Аннотация к рабочей программе дисциплины «Контроль защищённости информационно-телекоммуникационных систем»

Цель преподавания дисциплины

Дисциплина «Контроль защищённости информационно-телекоммуникационных систем» изучается с целью формирования у студентов знаний в области контроля защищённости информационно-телекоммуникационных систем.

Задачи изучения дисциплины

– сформировать профессиональные навыки проведения оценки состояния защищенности информационно-телекоммуникационных систем (ИТС);

– понимать принципы построения защищенных ИТС;

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

– изучить подходы и методы обеспечения безопасности (ИБ) ИТС, а также анализировать риски ИБ.

Компетенции, формируемые в результате освоения дисциплины

Способен эксплуатировать средства обеспечения информационной безопасности для реализации политик безопасности (ПК-10).

Разделы дисциплины

1 Нормативная база оценки защищенности ИТ
2 Основные аспекты построения системы информационной безопасности
3 Базовые вопросы проверки защищенности ИТ
4 Виды проверок
5 Внутренний аудит ИБ
6 Внешний аудит ИБ
7 Системы анализа защищенности
8 Системы обнаружения и предотвращения вторжений

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

Контроль защищённости информационно-телекоммуникационных систем
(наименованиедисциплины)

ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем
(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Управление безопасностью телекоммуникационных систем и сетей
наименование направленности (профиля, специализации)

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

Курск – 2022

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – специалитетпо направлению подготовки (специальности) 10.05.02 Информационная безопасность телекоммуникационных систем на основании учебного плана ОПОП ВО10.05.02 Информационная безопасность телекоммуникационных систем, специализация Управление безопасностью телекоммуникационных систем и сетей, 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 10.05.02 Информационная безопасность телекоммуникационных систем, специализация Управление безопасностью телекоммуникационных систем и сетей на заседании кафедры информационной безопасности Протокол № 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 обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация Управление безопасностью телекоммуникационных систем и сетей на заседании кафедры информационной безопасности Протокол №_ «__»____ 20_ г., на заседании кафедры_____.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация Управление безопасностью телекоммуникационных систем и сетей на заседании кафедры информационной безопасности 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 "Контроль защищённости информационно-телекоммуникационных систем" преподается с целью обучения студентов основным способам, методам, принципам, технологиям и средствам оценки защищенности информационных систем с применением актуальных инструментальных средств с учетом требований нормативно-правовой базы Российской Федерации.

1.2. Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

– сформировать профессиональные навыки проведения оценки состояния защищенности информационно-телекоммуникационных систем (ИТС);

– понимать принципы построения защищенных ИТС;

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

– изучить подходы и методы обеспечения безопасности (ИБ) ИТС, а также анализировать риски ИБ.

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 комп	*наименование компетенции*		
ПК-10	Способен эксплуатировать средства обеспечения информационной безопасности для реализации политик безопасности	ПК-10.1 Проверяет корректность работы программных компонент телекоммуникационной системы	Знать: технические характеристики современных информационно-телекоммуникационных систем и их защиты; Уметь: определять показатели технического уровня информационно-телекоммуникационных систем; Владеть: навыками управления работой информационно-телекоммуникационными системами.
		ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты	Знать: математические модели информационно-телекоммуникационных систем и процессов их функционирования и защиты; Уметь: использовать инновационные решения и технологии при проектировании ИТС; Владеть: навыками сбора, анализа, обработки и систематизации технической работы информационно-телекоммуникационных систем.
		ПК-10.3 Формирует систематизированные политики информационной безопасности	Знать: содержание основных патентных исследований в области создания ИТС и их защиты; Уметь: использовать инновационные решения и технологии при проектировании ИТС; Владеть: навыками разработки методических и нормативных документов, регламентирующих работы по проектированию ТКС и их защиты.
		ПК-10.4 Разрабатывает профили заданий по безопасности для оборудования телекоммуникационных систем в защищённом исполнении	Знать: математические модели информационно-телекоммуникационных систем и процессов их функционирования и защиты; Уметь: готовить задания на разработку проектных решений; создавать компьютерные программы с использованием как стандартных пакетов автоматизированного проектирования, так и разрабатываемых самостоятельно; Владеть: навыками составления описаний принципов действия и структуры проектируемых систем и средств ИТС и их защиты

2. Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Контроль защищённости информационно-телекоммуникационных систем» входит в часть, формируемую участниками образовательных отношений блока 1 «Дисциплины (модули)») основной профессиональной образовательной программы – программы магистратуры 10.05.02 Информационная безопасность телекоммуникационных систем, специализация Управление безопасностью телекоммуникационных систем и сетей. Дисциплина изучается на 5 курсе в 10 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 5 зачётные единицы, 180 часов

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	180
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	84
в том числе:	
лекции	42
лабораторные занятия	42
практические занятия	
Самостоятельная работа обучающихся (всего)	67,85
Контроль (подготовка к экзамену)	
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.	Нормативная база оценки защищенности ИТ	Существующие стандарты и методологии проверки и оценки защищенности ИТ и СУИБ: их отличия, сильные и слабые стороны. История развития
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.	Базовые вопросы проверки защищенности ИТ	Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Основные процессы. Понятие процессного подхода. Цели и задачи процессов оценки защищенности ИТ и СУИБ. Важность процесса с точки зрения управления ИБ. Участники процесса. Связи с другими процессами СУИБ.
4.	Виды проверок	Мониторинг ИБ. Самооценка ИБ. Внутренний и внешний аудиты ИБ. Анализ СУИБ со стороны высшего руководства организации.
5.	Внутренний аудит ИБ	Цели и задачи, организационные принципы, принципы обеспечения эффективности. Подразделение внутреннего аудита, контролирующее вопросы ОИБ в организации.
6.	Внешний аудит ИБ	Цели и задачи, принципы проведения, управление программой, этапы проведения. Компетентность аудиторов. Взаимоотношения представителей аудиторской группы и проверяемых организаций.
7.	Системы анализа защищенности	Виды систем, решаемые задачи, использование в целях оценки защищенности ИТ.
8.	Системы обнаружения и предотвращения вторжений	Виды систем, решаемые задачи, использование в целях оценки защищенности ИТ.

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.	Нормативная база оценки защищенности ИТ	5			У-1-5 МУ-1	С	ПК-10
2.	Основные аспекты построения системы информационной безопасности	5	1		У-1-5 МУ-1-5	С, ЗЛР	ПК-10
3.	Базовые вопросы проверки защищенности ИТ	5	2		У-1-5 МУ-1-5	С, ЗЛР	ПК-10
4.	Виды проверок	5	3		У-1-5 МУ-1-5	С, ЗЛР	ПК-10
5.	Внутренний аудит ИБ	5			У-1-5 МУ-1-5	С	ПК-10
6.	Внешний аудит ИБ	5			У-1-5 МУ-1-5	С	ПК-10
7.	Системы анализа защищенности	5	4		У-1-5 МУ-1-5	С, ЗЛР	ПК-10
8.	Системы обнаружения и предотвращения вторжений	7	5		У-1-5 МУ-1-5	С, ЗЛР	ПК-10
9.	Итого	42					

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.	Разработка регламента защищенности к проектируемым информационным системам	8
2.	Контроль защищенности информационных систем	8
3.	Анализ типовых уязвимостей распределенных информационных систем	8
4.	Сетевые и узловые системы анализа защищенности;	8
5.	Сетевые и узловые системы обнаружения и предотвращений вторжений.	10
Итого		42

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок	Время на выполнение СРС, час.
1.	Нормативная база оценки защищенности ИТ	1-2 недели	8
2.	Основные аспекты построения системы информационной безопасности	2-3 недели	8
3.	Базовые вопросы проверки защищенности ИТ	4-5 недели	8

4.	Виды проверок	5-6 недели	8
5.	Внутренний аудит ИБ	7-10 недели	8
6.	Внешний аудит ИБ	11-14 недели	9
7.	Системы анализа защищенности	13-15 недели	9.85
8.	Системы обнаружения и предотвращения вторжений	16-18 недели	9
Итого			67.85

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 предусмотрены встречи с экспертами и специалистами Комитета цифрового развития и связи Курской области.

Таблица 6.1 - Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем в часах
1	2	3	4
1	Лабораторная работа №1. Разработка регламента защищенности к проектируемым информационным системам	Анализ конкретных ситуаций	1
2	Лабораторная работа №2 Контроль защищенности информационных систем	Анализ конкретных ситуаций	1
3	Лабораторная работа №3. Анализ типовых уязвимостей распределенных информационных систем	Анализ конкретных ситуаций	2
4	Лабораторная работа №4. Сетевые и узловые системы анализа защищенности	Анализ конкретных ситуаций	2
5	Лабораторная работа №5. Сетевые и узловые системы обнаружения и предотвращений вторжений	Анализ конкретных ситуаций	2
Итого			8

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 значимый 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-10 Способен эксплуатировать средства обеспечения информационной безопасности для реализации политик	Инфокоммуникационные системы навигации и диспетчеризации и их защита Безопасность средств		Производственная преддипломная практика Информационная

безопасности	мониторинга территорий и объектов	безопасность телекоммуникационных систем Контроль защищённости информа

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-10 / завершающий	ПК-10.1 Проверяет корректность работы программных компонент телекоммуникационной системы	**Знать:** - правила и особенности обращения с информационно-телекоммуникационными системами; **Уметь:** - определять показатели технического уровня информационно-телекоммуникационных систем; **Владеть** *(или* ***Иметь опыт деятельности)*****:** - навыками управления работой информационно-телекоммуникационными системами.	**Знать:** - правила и особенности обращения с информационно-телекоммуникационными системами; - методы защиты информационно-телекоммуникационных систем; **Уметь:** - определять показатели технического уровня информационно-телекоммуникационных систем; - выполнять комплекс мер по обеспечению функционирования информационно-телекоммуникационных систем; **Владеть** *(или* ***Иметь опыт деятельности)*****:** - навыками управления работой информационно-телекоммуникационными системами. - навыками определения угроз для защищаемой ИТС;	**Знать:** - правила и особенности обращения с информационно-телекоммуникационными системами; - технические характеристики современных информационно-телекоммуникационных систем; - методы защиты информационно-телекоммуникационных систем; **Уметь:** - определять показатели технического уровня информационно-телекоммуникационных систем; - выполнять комплекс мер по обеспечению функционирования информационно-телекоммуникационных систем; - выполнять комплекс мер по обеспечению защиты информационно-телекоммуникационных систем; **Владеть** *(или* ***Иметь опыт деятельности)*****:** - навыками управления

				работой информационно-телекоммуникационным и системами. - навыками определения угроз для защищаемой ИТС; - навыками проведения анализа рисков.
	ПК-10.2 Определяет соответствие текущего функционала системы требованиям профилей защиты	***Знать:*** - основные подходы к оценке качества защищённых ИТС; ***Уметь:*** - определять функциональные характеристики отдельных структурных компонентов ИТС ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа защищённых ИТС и выявления характеристик, как всех систем в целом, так и их отдельных функциональных блоков; - навыками разработки технического облика средств обработки и передачи данных в информационных системах; - навыками разработки методик теоретических и экспериментальных исследований защищённости информационных систем.	***Знать:*** - методики проведения натурных и математических экспериментов характеристики защищённых ИТС; - методологические аспекты для выявления соответствия характеристик защищённых ИТС требованиям, к ним предъявляемым. ***Уметь:*** - определять на основе функционала компонентов защищённых ИТС уровень защищённости системы в целом; - самостоятельно разрабатывать программы и методики проведения натурных и математических исследований средств и систем обеспечения информационной безопасности. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки технического облика средств обработки и передачи данных в информационных системах; - навыками разработки методик теоретических и экспериментальных исследований защищённости информационных систем.	***Знать:*** - методики проведения натурных и математических экспериментов, характеристики защищённых ИТС; - методологические аспекты для выявления соответствия характеристик защищённых ИТС требованиям, к ним предъявляемым. ***Уметь:*** - определять на основе функционала компонентов защищённых ИТС уровень защищённости системы в целом; - самостоятельно разрабатывать программы и методики проведения натурных и математических исследований средств и систем обеспечения информационной безопасности. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа защищённых ИТС и выявления характеристик, как всех систем в целом, так и их отдельных функциональных блоков; - навыками разработки технического облика средств обработки и передачи данных в информационных системах; - навыками разработки методик теоретических и экспериментальных исследований защищённости информационных систем.

	ПК-10.3 Формирует систематизированные политики информационной безопасности	***Знать*** -определение угрозы защищённой ИТС; -классификацию и общий анализ угроз; - стек технологий обеспечения информационной безопасности. ***Уметь:*** - проводить анализ возможных угроз и каналов утечки информации; - проводить анализ, используя ГОСТ и международные стандарты; ***Владеть (или Иметь опыт деятельности):*** - навыками определения угроз для защищаемой ИТС;	***Знать*** -классификацию и общий анализ угроз; -отличие случайных и преднамеренных угроз; - стек технологий обеспечения информационной безопасности. ***Уметь:*** - проводить анализ рисков; - проводить анализ, используя ГОСТ и международные стандарты; ***Владеть (или Иметь опыт деятельности):*** - навыками определения угроз для защищаемой ИТС; - навыками проведения анализа рисков.	***Знать*** -определение угрозы защищённой ИТС; -классификацию и общий анализ угроз; -отличие случайных и преднамеренных угроз; - стек технологий обеспечения информационной безопасности. ***Уметь:*** - проводить анализ возможных угроз и каналов утечки информации; - проводить анализ рисков; - проводить анализ, используя ГОСТ и международные стандарты; ***Владеть (или Иметь опыт деятельности):*** - навыками определения угроз для защищаемой ИТС; - навыками проведения анализа рисков.
	ПК-10.4 Разрабатывает профили заданий по безопасности для оборудования телекоммуникационных систем в защищённом исполнении	***Знать:*** - основные характеристики ИТС; - виды уязвимостей в ИТС. ***Уметь:*** - собирать данные о самой ИТС; - найти потенциальные уязвимости в ИТС. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками сбора данных о самой ИТС; - навыками определения потенциальных угроз;	***Знать:*** - классификацию угроз и критерии оценки каждого вида; - виды уязвимостей в ИТС. ***Уметь:*** - собирать данные о самой ИТС; - формировать критерии каждого вида угрозы в защищаемой системе; - найти потенциальные уязвимости в ИТС. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками определения потенциальных угроз;	***Знать:*** - основные характеристики ИТС; - классификацию угроз и критерии оценки каждого вида; - виды уязвимостей в ИТС. ***Уметь:*** - собирать данные о самой ИТС; - формировать критерии каждого вида угрозы в защищаемой системе; - найти потенциальные уязвимости в ИТС. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками сбора данных о самой ИТС; - навыками определения потенциальных угроз; - навыками выявления потенциальных уязвимостей в ИТС.

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.	Нормативная база оценки защищенности ИТ	ПК-10	Лекция, СРС	Собеседование	1-5	Согласно табл. 7.2
2.	Основные аспекты построения системы информационной безопасности	ПК-10	Лекция, СРС, лабораторная работа	Собеседование КВЗЛР	1-5 1-5	Согласно табл. 7.2
3.	Базовые вопросы проверки защищенности ИТ	ПК-10	Лекция, СРС, лабораторная работа	Собеседование, КВЗЛР	1-5 1-5	Согласно табл. 7.2
4.	Виды проверок	ПК-10	Лекция, СРС, лабораторная работа	Собеседование, КВЗЛР	1-5 1-5	Согласно табл. 7.2
5.	Внутренний аудит ИБ	ПК-10	Лекция, СРС	Собеседование	1-5	Согласно табл. 7.2
6.	Внешний аудит ИБ	ПК-10	Лекция, СРС,	Собеседование	1-5	Согласно табл. 7.2
7.	Системы анализа защищенности	ПК-10	Лекция, СРС, лабораторная работа	Собеседование, КВЗЛР	1-5 1-5	Согласно табл. 7.2

8.	Системы обнаружения и предотвращения вторжений	ПК-10	Лекция, СРС, лабораторная работа	Собеседование, КВЗЛР	1-5 1-5	Согласно табл. 7.2

КВЗЛР – контрольные вопросы для защиты лабораторной работы

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для собеседования

Базовые вопросы проверки защищенности ИТ.

1. Дайте определение процессу в контексте ИТ.
2. Опишите методы формализации процессов.
3. Сформулируйте цели и задачи формализации процессов.
4. В чем заключается важность процесса с точки зрения управления ИБ.

Контрольные вопросы для защиты лабораторной работы №1 «Разработка регламента защищенности к проектируемым информационным системам»

1. Назвать основные цели защиты информации.
2. Назвать основные задачи защиты информации.
3. Назвать требования к методам обеспечения защиты проектируемых информационных систем.
4. Назвать основные методы обеспечения защиты проектируемых информационных систем.
5. Назвать факторы влияющие на организацию системы защиты информации.

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

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 открытой форме:

При разработке регламента оценки защищенности ИС необходимо учитывать _____.

Задание в закрытой форме:

Из перечисленного: 1) идентификация и аутентификация; 2) регистрация и учет; 3) непрерывность защиты; 4) политика безопасности -- согласно «Оранжевой книге» требованиями в области аудита являются

a. 3, 4
b. 1, 2
c. 2, 4
d. 1, 3

Задание на установление правильной последовательности,

Расположите этапы в порядке их выполнения при разработки модели угроз

Оценка возможностей нарушителя, выбор угроз из банка угроз ФСТЭК, создание уточнённой модели нарушителя, формирование перечня актуальных угроз .

Задание на установление соответствия:

Для 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 беспроводного канала связи (Wi-fi), соединяющей компьютеры, находящиеся в аттестованных помещениях. Распространение сети проходит через неаттестованное помещение. Предложите перечень мероприятий, направленных на сохранение класса защиты данной 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 Разработка регламента защищенности к проектируемым информационным системам	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Выполнение лабораторной работы Контроль защищенности информационных систем	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Выполнение лабораторной работы Анализ типовых уязвимостей распределенных информационных систем	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Выполнение лабораторной работы Сетевые и узловые системы анализа защищенности;	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Выполнение лабораторной работы Сетевые и узловые системы обнаружения и предотвращений вторжений.	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	4	Доля правильных ответов от 50% до 90%	8	Доля правильных ответов более 90%
Собеседование по темам 5-6	4	Доля правильных ответов от 50% до 90%	8	Доля правильных ответов более 90%
Собеседование по темам 7-8	4	Доля правильных ответов от 50% до 90%	8	Доля правильных ответов более 90%
ИТОГО	24		48	
Посещаемость	0		16	
Зачет	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 –2 балла,
- 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 литература

1) Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 16.02.2023). – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.

2) Основы администрирования информационных систем : учебное пособие / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко [и др.]. - Москва ; Берлин : Директ-Медиа, 2021. - 201 с. : ил., табл. - URL: http://biblioclub.ru/index.php?page=book&id=598955 (дата обращения: 16.02.2023) . - Режим доступа: по подписке. - ISBN 978-5-4499-1674-7. - Текст : электронный.

8.2 Дополнительная 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.: ил., табл. - URL: http://biblioclub.ru/index.php?page=book&id=576354 (дата обращения: 16.02.2023) . - Режим доступа: по подписке. - Текст: электронный

4) Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 255 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 16.02.2023). – Библиогр. в кн. – ISBN 978-5-4475-3946-7. – DOI 10.23681/276557. – Текст : электронный.

5) Инструментальный контроль и защита информации : учебное пособие : [16+] / Н. А. Свинарев, О. В. Ланкин, А. П. Данилкин [и др.] ;

Воронежский государственный университет инженерных технологий. – Воронеж : Воронежский государственный университет инженерных технологий, 2013. – 192 с. : табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=255905 (дата обращения: 16.02.2023). – Библиогр. в кн. – ISBN 978-5-00032-018-1. – Текст : электронный.

8.3 Перечень методических указаний

1) Разработка регламента защищенности к проектируемым информационным системам : 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. (282 КБ). - Курск : ЮЗГУ, 2022. - 15 с. - Загл. с титул. экрана. - Б. ц.

2) Контроль защищенности информационных систем : 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. (329 КБ). - Курск : ЮЗГУ, 2022. - 9 с. - Загл. с титул. экрана. - Б. ц.

3) Анализ типовых уязвимостей распределенных информационных систем : 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. (439 КБ). - Курск : ЮЗГУ, 2022. - 17 с. - Загл. с титул. экрана. - Б. ц.

4) Сетевые и узловые системы анализа защищенности : 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. (523 КБ). - Курск : ЮЗГУ, 2022. - 12 с. - Загл. с титул. экрана. - Б. ц.

5) Сетевые и узловые системы обнаружения и предотвращений вторжений : 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. (332 КБ). - Курск : ЮЗГУ, 2022. - 9 с. - Загл. с титул. экрана. - 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 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: 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 с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины - 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: ноут-букASUSX50VLPMD-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
	Изме-нённых	Заменённых	Аннулированных	новых			