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

Цель преподавания дисциплины

Целью преподавания дисциплины «Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем» является 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..

Задачи изучения дисциплины

Дисциплина играет особую роль в

- освещение и понимание угроз, рисков и атак на информационные и телекоммуникационные системы,
- ознакомление с основными классами технологий, методов и алгоритмов экспертных систем комплексной оценки безопасности.
- подготовка к научным исследованиям с использованием и разработкой экспертных систем
- приобретение навыков применения в инженерной практике современных интеллектуальных систем в области защиты информации.

Компетенции, формируемые в результате освоения дисциплины

Способен управлять рисками информационной безопасности (ПК-8);

Способен оценивать эффективность механизмов безопасности в информационных системах (ПК-10).

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
фундаментальной и прикладной
(наименование ф-та полностью)
информатики

М.О. Таныгин
(подпись, инициалы, фамилия)
«30» 06 2022 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 направление подготовки (специальности)

Защищённые информационные системы
наименование направленности (профиля, специализации)

форма обучения очная
очная, очно-заочная, заочная

Курск – 2022

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – магистратура по направлению подготовки 10.04.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищенные информационные системы», одобренного Ученым советом университета (протокол № 7 «28» февраля 2022 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы» на заседании кафедры информационной безопасности № 11 «30» июня 2022 г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы

к.т.н., доцент _____ Марухленко А.Л.

(ученая степень и ученое звание, Ф.И.О.)

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол № 7 «28» 02 2022 г., на заседании кафедры ИБ протокол №1 от 30.08.2023 .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Марухленко А.Л.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол №___ «__» _____ 20___ г., на заседании кафедры _____ .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол №___ «__» _____ 20___ г., на заседании кафедры _____ .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

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

1.1 Цель дисциплины

Целью преподавания дисциплины «Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем» является 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.

1.2 Задачи изучения дисциплины

Дисциплина играет особую роль в освещении и понимании угроз, рисков и атак на информационные и телекоммуникационные системы, ознакомлении с основными классами технологий, методов и алгоритмов экспертных систем комплексной оценки безопасности. В задачи дисциплины входит 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.

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

Таблица 1.3 – Результаты обучения по дисциплине

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

ПК-8	Способен управлять рисками информационной безопасности	ПК-8.1 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-8.2 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-8.3 Классифицирует угрозы информационной безопасности исходя из существующих и оригинальных методик	***Знать:*** Методику анализа классификации угрозы информационной безопасности исходя из существующих и оригинальных методик. ***Уметь:*** Анализировать и оформлять и классификации угрозы информационной безопасности исходя из существующих и оригинальных методик. ***Владеть (или Иметь опыт деятельности):*** Навыками классификации угрозы информационной безопасности исходя из существующих и оригинальных методик.
		ПК-8.4 Формирует перечень нарушителей информационной безопасности и их возможностей	***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.
ПК-10	Способен оценивать эффективность механизмов безопасности в информационных системах	ПК-10.1 Оценивает эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик	***Знать:*** Методику анализа оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик. ***Уметь:*** Анализировать оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.

			Владеть (или Иметь опыт деятельности): навыками оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.
		ПК-10.2 Оценивает соответствие механизмов безопасности системы требованиям нормативных документов и рискам	***Знать:*** Методику анализа и оценки соответствия механизмов безопасности системы требованиям нормативных документов и рискам. ***Уметь:*** Анализировать и оценивать соответствие механизмов безопасности системы требованиям нормативных документов и рискам. ***Владеть (или Иметь опыт деятельности):*** навыками оценки соответствия механизмов безопасности системы требованиям нормативных документов и рискам.
		ПК-10.3 Формулирует критерии оценки эффективности механизмов безопасности, используемых в информационных системах	***Знать:*** Методику анализа критериев оценки эффективности механизмов безопасности, используемых в информационных системах. ***Уметь:*** Анализировать и формулировать критерии оценки эффективности механизмов безопасности, используемых в информационных системах. ***Владеть (или Иметь опыт деятельности):*** навыками анализа, управления и формулировки критериев оценки эффективности механизмов безопасности, используемых в информационных системах.
		ПК-10.4 Формулирует предложения по повышению эффективности механизмов безопасности, используемых в информационных системах	***Знать:*** Методику анализа формулировки предложения по повышению эффективности механизмов безопасности, используемых в информационных системах. ***Уметь:*** Анализировать формулировки предложения по повышению эффективности механизмов безопасности, используемых в информационных системах. ***Владеть (или Иметь опыт деятельности):*** навыками формулировки предложения по повышению эффективности механизмов безопасности, используемых в информационных системах.

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Экспертные системы информационных и телекоммуникационных систем» входит в базовую часть, формируемую участниками образовательных отношений, блока 1 «Дисциплины (модули»)) основной профессиональной образовательной программы – программы магистратуры 10.04.01.Информационная безопасность профиль «Защищённые информационные системы». Дисциплина изучается на 2 курсе в 3 семестре.

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

Общая трудоёмкость (объём) дисциплины составляет 3 зачётные единицы, 108 часа

Таблица 3.1 – Объём 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
Самостоятельная работа обучающихся (всего)	53,9
Контроль (подготовка к экзамену)	36
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
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 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
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. Защита информации как непрерывный процесс.
2.	Экспертные системы информационных систем.	Введение в экспертные системы. Требования к экспертным системам. Экспертные системы информационной безопасности как часть информационных, автоматизированных и телекоммуникационных систем. 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. 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. Использование процедур. Представление неопределённости в информационных приложениях с базами знаний.
4.	Нечеткая логика	Понятие о нечетких множествах и их связь с теорией

	в экспертных системах.	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.
5.	Экспертиза криптографических систем защиты информации.	Криптографическая защита информации. Основы криптографии. Симметричные криптосистемы. Криптосистемы с открытым ключом. Системы электронной подписи. Криптоанализ. Экспертная система оценки стойкости криптосистем.

Таблица 4.2 – Содержание дисциплины и ее методическое обеспечение

п/п	Раздел (тема) Дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек, час	пр	лб.			
	2				6	7	8
1.	Основы безопасности информационных, автоматизированных и телекоммуникационных систем.	2	-	-	У-1-5	С (1-3)	ПК-8 ПК-10
2.	Экспертные системы информационных систем.	2	1	-	У-1-5 МУ-1-2	С, ЗПР (4-7)	ПК-8 ПК-10
3.	Искусственный интеллект в экспертных системах.	4	2	-	У-1-5 МУ-1-2	С, ЗПР (8-11)	ПК-8 ПК-10
4.	Нечеткая логика в экспертных системах.	4	4	-	У-1-5 МУ-1-2	С, ЗПР (12-14)	ПК-8 ПК-10
5.	Экспертиза криптографических систем защиты информации.	4	4	-	У-1-5 МУ-1-2	С, ЗПР (15-18)	ПК-8 ПК-10
	Итого	18	-	-	-	-	-

С – собеседование, ЗПР – защита практической работы

4.2 Лабораторные работы и практические занятия

Таблица 4.3 – Практические занятия

№	Наименование практического (семинарского) занятия	Объем, час.
1	2	3
1	Создание классификации существующих экспертных систем информационной безопасности.	8
2	Организация вывода нечеткой логики в экспертных системах.	8
3	Экспертные системы на основе логического программирования.	10
4	Экспертные системы оценки стойкости криптосистем.	10
Итого		36

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.4 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1	Основы безопасности информационных, автоматизированных и телекоммуникационных систем.	1-3 недели	10
2	Экспертные системы информационных систем.	4-7 недели	10
3	Искусственный интеллект в экспертных системах.	8-11 недели	10
4	Нечеткая логика в экспертных системах.	12-14 недели	10
5	Экспертиза криптографических систем защиты информации.	15-18 недели	10
Итого			53,9

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

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

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

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала за счёт выкладывания на сайт кафедры ИБ в интернете;

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

– путем разработки вопросов к зачету

– методических указаний к выполнению практических работ.

типографией университета

– путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;

путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

и научной, учебной, учебно-методической литературы.

6 Образовательные технологии.

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования общепрофессиональных компетенций обучающихся. В рамках дисциплины предусмотрены выполнение в ходе лабораторных работ практико-ориентированных заданий.

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

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объём, час.
1.	Создание классификации существующих экспертных систем информационной безопасности.	Разбор конкретных ситуаций.	4
2.	Организация вывода нечеткой логики в экспертных системах.	Разбор конкретных ситуаций.	4
3.	Экспертные системы на основе логического программирования.	Разбор конкретных ситуаций.	4
4.	Экспертные системы оценки стойкости криптосистем.	Разбор конкретных ситуаций.	4
	Итого		16

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

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

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

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

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

7 Фонд оценочных средств для проведения промежуточной аттестации

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

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
Способен управлять рисками информационной безопасности (ПК-8).	Оценка защищённости информационных систем Теоретические основы компьютерной безопасности Информационно-аналитические системы безопасности Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем		Производственная преддипломная практика
Способен оценивать эффективность механизмов безопасности в информационных системах (ПК-10).	Технологии обеспечения информационной безопасности объектов Информационно-аналитические системы безопасности Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем		Производственная преддипломная практика

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ПК-8 /основной	ПК-8.1 Формирует перечень угроз для защищаемой информационной системы	***Знать:*** Методику анализа перечня угроз для защищаемой информационной системы ***Уметь:*** Анализировать перечень угроз для защищаемой информационной системы. ***Владеть (или Иметь опыт деятельности):*** методом анализа каких-либо угроз.	***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 анализа каких-либо угроз.	***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-8.2 Формирует критерии оценки каждого вида угроз в защищаемой системе	***Знать:*** Методику формирования критериев оценки угроз в защищаемой системе. ***Уметь:*** Анализировать критерии оценки угроз в защищаемой системе. ***Владеть (или Иметь опыт***	***Знать:*** Методику формирования критериев оценки каждого вида угроз в защищаемой системе. ***Уметь:*** Анализировать 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 угроз.	***Владеть (или Иметь опыт деятельности):*** Навыками формирования критериев оценки любого вида угроз в защищаемой системе.	***деятельности):*** Навыками формирования критериев оценки каждого вида угроз в защищаемой системе.
	ПК-8.3 Классифицирует угрозы информационной безопасности исходя из существующих и оригинальных методик	***Знать:*** Методику анализа классификации угрозы информационной безопасности. ***Уметь:*** Анализировать и оформлять и классификации угрозы информационной безопасности исходя из существующих и оригинальных методик. ***Владеть (или Иметь опыт деятельности):*** Навыками классификации угрозы информационной безопасности.	***Знать:*** Методику анализа классификации угрозы информационной безопасности исходя из существующих и оригинальных методик. ***Уметь:*** Анализировать и оформлять и классификации угрозы информационной безопасности исходя из существующих и оригинальных методик. ***Владеть (или Иметь опыт деятельности):*** Навыками классификации угрозы информационной безопасности.	***Знать:*** Методику анализа классификации угрозы информационной безопасности исходя из существующих и оригинальных методик. ***Уметь:*** Анализировать и оформлять и классификации угрозы информационной безопасности исходя из существующих и оригинальных методик. ***Владеть (или Иметь опыт деятельности):*** Навыками классификации угрозы информационной безопасности исходя из существующих и оригинальных методик.
	ПК-8.4 Формирует перечень нарушителей информационной безопасности и их возможностей	***Знать:*** Методику анализа формирования перечня нарушителей информационной безопасности. ***Уметь:*** Анализировать и формировать перечень	***Знать:*** Методику анализа формирования перечня нарушителей информационной безопасности и их возможностей. ***Уметь:*** Анализировать и формировать	***Знать:*** Методику анализа формирования перечня нарушителей информационной безопасности и их возможностей. ***Уметь:*** Анализировать и формировать

		нарушителей информационной безопасности. ***Владеть (или Иметь опыт деятельности):*** Навыками формирования перечня нарушителей информационной безопасности.	перечень нарушителей информационной безопасности и их возможностей. ***Владеть (или Иметь опыт деятельности):*** Навыками формирования перечня нарушителей информационной безопасности.	перечень нарушителей информационной безопасности и их возможностей. ***Владеть (или Иметь опыт деятельности):*** Навыками формирования перечня нарушителей информационной безопасности и их возможностей.
ПК-10 / основной	ПК-10.1 Оценивает эффективности применяемых программно-аппаратных средств защиты информации с использование м штатных средств и методик	***Знать:*** Методику анализа оценки эффективности применяемых программно-аппаратных средств защиты информации. ***Уметь:*** Анализировать оценки эффективности применяемых программно-аппаратных средств защиты информации. ***Владеть (или Иметь опыт деятельности):*** навыками оценки эффективности применяемых программно-аппаратных средств защиты информации.	***Знать:*** Методику анализа оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик. ***Уметь:*** Анализировать оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик. ***Владеть (или Иметь опыт деятельности):*** навыками оценки эффективности применяемых программно-аппаратных средств защиты информации.	***Знать:*** Методику анализа оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик. ***Уметь:*** Анализировать оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик. ***Владеть (или Иметь опыт деятельности):*** навыками оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.
	ПК-10.2 Оценивает соответствие	***Знать:*** Методику оценки соответствия	***Знать:*** Методику анализа и оценки соответствия	***Знать:*** Методику анализа и оценки соответствия

	механизмов безопасности системы требованиям нормативных документов и рискам	механизмов безопасности системы требованиям нормативных документов ***Уметь:*** оценивать соответствие механизмов безопасности системы требованиям нормативных документов ***Владеть (или Иметь опыт деятельности):*** навыками оценки механизмов безопасности системы.	механизмов безопасности системы требованиям нормативных документов и рискам. ***Уметь:*** оценивать соответствие механизмов безопасности системы требованиям нормативных документов. ***Владеть (или Иметь опыт деятельности):*** навыками оценки механизмов безопасности системы.	механизмов безопасности системы требованиям нормативных документов и рискам. ***Уметь:*** Анализировать и оценивать соответствие механизмов безопасности системы требованиям нормативных документов и рискам. ***Владеть (или Иметь опыт деятельности):*** навыками оценки соответствия механизмов безопасности системы требованиям нормативных документов и рискам.
	ПК-10.3 Формулирует критерии оценки эффективности механизмов безопасности.	***Знать:*** Методику анализа критериев оценки эффективности механизмов безопасности информационных системах. ***Уметь:*** Анализировать и формулировать критерии оценки эффективности механизмов безопасности, используемых в информационных системах. ***Владеть (или Иметь опыт деятельности):***	***Знать:*** Методику анализа критериев оценки эффективности механизмов безопасности, используемых в информационных системах. ***Уметь:*** Анализировать и формулировать критерии оценки эффективности механизмов безопасности, используемых в информационных системах. ***Владеть (или Иметь опыт***	***Знать:*** Методику анализа критериев оценки эффективности механизмов безопасности, используемых в информационных системах. ***Уметь:*** Анализировать и формулировать критерии оценки эффективности механизмов безопасности, используемых в информационных системах. ***Владеть (или Иметь опыт***

		навыками анализа, и формулировки критериев оценки эффективности механизмов безопасности.	***деятельности):*** навыками анализа, и формулировки критериев оценки эффективности механизмов безопасности.	***деятельности):*** навыками анализа, управления и формулировки критериев оценки эффективности механизмов безопасности, используемых в информационных системах.
	ПК-10.4 Формулирует предложения по повышению эффективности механизмов безопасности, используемых в информационных системах	***Знать:*** Методику анализа формулировки предложения по повышению эффективности механизмов безопасности. ***Уметь:*** Анализировать формулировки предложения по повышению эффективности механизмов безопасности. ***Владеть (или Иметь опыт деятельности):*** навыками формулировки предложения по повышению безопасности.	***Знать:*** Методику анализа формулировки предложения по повышению эффективности механизмов безопасности, используемых в информационных системах. ***Уметь:*** Анализировать формулировки предложения по повышению эффективности механизмов безопасности, используемых в информационных системах. ***Владеть (или Иметь опыт деятельности):*** навыками формулировки предложения по повышению эффективности механизмов безопасности.	***Знать:*** Методику анализа формулировки предложения по повышению эффективности механизмов безопасности, используемых в информационных системах. ***Уметь:*** Анализировать формулировки предложения по повышению эффективности механизмов безопасности, используемых в информационных системах. ***Владеть (или Иметь опыт деятельности):*** навыками формулировки предложения по повышению эффективности механизмов безопасности, используемых в информационных системах.

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

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля успеваемости

п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№ заданий	
1	2	3	4	5	6	7
1.	Основы безопасности информационных, автоматизированных и телекоммуникационных систем.	ПК-8 ПК-10	Лекция, СРС	ВС	1-5	Согласно табл.7.2
2.	Экспертные системы информационных систем.	ПК-8 ПК-10	Лекция, СРС, практическая работа	ВС, КВЗПР	1-5 1-5	Согласно табл.7.2
3.	Искусственный интеллект экспертных системах.	ПК-8 ПК-10	Лекция, СРС, практическая работа	ВС, КВЗПР	1-5 1-5	Согласно табл.7.2
4.	Нечеткая логика в экспертных системах.	ПК-8 ПК-10	Лекция, СРС, практическая работа	ВС, КВЗПР	1-5 1-5	Согласно табл.7.2
5.	Экспертиза криптографических систем защиты информации.	ПК-8 ПК-10	Лекция, СРС, практическая работа	ВС, КВЗПР	1-5 1-5	Согласно табл.7.2

ВС- вопросы для собеседования, КВЗПР- контрольные вопросы для защиты практической работы

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для собеседования 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 практических работ

1. Что такое нечеткая логика?
2. Для чего в нечетких выводах используются нечеткие правила?
3. Напишите формулы для нескольких функций принадлежности?
4. В чем суть алгоритма Мамдани?
5. В чем суть алгоритма Ларсена?
6. В чем суть алгоритма Тсукамото?
7. В чем суть алгоритма Сугэно?
8. В чем суть алгоритма Такаги-Сугэно?

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в виде компьютерного тестирования.

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

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

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

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

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

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

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно

определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

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.

Компетентностно-ориентированная задача:

Разработать экспертную системы на основе алгоритма модифицированного Мамдани используя трапециевидные функции принадлежности.

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

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

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

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

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

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

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	Балл	примечание	балл	примечание
Выполнение практической работы №1	4	Выполнил, доля правильных ответов менее 50%	8	Выполнил и доля правильных ответов более 50%
Выполнение практической работы №2	4	Выполнил, доля правильных ответов менее 50%	8	Выполнил и доля правильных ответов более 50%

Выполнение практической работы №3	4	Выполнил, доля правильных ответов менее 50%	8	Выполнил и доля правильных ответов более 50%
Выполнение практической работы №4	4	Выполнил, доля правильных ответов менее 50%	8	Выполнил и доля правильных ответов более 50%
Собеседование по теме 1	2	Доля правильных ответов менее 50%	4	Доля правильных ответов более 50%
Собеседование по теме 2	2	Доля правильных ответов менее 50%	4	Доля правильных ответов более 50%
Собеседование по теме 3	2	Доля правильных ответов менее 50%	4	Доля правильных ответов более 50%
Собеседование по темам 4-5	2	Доля правильных ответов менее 50%	4	Доля правильных ответов более 50%
ИТОГО	24		48	

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

Каждый верный ответ оценивается следующим образом:

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

Максимальное количество баллов за тестирование –36 баллов.

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

8.1 Основная литература

1) Ипатова, Э. Р. Методологии и технологии системного проектирования информационных систем : учебник / Э. Р. Ипатова, Ю. В. Ипатов. – 3-е изд., стер. – Москва : ФЛИНТА, 2021. – 256 с. – URL: https://biblioclub.ru/index.php?page=book&id=79551 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

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

8.2 Дополнительная литература

3) Аверченков, В. И. История развития системы государственной безопасности России : учебное пособие / В. И. Аверченков, В. В. Ерохин, О. М. Голембиовская ; науч. ред. Ю. Т. Трифанков. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 193 с. – URL: https://biblioclub.ru/index.php?page=book&id=93267 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

4) Алдохина, О. И. Информационно-аналитические системы и сети : учебное пособие / О. И. Алдохина, О. Г. Басалаева. – Кемерово : КемГУКИ, 2010. – Часть 1. Информационно-аналитические системы. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=227684 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

5) Ветошкин, А. Г. Нормативное и техническое обеспечение безопасности жизнедеятельности: учебно-практическое пособие : в 2 частях / А. Г. Ветошкин. – Москва ; Вологда : Инфра-Инженерия, 2017. – Часть 1. Нормативно-управленческое обеспечение безопасности жизнедеятельности. – 471 с. – URL: https://biblioclub.ru/index.php?page=book&id=466497 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

8.3 Перечень методических указаний

1. Разработка экспертных систем на основе нечетких правил вывода : методические указания по выполнению лабораторной работы по дисциплине «Теория нечеткой логики и множеств» для студентов специальности 09.03.01 «Информатика и вычислительная техника» / Юго-Зап. гос. ун-т ; сост. М. В. Бобырь. - Курск : ЮЗГУ, 2016. - 45 с. - Текст : электронный.

2. Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем : методические указания по выполнению самостоятельной работы для студентов направления подготовки 10.04.01 / Юго-Зап. гос. ун-т ; сост. В. П. Добрица. - Курск : ЮЗГУ, 2018. - 19 с. - Текст : электронный

9 Перечень ресурсов информационно-телекоммуникационной сети Интернет

Электронно-библиотечная система «Лань» - http://e.lanbook.com/

Электронно-библиотечная система IQLib – http://www.iqlib.ru

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 «Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем» являются лекции и практические занятия. Студент не имеет права пропускать занятия без уважительных причин.

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

Изучение наиболее важных тем или разделов дисциплины завершают практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта отстаивания своей точки зрения, 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.

По согласованию с преподавателем или по его заданию студенты готовят рефераты по отдельным темам дисциплины, выступают на занятиях с докладами. Основу докладов составляет, как правило, содержание подготовленных студентами рефератов.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты практических работ, а также по результатам докладов. Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем»: конспектирование учебной литературы и лекций, составление словарей понятий и терминов, прорешивание предлагаемых упражнений и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому

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

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

Основная цель самостоятельной работы студента при изучении дисциплины «Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

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

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234, Windows 7, договор IT000012385

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

Учебная аудитория для проведения занятий лекционного и практического типа или лаборатории кафедры информационная безопасность, оснащенные мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска, проектор для демонстрации презентаций. Помещение для самостоятельной работы Компьютер PDC2160/iC33/2*512Mb/HDD 160Gb/DVD-ROM/FDD/ATX350W/ K/m/ OFF/l 7"TFT E700 (6 шт)

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

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

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

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

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и

промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	изменённых	заме-нённых	аннулиро-ванных	новых			