультета (протокол № 6 от 27 июня 2018 г.)

Председатель методической комиссии /Жестовский А.Г./