Аннотация к рабочей программе дисциплины «Управление информационной безопасностью»

Цель преподавания дисциплины

Цель дисциплины – получение студентами знаний об основных подходах к разработке организационно-распорядительной документации, аудиту, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью информационных систем для успешной профессиональной деятельности.

Задачи изучения дисциплины

Задачами дисциплины являются:

- изучение основ управления информационной безопасности информационных систем (ИС);
- изучение и анализ классификации угроз информационной безопасности ИС;
- изучение принципов действия основных видов сетевых атак и методов борьбы с ними;
- изучение структуры политики безопасности организации и основных этапов ее разработки;
- анализ оценочных стандартов в информационной безопасности;
- изучение подходов создания системы управления информационной безопасностью ИС на предприятии;
- анализ методик и технологий управления рисками;
- изучение современных методов и средств анализа и управления рисками ИС компаний;
- анализ правовых мер обеспечения информационной безопасности;
- анализ организационных мер обеспечения безопасности компьютерных ИС;
- изучение методов аутентификации на основе паролей, на основе PIN-кода, принципов работы аппаратно-программных систем идентификации и аутентификации;
- изучение классификации межсетевых экранов, функций межсетевых экранов, схем подключения межсетевых экранов;
- изучение классификации компьютерных вирусов, методов обнаружения компьютерных вирусов, обзор современных антивирусных программ;
- изучение основных требований и рекомендаций по защите информации в ИС;
- изучение основных юридических законов в области защиты информации.

Индикаторы компетенций, формируемые в результате освоения дисциплины

УК-2.1 Формулирует на основе поставленной проблемы проектную задачу и способ ее решения через реализацию проектного управления.

УК-2.2 Разрабатывает концепцию проекта в рамках обозначенной проблемы: формулирует цель, задачи, обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения.

УК-2.3 Планирует необходимые ресурсы, в том числе с учетом их заменимости

УК-2.4 Разрабатывает план реализации проекта с использованием инструментов планирования.

УК-2.5 Осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта, уточняет зоны ответственности участников проекта.

УК-3.1 Вырабатывает стратегию сотрудничества и на ее основе организует отбор членов команды для достижения поставленной цели.

УК-3.2 Планирует и корректирует работу команды с учетом интересов, особенностей поведения и мнений ее членов.

УК-3.3 Разрешает конфликты и противоречия при деловом общении на основе учета интересов всех сторон.

УК-3.4 Организует дискуссии по заданной теме и обсуждение результатов работы команды с привлечением оппонентов разработанным идеям.

УК-3.5 Планирует командную работу, распределяет поручения и делегирует полномочия членам команды.

УК-6.1 Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания.

УК-6.2 Определяет приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям.

УК-6.3 Выстраивает гибкую профессиональную траекторию, используя инструменты непрерывного образования, с учетом накопленного опыта профессиональной деятельности и динамично изменяющихся требований рынка труда.

ОПК-3.2 Рассчитывает риски информационной безопасности.

ОПК-3.3 Выбирает инструментарий в области проектирования и управления информационной безопасности.

ОПК-3.4 Разрабатывает организационно-распорядительную документацию по обеспечению информационной безопасности.

ОПК-3.5 Разрабатывает модели угроз и нарушителей информационной безопасности информационных систем.

Разделы дисциплины

Основные понятия и анализ угроз информационной безопасности. Проблемы информационной безопасности сетей. Политика безопасности. Криптографическая защита информации. Технологии аутентификации. Технологии межсетевых экранов. Технологии защиты от вирусов. Требования к системам защиты информации. Основы правового обеспечения защиты информации.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета ФиПИ
_____ Таныгин М.О.
(подпись, инициалы, фамилия)
«30» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Управление информационной безопасностью
(наименование дисциплины)

ОПОП ВО 10.04.01 Информационная безопасность,
(шифр и наименование направления подготовки)

направленность (профиль) «Защищенные информационные системы»
(наименование направленности (профиля))

форма обучения очная

ОПОП ВО реализуется по модели дуального обучения

Курск – 2023

Рабочая программа дисциплины составлена:

– в соответствии с ФГОС ВО – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденным приказом Минобрнауки России от 26.11.2020 г. № 1455;

– на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», одобренного Ученым советом университета (протокол №12 от 29.05.2023).

– с учетом заказа-требования от 28.04.2023 на результаты освоения ОПОП ВО – программы магистратуры 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», реализуемой по модели дуального обучения в ФГБОУ ВО «Юго-Западный государственный университет», от ООО ЦСБ «ЩИТ-ИНФОРМ»
(наименование предприятия (организации))
(приложение к общей характеристике ОПОП ВО).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для дуального обучения студентов по ОПОП ВО 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы» на совместном заседании кафедры информационной безопасности
(наименование кафедры)
с представителями ООО ЦСБ «ЩИТ-ИНФОРМ»
(наименование предприятия (организации))
(протокол № 8 от 29. 05. 2023).

Зав. кафедрой _____ А.Л. Марухленко

Разработчик программы
к.т.н. _____ Е.А. Кулешова

Директор научной библиотеки _____ В.Г. Макаровская

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО дуального обучения 10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы», одобренного Ученым советом университета (протокол № __ от __. __. 20__), на совместном заседании кафедры информационной безопасности
(наименование кафедры)
с представителями ООО ЦСБ «ЩИТ-ИНФОРМ»
(наименование предприятия (организации))
(протокол № __ от __. __. 20__).

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 дисциплины

Цель дисциплины – получение студентами знаний об основных подходах к разработке организационно-распорядительной документации, аудиту, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью информационных систем для успешной профессиональной деятельности.

1.2 Задачи дисциплины

Задачами дисциплины являются:

- изучение основ управления информационной безопасности информационных систем (ИС);
- изучение и анализ классификации угроз информационной безопасности ИС;
- изучение принципов действия основных видов сетевых атак и методов борьбы с ними;
- изучение структуры политики безопасности организации и основных этапов ее разработки;
- анализ оценочных стандартов в информационной безопасности;
- изучение подходов создания системы управления информационной безопасностью ИС на предприятии;
- анализ методик и технологий управления рисками;
- изучение современных методов и средств анализа и управления рисками ИС компаний;
- анализ правовых мер обеспечения информационной безопасности;
- анализ организационных мер обеспечения безопасности компьютерных ИС;
- изучение методов аутентификации на основе паролей, на основе PIN-кода, принципов работы аппаратно-программных систем идентификации и аутентификации;
- изучение классификации межсетевых экранов, функций межсетевых экранов, схем подключения межсетевых экранов;
- изучение классификации компьютерных вирусов, методов обнаружения компьютерных вирусов, обзор современных антивирусных программ;
- изучение основных требований и рекомендаций по защите информации в ИС;
- изучение основных юридических законов в области защиты информации.

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 компетенции	*наименование компетенции*		
УК-2	Способен управлять проектом на всех этапах его жизненного цикла.	УК-2.1 Формулирует на основе поставленной проблемы проектную задачу и способ ее решения через реализацию проектного управления.	***Знать***: сетевой график проведения работ в рамках проекта, технологический цикл проведения разработок, состав материально технической и лабораторной базы необходимой для разработки программно-аппаратных средств, сборки и монтажа сетевого оборудования ИС; порядок разработки и согласования расчётно-калькуляционных материалов проекта по разработке ИС, знать состав и структуру планово-хозяйственных документов, финансовых документов, отчётных документов, порядок их оформления, программные продукты и системы управления хозяйственной деятельностью. ***Уметь:*** управлять материальными, нематериальными, финансовыми ресурсами, инструментами и оборудованием необходимыми для выполнения работ по проектированию ИС. ***Владеть:*** навыками управления и распределения материальными, нематериальными, финансовыми ресурсами, инструментами и оборудованием необходимыми для выполнения работ по проектированию ИС.
		УК-2.2 Разрабатывает концепцию проекта в рамках обозначен-	***Знать:*** нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, проведению пусконаладочных работ; требования к

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 компетенции	*наименование компетенции*		
		ной проблемы: формулирует цель, задачи, обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения.	разработке алгоритмов, программных средств, параметры и характеристики покупных комплектующих изделий, спецификации комплектующих компьютерных средств, параметры и характеристики сетевого оборудования, компоненты и архитектуру ИС, задачи, решаемые разрабатываемой ИС; функциональные обязанности руководителя проекта и персонала (разработчиков инженерных тем) ***Уметь:*** организовать и распределить задачи по проектированию ИС среди исполнителей в соответствии с требованиями ТЗ, договорных документов, контракта; осуществлять контроль выполнения работ, проверять разработанную НТД на соответствие требованиям ТЗ, нормативным документа, ГОСТ; требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала. ***Владеть:*** навыками организации, распределения, контроля и выполнения задач по проектированию ИС, проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом.
		УК-2.3 Планирует необходимые ресурсы, в том числе с учетом их заменимости	***Знать:*** требования к разработке научно-технической и планово-экономической документации, этапы и технологические циклы проведения работ по проекту, классификацию, номенклатуру и архитектуру и состав типовых прикладных ИС, этапы разработки типовой прикладной ИС, сетевой график выполнения проекта,

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 компетенции	*наименование компетенции*		
			должностные обязанности руководителя проекта и инженерно-технического персонала, нормативные документы и ГОСТы, требования к разработке, состав и перечень РКД, ЭД, ПД, основные требования к системам защиты информации; показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем. ***Уметь***: организовать выполнение работ в рамках проекта по разработке прикладных ИС, контролировать выполнение задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов, своевременно вносить коррективы в разработанную документацию и устранять замечания, недостатки и несоответствия, выявленные в ходе выполнения работ проекта. ***Владеть:*** навыками организации выполнения работ в рамках проектов по разработке прикладных ИС, контроля выполнения задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов; своевременного внесения корректив в разработанную документацию и устранения замечаний, недостатков и несоответствий, выявленных в ходе выполнения работ в рамках проектов.

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 компетенции	*наименование компетенции*		
		УК-2.4 Разрабатывает план реализации проекта с использованием инструментов планирования.	***Знать:*** требования к разработке проектной и планово-экономической документации, этапы и технологические циклы проведения работ по проекту, классификацию, номенклатуру, архитектуру и состав типовых защищённых ИС, этапы разработки типовой защищённой ИС, сетевой график выполнения проекта, должностные обязанности руководителя проекта и инженерно-технического персонала, нормативные документы и ГОСТы, требования к разработке, состав и перечень РКД, ЭД, ПД, основные требования к системам защиты информации. ***Уметь***: организовать выполнение работ в рамках проекта по разработке защищённых ИС, контролировать выполнение задач персоналом на соответствие требованиям ТЗ, других нормативных и планово-экономических документов, разрабатывать плановые документы, сетевые графики, рассчитывать нагрузку персонала в соответствии с должностными обязанностями. ***Владеть:*** навыками организации выполнения работ в рамках проектов по разработке защищённых ИС, контроля выполнения задач персоналом на соответствие требованиям ТЗ, других нормативных документов; разработки плановых документов, сетевых графиков, расчёта нагрузки персонала в соответствии с должностными обязанностями.

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 компетенции	*наименование компетенции*		
		УК-2.5 Осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта, уточняет зоны ответственности участников проекта.	***Знать:*** требования к разработке научно-технической и планово-экономической документации, этапы и технологические циклы проведения работ по проекту, классификацию, номенклатуру и архитектуру и состав типовых прикладных ИС, этапы разработки типовой прикладной ИС, сетевой график выполнения проекта, должностные обязанности руководителя проекта и инженерно-технического персонала, нормативные документы и ГОСТы, требования к разработке, состав и перечень РКД, ЭД, ПД, основные требования к системам защиты информации. ***Уметь***: организовать выполнение работ в рамках проекта по разработке прикладных ИС, контролировать выполнение задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов, своевременно вносить коррективы в разработанную документацию и изменения в план реализации проекта, устранять замечания, недостатки и несоответствия, выявленные в ходе выполнения работ проекта. ***Владеть:*** навыками организации выполнения работ в рамках проектов по разработке прикладных ИС, контроля выполнения задач персоналом на соответствие требованиям ТЗ, других нормативных и юридических документов; своевременного внесения корректив в разработанную документацию и

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 компетенции	*наименование компетенции*		
			изменения в план реализации проекта, устранения замечаний, недостатков и несоответствий, выявленных в ходе выполнения работ в рамках проектов, применения средств контроля и мониторинга бесперебойного функционирования защищённых ИС.
УК-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.	УК-3.1 Вырабатывает стратегию сотрудничества и на ее основе организует отбор членов команды для достижения поставленной цели.	***Знать:*** нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, проведению пусконаладочных работ; требования к разработке алгоритмов, программных средств, параметры и характеристики покупных комплектующих изделий, спецификации комплектующих компьютерных средств, параметры и характеристики сетевого оборудования, компоненты и архитектуру ИС, задачи, решаемые разрабатываемой ИС; функциональные обязанности руководителя проекта и персонала (разработчиков инженерных тем) ***Уметь:*** организовать и распределить задачи по проектированию ИС среди исполнителей в соответствии с требованиями ТЗ, договорных документов, контракта; осуществлять контроль выполнения работ, проверять разработанную НТД на соответствие требованиям ТЗ, нормативным документа, ГОСТ; требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала. ***Владеть:*** навыками организации, распределения, контроля и выполнения задач по проектированию ИС, проверки требований выполнения функциональных обязанно-

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 компетенции	*наименование компетенции*		
			стей инженерно-техническим персоналом.
		УК-3.2 Планирует и корректирует работу команды с учетом интересов, особенностей поведения и мнений ее членов.	***Знать***: сетевой график проведения работ в рамках проекта, технологический цикл проведения разработок, состав материально технической и лабораторной базы необходимой для разработки программно-аппаратных средств, сборки и монтажа сетевого оборудования защищённых ИС; порядок разработки и согласования расчётно-калькуляционных материалов проекта по разработке защищённых ИС, знать состав и структуру планово-хозяйственных документов, финансовых документов, отчётных документов, порядок их оформления, программные продукты и системы управления хозяйственной деятельностью. ***Уметь:*** управлять материальными, нематериальными, финансовыми ресурсами, инструментами и оборудованием необходимыми для выполнения работ по проектированию защищённых ИС, корректировать и планировать работу персонала в зависимости от поставленных задач и профессиональных навыков членов команды. ***Владеть:*** навыками управления и распределения материальными, нематериальными, финансовыми ресурсами, инструментами и оборудованием необходимыми для выполнения работ по проектированию защищённых ИС, корректировки и планирования работы персонала в зависимости от поставленных задач и профессиональных навыков членов команды..

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 компетенции	*наименование компетенции*		
		УК-3.3 Разрешает конфликты и противоречия при деловом общении на основе учета интересов всех сторон.	***Знать:*** классификацию, назначение, конфигурацию, состав, структуру, принципы функционирования типовых защищенных ИС предприятий; основы управления ИС; виды, состав, назначение, принципы функционирования, функции и взаимосвязь основных элементов и компонентов ИС; понятие, типы, примеры архитектур ИС, принципы работы ИС; типовые архитектуры ИС с точки зрения программно-аппаратной реализации; классификацию архитектур; особенности проектирования распределённых систем; методы и средства защиты информации в ИС, способы защиты информационных систем, методы анализа угроз и оценки рисков информационной безопасности ИС. ***Уметь:*** проводить сравнительный анализ состава, технических характеристик, решаемых задач компонентов ИС прикладного характера, системного и прикладного ПО, обеспечивающего функционирование ИС; оценку вариантов предлагаемых к реализации архитектур ИС; выбор наиболее оптимального варианта построения предлагаемой архитектуры ИС; формировать требования к структуре ИС исходя из решаемых задач; разрабатывать регламентирующие документы для принятия решения на технических совещаниях; предложения для технических советов с обоснованием выбора предлагаемой архитектуры прикладной ИС. ***Владеть:*** навыками сравнительного анализа технических средств

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 компетенции	*наименование компетенции*		
			и оборудования из состава прикладных ИС, оценки предлагаемых к реализации вариантов построения прикладных ИС, выбора оптимальной архитектуры прикладной ИС исходя из решаемых системой задач, разрешения конфликтных ситуаций в ходе выполнения работ по разработке защищённых ИС.
		УК-3.4 Организует дискуссии по заданной теме и обсуждение результатов работы команды с привлечением оппонентов разработанным идеям.	***Знать:*** порядок внедрения, отладки и этапы разработки систем обеспечения информационной безопасности ИС. ***Уметь:*** организовать и управлять внедрением, отладкой и развитием процессами и этапами разработки систем обеспечения информационной безопасности защищённых ИС. ***Владеть:*** навыками организации и управления внедрением, отладкой и развитием процессами и этапами разработки систем обеспечения информационной безопасности защищённых ИС, организации обсуждений результатов работы команды с привлечением оппонентов разработанным идеям в рамках создания защищённых ИС.
		УК-3.5 Планирует командную работу, распределяет поручения и делегирует полномочия членам команды.	***Знать:*** нормативные документы и госты по разработке ТЗ, НИОКР, РКД, ЭД, ПД, проведению пусконаладочных работ; требования к разработке алгоритмов, программных средств, параметры и характеристики покупных комплектующих изделий, спецификации комплектующих компьютерных средств, параметры и харак-

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 компетенции	*наименование компетенции*		
			теристики сетевого оборудования, компоненты и архитектуру ИС, задачи, решаемые разрабатываемой ИС; функциональные обязанности руководителя проекта и персонала (разработчиков инженерных тем) ***Уметь:*** организовать и распределить задачи по проектированию защищённых ИС среди исполнителей в соответствии с требованиями ТЗ, договорных документов, контракта; осуществлять контроль выполнения работ, проверять разработанную НТД на соответствие требованиям ТЗ, нормативным документа, ГОСТ; требовать выполнения функциональных обязанностей разработчиками инженерно-технического персонала. ***Владеть:*** навыками планирования, организации, распределения, контроля и выполнения задач исполнителями по проектированию защищённых ИС, проверки требований выполнения функциональных обязанностей инженерно-техническим персоналом.
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки.	УК-6.1 Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания.	***Знать:*** классификацию программно-аппаратных и телекоммуникационных средств защиты, технические характеристики и возможности сетевого оборудования инфокоммуникационных сетей, каналы распространения вредоносных программ, методы обнаружения компьютерных вирусов, показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности систем и сетей, основные действующие

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 компетенции	*наименование компетенции*		
			нормативные документы и юридические законы в области защиты информации. ***Уметь:*** проводить анализ защищенности локальной вычислительной сети, настраивать режимы работы межсетевых экранов, проводить анализ информационных рисков, определять оптимальный состав программных и аппаратных средств для построения инфо-коммуникационных сетей, применять действующие нормативные документы и юридические законы в области защиты информации. ***Владеть:*** навыками выбора программно-аппаратных средств и телекоммуникационного оборудования, эксплуатации программных средств анализа и управления рисками, навыками разработки защищенных сайтов, разработки и установки программных средств защиты инфо-коммуникационных сетей, определения действующих нормативных требований и юридических законов в области защиты информации.
		УК-6.2 Определяет приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям.	***Знать:*** методы профессионального развития и совершенствования собственной деятельности. ***Уметь:*** определять приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям. ***Владеть:*** навыками определения приоритетов профессионального

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 компетенции	*наименование компетенции*		
			роста и способов совершенствования собственной деятельности.
		УК-6.3 Выстраивает гибкую профессиональную траекторию, используя инструменты непрерывного образования, с учетом накопленного опыта профессиональной деятельности и динамично изменяющихся требований рынка труда.	***Знать:*** психологические основы и способы формирования профессиональной траектории с использованием инструментов непрерывного образования. ***Уметь:*** применять приемы и алгоритмы выстраивания гибкой профессиональной траектории. ***Владеть:*** навыками анализа профессиональной траектории с учетом накопленного опыта профессиональной деятельности и динамично изменяющихся требований рынка труда.
ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности.	ОПК-3.2 Рассчитывает риски информационной безопасности.	***Знать:*** классификацию, виды и типы угроз безопасности ИС, принципы построения средств защиты информации и возможные риски нарушения безопасности функционирования ИС; основные компоненты ИС, состав, структуры и принципы функционирования современных ИС, требования основных законов и нормативных документов в области безопасности ИС; методы, способы и методики анализа рисков безопасности ИС; классификацию основных источников угроз, комплекс мероприятий, технических мер и методов, направленных на повышение защищенности и снижения рисков нарушения безопасности ИС; основные принципы построения комплексной системы защиты ИС. ***Уметь:*** определять угрозы безопасности ИС, определять возможные риски нарушения безопасности функционирования ИС; определять состав, структуру и

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 компетенции	*наименование компетенции*		
			принципы функционирования современных ИС, анализировать требования основных законов и нормативных документов в области безопасности ИС; применять методики анализа рисков безопасности ИС; определять основные источники угроз, принимать технические меры, направленные на повышение защищенности и снижения рисков нарушения безопасности ИС. ***Владеть:*** навыками анализа защищенности ИС; навыками защиты информации в компьютерных системах; навыками определения угроз безопасности ИС, выбора средств защиты информации; требованиями основных законов и нормативных документов в области безопасности автоматизированных систем; методиками анализа рисков безопасности автоматизированных систем и выявления источников угроз; навыками проведения и организации комплекса мероприятий по повышению защищенности и снижению рисков нарушения безопасности автоматизированных систем; навыками построения комплексной системы защиты ИС, методами расчёта рисков ИБ ИС.

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 компетенции	*наименование компетенции*		
		ОПК-3.3 Выбирает инструментарий в области проектирования и управления информационной безопасности.	***Знать:*** типовые архитектуры, модели, компоненты, интерфейсы, технические характеристики ИС, виды и методы проектирования ИС; способы конструирования, принципы проектирования, структуру, стадии и этапы разработки проекта, методы и способов управления персоналом и проектом, порядок разработки технической и конструкторской документации, программные средства разработки проектов, конструкторской и технической документации. ***Уметь:*** выбирать архитектуры ИС, модели, компоненты, интерфейсы, технические характеристики ИС, применять методы проектирования ИС; применять методы для управления персоналом и проектом, разрабатывать техническую и конструкторскую документацию, применять программные средства для разработки проектов, конструкторской и технической документации. ***Владеть:*** навыками выбора архитектуры ИС, моделей, компонентов, интерфейсов ИС, методами и способами проектирования ИС; методами и методиками управления персоналом и проектами, применения программных средств разработки проектов, конструкторской и технической документации.

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 компетенции	*наименование компетенции*		
		ОПК-3.4 Разрабатывает организационно-распорядительную документацию по обеспечению информационной безопасности.	***Знать:*** основные принципы организации технического, программного и информационного обеспечения защищенных ИС, методы концептуального проектирования технологий обеспечения информационной безопасности; основные нормативные правовые акты в области информационной безопасности и защиты информации; основные понятия, законы, модели и структуры обеспечения организационной безопасности на предприятии; основные понятия, законы и модели прогнозирования принятия решений. ***Уметь:*** осуществлять выбор функциональной структуры системы обеспечения информационной безопасности, обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности, осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; использовать нормативные правовые документы в своей профессиональной деятельности; применять основные закономерности принятия управленческих решений и управления коллективом при решении прикладных задач обеспечения информационной безопасности. ***Владеть:*** навыками управления информационной безопасностью ИС, освоения, внедрения и сопро-

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 компетенции	*наименование компетенции*		
			вождения документации, в том числе и в команде; нахождения организационно-управленческих решений в нестандартных ситуациях на основе результатов анализа документации и потоков документов; знаниями в области правового обеспечения информационной безопасности и навыками правового применения нормативного законодательства в данной сфере; поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы.
		ОПК-3.5 Разрабатывает модели угроз и нарушителей информационной безопасности информационных систем.	***Знать:*** этапы построения системы информационной безопасности ИС, условия и факторы, приводящие к нарушению целостности, доступности и конфиденциальности информации, классификацию угроз, основные направления защиты информации на объекте, последствия и виды несанкционированных действий с информацией, классификацию нарушителей, методы и способы оценки ущерба от различных рисков потери информации, анализа уровня информационной безопасности объекта, оценки состояния степени защищённости информации, методы и методики оценки рисков информационной безопасности при использовании программных средств и информационных систем управления, модели, методы и методики оценки угроз и уязвимостей, инструментальные

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 компетенции	*наименование компетенции*		
			средства анализа угроз. ***Уметь:*** применять известные методики оценки угроз, разрабатывать корпоративную политику управления рисками, анализировать и классифицировать угрозы, применять типовые методики для получения характеристик рисков и угроз, использовать основные модели оценки рисков для получения количественных и качественных оценок рисков, использовать модели оценки рисков для формирования политики управления рисками и проектирования системы управления рисками. ***Владеть:*** навыками анализа защищенности объекта информатизации, методами проведения анализа угроз информационной безопасности; разделения рисков на приемлемые и неприемлемые, оценки рисков информационной безопасности и проектирования систем управления корпоративными рисками, разработки моделей угроз и нарушителей информационной безопасности ИС.

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Управление информационной безопасностью» входит в обязательную часть блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы магистратуры 10.04.01 Информационная безопасность, направленность (профиль) «Защищённые информационные системы», реализуемой по модели дуального обучения.

Дисциплина изучается на 1 курсе во 2 семестре.

Дисциплина имеет практико-ориентированный характер и изучается до прохождения обучающимися производственной практики по получению умений и навыков управленческой деятельности, завершающей данный семестр.

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 трудоемкость (объем) дисциплины составляет 5 зачетных единиц (з.е.), 180 академических часов.

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	180
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	106
в том числе:	
лекции	30
лабораторные занятия	30
практические занятия	46, из них практическая подготовка обучающихся – 4.
Самостоятельная работа обучающихся (всего)	44,85
Контроль (подготовка к экзамену)	27
Контактная работа по промежуточной аттестации (всего АттКР)	2,15
в том числе:	
зачет	не предусмотрен
зачет с оценкой	не предусмотрен
курсовая работа (проект)	1
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	2	3
1	Основные понятия и анализ угроз информационной безопасности	Основные понятия защиты информации и информационной безопасности. Понятие угрозы информационной безопасности. Анализ и классификация угроз информационной безопасности. Угрозы нарушения конфиденциальности информации, целостности информации, доступности информации. Угроза раскрытия параметров автоматизированной системы.
2	Проблемы информационной безопасности сетей	Модель ISO/OSI и стек протоколов TCP/IP. Проблемы безопасности IP- сетей. Основные виды сетевых атак. Спам. Фишинг и фарминг. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей. Фрагментарный и комплексный подходы к проблеме обеспечения безопасности компьютерных сетей. Пути решения проблем защиты информации в сетях.
3	Политика безопасности	Основные понятия политики безопасности. Верхний, средний и нижний уровни политики безопасности. Структура политики безопасности организации. Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности. Основные этапы разработки политики безопасности организации. Компоненты архитектуры безопасности сети:
4	Криптографическая защита информации	Основные понятия криптографической защиты информации. Требования к криптографическим системам. Симметричные и ассиметричные крипто-системы шифрования. Блочные и потоковые шифры. Шифры простой замены. Шифры Виженера. Стандарт шифрования AES. Алгоритм шифрования RSA. Функция хэширования. Электронная цифровая подпись (ЭЦП). Защита электронного документооборота с использованием ЭЦП. Обзор программных и программно-аппаратных средств криптографической защиты.

5	Технологии аутентификации	Аутентификация, авторизация и администрирование действий пользователей. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе PIN-кода. Строгая аутентификация, основанная на симметричных алгоритмах. Биометрическая аутентификация пользователя. Аппаратно-программные системы идентификации и аутентификации.
6	Технологии межсетевых экранов	Классификация межсетевых экранов. Функции межсетевых экранов: фильтрация трафика, выполнение функций посредничества. Дополнительные возможности межсетевых экранов: идентификация и аутентификация пользователей, трансляция сетевых адресов, регистрация и анализ событий. Варианты исполнения межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Формирование политики межсетевого взаимодействия. Основные схемы подключения межсетевых экранов. Персональные и распределенные межсетевые экраны. Проблемы безопасности межсетевых экранов.
7	Технологии защиты от вирусов	Классификация компьютерных вирусов. Загрузочные вирусы. Файловые вирусы. Вирусы-сценарии. Макровирусы. Троянские программы. Черви. Жизненный цикл вирусов. Основные каналы распространения вредоносных программ. Методы обнаружения компьютерных вирусов: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод “белого списка”, обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ. Обзор современных антивирусных программ. Построение системы антивирусной защиты корпоративной сети.
8	Требования к системам защиты информации	Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных. Требования к защите информации в автоматизированных системах, локальных вычислительных сетях, на рабочих местах пользователей ПК. Требования к защите информации при работе с системами управления базами данных. Требования к защите информации при взаимодействии абонентов с сетями общего пользования.

9	Основы правового обеспечения защиты информации	Правовое обеспечение информационной собственности и его место в системе информационного права. Информация как объект юридической защиты. Формирование государственной системы правового обеспечения информационной безопасности. Правовое обеспечение защиты государственной тайны. Законодательство Российской Федерации в области информационной безопасности. Правовая защита информации в сфере высоких технологий. Правовая защита интеллектуальной собственности. Правовое регулирование деятельности организаций в области информационной безопасности.

Таблица 4.1.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		Лек. час	№ лаб	№ пр.			
1	2	3	4	5	6	7	8
1	Основные понятия и анализ угроз информационной безопасности	4	-	-	У 1-5	УО - 1	УК-2, УК-3, УК-6
2	Проблемы информационной безопасности сетей	4	-	-	У 1-5	УО - 2	УК-2, УК-3, УК-6, ОПК-3
3	Политика безопасности	3	1	-	У 1-5 МУ 1-4	УО, ЗЛР - 3	УК-2, УК-3, УК-6, ОПК-3
4	Криптографическая защита информации	4	-	1,2	У 1-5 МУ 1-4	УО, ПЗ, КЗ, ЗПР – 4	УК-2, УК-3, УК-6, ОПК-3
5	Технологии аутентификации	3	-	-	У 1-5	УО -5	УК-2, УК-3, УК-6, ОПК-3
6	Технологии межсетевых экранов	3	-	-	У 1-5	УО -6	УК-2, УК-3, УК-6, ОПК-3
7	Технологии защиты от вирусов	3	-	3	У 1-5 МУ 1-4	УО, КЗ, ЗПР, ККР – 7	УК-2, УК-3, УК-6, ОПК-3
8	Требования к системам защиты информации	3	2,3	-	У 1-5 МУ 1-4	УО, ЗЛР, ККР – 8	УК-2, УК-3, УК-6,

							ОПК-3
9	Основы правового обеспечения защиты информации	3	-	4	У 1-5 МУ 1-4	УО, КЗ, ЗПР, ККР - 9	УК-2, УК-3, УК-6, ОПК-3
	Всего	30					

УО – устный опрос, ЗЛР – лабораторная работа, ЗПР – практическая работа, ККР – контроль выполнения этапов курсовой работы, ПЗ – решение производственной задачи, КЗ – решение кейса.

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 – Лабораторные работы

№ п/п	Наименование лабораторной работы	Объем, час.
1	Система аудита информационной безопасности ГИС	10
2	Решение ситуационных задач (кейсов)	10
3	Основные методы управления информационной безопасностью в ГИС	10
Итого		30

4.2.2 Практические занятия

Таблица 4.2.2 - Практические занятия

№ п/п	Наименование практической работы	Объем, час.
1	Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение.	10, из них практическая подготовка обучающихся – 4.
2	Определение показателей защищенности информации при несанкционированном доступе.	12
3	Критерии оценки и выбора CASE-средств.	12
4	Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности.	12
Итого		46

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела (темы) дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	Основные понятия и анализ угроз информационной безопасности	1 неделя	4,85
2	Проблемы информационной безопасности сетей	2 неделя	5

3	Политика безопасности	3 неделя	5
4	Криптографическая защита информации	4 неделя	5
5	Технологии аутентификации	5 неделя	5
6	Технологии межсетевых экранов	6 неделя	5
7	Технологии защиты от вирусов	7 неделя	5
8	Требования к системам защиты информации	8 неделя	5
9	Основы правового обеспечения защиты информации	9 неделя	5
Итого			44,85

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

При самостоятельном изучении отдельных тем и вопросов дисциплины студенты могут пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры *информационной безопасности* в рабочее время, установленное Правилами внутреннего распорядка работников университета.

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

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с учебным планом и 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:

– методических рекомендаций, пособий по организации самостоятельной работы студентов;

– методических указаний к выполнению лабораторных и практических работ и т.д.

типографией университета:

– посредством оказания помощи авторам в подготовке и издании научной, учебной и методической литературы;

– посредством удовлетворения потребности в тиражировании научной, учебной и методической литературы.

6 Образовательные технологии. Практическая подготовка обучающихся

Реализация программы магистратуры по модели дуального обучения и компетентностного подхода предусматривают широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования универсальных и общепрофессиональных компетенций обучающихся.

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

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем, час.
1	2	3	4
1	Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение.	Кейс-технология	2
2	Определение показателей защищенности информации при несанкционированном доступе.	Кейс-технология	2
3	Критерии оценки и выбора CASE-средств.	Кейс-технология	2
4	Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности.	Кейс-технология	4
Итого:			10

Практическая подготовка обучающихся при реализации дисциплины осуществляется путем проведения лабораторных и практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по направленности (профилю) программы магистратуры.

Практическая подготовка обучающихся при реализации дисциплины организуется в модельных условиях.

Практическая подготовка обучающихся проводится в соответствии с положением П 02.181.

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

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

Таблица 7.1 – Этапы формирования компетенций

Код и наименование компетенции	Этапы[1] формирования компетенций и дисциплины (модули), практики, при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
УК-2. Способен управлять проектом на всех этапах его жизненного цикла.	Экономика и управление Управление информационной безопасностью		
УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.	Управление информационной безопасностью		Управление разработкой систем безопасности
УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки.	Управление информационной безопасностью		Управление разработкой систем безопасности
ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности.	Производственная практика (исследовательская работа)	Экономика и управление Управление информационной безопасностью	

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 *(наименование этапа по таблице 6.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за практикой)*	Критерии и шкала оценивания компетенций			
		Недостаточный уровень («неудовл.»)	Пороговый уровень («удовл.»)	Продвинутый уровень («хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5	6
УК-2/ основной	УК-2.1 Формулирует на основе поставленной проблемы проектную задачу и способ ее решения через реализацию проектного управления УК-2.2 Разрабатывает концепцию проекта в рамках обозначенной проблемы: формулирует цель, задачи, обосновывает актуальность, значимость,	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для УК-2. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для УК-2. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для УК-2. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для УК-2. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для УК-2.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для УК-2.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для УК-2.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для УК-2.

	ожидаемые результаты и возможные сферы их применения УК-2.3 Планирует необходимые ресурсы, в том числе с учетом их заменимости УК-2.4 Разрабатывает план реализации проекта с использованием инструментов планирования УК-2.5 Осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта, уточняет зоны ответственности участников проекта	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-2, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-2, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-2, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-2, доведены до автоматизма.
УК-3/ основной	УК-3.1 Вырабатывает стратегию со-	**Знать:** демонстрирует менее 60% знаний, ука-	**Знать:** демонстрирует 60-74% знаний, ука-	**Знать:** демонстрирует 75-89% знаний, ука-	**Знать:** демонстрирует 90-100% знаний, указан-

	трудничества и на ее основе организует отбор членов команды для достижения поставленной цели УК-3.2 Планирует и корректирует работу команды с учетом интересов, особенностей поведения и мнений ее членов УК-3.3 Разрешает конфликты и противоречия при деловом общении на основе учета интересов всех сторон УК-3.4 Организует дискуссии по заданной теме и обсуждение результатов работы команды с привлечением оппонентов разработанным идеям УК-3.5	занных в таблице 1.3 для УК-3. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	занных в таблице 1.3 для УК-3. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	занных в таблице 1.3 для УК-3. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	ных в таблице 1.3 для УК-3. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для УК-3.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для УК-3.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для УК-3.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для УК-3.
		Владеть (*или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-3, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-3, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-3, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-3, доведены до автоматизма.

	Планирует командную работу, распределяет поручения и делегирует полномочия членам команды				
УК-6/ основной	УК-6.1 Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания УК-6.2 Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для УК-6. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для УК-6. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для УК-6. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для УК-6. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для УК-6.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для УК-6.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для УК-6.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для УК-6.

	для успешного выполнения порученного задания УК-6.3 Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-6, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-6, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-6, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для УК-6, доведены до автоматизма.
ОПК-3/ основной	ОПК-3.2 Рассчитывает риски информационной безопасности ОПК-3.3 Выбирает инструментарий в области проектирования и управления информационной безопасности ОПК-3.4 Разрабатывает организационно-распорядительную документа-	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для ОПК-3. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	**Знать:** демонстрирует 60-74% знаний, указанных в таблице 1.3 для ОПК-3. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для ОПК-3. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для ОПК-3. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
		Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для ОПК-3.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ОПК-3.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ОПК-3.

	цию по обеспечению информационной безопасности ОПК-3.5 Разрабатывает модели угроз и нарушителей информационной безопасности информационных систем		для ОПК-3.		
		Владеть (*или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-3, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-3, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-3, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ОПК-3, доведены до автоматизма.

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/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Основные понятия и анализ угроз информационной безопасности	УК-2, УК-3, УК-6	Лекция, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
2	Проблемы информационной безопасности сетей	УК-2, УК-3, УК-6, ОПК-3	Лекция, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
3	Политика безопасности	УК-2, УК-3, УК-6, ОПК-3	Лекция, СРС, лабораторная работа №1	Вопросы для устного опроса КВЗЛР №1	1-10 1-10	Согласно таблице 7.2
4	Криптографи-	УК-2,	Лекция,	Вопросы для уст-	1-10	Согласно

	ческая защита информации	УК-3, УК-6, ОПК-3	практические работы №1 №2, СРС	ного опроса КВЗПР №1 Производственная задача КВЗПР №2 Кейс	 1-10 1-10 1-10 1,2	таблице 7.2
5	Технологии аутентификации	УК-2, УК-3, УК-6, ОПК-3	Лекция, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
6	Технологии межсетевых экранов	УК-2, УК-3, УК-6, ОПК-3	Лекция, СРС	Вопросы для устного опроса	1-10	Согласно таблице 7.2
7	Технологии защиты от вирусов	УК-2, УК-3, УК-6, ОПК-3	Лекция, Практическая работа №3, выполнение этапов курсовой работы, СРС	Вопросы для устного опроса КВЗПР №3, Кейс, ТКР, КРКр	1-10 1-10 3	Согласно таблице 7.2
8	Требования к системам защиты информации	УК-2, УК-3, УК-6	Лекция, лабораторные работы №2,3, выполнение этапов курсовой работы, СРС	Вопросы для устного опроса КВЗЛР №2, КВЗЛР №3, ТКР, КРКр	1-10 1-10 1-10	Согласно таблице 7.2
9	Основы правового обеспечения защиты информации	УК-2, УК-3, УК-6, ОПК-3	Лекция, Практическая работа №4, выполнение этапов курсовой работы, СРС	Вопросы для устного опроса КВЗПР №4, Кейс, ТКР, КРКр	1-10 1-10 4	Согласно таблице 7.2

СРС – самостоятельная работа студента,

КВЗЛР – контрольные вопросы для защиты лабораторных работ,

КВЗПР - контрольные вопросы для защиты практических работ,
ТКР – темы курсовых работ,
КРКр – критерии оценки курсовых работ

7.3.1 Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу (теме) 1. «Основные понятия и анализ угроз информационной безопасности».

1. Основные понятия защиты информации и информационной безопасности.
2. Классификация угроз информационной безопасности автоматизированных систем.
3. Непосредственные виды угроз для автоматизированных систем: угроза нарушения конфиденциальности, угроза нарушения целостности информации, угроза нарушения работоспособности. Угроза раскрытия параметров автоматизированной системы.

Контрольные вопросы для защиты лабораторной работы №1:
«Система аудита информационной безопасности ГИС».

1. Что такое политика информационной безопасности?
2. Какие организационные меры защиты существуют?
3. Назначение организационных мер?
4. Какие из них наиболее эффективны? Почему?
5. Перечислите основные нормативные документы, регламентирующие ИБ в России
6. Какой состав и организационная структура системы обеспечения информационной безопасности?
7. В чем заключается стандарт ISO 17799?
8. Опишите методику анализа рисков.

Контрольные вопросы для защиты практической работы №2
Определение показателей защищенности информации при несанкционированном доступе.

1. В чем заключаются основные принципы проектирования защищённых систем?
2. Перечислите показатели качества процесса проектирования.
3. Постановка проблемы комплексного обеспечения информационной безопасности защищённых систем.
4. Основы методологии многовариантного планирования процесса проектирования.
5. Методы и методики проектирования комплексных систем информационной безопасности от несанкционированного доступа.

Темы курсовых работ.

Практическая подготовка обучающихся при реализации данной дисциплины организуется, в частности, путем выполнения и защиты курсовой работы (проекта) на одну из тем, приведенных ниже.

Проектирование защищенной информационной системы для предприятий нефтегазовой отрасли.

Проектирование защищенной информационной системы для органов местного самоуправления.

Проектирование защищенной информационной системы для предприятий банковской сферы.

Проектирование защищенной информационной системы для муниципальных предприятий.

Проектирование защищенной информационной системы для машиностроительной отрасли.

Проектирование защищенной информационной системы для энергетической отрасли.

Проектирование защищенной информационной системы для военизированной отрасли.

Проектирование защищенной информационной системы для строительной отрасли.

Проектирование защищенной информационной системы для металлургической отрасли.

Проектирование защищенной информационной системы для жилищно-коммунального хозяйства.

Разработка модели угроз образовательного учреждения.

Разработка модели угроз образовательного учреждения.

Разработка модели угроз медицинского учреждения.

Разработка модели угроз муниципального учреждения.

Разработка модели угроз коммерческой организации.

Разработка модели угроз банка.

Требования к структуре, содержанию, объему, оформлению курсовых работ (курсовых проектов), процедуре защиты, а также критерии оценки определены в:

– стандарте СТУ 02.030 «Курсовые работы (проекты). Выпускные квалификационные работы. Общие требования к структуре и оформлению»;

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

– методических указаниях по выполнению курсовой работы (курсового проекта)

Производственная задача

Провести аудит информационной безопасности компании, исследовать возможные уязвимости в системах и предложить рекомендации по усовершенствованию безопасности.

Кейс

Крупная компания, занимающаяся производством и продажей электронных устройств, столкнулась с серьезной утечкой конфиденциальной информации. Известно, что злоумышленники получили доступ к базе данных клиентов, где были указаны их ФИО, контактные данные, а также информация о приобретенных товарах. В результате этого инцидента многие клиенты начали жаловаться на спам-рассылки и звонки от незнакомых компаний, что серьезно нанесло ущерб репутации компании.

Ваша задача как ответственного за информационную безопасность компании:

1) Собрать и проанализировать данные об инциденте.
2) Оценить уровень ущерба и потенциальных рисков для компании и ее клиентов.
3) Разработать план мероприятий для предотвращения подобных инцидентов в будущем.
4) Организовать и провести обучение сотрудников компании по вопросам информационной безопасности.
5) Внедрить необходимые технические решения и системы защиты данных для повышения уровня безопасности компании.
6) Разработать политику и процедуры по обеспечению безопасности данных, включая вопросы доступа, хранения и передачи конфиденциальной информации.
7) Регулярно проводить мониторинг и аудит безопасности информационных систем компании, чтобы обнаруживать и устранять уязвимости.
8) Провести расследование инцидента, чтобы выяснить причины и обстоятельства утечки информации, а также выявить виновных.

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

7.3.2 Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме экзамена. На промежуточной аттестации по дисциплине применяется механизм квалификационного экзамена. Экзамен имеет структуру квалификационного экзамена и состоит из 2 частей:

- теоретической (компьютерное тестирование);
- практической (решение компетентностно-ориентированной задачи).

На теоретической части экзамена (тестировании) проверяются знания и частично – умения и навыки обучающихся. 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.

На практической части экзамена проверяются компетенции (включая умения, навыки (или опыт деятельности)). Компетенции *(включая умения, навыки (или опыт деятельности))* проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных, кейс-задач или кейсов) 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.

а) Примеры типовых заданий для теоретической части экзамена (тестирования)

Задание в закрытой форме:

1. Руководитель, оценивая результаты создания системы безопасности, прежде всего, должен обратить внимание на:

А) Экономический эффект от внедрения системы.

Б) Функциональную полноту, адаптивность, корректность работы системы.

В) Эффективность использования системой существующей инфраструктуры.

Г) Степень достижения поставленных целей.

Задание в открытой форме:

1. Элементом архитектуры системы безопасности организации является…….

2. Архитектура информационных систем организации включает в себя……..

3. Формальное описание архитектуры предприятия впервые было сформулировано в……...

4. В системном проектировании существуют следующие уровни представления архитектуры ……

Задание на установление правильной последовательности.

Установите последовательность этапов проектирования и разработки защищённой ИС:

1. Внедрение
2. Эксплуатация и модификация
3. Разработка
4. Выявление требований

Задание на установление соответствия:

между ИТ- ресурсами защищённой ИС и описаниями функционирования её элементов

1	Информация	А	Автоматизированные пользовательские системы, которые собирают, хранят, обрабатывают и распространяют информацию
2	Инфраструктура	Б	Данные во всех формах ввода, хранения, обработки и вывода с помощью информационных систем, в любых формах, которые используются для принятия управленческих решений
3	Персонал	В	Средства (аппаратное и программное обеспечение, системы управления базами данных, сеть, мультимедиа, среда, в которой все это функционирует), которые делают возможным работу приложений
		Г	Люди (специалисты), требующиеся для планирования, организации, установки, эксплуатации и развития информационных систем и сервисов, нанимаемые по контрактам

б) Примеры типовых заданий для практической части экзамена

Компетентностно-ориентированная задача:

Компания обладает большим количеством конфиденциальных данных и вы недавно обнаружили случаи утечки данных. Как руководитель отдела информационной безопасности, вы должны разработать и реализовать меры безопасности, чтобы предотвратить будущие утечки данных. Вам нужно определить, какие технические и организационные меры будут приняты, а также определить, кто будет ответственен за их реализацию.

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»;

– положение П 02.207 «Проектирование и реализация основных профессиональных программ высшего образования – программ магистратуры по модели дуального обучения»;

– 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
1	2	3	4	5
Устный опрос по темам 1-3	1	Не ответил или неполно ответил на какой-либо вопрос	2	Правильно и полно ответил на все вопросы
Устный опрос по темам 4-6	1	Не ответил или неполно ответил на какой-либо вопрос	2	Правильно и полно ответил на все вопросы
Устный опрос по темам 7-9	1	Не ответил или неполно ответил на	2	Правильно и полно ответил на все вопро-

		какой-либо вопрос		сы
Практическая работа № 1 «Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение»	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы
Практическая работа № 2 «Определение показателей защищенности информации при несанкционированном доступе»	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы
Практическая работа № 3 «Критерии оценки и выбора CASE-средств»	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы
Практическая работа № 4 «Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности»	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы
Лабораторная работа №1 «Система аудита информационной безопасности ГИС»	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы
Лабораторная работа №2 «Решение ситуационных задач (кейсов)»	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы
Лабораторная работа №3 «Основные методы управления информационной безопасностью в ГИС»	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы
Кейс	4	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	8	Выполнил, правильно и полно ответил на все вопросы
Производственная задача	3	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	6	Выполнил, правильно и полно ответил на все вопросы
Итого	24		48	
Посещаемость	0		16	
Зачёт	0		36	
Итого	24		100	

Для проведения промежуточной аттестации обучающихся (теоретической части и практической части) используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов для тестирования и одна компетентностно-ориентированная 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 по промежуточной аттестации – 36.

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

8.1 Основная учебная литература

1. Анисимов, А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 211 с. — ISBN 978-5-4497-0328-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89443.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. Пользователе

2. Милославская, Н. Г. Управление информационной безопасностью. Конспект лекций : учебное пособие / Н. Г. Милославская, А. И. Толстой. — Москва : Национальный исследовательский ядерный университет «МИФИ», 2020. — 534 с. — ISBN 978-5-7262-2694-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/125513.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

8.2 Дополнительная учебная литература

3. Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2018. — 120 с. — ISBN 978-5-9275-2742-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87643.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

4. Газизов, А. Р. Управление информационной безопасностью : учебное пособие / А. Р. Газизов, С. Б. Петренкова, Д. В. Фатхи. — Ростов-на-Дону : Донской государственный технический университет, 2019. — 115 с. — ISBN 978-5-7890-1775-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/117771.html

(дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/117771

5. Аверченков, В. И. Служба защиты информации. Организация и управление : учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов. — Брянск : Брянский государственный технический университет, 2012. — 186 с. — ISBN 5-89838-138-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/7008.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

8.3 Перечень методических указаний

1. Управление информационной безопасностью : методические указания для самостоятельной работы по изучению дисциплины для студентов направления подготовки (специальности) 10.04.01 «Информационная безопасность» / Юго-Зап. гос. ун-т ; сост. А. Л. Ханис. - Курск : ЮЗГУ, 2021. - 15 с. - Загл. с титул. экрана. - Текст : электронный.

2. Решение ситуационных задач (кейсов) : методические указания по выполнению практической работы по дисциплине «Управление информационной безопасностью» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 для всех форм обучения / Юго-Зап. гос. ун-т ; сост. О. А. Демченко. - Курск : ЮЗГУ, 2017. - 7 с. - Загл. с титул. экрана. - Текст : электронный.

3. Основные методы управления информационной безопасностью в ГИС : методические указания по выполнению практической работы по дисциплине «Управление информационной безопасностью» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 для всех форм обучения / Юго-Зап. гос. ун-т ; сост. О. А. Демченко. - Курск : ЮЗГУ, 2017. - 20 с. - Загл. с титул. экрана. - Текст : электронный.

4. 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. - Курск : ЮЗГУ, 2022. - 11 с. - Загл. с титул. экрана. - Текст : электронный.

9 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/
3. Электронно-библиотечная система «Лань» - http://e.lanbook.com/
4. Электронно-библиотечная система IQLib – http://www.iqlib.ru

5. Электронная библиотека «Единое окно доступа к образовательным ресурсам» - http://window.edu.ru/

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины являются лекции и лабораторные и практические занятия.

На лекциях излагаются и разъясняются основные понятия и положения каждой новой темы; важные положения аргументируются и иллюстрируются примерами из практики; объясняется практическая значимость изучаемой темы; делаются выводы; даются рекомендации для самостоятельной работы по данной теме. На лекциях необходимо задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных вопросов. В ходе лекции студент должен конспектировать учебный материал. Конспектирование лекций – сложный вид работы, предполагающий интенсивную умственную деятельность студента. Конспект является полезным тогда, когда записано самое существенное и сделано это лично студентом в режиме реального времени в течение лекции. Не следует стремиться записать лекцию дословно. Целесообразно вначале понять основную мысль, излагаемую лектором, а затем кратко записать ее. Желательно заранее оставлять в тетради пробелы, куда позднее, при самостоятельной работе с конспектом, можно внести дополнительные записи. Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, который преподаватель дает в начале лекционного занятия. Следует обращать внимание на акценты, выводы, которые делает лектор, отмечая наиболее важные моменты в лекционном материале.

Необходимым является глубокое освоение содержания лекции и свободное владение им, в том числе использованной в ней терминологией. Работу с конспектом лекции целесообразно проводить непосредственно после ее прослушивания, что способствует лучшему усвоению материала, позволяет своевременно выявить и устранить «пробелы» в знаниях. Работа с конспектом лекции предполагает перечитывание конспекта, внесение в него, по необходимости, уточнений, дополнений, разъяснений и изменений. Некоторые вопросы выносятся за рамки лекций. Изучение вопросов, выносимых за рамки лекционных занятий, предполагает самостоятельное изучение студентами дополнительной литературы, указанной в п.8.2.

Изучение наиболее важных тем или разделов дисциплины продолжается на лабораторных и практических занятиях, 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 и практическому 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. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. При работе с источниками и литературой необходимо:

– сопоставлять, сравнивать, классифицировать, группировать, систематизировать информацию в соответствии с определенной учебной задачей;

– обобщать полученную информацию, оценивать прочитанное;

– фиксировать основное содержание прочитанного текста; формулировать устно и письменно основную идею текста; составлять план, формулировать тезисы.

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 освоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю. Обязательным элементом самостоятельной работы по дисциплине является самоконтроль. Одной из важных задач обучения студентов способам и приемам самообразования является формирование у них умения самостоятельно контролировать и адекватно оценивать результаты своей учебной деятельности и на этой основе управлять процессом овладения знаниями. Овладение умениями самоконтроля приучает студентов к планированию учебного труда, способствует углублению их внимания, памяти и выступает как важный фактор развития познавательных способностей. Самоконтроль включает:

– оперативный анализ глубины и прочности собственных знаний и умений;

– критическую оценку результатов своей познавательной деятельности.

Самоконтроль учит ценить свое время, позволяет вовремя заметить и исправить свои ошибки. Формы самоконтроля могут быть следующими:

– устный пересказ текста лекции и сравнение его с содержанием конспекта лекции;

– составление плана, тезисов, формулировок ключевых положений текста по памяти;

– пересказ с опорой на иллюстрации, чертежи, схемы, таблицы, опорные положения.

Самоконтроль учебной деятельности позволяет студенту оценивать эффективность и рациональность применяемых методов и форм умственного труда, находить допускаемые недочеты и на этой основе проводить необходимую коррекцию своей познавательной деятельности.

При подготовке к промежуточной аттестации по дисциплине необходимо повторить основные теоретические положения каждой изученной темы и основные термины, самостоятельно решить несколько типовых компетентностно-ориентированных задач.

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

Информационные технологии:

1. Средства для просмотра презентаций;
2. Средства для проведения онлайн-конференций.
3. Электронно-образовательная среда ЮЗГУ

Программное обеспечение:

1. OpenOffice: режим доступа: свободный.
2. Яндекс.Телемост: режим доступа: свободный.

Информационные справочные системы:

1. Научно-информационный портал ВИНИТИ РАН. Режим доступа: свободный.
2. База данных "Патенты России". Режим доступа: свободный.
3. Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: по подписке.
4. Электронная библиотека диссертаций и авторефератов РГБ. Режим доступа: свободный.
5. Электронный каталог Научной библиотеки ЮЗГУ. Режим доступа: свободный.

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

Аудиторные занятия по дисциплине проводятся в учебной аудитории для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенных стандартной учебной мебелью (столы и стулья для обучающихся; стол и стул для преподавателя; доска).

Для организации образовательного процесса применяются технические средства обучения: Проекционный экран на штативе; Мультимедиа центр: ноутбук ASUS X50VL PMD-T2330/1471024Mb/160Gb/ сумка/ проектор inFocus IN24.

Для осуществления практической подготовки обучающихся при реализации дисциплины используются оборудование и технические средства обучения кафедры информационной безопасности:

1. Класс ПЭВМ - Asus-P7P55LX-/DDR34096Mb/Coree i3-540/SATA-11 500 Gb Hitachi/PCI-E 512Mb, Монитор TFT Wide 23.

2. Мультимедиацентр: ноутбук ASUS X50VL PMD - T2330/14"/1024Mb/ 160Gb/ сумка/проектор inFocus IN24+ .

3. Экран мобильный Draper Diplomat 60x60.

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. 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
	измененных	замененных	аннулированных	новых			