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

СИСТЕМЫ ЗАЩИТЫ ОТ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

(наименование дисциплины)

вариативной 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

«14» июня 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./

1. Цель освоения дисциплины.

1.1 Цели дисциплины

Целью дисциплины «Системы защиты от утечки конфиденциальной информации» является ознакомление обучающихся с основными направлениями деятельности по обеспечению корпоративной защиты от внутренних угроз, рассмотрение аспектов нормативно-правовой базы, регламентирующей данную деятельность, задач специалистов по сохранности корпоративной информации, инструментов, технологий и методик их применения для достижения данных целей.

1.2 Задачи изучения дисциплины:

- сформировать общее представление о защите корпоративной информации, методах и способах ее достижения в современных условиях деятельности хозяйствующего субъекта;
- изучить практическую реализацию последовательности действий и мероприятий по обеспечению защиты хозяйствующего субъекта от внутренних угроз;
- привить навыки системного подхода к анализу обеспечения безопасности корпоративной информации.
- рассмотреть основные типы внутренних информационных угроз и связанные с ними риски;
- раскрыть принципы проведения профилактических мероприятия по предотвращению утечек информации, а также устранению последствий в случае утечки информации.
- показать особенности утечки информации по различным каналам, связанным с инфраструктурой организации, а также человеческим фактором.

1.3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-3 способность проводить анализ защищенности автоматизированных систем;

– ПК-17 способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации;

– ПК-22 способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации;

– ПСК-7.5 способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных систем.

1.4 Объекты предмета изучения дисциплины:

принципы обеспечения информационной безопасности; цели, задачи, сущность и содержание государственной информационной политики; информационные ресурсы; информационно-телекоммуникационная система; правовые основы организации защиты государственной тайны и конфиденциальной информации; стандарты по лицензированию в области обеспечения защиты государственной тайны; сертификация средств защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; угрозы информационной безопасности объекта.

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
ПК-3 - способность проводить анализ защищенности автоматизированных систем	**Знать**		**Знать:** технические каналы утечки информации; возможности технических средств перехвата информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации **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 режима секретности
	Уровень 1	классификацию АС и перечень требований по защите информации к каждому классу автоматизированных систем	
	Уровень 2	требования стандарта ISO по номенклатуре услуг, предоставляемых системой безопасности	
	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-17 - способность 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 автомати-	

		зированных систем по каналам утечки информации	**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
	Уметь		
	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	
ПК-22 - способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	**Знать**		**Знать:** основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; принципы формирования политики информационной безопасности в автоматизированных системах **Уметь:** эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем **Владеть:** навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем
	Уровень 1	основные принципы, реализуемые при разработке политики информационной безопасности организации	
	Уровень 2	основные виды политики информационной безопасности организации	
	Уровень 3	основные этапы разработки концепции безопасности организации, содержание документов политики информационной безопасности	
	Уметь		
	Уровень 1	разрабатывать функциональные обязанности должностных лиц организации по вопросам защиты информации	
	Уровень 2	вносить необходимые изменения и дополнения в организационно-распорядительные документы по вопросам обеспечения информационной безопасности программно-информационных ресурсов автоматизированных систем	
	Уровень 3	производить периодический анализ состояния и контроль эффективности реализуемых мер защиты информации	
	Владеть		
	Уровень 1	навыками соблюдения правил защиты информации	
	Уровень 2	навыками разработки концепции информационной безопасности организации (предприятия)	

	Уровень 3	методикой управления инцидентами и мониторингом подсистемы информационной безопасности АС	
ПСК-7.5 - способность координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации	**Знать**		**Знать:** принципы проектирования системы корпоративной защиты от внутренних угроз; основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах; инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз. **Уметь:** разрабатывать нормативно- правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности; проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации; администрировать автоматизированные технические средства управления и контроля информации и информационных потоков. **Владеть:** навыками подготовки нормативно- правовой базы и регламентирующих документов; разработки и внедрения политики информационной безопасности в хозяйствующем субъекте; проведения корпоративного информационного аудита; работы с автоматизированными техническими средствами управления и контроля информации и информационных потоков.
	Уровень 1	характер взаимодействия подразделений и служб организаций в процессе проведения исследований и разработок с использованием информации ограниченного доступа	
	Уровень 2	основные законодательные и правовые акты в области защиты информации, в том числе в области обеспечения безопасности персональных данных, и обеспечения безопасности информации в ключевых системах информационной инфраструктуры	
	Уровень 3	методы и средства ведения контроля состояния защищенности информации ограниченного доступа в органах государственной власти, организациях	
	Уметь		
	Уровень 1	разрабатывать категории доступа персонала на объекты защиты, порядок и правила поведения работников, в том числе при их перемещении, увольнении и взаимодействии с персоналом сторонних организаций	
	Уровень 2	проводить оценку технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений по обеспечению безопасности информации в ключевых системах информационной инфраструктуры	
	Уровень 3	осуществлять руководство и обучение персонала действиям в кризисных ситуациях, включая порядок действий руководящих и других ответственных лиц ключевых систем информационной инфраструктуры	
	Владеть		
	Уровень 1	навыками работы с правовыми базами данных, базами данных, содержащих информацию ограниченного доступа, в том числе по угрозам безопасности информации в органе государственной власти, организации, в ключевой системе информационной инфраструктуры	
	Уровень 2	навыками разработки необходимых документов в интересах организации работ по сертификации средств защиты информации и аттестации объектов информатизации	
	Уровень 3	навыками планирования и организации работ проведения работ в области технической защиты информации на уровне объекта информатизации	

3. Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.ДВ.07.01 «Системы защиты от утечки конфиденциальной информации» относится к числу дисциплин вариативной части модуля «Дисциплины по выбору Б1.В.ДВ.7».

Изучение её базируется на следующих дисциплинах: Основы управленческой деятельности; Математический анализ; Математическая логика и теория алгоритмов; Языки программирования; Технологии и методы программирования; Безопасность сетей электронных вычислительных машин; Безопасность систем баз данных; Криптографические методы защиты информации; Техническая защита информации; Сети и системы передачи информации; Организационное и правовое обеспечение информационной безопасности; Программно-аппаратные средства обеспечения информационной безопасности; Методы проектирования защищенных распределенных информационных систем; Экспертные системы.

Дисциплина необходима для освоения преддипломной практики. В свою очередь, данная дисциплина является обеспечивающей для написания выпускной квалификационной работы.

4. Содержание дисциплины

Тема 1. Теоретические основы защиты конфиденциальной информации от внутренних угроз.

Информация и информационные потоки. Внутренние и внешние угрозы ИБ. Модели угроз ИБ. Классификация нарушителей корпоративной информационной безопасности. Особенности оценки ущерба. Внутренние угрозы и каналы утечки конфиденциальной информации. Особенности реализации угроз утечки конфиденциальной информации. Современные технологии защиты от утечки конфиденциальной информации

Тема 2. Нормативно-правовые аспекты защиты конфиденциальной информации от внутренних угроз.

Системы DLP и требования по информационной безопасности. Категорирование информации в РФ. Юридические вопросы использования DLP-систем: личная и семейная тайны; тайна связи; специальные технические средства. Меры по обеспечению юридической значимости DLP (Pre-DLP). Обзор практики право применения при расследовании инцидентов, связанных с нарушениями режима внутренней информационной безопасности (Post-DLP).

Тема 3. Административно-организационные аспекты корпоративной защиты от внутренних угроз.

Архитектура систем защиты от утечки конфиденциальной информации. Изолированная автоматизированная система для работы с конфиденциальной информацией. Системы активного мониторинга рабочих станций пользователей. Формирование процессов и процедур аудита ИБ. Обследование корпоративных информационных систем. Состояние корпоративной информации. Инструменты и технологии обеспечения корпоративной защиты от внутренних угроз. Критерии эффективности проекта по обеспечению корпоративной защиты от внутренних угроз. Препятствия реализации проектов по обеспечению корпоративной защиты от внутренних угроз.

Тема 4. Защита корпоративной информации с использованием автоматизированной системы контроля информационных потоков.

Назначение системы IW Traffic monitor (IW TM). Контролируемые каналы передачи данных. Архитектура продукта IW TM. Технологии анализа детектируемых объектов. Задачи и принципы работы дополнительных модулей системы IW Device monitor (IW DM) и IW Crawler.

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	Всего
Семестр – А (4 ЗЕТ, 144 час.)					
Тема 1. Теоретические основы защиты конфиденциальной информации от внутренних угроз.	4	-	-	4	**8**
Тема 2. Нормативно-правовые аспекты защиты конфиденциальной информации от внутренних угроз.	10	-	12	8	**30**
Тема 3. Административно-организационные аспекты корпоративной защиты от внутренних угроз.	10	-	12	8	**30**
Тема 4. Защита корпоративной информации с использованием автоматизированной системы контроля информационных потоков.	12	-	24	36	**72**
Всего	**36**	**-**	**48**	**56**	**140**
Подготовка к сдаче зачета	-	-	-	**4**	**4**
Итого по дисциплине	**36**	**-**	**48**	**60**	**144**
	84				

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

6. Лабораторные занятия (работы)

Лабораторные занятия учебным планом не предусмотрены

7. Практические занятия

Таблица 3 – Практические занятия по очной форме обучения

№ ПЗ	Тема дисциплины	Тема и содержание ПЗ	Количество часов ПЗ
Семестр – А (48 час.)			
1.	Тема 2	Работа с нормативно-правовыми документами, регламентирующими вопросы правового регулирования защиты государственной тайны.	6
2.	Тема 2	Правовое регулирование взаимоотношений администрации и персонала в области защиты информации.	6
3.	Тема 3	Порядок определения актуальных угроз безопасности персональных данных в информационных системах персональных данных.	6
4.	Тема 3	Правовое регулирование защиты информации с использованием технических средств и противодействия угрозам информационной безопасности.	6
5.	Тема 4	Создание и использование политик ИБ в автоматизированной системе контроля информационных потоков организации	24
Всего за семестр:			48
Итого по дисциплине			**48**

8. Самостоятельная работа студента

Таблица 4 - Самостоятельная работа студента по очной форме обучения

№	Вид (содержание) СР	Количество часов СР	Форма контроля, аттестации
Семестр – А (60 час.)			
1.	Методы и формы организационной защиты конфиденциальной информации	4	опрос на занятиях, конспект лекций,
2.	Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ	4	опрос на занятиях, конспект лекций
3.	Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ	6	опрос на занятиях, конспект лекций
4.	Юридические вопросы использования DLP-систем: личная и семейная тайны; тайна связи; специальные технические средства	6	опрос на занятиях, конспект лекций
5.	DLP - системы и СКУД. Особенности их совместной эксплуатации	6	опрос на занятиях, конспект лекций, реферат
6.	Критерии эффективности проекта по обеспечению корпоративной защиты от внутренних угроз	6	опрос на занятиях, конспект лекций
7.	Назначение системы IW Traffic monitor (IW TM). Контролируемые каналы передачи данных.	6	опрос на занятиях, конспект лекций
8.	Использование DLP - системы для мониторинга анализа степени защищенности информации в АИС	6	опрос на занятиях, конспект лекций, реферат
9.	Контроль обмена информацией и предотвращение утечек	6	опрос на занятиях, конспект лекций
10.	Сбор событий и управление инцидентами	6	опрос на занятиях, конспект лекций
11.	Подготовка к сдаче зачета	4	конспект лекций
Всего за семестр:		**60**	
Итого по дисциплине		**60**	

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

9.1. Основная учебная литература

1. Ищейнов, В. Я. Защита конфиденциальной информации : учеб. пособие / В. Я. Ищейнов, М. В. Мецатунян. – М. : ФОРУМ, 2013. – 256 с. (наличие в библиотеке БГАРФ - 15 экз.)

2. Организационно-правовое обеспечение информационной безопасности : учеб. пособие / А. А. Стрельцов [и др.] ; под общ. ред. А. А. Стрельцова. – М. : Академия, 2008. – 256 с. (наличие в библиотеке БГАРФ - 12 экз.)

3. 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.)

9.2. Дополнительная учебная литература

1. Романов, О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 192 с. (наличие в библиотеке БГАРФ - 28 экз.)

2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – М. : ИД «Форум», 2013. – 416 с. (наличие в библиотеке БГАРФ - 20 экз.)

3. Родичев, Ю.А. Информационная безопасность: нормативно-правовые аспекты : учебное пособие для студентов, обучающихся по спец. "Комплексное обеспечение информационной безопасности автоматизированных систем" / Ю. А. Родичев. - СПб. : Питер, 2008. - 272 с. (наличие в библиотеке БГАРФ - 15 экз.)

4. 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.)

5. Кузнецов, А. В. Основы защиты информации : учеб. пособие / В. А. Иванов, О.П. Пономарев, И. А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 122 с. (наличие в библиотеке БГАРФ - 110 экз.)

9.3. Периодические издания

1. Защита информации. Инсайд : информационно-методический журнал. - СПб. : ООО "Изд. Дом "Афина".

2. Радиотехника : международный научно-технический журнал. - М. : ЗАО "Издательство "Радиотехника".

3. Вопросы радиоэлектроники : научный журнал. - М. : АО "ЦНИИ "Электроника".

4. Безопасность информационных технологий : научно-технический журнал. - М. : Изд-во журнала "Безопасность информационных технологий".

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.

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 PROJECTA – 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 практических занятий

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

При обучении студентов с нарушениями зрениями предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей 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 «Системы защиты от утечки конфиденциальной 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.

В процессе преподавания данной дисциплины используются такие виды учебной работы, как лекция, практические занятия, а также различные виды самостоятельной работы обучающихся по заданию преподавателя, направленные на развитие навыков использования профессиональной лексики, закрепление практических профессиональных компетенций, поощрение интеллектуальных инициатив.

Методические указания для обучающихся при работе над конспектом лекций во время проведения лекции

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект, что позволит впоследствии вспомнить изученный учебный материал, дополнить содержание при самостоятельной работе с литературой, подготовиться к зачету.

Следует также обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля,

на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Любая лекция должна иметь логическое завершение, роль которого выполняет заключение. Выводы по лекции подытоживают размышления преподавателя по учебным вопросам. Формулируются они кратко и лаконично, их целесообразно записывать. В конце лекции обучающиеся имеют возможность задать вопросы преподавателю по теме лекции.

Методические рекомендации по выполнению практических занятий

Практические занятия выполняются в соответствии с рабочим учебным планом при последовательном изучении тем дисциплины.

- Порядок проведения практикума:
- Получение задания и рекомендаций к выполнению практикума.
- Настройка инструментальных средств, необходимых для выполнения практикума.
- Выполнение заданий практикума.
- Подготовка отчета в соответствии с требованиями.
- Сдача отчета преподавателю.

В ходе выполнения практикума необходимо следовать технологическим инструкциям, использовать материал лекций, рекомендованных учебников, источников интернета, активно использовать помощь преподавателя на занятии.

Требования к оформлению результатов практикумов.

При подготовке отчета: изложение материала должно идти в логической последовательности, отсутствие грамматических и синтаксических ошибок, шрифт Times New Roman, размер – 14, выравнивание по ширине, отступ первой строки – 1,25, междустрочный интервал – 1,5, правильное оформление рисунков (подпись, ссылка на рисунок в тексте).

При подготовке презентации: строгий дизайн, минимум текстовых элементов, четкость формулировок, отсутствие грамматических и синтаксических ошибок, воспринимаемая графика, умеренная анимация.

Практические занятия направлены на закрепление лекционного материала. При подготовке к занятиям руководствоваться «Методическими указаниями по выполнению практических занятий по дисциплине «Системы защиты от утечки конфиденциальной информации».

Методические указания для обучающихся по организации самостоятельной работы

Самостоятельная работа обучающихся направлена на самостоятельное изучение отдельных тем/вопросов учебной дисциплины.

Самостоятельная работа является обязательной для каждого обучающегося, ее объем по дисциплине определяется учебным планом. При самостоятельной работе обучающиеся взаимодействуют с рекомендованными материалами при минимальном участии преподавателя. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Изучая материал по учебной книге (учебнику, учебному пособию, монографии, и др.), следует переходить к следующему вопросу только после полного уяснения предыдущего, фиксируя выводы и вычисления (конспектируя), в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода.

Особое внимание обучающийся должен обратить на определение основных понятий курса. Надо подробно разбирать примеры, которые поясняют определения. Полезно составлять опорные конспекты.

Выводы, полученные в результате изучения учебной литературы, рекомендуется в конспекте выделять, чтобы при перечитывании материала они лучше запоминались.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Вопросы, которые вызывают у обучающегося затруднение при подготовке, должны быть заранее сформулированы и озвучены во время занятий в аудитории для дополнительного разъяснения преподавателем.

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 обучения, 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 «Системы защиты от утечки конфиденциальной 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./