Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»

А. А. Бабаева

ПРОЕКТИРОВАНИЕ ОТКРЫТЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Учебно-методическое пособие по изучению дисциплины для студентов специальности 10.05.03 «Проектирование открытых систем в защищенном исполнении»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2022

Рецензент
доцент кафедры информационной безопасности ФГБОУ ВО
«Калининградский государственный технический университет»
А. Г. Жестовский

Бабаева, А. А.
Проектирование открытых систем в защищенном исполнении: учебно-методическое пособие по изучению дисциплины для студентов специальности 10.05.03 «Проектирование открытых систем в защищенном исполнении» / А. А. Бабаева. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 30 с.

Учебно-методическое пособие является руководством по изучению дисциплины «Проектирование открытых систем в защищенном исполнении» студентами, обучающимися по специальности 10.05.03 Информационная безопасность автоматизированных систем. Учебно-методическое пособие предназначено для изучения теоретического материала в области проектирования, создания, эксплуатации, открытых систем и обеспечения их безопасности на всех этапах жизненного цикла.
Список лит. – 6 наименований.

Пособие рассмотрено и одобрено в качестве локального электронного методического материала кафедрой информационной безопасности 19 мая 2022 г., протокол № 7

Учебно-методическое пособие по изучению дисциплины рекомендовано в качестве локального электронного методического материала для использования в учебном процессе методической комиссией института цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» 28 июня 2022 г., протокол № 4

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Данное учебно-методическое пособие предназначено для студентов специальности 10.05.03 «Проектирование открытых систем в защищенном исполнении», изучающих дисциплину «Информационная безопасность автоматизированных информационных систем».

Цель освоения дисциплины:

В результате освоения дисциплины ожидается, что студенты получат целостное представление о решении задач информационной безопасности открытых систем в защищенном исполнении, научатся анализировать угрозы информационной безопасности, создавать модель угроз и модель нарушителя с учетом специфики защищенной автоматизированной системы, проектировать открытые информационные системы в защитном исполнении.

Задачи дисциплины

- выявлять возможные способы нарушения информационной безопасности при работе в открытых системах;
- определять задачи обеспечения информационной безопасности;
- в рамках задач обеспечения информационной безопасности решать вопросы использования средств защиты информации;
- определять возможности применения стандартных криптографических решений для зашиты информации;
- определять особенности политики безопасности и способы ее внедрения на предприятии;
- давать оценку качества предлагаемых решений в области информационной безопасности открытых систем;
- применять системный подход к обеспечению информационной безопасности в различных сферах деятельности, включая комплекс организационных мер.

В соответствии с учебным планом для более успешного изучения дисциплине «Информационная безопасность автоматизированных информационных систем» предшествуют: «Основы информационной безопасности», «Сети и системы передачи информации», «Правовые основы информационной безопасности».

Далее в пособии представлен тематический план, содержащий перечень изучаемых тем, обязательных лабораторных/практических работ, мероприятий текущей аттестации и отводимое на них аудиторное время (занятия в соответствии с расписанием) и самостоятельную работу. При формировании личного образовательного плана на семестр

следует оценивать рекомендуемое время на изучение дисциплины, возможно, вам потребует больше времени на выполнение отдельных заданий или проработку отдельных тем.

В разделе Содержание дисциплины приведены подробные сведения об изучаемых вопросах, по которым вы можете ориентироваться в случае пропуска каких-то занятий, а также методические рекомендации преподавателя для самостоятельной подготовки; каждая тема имеет ссылки на литературу (или иные информационные ресурсы), а также контрольные вопросы для самопроверки.

Раздел «Текущая аттестация» содержит описание обязательных мероприятий контроля самостоятельной работы и усвоения разделов или отдельных тем дисциплины. Далее изложены требования к завершающей аттестации – зачет.

В разделе «Балльно-рейтинговая система» приведен порядок применения балльно-рейтинговой системы контроля успеваемости.

Помимо данного пособия, студентам следует использовать материалы, размещенные в соответствующем данной дисциплине разделу ЭИОС, в которые более оперативно вносятся изменения для адаптации дисциплины под конкретную группу.

2. ТЕМАТИЧЕСКИЙ ПЛАН

	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самост-ной работы, ч
		Лекции		
1.	Сущность, цели и задачи организации защиты информации открытых систем	Тема 1.1: Основные положения современной теории защиты информации для открытых систем.	2	2
		Тема 1.2: Современные теории систем для организации и обеспечения функционирования открытых систем.	2	2
		Тема 1.3: Базовые подсистемы защиты информации и требования к ним	2	2
2.	Основные принципы организации открытых систем в защищенном исполнении.	Тема 2.1: Факторы, оказывающие влияние на организацию защиты открытых систем.	4	2
		Тема 2.2: Функциональные и обеспечивающие подсистемы защиты информации.	2	2
		Тема 2.3: Требования, предъявляемые к сотрудникам, обеспечивающим функционирование открытых систем.	2	2

3.	Структура угроз для информационных ресурсов открытых систем.	Тема 3.1: Методы выявления состава защищаемых элементов. Объекты и субъекты защиты.	2	2
		Тема 3.2: Процедура выявления каналов несанкционированного доступа к информации в открытых системах	2	2
		Тема 3.3: Особенности построения модели угроз для ИС. Нормативные документы, этапы создания.	2	4
		Тема 3.4: Структура типовой базовой модели угроз для ИС. Способы определения актуальных угроз безопасности.	2	2
4.	Принципы криптографической защиты информации.	Тема 4.1: Нормативные документы ФСБ.	2	2
		Тема 4.2: Понятие ЭЦП. Особенности использования.	2	2
		Тема 4.3: Особенности контроля деятельности персонала, связанного с защитой информации.	2	4
5.	Аттестация средств защиты информации по требованиям безопасности	Тема 5.1: Способы оценки эффективности принятых мер защиты в ИС. Анализ защищенности.	2	2
		Тема 5.2: Эксплуатационная документация АС. Требования к ней, особенности эксплуатации.	2	4

		Тема 5.3: Основные нормативные документы, регламентирующие создание и функционирование открытых систем в защищенном исполнении.	2	2
			17	**55**

		Практические (лабораторные занятия)		
1.	Определение актуальных угроз для организации с открытой системой и составление модели угроз и нарушителя	Описание информационной системы персональных данных	8	1
		Определение задач защиты. Выделение основных функций и задач защиты информации	10	1
		Виды моделей угроз и уязвимостей. Создание модели угроз и уязвимостей для своего объекта	10	1
		Выявление возможных каналов несанкционированного доступа	10	2
		Определение класса средств криптографической защиты информации. Разработка модели угроз по документам ФСБ	10	2

		Оценка актуальных угроз безопасности информации	10	1
		Оценка эффективности средств защиты информации. Метод экспертных структурных вопросников	10	1
			34	**20**

		Рубежный (текущий) и итоговый контроль		
3.1				
		Итоговый контроль (зачет)	x	
			3,15	

Всего	**144**	**75**

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И УКАЗАНИЯ К ИЗУЧЕНИЮ

3.1 Раздел 1. Сущность, цели и задачи организации защиты информации открытых систем

3.1.1 Тема 1.1 Основные положения современной теории защиты информации для открытых систем

Перечень изучаемых вопросов:

Задачи и цели организации защиты информации в открытых информационных системах. Сущность вопроса защиты информации.

Методические указания к изучению:

Рассматриваются основные термины и определения в области информационной безопасности открытых систем. Раскрываются понятия задач и целей защиты информации и организации системы защиты в открытых системах. Изучаются особенности использования задач защиты при составлении элементов системы защиты для организации.

Предусмотрена лабораторная работа по теме: Определение задач защиты. Выделение основных функций и задач защиты информации.

Литература:

1. Бондарев, В. В. Введение в информационную безопасность автоматизированных систем: учебное пособие/ В. В. Бондарев. – Москва: МГТУ им. Н. Э. Баумана, 2016. – 252 с.

2. Нестеров, С. А. Информационная безопасность и защита информации: учебное пособие. – Санкт-Петербург: Изд-во Политехн. ун-та, 2009. - 126 с.

Контрольные вопросы:

1. Перечислить основные задачи защиты.
2. Указать цели организации системы защиты.
3. Сущность понятия системы информационной безопасности.

3.1.2 Тема 1.2 Современные теории систем для организации и обеспечения функционирования открытых систем

Перечень изучаемых вопросов:

Теории систем для организации функционирования открытых систем, современные стандарты организации работы и контроля эффективности открытых систем.

Методические указания к изучению:

Рассматриваются особенности создания открытых систем, область их применения и основные элементы с описанием теории систем для организации и обеспечения функционирования.

Литература:

1. Бондарев, В. В. Введение в информационную безопасность автоматизированных систем: учебное пособие/ В. В. Бондарев. – Москва: МГТУ им. Н. Э. Баумана, 2016. – 252 с.

2. Нестеров, С. А. Информационная безопасность и защита информации: учебное пособие. – Санкт-Петербург: Изд-во Политехн. ун-та, 2009. - 126 с.

Контрольные вопросы:

1. Теории организации открытых систем.
2. Особенности функционирования ОС.
3. Способы создания и организации работы ОС.

3.1.3. Тема 1.3 Базовые подсистемы защиты информации и требования к ним

Перечень изучаемых вопросов:

Подсистемы защиты информации, базовые и вспомогательные. Требования к подсистемам обеспечения информационной безопасности.

Методические указания к изучению:

Рассматриваются основные виды протоколов базовых подсистем безопасности информационных систем и группы требований к ним, для обеспечения функционирования и поддержания нужного уровня защищённости.

Литература:

1. Бондарев, В.В. Введение в информационную безопасность автоматизированных систем: учебное пособие/ В.В. Бондарев. – Москва МГТУ им. Н. Э. Баумана, 2016. – 252 с.

2. Нестеров, С.А. Информационная безопасность и защита информации: учебное пособие. - Санкт-Петербург: Изд-во Политехн. ун-та, 2009. - 126 с.

Контрольные вопросы:

1. Базовые подсистемы зашиты
2. Требования к подсистемам защиты информации
3. Состав мер и средств обеспечения информационной безопасности

3.2 Раздел 2. Основные принципы организации ИС в защищенном исполнении

3.2.1 Тема 2.1 Факторы, оказывающие влияние на организацию защиты открытых систем

Перечень изучаемых вопросов:

Факторы, оказывающие влияние на организацию защиты ОС, анализ рисков информационной безопасности, состав защищаемой информации, тип информационной системы.

Методические указания к изучению:

Рассматривается понятие факторов, оказывающих влияние на организацию защиты, таких как: риски ИБ, состав защищаемой информации, тип ОС и категория защищаемой информации.

Литература:

1. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности: учебное пособие/ Ю.А. Родичев. – Санкт-Петербург.: Питер, 2017. – 256 с.

2. Хореев, П.Б. Методы и средства защиты информации в компьютерных системах: учебное пособие для вузов / П.Б. Хореев. - Москва: Academia, 2008. - 256 с.

Контрольные вопросы:

1. Типы защищаемой информации.
2. Виды информационных систем и требования к их защите.

3.2.2 Тема 2.2 Функциональные и обеспечивающие подсистемы защиты информации открытых систем

Перечень изучаемых вопросов:

Функциональные и обеспечивающие подсистемы защиты ОС, состав этих подсистем защиты. Правила создания и разработки подсистем защиты и требования к ним.

Методические указания к изучению: Рассматривается состав функциональной и обеспечивающей подсистемы защиты для открытых информационных систем с целью повышения уровня защищенности ИС.

Литература:

1. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности: учебное пособие/ Ю.А. Родичев. – Санкт-Петербург.: Питер, 2017. – 256 с.
2. Хореев, П.Б. Методы и средства защиты информации в компьютерных системах: учебное пособие для вузов / П.Б. Хореев. - Москва: Academia, 2008.- 256 с.

Контрольные вопросы:

1. Состав функциональной подсистемы защиты ОС.
2. Состав обеспечивающей подсистемы защиты ОС.
3. Требования к подсистемам защиты ОС.

3.2.3 Тема 2.3 Требования, предъявляемые к сотрудникам, обеспечивающим функционирование открытых систем

Перечень изучаемых вопросов:

Состав требований, предъявляемых к сотрудникам, обеспечивающим функционирование ОС, и нормативно правовая база этого вопроса.

Методические указания к изучению:

Рассматриваются понятия требований, предъявляемых к сотрудникам, обеспечивающим функционирование ОС, и нормативно правовая база этого вопроса. Изучается состав мер и средств для обеспечения безопасности.

Литература:

1. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности: учебное пособие / Ю.А. Родичев. – Санкт-Петербург: Питер, 2017. – 256 с.

2. Хореев, П.Б. Методы и средства защиты информации в компьютерных системах: учебное пособие для вузов / П.Б. Хореев. - Москва: Academia, 2008.- 256 с.

3.3 Раздел 3. Структура угроз для информационных ресурсов открытой системы

3.3.1 Тема 3.1 Методы выявления состава защищаемых элементов. Объекты и субъекты защиты

Перечень изучаемых вопросов:

Объекты и субъекты защиты. Внешние и внутренние субъекты защиты. Структура угроз для информационных ресурсов ОС.

Методические указания к изучению:

Рассматривается понятие объекта и субъекта защиты для ОС. Изучаются способы выявления состава защищаемых элементов в ИС с целью повышения защищенности.

Литература:

1. Бондарев, В.В. Введение в информационную безопасность автоматизированных систем: учебное пособие / В.В. Бондарев. – Москва: МГТУ им. Н. Э. Баумана, 2016. – 252 с.

2. Нестеров, С.А. Информационная безопасность и защита информации: учебное пособие. - Санкт-Петербург: Изд-во Политехн. ун-та, 2009. - 126 с.

Контрольные вопросы:

1. Понятие объекта защиты ОС.
2. Понятие субъекта защиты ОС.
3. Методы выявления состава защищаемых объектов в ОС.

3.3.2 Тема 3.2 Процедура выявления каналов несанкционированного доступа к информации в ОС

Перечень изучаемых вопросов:

Каналы НСД к информации, способы выявления их и меры защиты.

Методические указания к изучению:

Рассматриваются способы выявления каналов НСД к информации в ОС, способы их локализации и защиты от НСД. Изучаются основные уязвимости в ОС, влекущие к появлению каналов НСД.

Литература:

1. Бондарев, В.В. Введение в информационную безопасность автоматизированных систем: учебное пособие / В.В. Бондарев. – Москва: МГТУ им. Н. Э. Баумана, 2016. – 252 с.

2. Нестеров, С.А. Информационная безопасность и защита информации: учебное пособие. - Санкт-Петербург: Изд-во Политехн. ун-та, 2009. - 126 с.

Контрольные вопросы:

1. Виды каналов НСД к информации.
2. Способы выявления каналов НСД.
3. Уязвимости в ОС, приводящие к появлению каналов НСД к информации.

3.3.3 Тема 3.3 Особенности построения модели угроз для ИС. Нормативные документы, этапы создания

Перечень изучаемых вопросов:

Модель угроз и модель нарушителя. Нормативно-правовые документы, отвечающие за выявления актуальных угроз безопасности. Этапы создания модели угроз. ФСТЭК.

Методические указания к изучению:

Рассматривается необходимость создания модели угроз и нарушителя для ИС. Изучаются основные угрозы и уязвимости из БДУ ФСТЭК, нормативные документы, регламентирующие создание модели угроз и определения актуальных угроз в организации.

Литература:

1. Черемушкин, А. В. Информационная безопасность. Глоссарий / Под ред. С. Пазизина. – Москва: «АВАНГАРД ЦЕНТР», 2013. – 322 с.

2. Методика оценки актуальных угроз безопасности, методический документ, Утвержден ФСТЭК России 5 февраля 2021 г.

Контрольные вопросы:

1). Этапы оценки актуальности угроз безопасности.

2). Нормативно-правовая база оценки актуальности угроз.

3). Модель нарушителя, модель угроз.

3.3.4 Тема 3.4 Структура типовой базовой модели угроз для ИС. Способы определения актуальных угроз безопасности

Перечень изучаемых вопросов:

Способы определение актуальных угроз безопасности. Состав модели угроз, структура типовой модели угроз для ИС.

Методические указания к изучению:

Рассматривается необходимость создания модели угроз и нарушителя для ИС. Изучаются основные угрозы и уязвимости из БДУ ФСТЭК, нормативные документы, регламентирующие создание модели угроз и определения актуальных угроз в организации.

Литература:

1. Черемушкин, А. В. Информационная безопасность. Глоссарий /под ред. С. Пазизина. – Москва: «АВАНГАРД ЦЕНТР», 2013. – 322 стр.

2. Методика оценки актуальных угроз безопасности, методический документ, Утвержден ФСТЭК России 5 февраля 2021 г.

3.3 Раздел 4**. Принципы криптографической защиты информации**

3.4.1 Тема 4.1 Нормативные документы ФСБ

Перечень изучаемых вопросов:

Криптографическая защиты и ее основные функции при составлении систем защиты ИС. Документы ФСБ в области защиты информации в ИС. Модель угроз по ФСБ.

Методические указания к изучению:

Рассматриваются вопросы создания модели угроз по документам ФСБ и необходимость применения криптографической зашиты в системе защиты организации.

Литература:

1. Нестеров, С.А. Информационная безопасность и защита информации: учебное пособие /С.А. Нестеров. – Санкт-Петербург: Изд-во Политехн. ун-та, 2009. - 126 с.

2. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности: учебное пособие/ Ю.А. Родичев. – Санкт-Петербург: Питер, 2017. – 256 с.

Контрольные вопросы:

1). В каких случаях необходимо применение документов ФСБ?

2). Особенности оценки актуальности угроз с применением средств криптографической защиты.

3.4.2 Тема 4.2 Понятие ЭЦП. Особенности использования

Перечень изучаемых вопросов:

Понятие электронной цифровой подписи для обеспечения безопасности передачи сообщений. Особенности и правила использования ЭЦП.

Методические указания к изучению:

Рассматриваются вопросы использования ЭЦП при документообороте в ИС. Особенности ее применения и получения сертификата от центра сертификации.

Литература:

1. Нестеров, С.А. Информационная безопасность и защита информации: учебное пособие / С.А. Нестеров. - Санкт-Петербург: Изд-во Политехн. ун-та, 2009. - 126 с.

2. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности: учебное пособие/ Ю.А. Родичев. – Санкт-Петербург: Питер, 2017. – 256 с.

Контрольные вопросы:

1). Понятие ЭЦП.

2). Способы использования и особенности применения ЭЦП .

3). Особенности настройки безопасности при использовании ЭЦП.

3.4.3 Тема 4.3 Особенности контроля деятельности персонала, связанного с защитой информации

Перечень изучаемых вопросов:

Контроль деятельности персонала, работающего с различными категориями информации с целью обеспечения информационной безопасности.

Методические указания к изучению:

Рассматриваются вопросы взаимодействия персонала и защищаемой информации. Особенности применения методов обучения и контроля персонала.

Литература:

1. Нестеров, С.А. Информационная безопасность и защита информации: учебное пособие / С.А. Нестеров. - Санкт-Петербург: Изд-во Политехн. ун-та, 2009. - 126 с.

2. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности: учебное пособие / Ю.А. Родичев. – Санкт-Петербург: Питер, 2017. – 256 с.

3.5 Раздел 5. Аттестация средств защиты информации по требованиям безопасности

3.5.1 Тема 5.1 Способы оценки эффективности принятых мер защиты в ОС. Анализ защищенности

Перечень изучаемых вопросов:

Способы оценки эффективности принятых мер защиты в ОС. Сравнения и выявление преимуществ и недостатков.

Методические указания к изучению:

Рассматриваются вопросы оценки эффективности принятых мер защиты. Метод экспертных структурных опросников для оценки.

Литература:

1. Нестеров, С.А. Информационная безопасность и защита информации: учебное пособие / С.А. Нестеров. - Санкт-Петербург: Изд-во Политехн. ун-та, 2009. - 126 с.

2. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности: учебное пособие/ Ю.А. Родичев. – Санкт-Петербург: Питер, 2017. – 256 с.

Контрольные вопросы:

1. *Для чего нужна оценка эффективности?*
2. *Способы оценки эффективности принятых мер зашиты.*

3.5.2 Тема 5.2: Эксплуатационная документация АС. Требования к ней, особенности эксплуатации.

Перечень изучаемых вопросов:

Эксплуатационная документация для АС. Требования к эксплуатационной документации. Обзор нормативно-правовой базы.

Методические указания к изучению:

Рассматриваются вопросы создания эксплуатационной документации и требования к ней. Особенности эксплуатации.

Литература:

1. Бондарев, В.В. Введение в информационную безопасность автоматизированных систем: учебное пособие/ В.В. Бондарев. – Москва: МГТУ им. Н. Э. Баумана, 2016. – 252 с.

2. Нестеров С.А. Информационная безопасность и защита информации: учебное пособие / С.А. Нестнров. - Санкт-Петербург: Изд-во Политехн. ун-та, 2009. - 126 с.

3.5.3 Тема 5.3 Основные нормативные документы, регламентирующие создание и функционирование ОС в защищенном исполнении

Перечень изучаемых вопросов:

Основные нормативные документы, регламентирующие создание и функционирование ОС в защищенном исполнении. Этапы создания ОС в защищенном исполнении.

Методические указания к изучению:

Рассматриваются вопросы создания и функционирования ОС в защищенном исполнении. Особенности и этапы разработки и проектирования ОС в защищенном исполнении.

Литература:

1. Бондарев, В.В. Введение в информационную безопасность автоматизированных систем: учебное пособие/ В.В. Бондарев. – Москва: МГТУ им. Н. Э. Баумана, 2016. – 252 с.

2. Нестеров, С.А. Информационная безопасность и защита информации: учебное пособие / С.А. Нестеров. - Санкт-Петербург: Изд-во Политехн. ун-та, 2009. - 126 с.

Контрольные вопросы:

1. *Какая ОС считается системой в защищенном исполнении?*
2. *Требования к созданию открытой системы в защищенном исполнении.*

4. ТРЕБОВАНИЯ К АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

4.1 Текущая аттестация

В ходе изучения дисциплины студентам предстоит пройти следующие этапы текущей аттестации: контроль самостоятельной работы по темам дисциплины, контроль выполнения лабораторных работ, контрольные работы в виде ответов на вопросы.

Преподаватель вправе выбрать методику оценивания знаний студентов: традиционная зачетно-экзаменационная, либо балльно-рейтинговая.

4.2 Порядок применения рейтинговой системы:

В рамках балльно-рейтинговой системы выставляется оценка за качество выполнения и защиту лабораторных и контрольных работ.

Виды деятельности и соотношение трудоемкости (таблица 1):

Таблица 1 – Виды деятельности и соотношение трудоемкости

Вид деятельности	Доля	Кол-во ед.	Макс. балл за ед.	Всего
Обязательные виды деятельности				
1 семестр				
Посещаемость занятий	20%	N1	=200/N1	200
Выполнение лаб. работ (защита)	40%	2	200	400
Контрольная работа 1	40%	1	400	400
Итого:	100%			1000
2 семестр				
Посещаемость занятий	20%	N2	=200/N2	200
Выполнение лаб. работ (защита)	40%	2	200	400
Контрольная работа 2	40%	1	400	400
Итого:	100%			1000
Всего				2000
Дополнительные задания (по выбору студента в каждом семестре)				
Подготовка реферата (видео-доклада)	20%		200	200
Решение дополнительных задач контрольной работы	10%		100	100
Выполнение задания в рамках НИРС	50%		500	500

4.3 Условия получения положительной оценки:

Завершающим этапом изучения дисциплины является промежуточная аттестация, представляющая собой:

Критерии оценок на **дифференцированном зачете** по дисциплине (отлично, хорошо, удовлетворительно, неудовлетворительно):

- «ОТЛИЧНО» выставляется в случае правильных, полных и четких ответов на теоретические вопросы, с их проецированием и интерпретацией на сегодняшнюю ситуацию. Допускаются непринципиальные погрешности или небольшая незавершенность ответов, диктуемых лимитом времени.

- «ХОРОШО» - в случаях: правильных и четких ответов при незначительных замечаниях, неточностях.

- «УДОВЛЕТВОРИТЕЛЬНО» - в случаях ответа на большую часть (не менее 50% основных положений); при правильном ответе на один вопрос или неполных ответах на два вопроса.

- «НЕУДОВЛЕТВОРИТЕЛЬНО» - при ответах, не удовлетворяющих критериям, указанным в предыдущих пунктах.

Зачет по дисциплине осуществляется при условии выполнения заданий всех лабораторных работ, самостоятельной работы, а также результатами проведенной оценки остаточных знаний.

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

4.4 Примерные вопросы к зачету по дисциплине:

1	Сущность, цели и задачи организации защиты информации
2	Основные положения современной теории защиты информации для открытых систем
3	Современные теории систем для организации и обеспечения функционирования ОС
4	Базовые подсистемы защиты информации и требования к ним
5	Структура угроз для информационных ресурсов ОС. Классификация угроз
6	Функциональные и обеспечивающие подсистемы защиты информации
7	Факторы, оказывающие влияние на организацию защиты ОС
8	Основные принципы организации ОС в защищенном исполнении
9	Функциональные и обеспечивающие подсистемы защиты информации
10	Требования к защите применительно к различным защищаемым элементам ОС
11	Факторы, определяющие состав защищаемой информации

12	Основные этапы работы по выявлению состава защищаемой информации
13	Какие компоненты входят в состав структуры ОС?
14	Управление рисками. Анализ рисков по методике оценки угроз безопасности
15	Методы выявления состава защищаемых элементов. Объекты и субъекты защиты
16	Какими факторами определяется состав угроз безопасности открытой системы?
17	Какова процедура выявления каналов несанкционированного доступа к информации в ОС?
18	Чем определяется состав нарушителей и как осуществляется их категорирование?
19	Каким образом может проводиться оценка степени уязвимости информации в результате действий нарушителей различных категорий?
20	Какие требования предъявляются к выбору методов и средств защиты при организации и функционировании ОС?
21	Какие компоненты входят в состав информационной модели ОС?
22	Требования, предъявляемые к сотрудникам, обеспечивающим функционирование ОС
23	Нормативные документы, регламентирующие деятельность и взаимодействие персонала с защищенной ОС
24	Особенности контроля деятельности персонала, связанного с защитой информации
25	Основные нормативные документы, регламентирующие создание и функционирование ОС в защищенном исполнении
26	Понятие ЭЦП. Особенности использования
27	Принципы криптографической защиты информации. Нормативные документы ФСБ
28	Особенности построения модели угроз для ИС. Нормативные документы, этапы создания
29	Структура типовой базовой модели угроз для ОС. Способы определения актуальных угроз безопасности
30	Обзор проекта новой методики моделирования угроз безопасности информации и сравнение со старой методикой по ФСТЭК
31	Способы оценки эффективности принятых мер защиты в ОС. Анализ защищенности
32	Аттестация средств защиты информации по требованиям безопасности
33	Эксплуатационная документация ОС. Требования к ней, особенности эксплуатации

5. ЗАКЛЮЧЕНИЕ

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.

В лекциях по предмету излагаются основные знания по курсу дисциплины. Самостоятельная работа имеет особое значение для прочного усвоения материала. Она помогает научиться правильно ориентироваться в научной литературе, самостоятельно мыслить и находить правильные ответы на возникающие вопросы. В ходе всех видов занятий происходит углубление и закрепление знаний студентов, вырабатывается умение правильно излагать свои мысли.

Самостоятельная работа выполняет ряд функций, к которым относятся:

- развивающая (повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей студентов);
- информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, не подкрепленная самостоятельной работой, становится малорезультативной);
- ориентирующая и стимулирующая (процессу обучения придается профессиональное ускорение);
- воспитывающая (формируются и развиваются профессиональные качества специалиста):
- исследовательская (новый уровень профессионально-творческого мышления).

В основе самостоятельной работы студентов лежат принципы: самостоятельности, развивающе-творческой направленности, целевого планирования, личностно-деятельностного подхода.

Самостоятельная работа студентов проводиться с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений студентов;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;

- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

- развития исследовательских умений.

Для достижения указанной цели студенты на основе плана самостоятельной работы должны решать следующие задачи:

- изучить рекомендуемые литературные источники:

- изучить основные понятия, представленные в глоссарии;

- ответить на контрольные вопросы:

- решить предложенные задачи, кейсы, ситуации;

- выполнить контрольные и курсовые работы.

Работа студентов в основном складывается из следующих элементов:

- изучение и усвоение в соответствии с учебным планом программного материала по всем учебным дисциплинам;

- выполнение письменных контрольных и курсовых работ;

- подготовка и сдача зачетов, курсовых работ, итоговых экзаменов;

- написание и защита дипломной работы.

Самостоятельная работа включает такие формы работы, как:

- индивидуальное занятие (домашние занятия) - важный элемент в работе студента по расширению и закреплению знаний;

- конспектирование лекций;

- получение консультаций для разъяснений по вопросам изучаемой дисциплины;

- подготовка ответов на вопросы тестов;

- подготовка к экзамену;

- выполнение контрольных, курсовых проектов и дипломных работ;

- подготовка научных докладов, рефератов, эссе;

- анализ деловых ситуаций (мини кейсов) и др.

Содержание внеаудиторной самостоятельной работы определяется в соответствии с рекомендуемыми видами заданий, рабочей программой учебной дисциплины. Распределение объема времени на внеаудиторную самостоятельную работу в режиме дня студента не регламентируется расписанием.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференциальный характер, учитывать специфику специальности, изучаемой дисциплины, индивидуальные особенности студента.

Для закрепления и систематизации знании необходимы:

- работа с конспектом лекции (обработка текста);
- повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудиовидеозаписей):
- составление плана и тезисов ответа;
- выполнение тестовых заданий;
- ответы на контрольные вопросы;
- аннотирование, реферирование, рецензирование текста;
- подготовка сообщений к выступлению на семинаре, конференции; подготовка рефератов, докладов;
- работа с компьютерными программами;
- подготовка к сдаче экзамена;

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.

Рабочая программа дисциплины «Информационная безопасность автоматизированных информационных систем» представляет собой компонент образовательной программы специалитета по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем и соответствует учебному плану, действующему для студентов.

6. ЛИТЕРАТУРА

1. Бондарев, В.В. Введение в информационную безопасность автоматизированных систем: учебное пособие/ В.В. Бондарев. – Москва: МГТУ им. Н. Э. Баумана, 2016. – 252 с.

2. Нестеров С.А. Информационная безопасность и защита информации: учебное пособие / С.А. Нестеров. - Санкт-Петербург: Изд-во Политехн. ун-та, 2009. - 126 с.

3. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности: учебное пособие/ Ю.А. Родичев. – Санкт-Петербург: Питер, 2017. – 256 с.

4. Хореев, П.Б. Методы и средства защиты информации в компьютерных системах: учебное пособие для вузов / П.Б. Хореев. - Москва: Academia, 2008.- 256 с.

5. Черемушкин, А. В. Информационная безопасность. Глоссарий /под ред. С. Пазизина. – Москва: «АВАНГАРД ЦЕНТР», 2013. – 322 с.

6. Методика оценки актуальных угроз безопасности, методический документ, Утвержден ФСТЭК России 5 февраля 2021 г.

Локальный электронный методический материал

Алина Андреевна Бабаева

ПРОЕКТИРОВАНИЕ ОТКРЫТЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Редактор Г. А. Смирнова

Уч.-изд. л. 1,4. Печ. л. 1,9

Издательство федерального государственного бюджетного образовательного учреждения
высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1