

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Таныгин Максим Олегович

Должность: и.о. декана факультета фундаментальной и прикладной информатики

Дата подписания: 10.09.2023 15:57:04

Уникальный программный ключ:

65ab2aa0d384efe8480e6a4c688eddbc475e411a

Аннотация к рабочей программе дисциплины «Организация работ по обеспечению безопасности в информационных системах»

Цель преподавания дисциплины

Цель дисциплины – формирование у студентов знаний в области работ по обеспечению безопасности в информационных системах, организации мероприятий по защите информации, формирования у коллектива представления о важности защиты персональных данных и конфиденциальной информации для решения задач профессиональной деятельности проектного и организационно-управленческого типов.

Задачи изучения дисциплины

Задачами дисциплины являются:

- 1 Получение углублённых знаний в теме кадровой политики в области информационной безопасности.
- 2 Получение навыков планирования работ по обеспечению информационной безопасности
- 3 Изучение методов решения проблемных ситуаций в коллективе, развитие организаторских навыков в роли руководителя.
4. Совершенствование знаний в сфере нормативно-правовых актов при организации работ по защите информации
5. Получение опыта деятельности в управлении разработкой информационных систем
6. Изучение способов создания комплекса мер по обеспечению информационной безопасности.
7. Изучение порядка разработки модели угроз при построении информационных систем
8. Обеспечение совместно с другими дисциплинами семестра теоретической подготовки обучающихся к производственной практике (исследовательской работе) на предприятии-заказчике.

Индикаторы компетенций, формируемые в результате освоения дисциплины

УК-1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению

УК-1.4 Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов

УК-5.1 Анализирует важнейшие идеологические и ценностные системы, сформировавшиеся в ходе исторического развития; обосновывает актуальность их использования при социальном и профессиональном взаимодействии

УК-5.2 Выстраивает социальное профессиональное взаимодействие с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других этносов и конфессий, различных социальных групп

УК-5.3 Обеспечивает создание недискриминационной среды взаимодействия при выполнении профессиональных задач

ПК-2.1 Формирует технологии, необходимые для функционирования защищённых информационных систем

ПК-2.2 Формирует комплекс мер для защиты информации в защищённых информационных системах

ПК-2.3 Формирует конфигурации и состав обеспечивающей части защищённой информационной системы

ПК-5.1 Определяет перечень объектов информатизации и информации (сведений) ограниченного доступа, подлежащих защите

ПК-5.2 Выявляет степень участия персонала в обработке защищаемой информации

ПК-5.3 Разрабатывает отчетные документы и разделы технических заданий

Разделы дисциплины

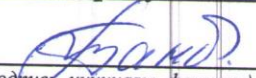
Кадровая политика в области информационной безопасности. Методы планирования работ по обеспечению информационной безопасности. Методы решения проблемных ситуаций в коллективе. Применение нормативно-правовых актов при организации работ по защите информации. Управление разработкой информационных систем. Формирование комплекса мер по обеспечению информационной безопасности. Порядок разработки модели угроз при построении информационных систем.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:

Декан факультета ФиПИ


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

« 30 » мая 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Организация работ по обеспечению безопасности в информационных системах

(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 – формирование у студентов знаний в области работ по обеспечению безопасности в информационных системах, организации мероприятий по защите информации, формирования у коллектива представления о важности защиты персональных данных и конфиденциальной информации для решения задач профессиональной деятельности проектного и организационно-управленческого типов.

1.2 Задачи дисциплины

Задачами дисциплины являются:

- 1 Получение углублённых знаний в теме кадровой политики в области информационной безопасности.
- 2 Получение навыков планирования работ по обеспечению информационной безопасности
- 3 Изучение методов решения проблемных ситуаций в коллективе, развитие организаторских навыков в роли руководителя.
4. Совершенствование знаний в сфере нормативно-правовых актов при организации работ по защите информации
5. Получение опыта деятельности в управлении разработкой информационных систем
6. Изучение способов создания комплекса мер по обеспечению информационной безопасности.
7. Изучение порядка разработки модели угроз при построении информационных систем
8. Обеспечение совместно с другими дисциплинами семестра теоретической подготовки обучающихся к производственной практике (исследовательской работе) на предприятии-заказчике.

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

Таблица 1.3 – Результаты обучения по дисциплине

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>	<i>Код и наименование индикатора достижения компетенции, закрепленного</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
---	--	--

код компетенции	наименование компетенции	за дисциплиной	
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий	<p>УК-1.2</p> <p>Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению</p>	<p>Знать: ряд проблемных ситуаций, которые могут возникать на предприятии</p> <p>Уметь: находить выход из сложившейся ситуации путём анализа опыта предыдущих проблем и конкурирующих организаций</p> <p>Владеть (или Иметь опыт деятельности): проектирования процессов исправления возникающего ряда трудностей в управлении</p>
		<p>УК-1.4</p> <p>Разрабатывает и содержит аргументированную стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов</p>	<p>Знать: принципы построения защищённых систем, методы и средства защиты операционных систем, сетевого оборудования, управления доступом, идентификации и аутентификации, настройки межсетевых экранов, защиты от компьютерных вирусов, вопросы организации системы защиты информации в информационных системах (ИС), этапы построения системы защиты информации, политики безопасности, виды угроз и возможные каналы утечки информации, основы проектирования и построения архитектур систем безопасности, методы, модели и технологии проектирования систем безопасности, требования стандартов и руководящих документов, стадии и этапы создания систем безопасности.</p> <p>Уметь: правильно эксплуатировать антивирусные программные комплексы, снижать вероятность отрицательных последствий сетевых атак путём правильной настройки операционной системы, применять</p>

<p>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</p>		<p>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</p>	<p>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</p>
код компетенции	наименование компетенции		
			<p>средства защиты информации для решения практических задач в области информационной безопасности.</p> <p>Владеть (или Иметь опыт деятельности): навыками применения программных средств защиты информации, разработки защищенных сайтов, разработки архитектуры инфокоммуникационных систем и сетевой защиты, поиска и обнаружения уязвимых узлов инфокоммуникационных систем и сетей.</p>
УК-5	<p>Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия</p>	<p>УК – 5.1 Анализирует важнейшие идеологические и ценностные системы, сформировавшиеся в ходе исторического развития; обосновывает актуальность их использования при социальном и профессиональном взаимодействии</p>	<p>Знать: историческое наследие и социокультурные традиции различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения</p> <p>Уметь: ориентироваться в историческом наследии и социокультурных традициях различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения</p> <p>Владеть (или Иметь опыт деятельности): навыками социального и профессионального общения, учитывая историческое наследие и социокультурные традиции различных социальных групп, этносов и конфессий, включая мировые религии, философские и этические учения</p>

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		
		<p>УК – 5.2 Выстраивает социальное профессиональное взаимодействие с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других этносов и конфессий, различных социальных групп</p>	<p>Знать: основные формы научного и религиозного сознания, общую культуру представителей других этносов и конфессий, различных социальных групп Уметь: выстраивать отношения с каждым представителем области профессиональных интересов, уметь наладить работу в коллективе из людей разных этносов и пр. Владеть (или Иметь опыт деятельности): навыками социального профессионального взаимодействия с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других этносов и конфессий, различных социальных групп</p>
		<p>УК – 5.3 Обеспечивает создание недискриминационной среды взаимодействия при выполнении профессиональных задач</p>	<p>Знать: принципы недискриминационного взаимодействия при личном и массовом общении Уметь: определять принципы недискриминационного взаимодействия при личном и массовом общении Владеть: навыками недискриминационного взаимодействия в целях выполнения профессиональных задач</p>
ПК-2	Способен организовывать работы по выполнению требований защиты информации ограниченного доступа в	ПК-2.1 Формирует технологии, необходимые для функционирования защищённых информационных систем	<p>Знать: нормативную базу, регламентирующую создание и эксплуатацию ЗИС, принципы эксплуатации и сопровождения ЗИС. Уметь: выбирать эффек-</p>

<p>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</p>		<p>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</p>	<p>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</p>
код компетенции	наименование компетенции		
	защищённых информационных системах		<p>тивную технологию функционирования ЗИС на базе моделирования.</p> <p>Владеть (или Иметь опыт деятельности): навыками формирования технологии функционирования ЗИС</p>
		<p>ПК-2.2 Формирует комплекс мер для защиты информации в защищённых информационных системах</p>	<p>Знать: правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности в защищённых информационных системах</p> <p>Уметь: - формулировать правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности в защищённых информационных системах</p> <p>Владеть (или Иметь опыт деятельности): -навыками разработки мер защиты информации, правил применения мер защиты информации, направленных на устранение причин возникновения инцидентов информационной безопасности в защищённых информационных системах</p>
		<p>ПК-2.3 Формирует конфигурации и состав обеспечивающей части защищённой информационной системы</p>	<p>Знать: структуру функциональной и обеспечивающих частей ЗИС, методы проектирования ЗИС</p> <p>Уметь: производить сравнительный анализ вариан-</p>

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		
			тов конфигураций и состава обеспечивающей части ЗИС Владеть (или Иметь опыт деятельности): формирования конфигурации и состава обеспечивающей части ЗИС
ПК-5	Способен обеспечивать документальное сопровождение процесса обеспечения информационной безопасности	ПК-5.1 Определяет перечень объектов информатизации и информации (сведений) ограниченного доступа, подлежащих защите	Знать: принципы организации телекоммуникационных систем и их уязвимости. Уметь: формулировать технические требования к телекоммуникационным системам и мерам по предотвращению уязвимостей. Владеть (или Иметь опыт деятельности): навыками создания моделей угроз и моделей злоумышленника для телекоммуникационных систем и устройств.
		ПК-5.2 Выявляет степень участия персонала в обработке защищаемой информации	Знать: принципы формирования политики информационной безопасности в автоматизированных системах, организационные меры по защите информации Уметь: определять класс защищенности автоматизированных систем и ее составных частей Владеть (или Иметь опыт деятельности): выявление степени участия персонала в обработке защищаемой информации
		ПК-5.3 Разрабатывает отчетные документы и раз-	Знать: порядок внедрения, отладки и развития процессов 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		
		дела технических заданий	<p>этапов разработки требований, задач, критериев качества и методов обеспечения информационной безопасности защищённых ТКС в процессе их эксплуатации и модернизации.</p> <p>Уметь: организовать и управлять внедрением, отладкой и развитием процессов и этапов работ, методов обеспечения информационной безопасности защищённых ТКС в процессе их эксплуатации и модернизации.</p> <p>Владеть (или Иметь опыт деятельности): : навыками организации и управления внедрением, отладкой и развитием процессами и этапами разработки системобеспечения информационной безопасности ТКС в процессе их эксплуатации и модернизации.</p>

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Организация работ по обеспечению безопасности в информационных системах» входит в часть, формируемую участниками образовательных отношений 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 в 1 семестре.

Дисциплина имеет практико-ориентированный характер и изучается до прохождения обучающимися производственной практики (исследовательской работы), 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 зачетные единицы (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)	90
в том числе:	
лекции	36
лабораторные занятия	-
практические занятия	54, из них практическая подготовка обучающихся – 4.
Самостоятельная работа обучающихся (всего)	52,85
Контроль (подготовка к экзамену)	36
Контактная работа по промежуточной аттестации (всего АттКР)	1,15
в том числе:	
зачет	не предусмотрен
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрен(-а)
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	Кадровая политика в области информационной безопасности	Цель и задачи кадрового обеспечения в ООО ЦСБ «ЩИТ-ИНФОРМ». Основные принципы подготовки кадров в ООО ЦСБ «ЩИТ-ИНФОРМ». Виды преступлений и правонарушений так или иначе связаны с конкретными действиями сотрудников коммерческих структур. Программа работы с персоналом в ООО ЦСБ «ЩИТ-ИНФОРМ».

2	Методы планирования работ по обеспечению информационной безопасности	Организационные методы, инженерно-технические методы, технические методы, программно-аппаратные методы обеспечения информационной безопасности в ООО ЦСБ «ЩИТ-ИНФОРМ». Комплексный подход: использование нескольких способов защиты информации.
3	Методы решения проблемных ситуаций в коллективе	Типы конфликтов в коллективе. Причины, порождающие конфликты. Меры по предотвращению и разрешению конфликтных ситуаций в ООО ЦСБ «ЩИТ-ИНФОРМ».
4	Применение нормативно-правовых актов при организации работ по защите информации	Виды юридических документов, посвященных защите информации. Содержание законов, касающихся охраны секретных материалов. Федеральные законы, касающиеся защиты информации и информационной безопасности в ООО ЦСБ «ЩИТ-ИНФОРМ».
5	Управление разработкой информационных систем	Принципы создания информационной системы. Структура среды информационной системы. Модель создания информационной системы. Реинжиниринг бизнес-процессов. Внедрение информационных систем в ООО ЦСБ «ЩИТ-ИНФОРМ».
6	Формирование комплекса мер по обеспечению информационной безопасности	Концепция безопасности. Объекты защиты. Меры по обеспечению информационной безопасности. Организационные и технические меры обеспечения информационной безопасности предприятия в ООО ЦСБ «ЩИТ-ИНФОРМ».
7	Порядок разработки модели угроз при построении информационных систем	Принципы разработки модели угроз безопасности информации. Методы выявления и анализа угроз безопасности информации и уязвимостей программного обеспечения в ООО ЦСБ «ЩИТ-ИНФОРМ». Характеристика степени ущерба. Вероятность реализации угроз.

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	Кадровая политика в области информационной безопасности	4		1	У-1-5 МУ-1-2	УО, ЗПР, ПЗ 1-2	УК-1 УК-5 ПК-2 ПК-5
2	Методы планирования работ по обеспечению информационной безопасности	4		2	У-1-5 МУ-1-2	УО, ЗПР, КЗ 3-4	УК-1 УК-5 ПК-2 ПК-5
3	Методы решения проблемных ситуаций в коллективе	4		3	У-1-5 МУ-1-2	УО, ЗПР 5-6	УК-1 УК-5 ПК-2 ПК-5
4	Применение нормативно-правовых актов при организации работ по защите информации	6		4	У-1-5 МУ-1-2	УО, ЗПР 7-8	УК-1 УК-5 ПК-2 ПК-5
5	Управление разра-	6		5	У-1-5	УО, ЗПР	УК-1

	боткой информационных систем				МУ-1-2	9-10	УК-5 ПК-2 ПК-5
6	Формирование комплекса мер по обеспечению информационной безопасности	6		6	У-1-5 МУ-1-2	УО, ЗПР 11-12	УК-1 УК-5 ПК-2 ПК-5
7	Порядок разработки модели угроз при построении информационных систем	6		7	У-1-5 МУ-1-2	УО, ЗПР 13-14	УК-1 УК-5 ПК-2 ПК-5

УО – устный опрос, ЗПР – защита практической работы, ПЗ – решение производственных задач; КЗ – решение кейса.

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические занятия

Таблица 4.2.1 – Практические занятия

№	Наименование практической работы	Объем, час.
1	2	3
1	Система анализа рисков и проверки политики информационной безопасности предприятия	8, из них практическая подготовка обучающихся – 4
2	Моделирование объектов защиты	8
3	Организационная культура и управление конфликтами	6
4	Работа с нормативно-правовыми документами	8
5	Разработка организационных и технических мер по инженерно-технической защите информации	8
6	Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение	8
7	Разработка модели угроз информационной безопасности	8
Итого		54, из них практическая подготовка обучающихся – 4

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	2	3	4
1.	Кадровая политика в области информационной безопасности	1-2 недели	6
2.	Методы планирования работ по обеспечению информационной безопасности	3-4 недели	6
3.	Методы решения проблемных ситуаций в коллективе	5-6 недели	8
4.	Применение нормативно-правовых актов при организации работ по защите информации	7-8 недели	8
5.	Управление разработкой информационных систем	9-10 недели	8
6.	Формирование комплекса мер по обеспечению информационной безопасности	11-12 недели	8
7.	Порядок разработки модели угроз при построении информационных систем	13-14 недели	8,85
Итого			52,85

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 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 профессиональных 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	Методы планирования работ по обеспечению информационной безопасности	Кейс-технология	2
2	Моделирование объектов защиты	Кейс-технология	8
Итого:			10

Практическая подготовка обучающихся при реализации дисциплины осуществляется путем проведения или 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 включает в себя отдельные занятия лекционного типа, которые проводятся на предприятии-заказчике и предусматривают передачу учебной информации обучающимся, необходимой для последующего выполнения работ, связанных с будущей профессиональной деятельностью, на производственной практике (исследовательской работе), которой завершается данный семестр.

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-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Современная философия и методология науки Прикладные математические задачи информационной безопасности Организация работ по обеспечению безопасности в информационных системах	Управление разработкой систем безопасности	
УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	Современная философия и методология науки Организация работ по обеспечению безопасности в информационных системах		
ПК-2 Способен организовать работы по выполнению требований защиты информации ограниченного доступа в защищённых информационных системах	Организация работ по обеспечению безопасности в информационных системах	Технологии распределённых реестров Безопасность распределённых систем	Методы и средства защиты информации в системах электронного документооборота Производственная проектно-технологическая практика Производственная преддипломная практика
ПК-5 Способен обеспечивать документальное сопровождение процесса обеспечения информационной безопасности	Организация работ по обеспечению безопасности в информационных системах Организация аудита информационной безопасности Нормативно-правовое регулирование в сфере информационной безопасности	Производственная практика по получению умений и навыков управленческой деятельности	Производственная преддипломная практика

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

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап (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-1/ начальный	<p>УК-1.2 Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению</p> <p>УК-1.4 Разрабатывает и содержит аргументированно стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов</p>	<p>Знать: демонстрирует менее 60% знаний, указанных в таблице 1.3 для УК-1. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.</p>	<p>Знать: демонстрирует 60-74% знаний, указанных в таблице 1.3 для УК-1. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.</p>	<p>Знать: демонстрирует 75-89% знаний, указанных в таблице 1.3 для УК-1. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.</p>	<p>Знать: демонстрирует 90-100% знаний, указанных в таблице 1.3 для УК-1. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.</p>
		<p>Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для УК-1.</p>	<p>Уметь: в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для УК-1.</p>	<p>Уметь: сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для УК-1.</p>	<p>Уметь: хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для УК-1.</p>
		<p>Владеть (или Иметь опыт деятельности)</p>	<p>Владеть (или Иметь опыт дея-</p>	<p>Владеть (или Иметь опыт деятельности)</p>	<p>Владеть (или Иметь опыт деятельности)</p>

		сти): навыки, указанные в таблице 1.3 для УК-1, не развиты.	тельно-сти): навыки, указанные в таблице 1.3 для УК-1, развиты на элементарном уровне.	сти): навыки, указанные в таблице 1.3 для УК-1, хорошо развиты.	сти): навыки, указанные в таблице 1.3 для УК-1, доведены до автоматизма.
УК-5/ началь- ный	УК-5.1 Анализирует важнейшие идеологические и ценностные системы, сформировавшиеся в ходе исторического развития; обосновывает актуальность их использования при социальном и профессиональном взаимодействии УК-5.2 Выстраивает социальное профессиональное взаимодействие с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представи-	Знать: демонстрирует менее 60% знаний, указанных в таблице 1.3 для УК-5. 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-5. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	Знать: демонстрирует 75-89% знаний, указанных в таблице 1.3 для УК-5. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	Знать: демонстрирует 90-100% знаний, указанных в таблице 1.3 для УК-5. 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-5.	Уметь: в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для УК-5.	Уметь: сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для УК-5.	Уметь: хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для УК-5.
		Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для УК-5, не развиты.	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для УК-5, развиты на элементарном уровне.	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для УК-5, хорошо развиты.	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для УК-5, доведены до автоматизма.

	<p>телей других этносов и конфессий, различных социальных групп</p> <p>УК-5.3 Обеспечивает создание недискриминационной среды взаимодействия при выполнении профессиональных задач</p>				
ПК-2/ начальный	<p>ПК-2.1 Формирует технологии, необходимые для функционирования защищённых информационных систем</p> <p>ПК-2.2 Формирует комплекс мер для защиты информации в защищённых информационных системах</p> <p>ПК-2.3 Формирует конфигурации и состав бес-</p>	<p>Знать: демонстрирует менее 60% знаний, указанных в таблице 1.3 для ПК-2. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.</p> <p>Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для ПК-2.</p>	<p>Знать: демонстрирует 60-74% знаний, указанных в таблице 1.3 для ПК-2. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.</p> <p>Уметь: в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ПК-2.</p>	<p>Знать: демонстрирует 75-89% знаний, указанных в таблице 1.3 для ПК-2. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.</p> <p>Уметь: сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ПК-2.</p>	<p>Знать: демонстрирует 90-100% знаний, указанных в таблице 1.3 для ПК-2. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.</p> <p>Уметь: хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ПК-2.</p>

	печивающей части защищённой информационной системы	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для ПК-2, не развиты.	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для ПК-2, развиты на элементарном уровне.	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для ПК-2, хорошо развиты.	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для ПК-2, доведены до автоматизма.
ПК-5/ начальный	ПК-5.1 Определяет перечень объектов информатизации и информации (сведений) ограниченного доступа, подлежащих защите	Знать: демонстрирует менее 60% знаний, указанных в таблице 1.3 для ПК-5. Обучающийся нуждается в постоянных подсказках; допускает грубые ошибки, которые не может исправить самостоятельно.	Знать: демонстрирует 60-74% знаний, указанных в таблице 1.3 для ПК-5. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	Знать: демонстрирует 75-89% знаний, указанных в таблице 1.3 для ПК-5. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	Знать: демонстрирует 90-100% знаний, указанных в таблице 1.3 для ПК-5. Знания обучающегося являются прочными и глубокими, имеют системный характер. Обучающийся свободно оперирует знаниями.
	ПК-5.2 Выявляет степень участия персонала в обработке защищаемой информации	Уметь: демонстрирует менее 60% умений, установленных в таблице 1.3 для ПК-5.	Уметь: в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ПК-5.	Уметь: сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ПК-5.	Уметь: хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ПК-5.
	ПК-5.3 Разрабатывает отчетные документы и разделы технических заданий	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для ПК-5, не развиты.	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для ПК-5, развиты на	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для ПК-5, хорошо развиты.	Владеть (или Иметь опыт деятельности): навыки, указанные в таблице 1.3 для ПК-5, доведены до автоматизма.

			элементарном уровне.		
--	--	--	----------------------	--	--

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 ее части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Кадровая политика в области информационной безопасности	УК-1 УК-5 ПК-2 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО КВЗП Производственная задача	1-10 1-10 1-10	Согласно табл.7.2
2	Методы планирования работ по обеспечению информационной безопасности	УК-1 УК-5 ПК-2 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО КВЗП Кейс	1-10 1-10 1-2	Согласно табл.7.2
3	Методы решения проблемных ситуаций в коллективе	УК-1 УК-5 ПК-2 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО КВЗП	1-10 1-10	Согласно табл.7.2
4	Применение нормативно-правовых актов при организации работ по защите информации	УК-1 УК-5 ПК-2 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО КВЗП	1-10 1-10	Согласно табл.7.2
5	Управление разработкой информационных систем	УК-1 УК-5 ПК-2 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО КВЗП	1-10 1-10	Согласно табл.7.2
6	Формирование комплекса мер по обеспечению информационной безопасности	УК-1 УК-5 ПК-2 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО КВЗП	1-10 1-10	Согласно табл.7.2

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или ее части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
7	Порядок разработки модели угроз при построении информационных систем	УК-1 УК-5 ПК-2 ПК-5	лекция, практическое занятие, СРС	Вопросы для УО КВЗПР	1-10 1-10	Согласно табл.7.2

КВЗПР – контрольные вопросы для защиты практической работы

7.3.1 Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу (теме) 1. «Кадровая политика в области информационной безопасности»:

1. Что такое «политика безопасности»?
2. От каких факторов зависит выбор персонала?
3. Какие существуют механизмы обеспечения безопасности в распределённых системах?
4. Что такое требования доверия безопасности и для чего они нужны?
5. Задачи, возникающие при выполнении информационно-аналитической работы

Контрольные вопросы для защиты практической работы №1:

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

Производственная задача по теме 1

Задача разработки политики резервного копирования и восстановления: Разработайте политику резервного копирования и восстановления данных компании. Определите частоту и методы резервного копирования, хранение резервных копий и процедуры восстановления данных в случае чрезвычайных ситуаций.

Кейс по теме 2

Компания XYZ является крупным финансовым учреждением, которое хранит и обрабатывает большое количество конфиденциальной информации о клиентах. В последнее время наблюдается увеличение угроз безопасности,

связанных с хакерскими атаками и утечками данных. Ваша задача - организовать работы по обеспечению безопасности в информационных системах компании XYZ.

Для этого необходимо провести следующие мероприятия:

1. Анализ уязвимостей: Проведите комплексный анализ уязвимостей информационных систем компании XYZ. Исследуйте сетевую инфраструктуру, приложения, серверы и рабочие станции на предмет возможных уязвимостей. Создайте отчет о найденных уязвимостях и определите приоритеты для их устранения.

2. Разработка политики безопасности: Разработайте политику безопасности для компании XYZ, учитывая специфику финансовой индустрии и требования соответствующих регуляторов. Определите правила и процедуры, касающиеся доступа к системам, защиты паролей, шифрования данных, управления учетными записями и резервного копирования.

3. Защита периметра: Организуйте защиту периметра сети компании XYZ. Разработайте и реализуйте систему брандмауэров, интра-систем и внутренней сетевой сегментации, чтобы предотвратить несанкционированный доступ к системам и данным.

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 результаты практической подготовки: *компетенции, включая умения, навыки (или опыт деятельности)*). Результаты практической подготовки (*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:

В обязанности какого сотрудника входит разработка и поддержка эффективных мер защиты по обработке информации для обеспечения сохранное данных

- 1) Сотрудник группы безопасности
- 2) Администратор безопасности системы
- 3) Администратор безопасности данных
- 4) Руководитель группы

Задание в открытой форме:

Все нарушения единого информационного процесса на предприятии связаны с материальных ценностей: бумажных и электронных носителей информации, компьютеров и периферийного оборудования.

Задание на установление правильной последовательности:

Обследование состояния объекта и уровня организации защиты информации, разработка и обоснование задач по защите информации, выявление потенциально возможных угроз информации, внедрение системы защиты информации, анализ безопасности используемых для передачи конфиденциальной информации линий связи.

Задание на установление соответствия:

1. режимно-секретное подразделение;
2. бюро пропусков;
3. контрольно-пропускной пункт (КПП).

А) отвечает за выполнение комплекса мероприятий по пропускному режиму и осуществляют постоянный контроль над их выполнением

Б) служат для непрерывного осуществления пропускного режима на территорию и объекты предприятия, контролируют вход и выход лиц с территории предприятия

В) решает непосредственно задачи по учету, хранению, уничтожению и выдаче пропусков сотрудникам предприятия, а также другим лицам, имеющим на это право

б) Примеры типовых заданий для практической части экзамена

Компетентностно-ориентированная задача:

Провести анализ потенциальных каналов утечки в аудитории проведения занятий. Составить перечень каналов утечки информации на защищаемом объекте с указанием места расположения и предлагаемые технические и организационные меры противодействия.

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
Практическая работа № 1-7	8	Выполнил, но не ответил или неполно ответил на какой-либо вопрос по работе	16	Выполнил, правильно и полно ответил на все вопросы по работе
Устный опрос по темам 1-7	8	Не ответил или неполно ответил на какой-либо вопрос	16	Правильно и полно ответил на все вопросы
Производственная задача	4	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	8	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
Итого	24		48	
Посещаемость	0		16	
Экзамен	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. Гулак, М. Л. Аудит информационной безопасности. Прикладная статистика : учебное пособие / М. Л. Гулак, М. Ю. Рытов, О. М. Голембиовская. — Москва : Ай Пи Ар Медиа, 2020. — 121 с. — ISBN 978-5-4497-0713-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/97630.html> (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

2. 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. Пользователей

8.2 Дополнительная учебная литература

3. Мартынов, А. П. Информационная безопасность и защита информации : учебное пособие / А. П. Мартынов, И. А. Мартынова, А. А. Русаков. — Москва : Ай Пи Ар Медиа, 2023. — 122 с. — ISBN 978-5-4497-2247-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/131797.html> (дата обращения: 04.10.2023). — Режим доступа: для авторизир. пользователей. - DOI: <https://doi.org/10.23682/131797>

4. Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко. — Ставрополь : Северо-Кавказский федеральный университет, 2015. — 222 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/63138.html> (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

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. Организация работ по обеспечению безопасности в информационных системах: методические указания по выполнению практических работ / Юго-

Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 41 с.: Библиогр.: с. 40. – Текст : электронный.

2. Организация работ по обеспечению безопасности в информационных системах: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 9с.: Библиогр.: с. 9. – 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 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 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.

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, способ-

ствуется 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 ВИНТИ 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 звукозаписи-

вающих 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, прочесть 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			