Аннотация к рабочей программе дисциплины «Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем»

Цель преподавания дисциплины

Цель дисциплины – введение студентов в современную проблематику теории экспертных систем посредством решения теоретических и прикладных задач оценки надежности защиты информационных и телекоммуникационных систем. Дисциплина нацелена на подготовку студентов к освоению принципов функционирования и построения экспертных систем, способных осуществлять комплексную оценку безопасности современных автоматизированных информационных и телекоммуникационных систем, решению задач принятия решений в условиях риска и неопределенности, используя различные критерии, для решения задач профессиональной деятельности контрольно-аналитического типа.

Задачи изучения дисциплины

Задачами дисциплины являются:

1. Понимание угроз, рисков и атак на информационные и телекоммуникационные системы.
2. Ознакомление с основными классами технологий, методов и алгоритмов экспертных систем комплексной оценки безопасности.
3. Подготовка к научным исследованиям с использованием и разработкой экспертных систем, а также приобретение навыков применения в инженерной практике современных интеллектуальных систем в области защиты информации.
4. Обеспечение совместно с другими дисциплинами семестра теоретической подготовки обучающихся к производственной эксплуатационной практике на предприятии-заказчике.

Индикаторы компетенций, формируемые в результате освоения дисциплины

ПК-6.1 Формирует перечень угроз для защищаемой информационной системы

ПК-6.2 Формирует критерии оценки каждого вида угроз в защищаемой системе

ПК-6.3 Формирует перечень нарушителей информационной безопасности в защищаемой системе

Разделы дисциплины

Основы безопасности информационных, автоматизированных и телекоммуникационных систем. Экспертные системы информационных систем. Искусственный интеллект в экспертных системах. Нечеткая логика в экспертных системах. Экспертиза криптографических систем 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

Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем
(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., доцент _____ А.Л. Марухленко

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 – введение студентов в современную проблематику теории экспертных систем посредством решения теоретических и прикладных задач оценки надежности защиты информационных и телекоммуникационных систем. Дисциплина нацелена на подготовку студентов к освоению принципов функционирования и построения экспертных систем, способных осуществлять комплексную оценку безопасности современных автоматизированных информационных и телекоммуникационных систем, решению задач принятия решений в условиях риска и неопределенности, используя различные критерии, для решения задач профессиональной деятельности контрольно-аналитического типа.

1.2 Задачи дисциплины

Задачами дисциплины являются:

1. Понимание угроз, рисков и атак на информационные и телекоммуникационные системы.
2. Ознакомление с основными классами технологий, методов и алгоритмов экспертных систем комплексной оценки безопасности.
3. Подготовка к научным исследованиям с использованием и разработкой экспертных систем, а также приобретение навыков применения в инженерной практике современных интеллектуальных систем в области защиты информации.
4. Обеспечение совместно с другими дисциплинами семестра теоретической подготовки обучающихся к производственной эксплуатационной практике 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

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код комп-ии	*наименование компетенции*		

ПК-6	Способен управлять рисками информационной безопасности	ПК-6.1 Формирует перечень угроз для защищаемой информационной системы	***Знать:*** Методику анализа перечня угроз для защищаемой информационной системы ***Уметь:*** Анализировать и формировать перечень угроз для защищаемой информационной системы. ***Владеть (или Иметь опыт деятельности):*** методом формулировки перечня угроз для защищаемой информационной системы.
		ПК-6.2 Формирует критерии оценки каждого вида угроз в защищаемой системе	***Знать:*** Методику формирования критериев оценки каждого вида угроз в защищаемой системе. ***Уметь:*** Анализировать критерии оценки каждого вида угроз в защищаемой системе. ***Владеть (или Иметь опыт деятельности):*** Навыками формирования критериев оценки каждого вида угроз в защищаемой системе.
		ПК-6.3 Формирует перечень нарушителей информационной безопасности в защищаемой системе	***Знать:*** Методику анализа формирования перечня нарушителей информационной безопасности и их возможностей. ***Уметь:*** Анализировать и формировать перечень нарушителей информационной безопасности и их возможностей. ***Владеть (или Иметь опыт деятельности):*** Навыками формирования перечня нарушителей информационной безопасности и их возможностей.

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем» входит в часть, формируемую участниками образовательных отношений, блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы магистратуры 10.04.01 Наименование направления подготовки, направленность (профиль) «Информационная безопасность», реализуемой по модели дуального обучения.

Дисциплина изучается на 2 курсе в 3 семестре.

Дисциплина имеет практико-ориентированный характер и изучается до прохождения обучающимися производственной эксплуатационной практики, 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 3 зачетные единицы (з.е.), 108 академических часов.

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	54
в том числе:	
лекции	18
лабораторные занятия	
практические занятия	36, из них практическая подготовка обучающихся – 4.
Самостоятельная работа обучающихся (всего)	53,9
Контроль (подготовка к экзамену)	-
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрен(-а)
экзамен (включая консультацию перед экзаменом)	не предусмотрен

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	Основы безопасности информационных, автоматизированных и телекоммуникационных систем.	Основные понятия в области безопасности информационных технологий. Угрозы безопасности информационных технологий. Оценка рисков. Принципы обеспечения безопасности информационных технологий. Основные цели обеспечения информационной безопасности. Комплексный подход обеспечения информационной безопасности на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Защита информации на примере ООО ЦСБ «ЩИТ-ИНФОРМ».

2	Экспертные системы информационных систем.	Введение в экспертные системы. Требования к экспертным системам. Экспертные системы информационной безопасности как часть информационных, автоматизированных и телекоммуникационных систем на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Роли эксперта, инженера знаний и пользователя. Общее описание архитектуры экспертных систем. База знаний, правила, машина вывода, интерфейс пользователя, средства работы с файлами.
3	Искусственный интеллект в экспертных системах.	Базы данных, ориентированные на искусственный интеллект: Экспертные системы и их особенности с точки зрения интеллекта. Основные типы задач, решаемых с помощью экспертных систем. Особенности разработки экспертных систем . Виды экспертных систем. Представление знаний в системах искусственного интеллекта. Организация принятия решений в экспертных системах на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Организация логического вывода в экспертных системах. Правила. Поиск решений. Управляющая структура. Технология принятия решений в системах с базами знаний. Методы поиска, реализованные в экспертных системах на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Использование процедур. Представление неопределённости в информационных приложениях с базами знаний.
4	Нечеткая логика в экспертных системах.	Понятие о нечетких множествах и их связь с теорией построения экспертных систем. Коэффициенты уверенности. Взвешивание свидетельств. Отношение правдоподобия гипотез. Функция принадлежности элемента подмножеству. Операции над нечеткими множествами. Дефаззификация нечеткого множества. Нечеткие правила вывода в экспертных системах на примере ООО ЦСБ «ЩИТ-ИНФОРМ».
5	Экспертиза криптографических систем защиты информации.	Криптографическая защита информации на примере ООО ЦСБ «ЩИТ-ИНФОРМ». Основы криптографии. Симметричные криптосистемы. Криптосистемы с открытым ключом. Системы электронной подписи. Криптоанализ. Экспертная система оценки стойкости криптосистем.

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	Основы безопасности информационных, автоматизированных и телекоммуникационных систем.	2	-	-	У-1-5 МУ-2	УО (1-2)	ПК-6
2	Экспертные системы информационных систем.	2	1	-	У-1-5 МУ-1-2	УО, ЗПР (3-5)	ПК-6
3	Искусственный интел-	4	2	-	У-1-5	УО, ЗПР,	ПК-6

	лект в экспертных системах.				МУ-1-2	КЗ (6-8)	
4	Нечеткая логика в экспертных системах.	4	3	-	У-1-5 МУ-1-2	УО, ЗПР, КЗ (9-11)	ПК-6
5	Экспертиза криптографических систем защиты информации.	4	4	-	У-1-5 МУ-1-2	УО, ЗПР, ПЗ (12-13)	ПК-6

УО – устный опрос; ПЗ – решение производственных задач; ЗПР – защита практической работы; 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	«Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации».	8
2	«Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности».	8
3	«Анализ заданного нормативно-правового акта Российской Федерации».	10
4	«Определение класса государственной информационной системы (ГИС)».	10, из них практическая подготовка обучающихся – 4
Итого		36, 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.	Основы безопасности информационных, автоматизированных и телекоммуникационных систем.	1-2 недели	10
2.	Экспертные системы информационных систем.	4-5 недели	10
3.	Искусственный интеллект в экспертных	6-8	10

	системах.	недели	
4.	Нечеткая логика в экспертных системах.	9-11 недели	10
5.	Экспертиза криптографических систем защиты информации.	12-14 недели	13,9
Итого			53,9

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 об-

разовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования 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	Организация вывода нечеткой логики в экспертных системах.	Кейс-технология	8
2	Экспертные системы на основе логического программирования.	Кейс-технология	8
Итого:			16

Практическая подготовка обучающихся при реализации дисциплины осуществляется путем проведения 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 формирования компетенций и дисциплины (модули), практики, при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-6 Способен управлять рисками информационной безопасности	Оценка защищённости информационных систем Теоретические основы компьютерной безопасности Информационно-аналитические системы безопасности Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем Производственная эксплуатационная практика 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

ПК-6/ завершающий	ПК-6.1 Формирует перечень угроз для защищаемой информационной системы ПК-6.2 Формирует критерии оценки каждого вида угроз в защищаемой системе ПК-6.3 Формирует перечень нарушителей информационной безопасности в защищаемой системе	**Знать:** демонстрирует менее 60% знаний, указанных в таблице 1.3 для ПК-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 ПК-6. Знания обучающегося имеют поверхностный характер, имеют место неточности и ошибки.	**Знать:** демонстрирует 75-89% знаний, указанных в таблице 1.3 для ПК-6. Обучающийся имеет хорошие, но не исчерпывающие знания; допускает неточности.	**Знать:** демонстрирует 90-100% знаний, указанных в таблице 1.3 для ПК-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 ПК-6.	**Уметь:** в целом сформированные, но вызывающие затруднения при самостоятельном применении умения, указанные в таблице 1.3 для ПК-6.	**Уметь:** сформированные и самостоятельно применяемые умения, указанные в таблице 1.3 для ПК-6.	**Уметь:** хорошо развитые, уверенно и успешно применяемые умения, указанные в таблице 1.3 для ПК-6.
		Владеть (*или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-6, не развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-6, развиты на элементарном уровне.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-6, хорошо развиты.	***Владеть (****или* ***Иметь опыт деятельности):*** навыки, указанные в таблице 1.3 для ПК-6, 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 ее части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Основы безопасности информационных, автоматизированных и телекоммуникационных систем.	ПК-6	Лекция, СРС	Вопросы для УО	1-10	Согласно табл.7.2
2	Экспертные системы информационных систем.	ПК-6	Лекция, СРС, практическая работа	Вопросы для УО КВЗПР	1-10 1-10	Согласно табл.7.2
3	Искусственный интеллект в экспертных системах.	ПК-6	Лекция, СРС, практическая работа	Вопросы для УО КВЗПР Кейс	1-10 1-10 1	Согласно табл.7.2
4	Нечеткая логика в экспертных системах.	ПК-6	Лекция, СРС, практическая работа	Вопросы для УО КВЗПР Кейс	1-10 1-10 2	Согласно табл.7.2
5	Экспертиза криптографических систем защиты информации.	ПК-6	Лекция, СРС, практическая работа	Вопросы для УО КВЗПР Производственная задача	1-10 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 теме 1 «Основы безопасности информационных, автоматизированных и телекоммуникационных систем».

1. Основные понятия безопасности информационных систем.
2. Угрозы и риски информационной безопасности.
3. Модели угроз и рисков информационной безопасности.

4. Методы оценки рисков информационной безопасности.
5. Цели и задачи обеспечения информационной безопасности.

Контрольные вопросы для защиты практической работы №1

1. Какова роль государственных стандартов в обеспечении информационной безопасности в Российской Федерации?
2. Какие международные стандарты по информационной безопасности применяются в России?
3. Каков процесс разработки и утверждения стандартов в области информационной безопасности в РФ?
4. Какие органы и учреждения ответственны за разработку стандартов в области информационной безопасности в России?
5. Какие критерии определяют уровень защиты информации по российским стандартам?

Производственная задача

Задача по разработке экспертной системы для оценки уровня безопасности ИТ-инфраструктуры: Ваша задача - разработать экспертную систему, способную оценить уровень безопасности информационно-телекоммуникационных систем (ИТС) в производственной среде. Система должна учитывать различные факторы безопасности, такие как физическая защита, контроль доступа, шифрование данных, управление уязвимостями и др. Разработайте алгоритмы и правила, которые помогут оценить безопасность ИТС и предложить рекомендации по улучшению.

Кейс

Ваша задача состоит в разработке и внедрении экспертной системы комплексной оценки безопасности информационных и телекоммуникационных систем. Система должна предоставлять высокоточные и надежные рекомендации по обеспечению безопасности, основываясь на анализе уязвимостей и рисков.

Задача: Ваша задача состоит в разработке и внедрении экспертной системы комплексной оценки безопасности информационных и телекоммуникационных систем в компании. Система должна учитывать различные аспекты безопасности, такие как защита от несанкционированного доступа, уязвимости приложений, защита данных и сетевая безопасность.

Шаги кейса:

1. Анализ безопасности: Проведите анализ безопасности в компании. Изучите текущие политики, процедуры и меры безопасности, а также выявите уязвимые места и потенциальные риски в информационных и телекоммуникационных системах.
2. Разработка базы знаний: Создайте базу знаний, которая будет содержать экспертную информацию о различных уязвимостях, атаках, методах защиты и лучших практиках в области безопасности. Объедините опыт ва-

ших экспертов и доступные источники информации для создания обширной базы знаний.

3. Разработка алгоритмов оценки: Разработайте алгоритмы оценки безопасности, которые будут использовать базу знаний для анализа систем и выявления уязвимостей и рисков. Учтите различные факторы, такие как типы уязвимостей, их влияние на безопасность и приоритетность мер по устранению.

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 зачета. На промежуточной аттестации по дисциплине применяется механизм квалификационного экзамена. Зачет имеет структуру квалификационного экзамена и состоит из 2 частей:

– теоретической (компьютерное тестирование);

– практической (решение компетентностно-ориентированной задачи).

На теоретической части зачета (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 зачета 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 зачета (тестирования)

Задание в закрытой форме:

В какой архитектуре систем поддержки принятия решений данные синхронизированы и совместимы.

a) Функциональные системы поддержки принятия решений.
b) Трехуровневое хранилище данных.
c) Независимые витрины данных.
d) Двухуровневое хранилище данных.
f) Нет правильного ответа.

Задание в открытой форме:

1) … - характеристика средств системы, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню и глубине в зависимости от класса защищенности

2) … - это активный компонент защиты, включающий в себя анализ возможных угроз и рисков, выбор мер противодействия и методологию их применения.

3) Под термином … понимается системный процесс получения и оценки объективных данных о текущем состоянии обеспечения безопасности информации.

Задание на установление правильной последовательности

Расположите этапы построения экспертной системы в правильной последовательности:

1) Формализация,
2) Выполнение,
3) Тестирование
4) Опытная экспертиза
5) Идентификация,
6) Концептуализация,

Задание на установление соответствия:

1. Установить соответствие видов угроз:

1) Аппаратная	a) Когда возможен несанкционированный доступ к данным и их потеря.
2) Вероятность утечки	b) Когда существует вероятность нарушения работоспособности оборудования.
3) Нестабильность ПО	c) Когда есть вероятность некорректной работы программного обеспечения.
	d) Когда существует вероятность сбоев в работе ПО.

б) Примеры типовых заданий для практической части зачета

Компетентностно-ориентированная задача:

Задача по созданию базы знаний для экспертной системы: Ваша задача - создать базу знаний, которая будет использоваться экспертной системой для оценки безопасности информационных и телекоммуникационных систем. База знаний должна содержать информацию о типичных угрозах, уязвимостях, методах атак и мероприятиях по защите системы. Разработайте структуру базы знаний и заполните ее релевантными данными.

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	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы
Практическая работа № 2	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы
Практическая работа № 3	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы
Практическая работа № 4	2	Выполнил, но не ответил или неполно ответил на какой-либо вопрос	4	Выполнил, правильно и полно ответил на все вопросы
Устный опрос по темам 1-5	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	
Зачет	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 литература

1) Павлова, Е. А. Технологии разработки современных информационных систем на платформе Microsoft.NET : учебное пособие / Е. А. Павлова. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 128 с. — ISBN 978-5-4497-0360-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89479.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

2) Шинаков, К. Е. Анализ рисков безопасности информационных систем персональных данных : монография / К. Е. Шинаков, М. Ю. Рытов, О. М. Голембиовская. — Москва : Ай Пи Ар Медиа, 2020. — 236 с. — ISBN 978-5-4497-0535-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/95150.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

8.2 Дополнительная литература

3) Алдохина, О. И. Информационно-аналитические системы и сети. Часть 1. Информационно-аналитические системы : учебное пособие по специальности 080801 «Прикладная информатика (в информационной сфере)», квалификации «Информатик-аналитик» / О. И. Алдохина, О. Г. Басалаева. — Кемерово : Кемеровский государственный институт культуры, 2010. — 148 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/21973.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

4) Программно-аппаратные средства защиты информации : учебное пособие для студентов вузов по направлению подготовки «Информационная безопасность» / Л. Х. Мифтахова, А. Р. Касимова, В. Н. Красильников [и др.] ; под редакцией В. К. Головати. — Санкт-Петербург : Интермедия, 2018. — 408 с. — ISBN 978-5-4383-0157-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/73644.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

5) Башлы, П. Н. Информационная безопасность и защита информации : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва : Евразийский открытый институт, 2012. — 311 с. — ISBN 978-5-374-00301-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/10677.html (дата обращения: 09.10.2023). — Режим доступа: для авторизир. пользователей

8.3 Перечень методических указаний

1) Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем: методические указания по выполнению практических работ / Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2024. – 23 с.: Библиогр.: с. 23.

2) Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: М.О. Таныгин, Е.А. Кулешова. – Курск, 2024. – 9 с.: Библиогр.: с. 9.

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, 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			