Аннотация к рабочей программе дисциплины «Проектирование защищенных автоматизированных систем»

Цель преподавания дисциплины

Дисциплина "Проектирование защищенных автоматизированных систем" изучается с целью изучения технологий, методов и средств создания защищенных автоматизированных систем.

Задачи изучения дисциплины

– сформировать профессиональную культуру проектирования защищенных автоматизированных систем;

– понимать принципы построения защищенных автоматизированных систем;

– познакомиться с уязвимостями, угрозами ИБ и видами деструктивного воздействия, характерными для современных автоматизированных систем;

– изучить подходы и методы обеспечения ИБ автоматизированных систем.

Компетенции, формируемые в результате освоения дисциплины

Способен обеспечивать безопасную обработку данных в автоматизированных системах (ПК-3).

Способен выполнять работы по проектированию автоматизированных систем в защищенном исполнении (ПК-4).

Разделы дисциплины

Понятие автоматизированной информационной системы (АС). Основные аспекты построения системы информационной безопасности. Мероприятия по защите информации. Требования к архитектуре АС для обеспечения безопасности ее функционирования. Оценочные стандарты и технические спецификации. Критерии оценки безопасности информационных технологий. Руководящие документы ФСТЭК России. Описание информационной системы и особенностей ее функционирования. Перечень потенциальных источников атак и определение их возможностей (модель нарушителя). Определение уровня защищенности данных в АС. Описание угроз безопасности информации (модель угроз безопасности информации). Методы выбора системы защиты информации.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.О. декана факультета
Фундаментальной и прикладной информатики
(наименование ф-та полностью)

_____М.О. Таныгин
(подпись, инициалы, фамилия)

«30» 06 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Проектирование защищенных автоматизированных систем

(наименование дисциплины)

ОПОП ВО 10.03.01 Информационная безопасность
(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий»
наименование направленности (профиля, специализации)

форма обучения очная
(очная, очно-заочная, заочная)

Курск – 2022

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета (протокол № 7 «28» февраля 2022 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий» на заседании кафедры информационной безопасности№11 «30» июня 2022 г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы
к.т.н., доцент _____ Марухленко А.Л.
(ученая степень и ученое звание, Ф.И.О.)

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета протокол №___«__»_____20___г., на заседании кафедры _____ .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета протокол №___«__»_____20___г., на заседании кафедры _____ .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1. Цель преподавания дисциплины

Дисциплина "Проектирование защищенных автоматизированных систем" изучается с целью изучения технологий, методов и средств создания защищенных автоматизированных систем.

1.2. Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

- сформировать профессиональную культуру проектирования защищенных автоматизированных систем;
- понимать принципы построения защищенных автоматизированных систем;
- познакомиться с уязвимостями, угрозами ИБ и видами деструктивного воздействия, характерными для современных автоматизированных систем;
- изучить подходы и методы обеспечения ИБ автоматизированных систем.

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Таблица 1.3 – Результаты обучения по дисциплине

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компции	*наименование компетенции*		
ПК-3	Способен обеспечивать безопасную обработку данных в автоматизированных системах	ПК-3.1 Фиксирует возникновение инцидентов информационной безопасности	***Знать:*** - понятие инцидент; - классификация и параметры инцидентов информационной безопасности; - регламенты, определяющие порядок управления инцидентами информационной безопасности; - принципы управления инцидентами.

			Уметь: - определить тип инцидента; - зарегистрировать инцидент информационной безопасности; ***Владеть (или Иметь опыт деятельности):*** - навыками определения типа инцидента; - навыками управления инцидентами информационной безопасности.
		ПК-3.2 Использует методы и средства резервного копирования информации	***Знать:*** - методы резервного копирования информации; - типы и характеристики носителей хранения данных; - типы и характеристики используемых платформ; - схемы копирования; - базовые функции резервного копирования информации. ***Уметь:*** - определить необходимый тип носителя хранения данных; - использовать оптимальную схему копирования; - применить оптимальный тип резервного копирования. ***Владеть (или Иметь опыт деятельности):*** - навыками выбора необходимой для копирования информации; - навыками организации процесса резервного копирования. ***Знать:***
		ПК-3.3 Устраняет уязвимости в автоматизированной системе	***Знать:*** - понятие уязвимости, классификация уязвимостей в автоматизированной системе; - поисковые признаки; - методы оценки опасности угроз; - методы устранения угроз. ***Уметь:*** - анализировать уязвимости в автоматизированной системе; - выбрать средства для поиска уязвимостей; - устранять уязвимости в автоматизированной системе. ***Владеть (или Иметь опыт деятельности):***

			- навыками анализа уязвимости в автоматизированной системе; - навыками поиска уязвимости; - навыками устранения уязвимости в автоматизированной системе.
		ПК-3.4 Соотносит изменения в конфигурации автоматизированной системы с её защищенностью	***Знать:*** - основные методы управления защитой информации; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - методы защиты информации от "утечки" по техническим каналам; - нормативные правовые акты в области защиты информации ***Уметь:*** - анализировать воздействия изменений конфигурации автоматизированной системы на ее защищенность; - оценивать информационные риски в автоматизированных системах - классифицировать и оценивать угрозы безопасности информации - конфигурировать параметры системы защиты информации автоматизированных систем - применять технические средства контроля эффективности мер защиты информации. ***Владеть (или Иметь опыт деятельности):*** - навыками анализа, оценки информационных рисков в автоматизированных системах; - навыками настройки системы защиты информации.
ПК-4	Способен выполнять работы по проектированию автоматизированных систем в защищенном исполнении	ПК-4.1 Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем	***Знать:*** - методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности; - основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно распорядительных документов;

			- основные нормативные правовые акты в области обеспечения информационной безопасности. ***Уметь:*** - уметь проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности; - уметь разрабатывать технические задания на создание подсистем обеспечения информационной безопасности; - разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации. ***Владеть (или Иметь опыт деятельности):*** - навыками разработки политик безопасности различных уровней; - правилами построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости и сроков реализации; - навыками работы с нормативными правовыми актами в области информационной безопасности.
		ПК-4.2 Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем	***Знать:*** -основные нормативно-правовые акты в области информационной безопасности и защиты информации; - правовые основы организации защиты государственной тайны и конфиденциальной ин- формации; - основные методы организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации. ***Уметь:*** - оформлять техническую и проектную документацию по регламентации вопросов создания и эксплуатации автоматизированных систем; - оформлять техническую документацию в соответствии с действующими нормативными документами. ***Владеть (или Иметь опыт деятельности):***

			- навыками ведения документов учета, обработки, хранения и передачи информации, составляющей профессиональную, коммерческую, служебную или иную тайну.
		ПК-4.3 Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации	***Знать:*** - требования защиты информации; -методы повышения уровня защищенности информационных систем; - стандарты, предназначенные для контроля функциональных характеристик работы системы; ***Уметь:*** - формализовать выборки для формирования сообщений; - составлять простые и составные запросы к системам учета. - проводить анализ основных характеристик системы. ***Владеть (или Иметь опыт деятельности):*** - общими приемами организации поиска; - алгоритмическими схемами оценки характеристик; - навыками анализа ожидаемых и фактических результатов работы системы.
		ПК-4.4 Проводит сравнительный анализ вариантов конфигураций и состава автоматизированных систем	***Знать:*** - основные методы управления защитой информации; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические) - Методы защиты информации в автоматизированных системах - варианты конфигураций и их характеристики. ***Уметь:*** - оценивать информационные риски в автоматизированных системах; - классифицировать и оценивать угрозы безопасности информации; - определять подлежащие защите информационные ресурсы автоматизированных систем;

			-разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; - конфигурировать параметры системы защиты информации автоматизированных систем. ***Владеть (или Иметь опыт деятельности):*** - навыками проведения сравнительного анализа; - навыками проведения различных конфигураций; - навыками разработки предложений по совершенствованию систем защиты информации.
		ПК-4.5 Предлагает конфигурации и состав автоматизированной системы	***Знать*** основные методы исследования характеристик информационных систем. ***Уметь:*** определять методы и средства для проведения предпроектных исследований и теоретически достигаемых характеристик информационных систем ***Владеть (****или* ***Иметь опыт деятельности):*** проведения предпроектных исследований характеристик информационных систем

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Проектирование защищенных автоматизированных систем» входит часть, формируемую участниками образовательных отношений блока 1 «Дисциплины (модули»)) основной профессиональной образовательной программы – программы магистратуры 10.03.01 Информационная безопасность профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий». Дисциплина изучается на 4 курсе в 8 семестре.

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

Общая трудоёмкость (объём) дисциплины составляет 4 зачётные единицы, 144 часа

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	144
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	72
в том числе:	
лекции	36
лабораторные занятия	36
практические занятия	-
Самостоятельная работа обучающихся (всего)	43.85
Контроль (подготовка к экзамену)	27
Контактная работа по промежуточной аттестации (всего АттКР)	1,15
в том числе:	
зачет	не предусмотрен
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	1,15

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

4.1. Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Понятие автоматизированной системы (АС)	Понятие автоматизированной информационной системы и ее основные компоненты. Виды АС. Особенности различных архитектур АС. Уровни организации архитектур АС. Особенности распределённых АС
2.	Основные аспекты построения системы информационной безопасности	Регулирование ответственности нарушений информационной безопасности. Программа информационной безопасности. Контроль деятельности в области безопасности. Модели представления информационной защиты. Формирование требований к системе информационной безопасности. Этапы обеспечения информационной безопасности.
3.	Мероприятия по защите информации.	Нормативно-законодательный аспект. Процедурный аспект. Программно-технический аспект.
4.	Требования к архитектуре АС для обеспечения безопасности ее функционирования.	Структурирование ЗАС. Анализ безопасности АС. Критерии адекватности средств защиты**.** Структура профиля защиты ИТ-продукта. Соотношение эффективности и рентабельно-

		сти систем информационной безопасности. Зависимость эффективности защиты от величины ущерба
5.	Оценочные стандарты и технические спецификации.	"Оранжевая книга" как оценочный стандарт. Стандарты информационной безопасности распределенных систем. Механизмы реализации сервисов (функций) безопасности. Администрирование средств безопасности
6.	Критерии оценки безопасности информационных технологий.	Основные понятия. Стандарт "Критерии оценки безопасности информационных технологий". Иерархия класс-семейство-компонент-элемент. Требования доверия безопасности.
7.	Руководящие документы ФСТЭК России.	Требования к защищенности автоматизированных систем. Классы защищённости информационных систем. Аспекты защищённых АС, фигурирующие в требованиях ФСТЭК. Классификация защищённых информационных ситсем
8.	Описание информационной системы и особенностей ее функционирования	Структура и состав информационной системы. Описание физических, функциональных, технологических и логических взаимосвязей
9.	Перечень потенциальных источников атак и определение их возможностей (модель нарушителя	Категория лиц, рассматриваемых и не рассматриваемых в качестве нарушителей. Обобщенные возможности нарушителя. Уточненные возможности нарушителя. Актуальность использования (применения) возможностей нарушителя для построения и реализации атак. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности данных
10.	Определение уровня защищенности данных в АС	Определение типа угроз безопасности информации. Определение категории обрабатываемых данных. Определение количества субъектов данных. Определение уровня защищенности данных. Определение класса АС. Оценка степени возможного ущерба. Определение класса защищенности АС.
11.	Описание угроз безопасности информации (модель угроз безопасности информации)	Определение перечня угроз безопасности информации, возможных с учетом потенциала нарушителя. Определение перечня угроз безопасности информации, возможных с учетом применяемых технологий. Определение исходной защищенности информационной системы. Определение частоты (вероятности) реализации угроз. Определение объема негативных последствий. Способы реализации угроз безопасности информации. Возможные уязвимости информационной системы.
12.	Методы выбора системы защиты информации	Классификация методов выбора систем защиты информации. Метод анализа иерархий. Метод парных сравнений альтернатив. Многокритериальный выбор в иерархических структурах с множеством различных альтернатив под критериями. Методы принятия решений, основанные на исследовании операций. Сопоставление угроз и методов и средств их устранения. Игровые стратегии выбора системы защиты информации

Таблица 4.1.2 – Содержание дисциплины и её методическое обеспечение

№ Пп /п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лб.	№ пр.			
1	2	3	4	5	6	7	8
1.	Понятие автоматизированной информационной системы (АС)	3			У-1-5 МУ 1-4	С 1-2 недели	ПК-3, ПК-4
2.	Основные аспекты построения системы информационной безопасности	3	1		У-1-5 МУ 1-4	С, ЗЛР 2-3 недели	ПК-3, ПК-4
3.	Мероприятия по защите информации.	3	2		У-1-5 МУ 1-4	С, ЗЛР 4-5 недели	ПК-3, ПК-4
4.	Требования к архитектуре АС для обеспечения безопасности ее функционирования.	3	3		У-1-5 МУ 1-4	С, ЗЛР 5-6 недели	ПК-3, ПК-4
5.	Оценочные стандарты и технические спецификации.	3			У-1-5 МУ 1-4	С, 7-8 недели	ПК-3, ПК-4
6.	Критерии оценки безопасности информационных технологий.	3			У-1-5 МУ 1-4	С, 8-9 недели	ПК-3, ПК-4
7.	Руководящие документы ФСТЭК России.	3	4		У-1-5 МУ 1-4	С, ЗЛР 10-11 недели	ПК-3, ПК-4
8.	Описание информационной системы и особенностей ее функционирования	3			У-1-5 МУ 1-4	С, 11-12 недели	ПК-3, ПК-4
9.	Перечень потенциальных источников атак и определение их возможностей (модель нарушителя	3	5		У-1-5 МУ 1-4	С, ЗЛР 13-14 недели	ПК-3, ПК-4
10.	Определение уровня защищенности данных в АС	3	6		У-1-5 МУ 1-4	С, ЗЛР 14-15 недели	ПК-3, ПК-4
11.	Описание угроз безопасности информации (модель угроз безопасности информации)	3			У-1-5 МУ 1-4	С, 16-17 недели	ПК-3, ПК-4
12.	Методы выбора системы защиты информации	3			У-1-5 МУ 1-4	С, 17-18 недели	ПК-3, ПК-4
	Итого	36					

С – собеседование, ЗЛР – защита лабораторной работы

4.2. Лабораторные работы и практические занятия

4.2.1. Лабораторные работы

Таблица 4.2.1 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1.	Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение	6
2.	Определение показателей защищенности информации при несанкционированном доступе	6
3.	Критерии оценки и выбора CASE-средств.	6
4.	Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности.	6
5.	Создание модели вероятного нарушителя	6
6.	Оценка защищённости информационной системы на основании методики ФСТЭК	6
Итого		36

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Понятие автоматизированной информационной системы (АС)	1-2 недели	3
2.	Основные аспекты построения системы информационной безопасности	2-3 недели	3
3.	Мероприятия по защите информации.	4-5 недели	3
4.	Требования к архитектуре АС для обеспечения безопасности ее функционирования.	5-6 недели	3
5.	Оценочные стандарты и технические спецификации.	7-8 недели	4
6.	Критерии оценки безопасности информационных технологий.	8-9 недели	4
7.	Руководящие документы ФСТЭК России.	10-11 недели	4
8.	Описание информационной системы и особенностей ее функционирования	11-12 недели	4
9.	Перечень потенциальных источников атак и определение их возможностей (модель нарушителя	13-14 недели	4
10.	Определение уровня защищенности данных в АС	14-15 недели	4,85
11.	Описание угроз безопасности информации (модель угроз безопасности информации)	16-17 недели	4
12.	Методы выбора системы защиты информации	17-18 недели	4
Итого			43,85

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

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;
- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно- методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;
- путем разработки вопросов к экзамену, методических указаний к выполнению лабораторных работ.

типографией университета:

- путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;
- путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

6. Образовательные технологии

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования профессиональных компетенций обучающихся. В рамках дисциплины не предусмотрено использование интерактивных технологий.

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит зна-

чимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических и (или) лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций)*;*

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

7. Фонд оценочных средств для проведения промежуточной аттестации

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-3 Способен обеспечивать безопасную обработку данных в автоматизированных системах	Проектирование защищенных автоматизированных систем Производственная технологическая практика		
ПК-4 Способен выполнять работы по проектированию автоматизированных систем в защищенном исполнении	Проектирование защищенных автоматизированных систем Производственная технологическая практика		

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
ПК-3/ завершающий	ПК-3.1 Фиксирует возникновение инцидентов информационной безопасности;	***Знать:*** - понятие инцидент; - классификация и параметры инцидентов информационной безопасности; ***Уметь:*** - определить тип инцидента; ***Владеть (или Иметь опыт деятельности):*** - навыками определения типа инцидента;	***Знать:*** - понятие инцидент; - классификация и параметры инцидентов информационной безопасности; - регламенты, определяющие порядок управления инцидентами информационной безопасности; ***Уметь:*** - определить тип инцидента; ***Владеть (или Иметь опыт деятельности):*** - навыками определения типа инцидента;	***Знать:*** - понятие инцидент; - классификация и параметры инцидентов информационной безопасности; - регламенты, определяющие порядок управления инцидентами информационной безопасности; - принципы управления инцидентами. ***Уметь:*** - определить тип инцидента; - зарегистрировать инцидент информационной безопасности; ***Владеть (или Иметь опыт деятельности):*** - навыками определения типа инцидента; - навыками управления инцидентами информационной безопасности.
	ПК-3.2 Использует методы и средства резервного копирования информации	***Знать:*** - методы резервного копирования информации; - типы и характеристики носителей хранения данных; ***Уметь:***	***Знать:*** - методы резервного копирования информации; - типы и характеристики носителей хранения данных;	***Знать:*** - методы резервного копирования информации; - типы и характеристики носителей хранения данных;

		- определить необходимый тип носителя хранения данных; ***Владеть (или Иметь опыт деятельности):*** - навыками выбора необходимой для копирования информации;	- типы и характеристики используемых платформ; - схемы копирования; ***Уметь:*** - определить необходимый тип носителя хранения данных; - использовать оптимальную схему копирования; ***Владеть (или Иметь опыт деятельности):*** - навыками выбора необходимой для копирования информации;	- типы и характеристики используемых платформ; - схемы копирования; - базовые функции резервного копирования информации. ***Уметь:*** - определить необходимый тип носителя хранения данных; - использовать оптимальную схему копирования; - применить оптимальный тип резервного копирования. ***Владеть (или Иметь опыт деятельности):*** - навыками выбора необходимой для копирования информации; - навыками организации процесса резервного копирования.
	ПК-3.3 Устраняет уязвимости в автоматизированной системе	***Знать:*** - понятие уязвимости, классификация уязвимостей в автоматизированной системе; - поисковые признаки; ***Уметь:*** - анализировать уязвимости в автоматизированной системе; ***Владеть (или Иметь опыт деятельности):*** - навыками анализа уязвимости в автоматизированной системе;	***Знать:*** - понятие уязвимости, классификация уязвимостей в автоматизированной системе; - поисковые признаки; - методы оценки опасности угроз; ***Уметь:*** - анализировать уязвимости в автоматизированной системе; - выбрать средства для поиска уязвимостей; ***Владеть (или Иметь опыт деятельности):*** - навыками анализа уязвимости в автоматизированной системе; - навыками поиска уязвимости;	***Знать:*** - понятие уязвимости, классификация уязвимостей в автоматизированной системе; - поисковые признаки; - методы оценки опасности угроз; - методы устранения угроз. ***Уметь:*** - анализировать уязвимости в автоматизированной системе; - выбрать средства для поиска уязвимостей; - устранять уязвимости в автоматизированной системе. ***Владеть (или Иметь опыт деятельности):*** - навыками анализа уязвимости в автоматизированной системе; - навыками поиска уязвимости; - навыками устранения уязвимости в автоматизированной системе.
	ПК-3.4	***Знать:*** - основные методы	***Знать:*** - основные методы	***Знать:*** - основные методы

	Соотносит изменения в конфигурации автоматизированной системы с её защищенностью	управления защитой информации; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; ***Уметь:*** - анализировать воздействия изменений конфигурации автоматизированной системы на ее защищенность; - оценивать информационные риски в автоматизированных системах ***Владеть (или Иметь опыт деятельности):*** - навыками анализа, оценки информационных рисков в автоматизированных системах;	управления защитой информации; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - методы защиты информации от "утечки" по техническим каналам; ***Уметь:*** - анализировать воздействия изменений конфигурации автоматизированной системы на ее защищенность; - оценивать информационные риски в автоматизированных системах - классифицировать и оценивать угрозы безопасности информации ***Владеть (или Иметь опыт деятельности):*** - навыками анализа, оценки информационных рисков в автоматизированных системах;	управления защитой информации; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - методы защиты информации от "утечки" по техническим каналам; - нормативные правовые акты в области защиты информации ***Уметь:*** - анализировать воздействия изменений конфигурации автоматизированной системы на ее защищенность; - оценивать информационные риски в автоматизированных системах - классифицировать и оценивать угрозы безопасности информации - конфигурировать параметры системы защиты информации автоматизированных систем - применять технические средства контроля эффективности мер защиты информации. ***Владеть (или Иметь опыт деятельности):*** - навыками анализа, оценки информационных рисков в автоматизированных системах; - навыками настройки системы защиты информации.
ПК-4 / завершающий	ПК-4.1 Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных	***Знать:*** - методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и	***Знать:*** - методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и	***Знать:*** - методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности;

	систем	оценки надёжности; - основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно распорядительных документов; ***Уметь:*** - уметь проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности; ***Владеть (или Иметь опыт деятельности):*** - навыками разработки политик безопасности различных уровней;	оценки надёжности; - основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно распорядительных документов; ***Уметь:*** - уметь проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности; - уметь разрабатывать технические задания на создание подсистем обеспечения информационной безопасности; ***Владеть (или Иметь опыт деятельности):*** - навыками разработки политик безопасности различных уровней; - правилами построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости и сроков реализации;	- основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно распорядительных документов; - основные нормативные правовые акты в области обеспечения информационной безопасности. ***Уметь:*** - уметь проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности; - уметь разрабатывать технические задания на создание подсистем обеспечения информационной безопасности; - разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации. ***Владеть (или Иметь опыт деятельности):*** - навыками разработки политик безопасности различных уровней; - правилами построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости и сроков реализации; - навыками работы с нормативными правовыми актами в области информационной безопасности.

	ПК-4.2 Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем	***Знать:*** -основные нормативно-правовые акты в области информационной безопасности и защиты информации; ***Уметь:*** - оформлять техническую и проектную документацию по регламентации вопросов создания и эксплуатации автоматизированных систем; ***Владеть (или Иметь опыт деятельности):*** - навыками ведения документов учета, обработки, хранения и передачи информации, составляющей профессиональную, коммерческую, служебную или иную тайну.	***Знать:*** -основные нормативно-правовые акты в области информационной безопасности и защиты информации; - правовые основы организации защиты государственной тайны и конфиденциальной информации; ***Уметь:*** - оформлять техническую и проектную документацию по регламентации вопросов создания и эксплуатации автоматизированных систем; ***Владеть (или Иметь опыт деятельности):*** - навыками ведения документов учета, обработки, хранения и передачи информации, составляющей профессиональную, коммерческую, служебную или иную тайну.	***Знать:*** -основные нормативно-правовые акты в области информационной безопасности и защиты информации; - правовые основы организации защиты государственной тайны и конфиденциальной информации; - основные методы организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации. ***Уметь:*** - оформлять техническую и проектную документацию по регламентации вопросов создания и эксплуатации автоматизированных систем; - оформлять техническую документацию в соответствии с действующими нормативными документами. ***Владеть (или Иметь опыт деятельности):*** - навыками ведения документов учета, обработки, хранения и передачи информации, составляющей профессиональную, коммерческую, служебную или иную тайну.
	ПК-4.3 Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации	***Знать:*** - требования защиты информации; -методы повышения уровня защищенности информационных систем; - стандарты, предназначенные для контроля функциональных характеристик работы системы; ***Уметь:***	***Знать:*** - требования защиты информации; -методы повышения уровня защищенности информационных систем; - стандарты, предназначенные для контроля функциональных характеристик работы системы; ***Уметь:***	***Знать:*** - требования защиты информации; -методы повышения уровня защищенности информационных систем; - стандарты, предназначенные для контроля функциональных характеристик работы системы; ***Уметь:***

		- формализовать выборки для формирования сообщений; ***Владеть (или Иметь опыт деятельности):*** - общими приемами организации поиска;	- формализовать выборки для формирования сообщений; - составлять простые и составные запросы к системам учета. ***Владеть (или Иметь опыт деятельности):*** - общими приемами организации поиска; - алгоритмическими схемами оценки характеристик;	- формализовать выборки для формирования сообщений; - составлять простые и составные запросы к системам учета. - проводить анализ основных характеристик системы. ***Владеть (или Иметь опыт деятельности):*** - общими приемами организации поиска; - алгоритмическими схемами оценки характеристик; - навыками анализа ожидаемых и фактических результатов работы системы.
	ПК-4.4 Проводит сравнительный анализ вариантов конфигураций и состава автоматизированных систем	***Знать:*** - основные методы управления защитой информации; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические) ***Уметь:*** - оценивать информационные риски в автоматизированных системах; - классифицировать и оценивать угрозы безопасности информации; - определять подлежащие защите информационные ресурсы автоматизированных систем; ***Владеть (или Иметь опыт деятельности):***	***Знать:*** - основные методы управления защитой информации; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические) - Методы защиты информации в автоматизированных системах ***Уметь:*** - оценивать информационные риски в автоматизированных системах; - классифицировать и оценивать угрозы безопасности информации; - определять подлежащие защите информационные ре-	***Знать:*** - основные методы управления защитой информации; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические) - Методы защиты информации в автоматизированных системах - варианты конфигураций и их характеристики. ***Уметь:*** - оценивать информационные риски в автоматизированных системах; - классифицировать и оценивать угрозы безопасности информации; - определять подлежащие защите информационные ресурсы авто-

		- навыками проведения сравнительного анализа; - навыками проведения различных конфигураций;	сурсы автоматизированных систем; -разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; ***Владеть (или Иметь опыт деятельности):*** - навыками проведения сравнительного анализа; - навыками проведения различных конфигураций;	матизированных систем; -разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; - конфигурировать параметры системы защиты информации автоматизированных систем. ***Владеть (или Иметь опыт деятельности):*** - навыками проведения сравнительного анализа; - навыками проведения различных конфигураций; - навыками разработки предложений по совершенствованию систем защиты информации.
	ПК-4.5 Предлагает конфигурации и состав автоматизированной системы	***Знать:*** - основные методы исследования характеристик информационных систем; - основные методы построения информационных систем; ***Уметь:*** - определять методы и средства для проведения предпроектных исследований и теоретически достигаемых характеристик информационных систем; ***Владеть (или Иметь опыт деятельности):*** - проведения предпроектных исследований характеристик информационных систем	***Знать:*** - основные методы исследования характеристик информационных систем; - основные методы построения информационных систем; ***Уметь:*** - определять методы и средства для проведения предпроектных исследований и теоретически достигаемых характеристик информационных систем; - проводить анализ основных характеристик системы. ***Владеть (или Иметь опыт деятельности):*** - проведения предпроектных исследований характеристик информационных систем - навыками проведения различных	***Знать:*** - основные методы исследования характеристик информационных систем; - основные методы построения информационных систем; - основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические) ***Уметь:*** - определять методы и средства для проведения предпроектных исследований и теоретически достигаемых характеристик информационных систем; - проводить анализ основных характеристик системы. - оформлять техническую и проектную документацию по регла-

			конфигураций;	ментации вопросов создания и эксплуатации автоматизированных систем; ***Владеть (или Иметь опыт деятельности):*** - проведения предпроектных исследований характеристик информационных систем - навыками проведения различных конфигураций; - навыками разработки политик безопасности различных уровней;

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля успеваемости

/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или ее части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№ заданий	
	2	3	4	5	6	7
1.	Понятие автоматизированной информационной системы (АС)	ПК-3, ПК-4	Лекция, СРС	ВС	1-5	Согласно табл. 7.2
2.	Основные аспекты построения системы информационной безопасности	ПК-3, ПК-4	Лекция, СРС, лабораторная работа	ВС, КВЗЛР	1-5 1-5	Согласно табл. 7.2
3.	Мероприятия по защите информации.	ПК-3, ПК-4	Лекция, СРС, лабораторная работа	ВС КВЗЛР	1-5	Согласно табл. 7.2
4.	Требования к архитектуре АС для обеспечения безопасности ее функционирования.	ПК-3, ПК-4	Лекция, СРС, лабораторная работа	ВС КВЗЛР	1-5	Согласно табл. 7.2
5.	Оценочные стандарты и технические спецификации.	ПК-3, ПК-4	Лекция, СРС,	ВС	1-5	Согласно табл. 7.2

6.	Критерии оценки безопасности информационных технологий.	ПК-3, ПК-4	Лекция, СРС,	ВС	1-5	Согласно табл. 7.2
7.	Руководящие документы ФСТЭК России.	ПК-3, ПК-4	Лекция, СРС,	ВС	1-5	Согласно табл. 7.2
8.	Описание информационной системы и особенностей ее функционирования	ПК-3, ПК-4	Лекция, СРС, лабораторная работа	ВС, КВЗЛР	1-5	Согласно табл. 7.2
9.	Перечень потенциальных источников атак и определение их возможностей (модель нарушителя)	ПК-3, ПК-4	Лекция, СРС, лабораторная работа	ВС КВЗЛР	1-5	Согласно табл. 7.2
10.	Определение уровня защищенности данных в АС	ПК-3, ПК-4	Лекция, СРС, лабораторная работа	ВС КВЗЛР	1-5	Согласно табл. 7.2
11.	Описание угроз безопасности информации (модель угроз безопасности информации)	ПК-3, ПК-4	Лекция, СРС	ВС	1-5	Согласно табл. 7.2
12.	Методы выбора системы защиты информации	ПК-3, ПК-4	Лекция, СРС	ВС	1-5	Согласно табл. 7.2

ВС- вопросы для собеседования

КВЗЛР- контрольные вопросы для защиты лабораторной работы

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для собеседования по теме 2: «Основные аспекты построения системы информационной безопасности».

1. Чем регулируется ответственность нарушений информационной безопасности во внешней среде?
2. Что такое программа информационной безопасности?
3. Опишите структуру модели информационной безопасности.
4. Какие параметры СЗИ можно оценить с помощью системы количественных метрик?
5. Какие существуют модели и алгоритмы классификации СЗИ?
6. Опишите требований к системе информационной безопасности.
7. Назовите этапы обеспечения информационной безопасности.

Контрольные вопросы для защиты лабораторной работы №4 «Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности»

1. Для чего служит Доктрина информационной безопасности?
2. Что выступает в качестве средств защиты информации, подлежащих сертификации в Системе сертификации средств защиты информации по требованиям безопасности информации?
3. Основные схемы сертификации средств защиты информации.
4. Какие функции осуществляет ФСТЭК России в пределах своей компетенции?

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме экзамена. Экзамен проводится в виде компьютерного тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки (или опыт деятельности) и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов.

Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения
промежуточной аттестации обучающихся

Задание в закрытой форме:

Для чего производится предварительное обследование объекта автоматизации?

1) для формирования концепции создания системы
2) для создания прототипа системы
3) для выяснения готовности предприятия к автоматизации
4) для формирования команды, которая будет работать над созданием системы

Задание в открытой форме:

1. Автоматизированная система-это…
2. Автоматизированные системы можно классифицировать по признакам…
3. Подсистема-это…

Задание на установление правильной последовательности,

Установить порядок проведения аттестации АС по требованиям безопасности

1. Проведение аттестационных испытаний объекта
2. Предварительное ознакомление с аттестуемым объектом (при необходимости)
3. Оформление, регистрация и выдача аттестата соответствия
4. Подача и рассмотрение заявки на аттестацию
5. Разработка программы и методики аттестационных испытаний

Задание на установление соответствия:

Для автоматизированной информационной системы в составе нескольких защищаемых помещений с числом субъектов ПДн более 100 установите соответствие:

a. Угроза скрытной регистрации вредоносной программой учетных записей администраторов внешний нарушитель с потенциалом не ниже усиленного базового.

b. Угроза хищения аутентификационной информации из временных файлов cookie внешний нарушитель с потенциалом не ниже усиленного базового;

c. Угроза изменения системных и глобальных переменных внутренний нарушитель с потенциалом не ниже усиленного базового;

1 Опасность угрозы низкая
2 Опасность угрозы средняя
3 Опасность угрозы высокая

Компетентностно-ориентированная задача:

Для некоторой системы характерно наличие проводного канала связи (витой пары), соединяющей компьютеры, находящиеся в аттестованных помещениях. Витая пара проходит через неаттестованное помещение. Предложите перечень мероприятий, направленных на сохранения класса защиты данной автоматизированной информационной системы.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

− положение П 02.016 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;

− методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Выполнение лабораторной работы №1 «Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Выполнение лабораторной работы №2 «Определение показателей защищенности информации при несанкционированном доступе»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Выполнение лабораторной работы №3 «Критерии оценки и	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%

выбора CASE-средств»				
Выполнение лабораторной работы №4 «Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Выполнение лабораторной работы №5 «Создание модели вероятного нарушителя»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Выполнение лабораторной работы №6 «Оценка защищённости информационной системы на основании методики ФСТЭК»	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Собеседование по темам 1-2	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Собеседование по темам 3-4	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Собеседование по темам 5-6	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Собеседование по темам 7-8	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Собеседование по темам 9-10	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Собеседование по темам 11-12	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
ИТОГО	24		48	
Посещаемость	0		16	
Экзамен	0		36	
ИТОГО	24		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме –2балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование –36 баллов.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1) Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин :Директ-Медиа, 2021. – 210 с. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

2) Марухленко, А. Л. Разработка защищённых интерфейсов Web-приложений : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов. – Москва ; Берлин : Директ-Медиа, 2021. – 175 с. – URL: https://biblioclub.ru/index.php?page=book&id=599050 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

8.2 Дополнительная учебная литература

3) Кобылянский, В. Г. Операционные системы, среды и оболочки : учебное пособие / В. Г. Кобылянский ; Новосибирский государственный технический университет. - Новосибирск : Новосибирский государственный технический университет, 2018. - 80 с. - URL: http://biblioclub.ru/index.php?page=book&id=576354 (дата обращения: 16.02.2023) . - Режим доступа: по подписке. – Текст: электронный.

4) Основы администрирования информационных систем : учебное пособие / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко и др. – Москва ; Берлин : Директ-Медиа, 2021. – 201 с. – URL: https://biblioclub.ru/index.php?page=book&id=598955 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

5) Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

8.3 Перечень методических указаний

1) Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение [Электронный ресурс] : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Электрон. текстовые дан. (541 КБ). - Курск : ЮЗГУ, 2017. - 16 с. : ил., табл. - Библиогр.: с. 16. - Б. ц.

2) Определение показателей защищенности информации при несанкционированном доступе [Электронный ресурс] : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Электрон. текстовые дан. (342 КБ). - Курск : ЮЗГУ, 2017. - 7 с. : ил., табл. - Библиогр.: с. 7. - Б. ц.

3) Критерии оценки и выбора CASE-Средств : методические указания для выполнения лабораторных и практических работ студентами групп специальностей 02.03.03, 09.00.00, 10.00.00, 11.00.00, 12.03.04, 38.05.01, 45.03.03 / Юго-Зап. гос. ун-т ; сост. О. А. Демченко. - Электрон. текстовые дан. (298 КБ). - Курск : ЮЗГУ, 2022. - 11 с. - Загл. с титул. экрана. - Б. ц.

4) Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности [Электронный ресурс] : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Электрон. текстовые дан. (324 КБ). - Курск : ЮЗГУ, 2017. - 7 с. : ил., табл. - Библиогр.: с. 7. - Б. ц.

9. Перечень ресурсов информационно-телекоммуникационной сети Интернет

1) Облачный сервис математических вычислений SMath Studio in the Cloud [официальный сайт]. Режим доступа: https://ru.smath.com/cloud/

2) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru

3) Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/

4) Общероссийский портал Math-Net.Ru [официальный сайт]. Режим доступа: http://www.mathnet.ru/

5) База данных "Патенты России"

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Проектирование защищенных автоматизированных систем» являются лекции и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают

лабораторные и практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным и практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Проектирование защищенных автоматизированных систем»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Проектирование защищенных автоматизированных систем» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Проектирование защищенных автоматизированных систем» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,Windows 7, договор IT000012385, открытая среда разработки программного обеспечения Lazarus (Свободное ПО http://www.lazarus.freepascal.org/)

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

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10 шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноутбукASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/ проектор inFocusIN24+

13. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной

форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	Изменённых	Заменённых	Аннулированных	новых			