Аннотация к рабочей программе дисциплины «Комплексная защита объектов информатизации»

Цель преподавания дисциплины

Формирование у студентов знаний в области комплексной защиты объектов информатизации, построения систем информационной безопасности с использованием технических средств охраны, освоение дисциплинарных компетенций, связанных с раскрытием базовых и расширенных технологий обеспечения информационной безопасности сложных технических объектов и систем.

Задачи изучения дисциплины

– изучение основных положений, понятий и категорий, относящихся к базовым и расширенным технологиям обеспечения информационной безопасности;

– изучение принципов организации, комплексного подхода к выбору средств и технологий обеспечения информационной безопасности объектов защиты

– изучение методов проектирования систем безопасности охраняемого объекта;

– изучение принципов работы технических средств охраны;

– определение критериев защищенности охраняемого объекта;

– освоение механизмов защиты охраняемых объектов;

– формирование правильного подхода к проблемам информационной безопасности, который начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС).

Компетенции, формируемые в результате освоения дисциплины

Способен управлять работами по обеспечению информационной (ПК-6).

Способен эксплуатировать телекоммуникационные системы в защищённом исполнении (ПК-9).

Способен управлять жизненным циклом подсистем обеспечения информационной безопасности (ПК-11).

Разделы дисциплины

Понятия и определения технических средств охраны. Структура автоматизированной системы охраны. Варианты программно-аппаратной реализации ТСО. Методология разработки концепции комплексного обеспечения безопасности объектов охраны. Общий подход к категорированию объектов охраны. Классификация нарушителей информационной безопасности, угроз ИБ. Классификация технических средств охраны, необходимых для построения комплексной системы защиты информации.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.О. декана факультета
Фундаментальной и прикладной информатики
(наименование ф-та полностью)

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

«30» 06 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Комплексная защита объектов информатизации

(наименование дисциплины)

ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем

(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Управление безопасностью телекоммуникационных систем и сетей

наименование направленности (профиля, специализации)

форма обучения очная

(очная, очно-заочная, заочная)

Курск – 2022

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – специалитет по направлению подготовки (специальности) 10.05.02 Информационная безопасность телекоммуникационных систем на основании учебного плана ОПОП ВО10.05.02 Информационная безопасность телекоммуникационных систем, специализация Управление безопасностью телекоммуникационных систем и сетей, одобренного Ученым советом университета (протокол № 7 «28» февраля 2022 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация Управление безопасностью телекоммуникационных систем и сетей на заседании кафедры информационной безопасности Протокол № 11 «30» июня 2022 г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы _____ Кулешова Е.А.
(ученая степень и ученое звание, Ф.И.О.)

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация Управление безопасностью телекоммуникационных систем и сетей на заседании кафедры информационной безопасности Протокол №_

«__»___20_г., на заседании кафедры _____ .
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.05.02 Информационная безопасность телекоммуникационных систем, специализация Управление безопасностью телекоммуникационных систем и сетей на заседании кафедры информационной безопасности Протокол №_

«__»___ 20_ г., на заседании кафедры _____ .
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

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

1.1 Цель дисциплины

Формирование у студентов знаний в области комплексной защиты объектов информатизации, построения систем информационной безопасности с использованием технических средств охраны, освоение дисциплинарных компетенций, связанных с раскрытием базовых и расширенных технологий обеспечения информационной безопасности сложных технических объектов и систем.

1.2 Задачи дисциплины

– изучение основных положений, понятий и категорий, относящихся к базовым и расширенным технологиям обеспечения информационной безопасности;

– изучение принципов организации, комплексного подхода к выбору средств и технологий обеспечения информационной безопасности объектов защиты

– изучение методов проектирования систем безопасности охраняемого объекта;

– изучение принципов работы технических средств охраны;

– определение критериев защищенности охраняемого объекта;

– освоение механизмов защиты охраняемых объектов;

– формирование правильного подхода к проблемам информационной безопасности, который начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС).

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

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-6	Способен управлять работами по обеспечению информационной безопасности	ПК-6.1 Определяет перечень информации, подлежащей защите	***Знать:*** Принципы организации телекоммуникационных систем и их уязвимости. ***Уметь:*** Формулировать технические требования к

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			телекоммуникационным системам и мерам по предотвращению уязвимостей. ***Владеть:*** Навыками создания моделей угроз и моделей злоумышленника для телекоммуникационных систем и устройств.
		ПК-6.2 Определяет требуемый уровень защищённости информации, циркулирующей в телекоммуникационной системе	***Знать:*** законы, технологии, правила, приемы обработки исследования уровня защищенности объектов информатизации. ***Уметь:*** подготовить развернутый отчет по результатам обследования объекта. ***Владеть:*** навыками подготовки аттестационных документов на предмет соответствия объекта требованиям по информационной безопасности.
		ПК-6.3 Определяет меры для защиты в информации в телекоммуникационных системах и сетях	***Знать:*** Инструментальные средства обеспечения защиты информации телекоммуникационных систем. ***Уметь:*** Осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем. ***Владеть:***

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*		
			Навыками эксплуатации телекоммуникационных приборов и средств защиты информации.
ПК-9	Способен эксплуатировать телекоммуникационные системы в защищённом исполнении	ПК-9.1 Выявляет сбои и отказы устройств и программ	***Знать:*** основные признаки возникновения сбоев и отказов при эксплуатации ТКС ***Уметь:*** в процессе эксплуатации фиксировать режимы работы ТКС, отличные от штатных ***Владеть:*** обнаружения сбоев и отказов реальных ТКС
		ПК-9.2 Восстанавливает работоспособность систем после сбоев и отказов устройств и программ	***Знать:*** знать номенклатуру регламентных работ по восстановлению работоспособности устройств и программ ***Уметь:*** выполнять регламентные работы по восстановлению работоспособности устройств и программ ***Владеть:*** эксплуатации программного и аппаратного обеспечения ТКС в различных режимах работы
		ПК-9.3 Формулирует перечень действий для восстановления последствий сбоев и отказов	***Знать:*** назначение и классификацию программно-аппаратных средств ТКС; особенности функционирования ТКС; классификацию программных и

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			аппаратных средств анализа защищённости ТКС, систем обнаружения сетевых атак, антивирусного ПО; технические характеристики и правила эксплуатации средств восстановления последствий сбоев и отказов. ***Уметь:*** проводить мониторинг безопасности АС; обнаруживать уязвимые места в функционировании ПО и оборудования ТКС; провести настройку ПО и оборудования ТКС. ***Владеть:*** навыками настройки программных и аппаратных средств анализа защищённости ТКС, систем обнаружения сетевых атак, антивирусного ПО.
		ПК-9.4 Регистрирует сообщения об ошибках в сетевых устройствах и операционных системах	***Знать:*** основные признаки возникновения ошибок в сетевых устройствах и операционных системах ***Уметь:*** в процессе эксплуатации фиксировать режимы работы сетевых устройств и операционных систем, отличные от штатных ***Владеть:*** навыками обнаружения сбоев и отказов реальных сетевых устройств и

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
			операционных систем
		ПК-9.5 Формирует отчёты по результатам работ системы мониторинга	***Знать:*** структуру и содержание журналов аудита информационной безопасности ***Уметь:*** использовать технические средства ведения журналов аудита информационной безопасности ***Владеть:*** навыками анализа журналов аудита информационной безопасности
ПК-11	Способен управлять жизненным циклом подсистем обеспечения информационной безопасности	ПК-11.1 Определяет действия по обеспечению информационной безопасности на различных этапах жизненного цикла телекоммуникационной системы	***Знать:*** особенности различных этапов жизненного цикла ТКС ***Уметь:*** исходя их имеющегося перечня угроз реализовывать технологии обеспечения информационной безопасности ***Владеть:*** эксплуатации ТКС на различных этапах жизненного цикла
		ПК-11.2 Выбирает перечень реализуемых телекоммуникационной системой технологий для удовлетворения требований по информационной безопасности	***Знать:*** перечень реализуемых телекоммуникационной системой технологий для удовлетворения требований по информационной безопасности ***Уметь:*** соотносить технологии информационной безопасности существующим в ТКС

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*		
			уязвимостям ***Владеть:*** реализации технологий информационной безопасности
		ПК-11.3 Оценивает результат применения штатных средств обеспечения информационной безопасности	***Знать:*** критерии результативности применения штатных средств обеспечения информационной безопасности ***Уметь:*** формулировать количественные критерии результативности применения штатных средств обеспечения информационной безопасности ***Владеть:*** навыками оценки результативности применения штатных средств обеспечения информационной безопасности
		ПК-11.4 Формулирует предложения по совершенствованию подсистем обеспечения информационной безопасности	***Знать:*** меры и технологии, направленные на повышение защищённости процессов обработки информации в ТКС ***Уметь:*** определять меры и технологии, направленные на повышение защищённости процессов обработки информации в конкретной ТКС ***Владеть:***

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*		
			обеспечения процесса защиты информации в ТКС

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Комплексная защита объектов информатизации» входит в часть, формируемую участниками образовательных отношений, блока 1 «Дисциплины (модули»)) основной профессиональной образовательной программы – программы специалитета 10.05.02 Информационная безопасность телекоммуникационных систем, профиль «Управление безопасностью телекоммуникационных систем и сетей». Дисциплина изучается на 5 курсе в 9 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 6 зачётных единицы, 216 часов

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	216
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	90
в том числе:	
лекции	36
практические занятия	54, из них практическая подготовка 10
Самостоятельная работа обучающихся (всего)	88,85
Контроль (подготовка к экзамену)	36
Контактная работа по промежуточной аттестации (всего АттКР)	1,15
в том числе:	
зачет	не предусмотрен
зачет с оценкой	не предусмотрен

Виды учебной работы	Всего, часов
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	1,15

4 Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Понятия и определения технических средств охраны. Структура автоматизированной системы охраны	Основные термины и определения, используемые при решении вопросов обеспечения объектов техническими средствами охраны и безопасности. Основные составляющие автоматизированной системы охраны, такие как элементы предупреждения, датчики (системы) обнаружения, элементы (системы) поражения и электроснабжения
2	Варианты программно-аппаратной реализации ТСО	Варианты реализации аппаратных ключей и их технические характеристики. Технологическая схема аутентификации. Преимущества и недостатки аутентификации на основе аппаратных ключей. Примеры программной (программно-аппаратной) реализации
3	Методология разработки концепции комплексного обеспечения безопасности объектов охраны	Положения о разработке системной концепции обеспечения безопасности объектов охраны. Основные методологии, блок задач разработки концепции комплексного обеспечения их безопасности. Особенности общего подхода к категорированию объектов охраны
4	Общий подход к категорированию объектов охраны	Основополагающие, определяющие выбор уровня защиты объекта, признаки категория важности объекта и модели нарушителей, от проникновения которых данный объект должен быть защищен
5	Классификация нарушителей информационной безопасности, угроз ИБ	Внутренние и внешние нарушители. Причины и мотивы нарушений, возможности, преследуемые цели. Перечень угроз, оценки вероятностей их реализации, модели нарушителей, служащие основой для анализа риска реализации угроз и формулирования требований к системе защиты
6	Классификация технических средств охраны, необходимых для построения комплексной системы защиты информации	Виды техники, предназначенные для использования силами охраны с целью повышения эффективности обнаружения нарушителя и обеспечения контроля доступа на объект охраны

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	№пр			
1	2	3	4	5	6	7
1	Понятия и определения технических средств охраны. Структура автоматизированной системы охраны	6	1	У 1-6, МУ 1-6	С, ЗПР (1-3)	ПК-6, ПК-9, ПК-11
2	Варианты программно-аппаратной реализации ТСО	6	2	У 1-6, МУ 1-6	С, ЗПР (2-6)	ПК-6, ПК-9, ПК-11
3	Методология разработки концепции комплексного обеспечения безопасности объектов охраны	6	3	У 1-6, МУ 1-6	С, ЗПР (7-9)	ПК-6, ПК-9, ПК-11
4	Общий подход к категорированию объектов охраны	6	4	У 1-6, МУ 1-6	С, ЗПР (10-12)	ПК-6, ПК-9, ПК-11
5	Классификация нарушителей информационной безопасности, угроз ИБ	6	5	У 1-6, МУ 1-6	С, ЗПР (13-15)	ПК-6, ПК-9, ПК-11
6	Классификация технических средств охраны, необходимых для построения комплексной системы защиты информации	6	6	У 1-6, МУ 1-6	С, ЗПР (16-18)	ПК-6, ПК-9, ПК-11
	Итого	36				

С – собеседование, ЗПР – защита практической работы.

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Практические работы

Таблица 4.2.1 – Практические работы

№	Наименование практической работы	Объем, час.
1	Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение	10, из них практическая подготовка 2
2	Определение показателей защищенности информации при несанкционированном доступе	8
3	Критерии оценки и выбора CASE-средств	8
4	Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности	8
5	Исследование противодействия несанкционированной работе портативных звукозаписывающих устройств	10, из них практическая подготовка 4
6	Исследование акустического и виброакустического каналов утечки информации	10, из них практическая подготовка 4
Итого		54

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№ Раздела (Темы)	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	Понятия и определения технических средств охраны. Структура автоматизированной системы охраны	1-3 неделя	8,85
2	Варианты программно-аппаратной реализации ТСО	4-7 неделя	20
3	Методология разработки концепции комплексного обеспечения безопасности объектов охраны	8-11 неделя	20
4	Общий подход к категорированию объектов охраны	12-15 неделя	20
5	Классификация нарушителей информационной безопасности, угроз ИБ и технических средств охраны	16-18 неделя	20
Итого			88.85

5 Перечень учебно-методического обеспечение 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 УП 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;

– вопросов к экщамену;

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

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

–удовлетворение потребности в тиражировании научной, учебной и 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 универсальных, общепрофессиональных и профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета по труду и занятости населения Курской области.

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

№	Наименование раздела	Используемые интерактивные образовательные технологии	Объём, час.
1.	Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение	Разбор конкретных ситуаций	2
2.	Определение показателей защищенности информации при несанкционированном доступе	Разбор конкретных ситуаций	2

3.	Критерии оценки и выбора CASE-средств	Разбор конкретных ситуаций	2
4.	Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности	Разбор конкретных ситуаций	2
5.	Исследование противодействия несанкционированной работе портативных звукозаписывающих устройств	Разбор конкретных ситуаций	2
6.	Исследование акустического и виброакустического каналов утечки информации	Разбор конкретных ситуаций	2
Итого			12

Практическая подготовка обучающихся при реализации дисциплины осуществляется путем проведения практических и лабораторных 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 реальных производственных условиях (в профильных организациях) и (или) модельных условиях (оборудованных (полностью или частично) в подразделениях университета – на базе автономной некоммерческой организации дополнительного профессионального образования «ЩИТ-УЧЕБНЫЙ ЦЕНТР».

Практическая подготовка обучающихся проводится в соответствии с положением П 02.181.

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 профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки, высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для природы, человека и общества;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися,

представителями работодателей (командная работа, разбор конкретных ситуаций, и др.)*;*

– 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 обучающихся по дисциплине

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

Средствами промежуточного контроля успеваемости студентов являются защита лабораторных работ, опросы на лабораторных занятиях по темам лекций.

Таблица 7.1 – Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули)и практики, при изучении/ прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-6 Способен управлять работами по обеспечению информационной	Комплексная защита объектов информатизации Производственная преддипломная практика		
ПК-9 Способен эксплуатировать телекоммуникационные системы в защищённом исполнении	Комплексная защита объектов информатизации Производственная преддипломная практика		
ПК-11 Способен управлять жизненным циклом подсистем обеспечения информационной безопасности	Комплексная защита объектов информатизации Производственная преддипломная практика		

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

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ПК-6 /завершающий	ПК-6.1 Определяет перечень информации, подлежащей защите	***Знать:*** Основные уязвимости телекоммуникационных систем. ***Уметь:*** Формулировать отдельные требования к телекоммуникационным системам и мерам по предотвращению уязвимостей. ***Владеть:*** навыками создания примитивных моделей угроз и моделей злоумышленника для телекоммуникационных систем и устройств.	***Знать:*** Принципы организации телекоммуникационных систем и их основные уязвимости. ***Уметь:*** Формулировать технические требования к телекоммуникационным системам и мерам по предотвращению уязвимостей. ***Владеть:*** навыками создания стандартных моделей угроз и моделей злоумышленника для телекоммуникационных систем и устройств.	***Знать:*** Принципы организации телекоммуникационных систем и их уязвимости, в том числе нетиповые. ***Уметь:*** Прорабатывать и детализировать технические требования к телекоммуникационным системам и мерам по предотвращению уязвимостей. ***Владеть:*** навыками создания сложных и нетиповых моделей угроз и моделей злоумышленника для телекоммуникационных систем и устройств.
	ПК-6.2 Определяет требуемый уровень защищённости информации,	***Знать:*** Фрагменты и отдельные законов, технологий, правил, приемов	***Знать:*** Основные законы, технологии, правила, приемы обработки исследования	***Знать:*** Совокупность законов, технологий, правил, приемов обработки

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
	циркулирующей в телекоммуникационной системе	обработки исследования уровня защищенности объектов информатизации. ***Уметь:*** подготовить отдельные части отчета по результатам обследования объекта. ***Владеть:*** навыками подготовки отдельных аттестационных документов на предмет соответствия объекта требованиям по информационной безопасности.	уровня защищенности объектов информатизации. ***Уметь:*** подготовить отчет по результатам обследования объекта. ***Владеть:*** навыками подготовки аттестационных документов на предмет соответствия объекта требованиям по информационной безопасности.	исследования уровня защищенности объектов информатизации. ***Уметь:*** подготовить развернутый отчет по результатам обследования объекта. ***Владеть:*** уверенными навыками подготовки аттестационных документов на предмет соответствия объекта требованиям по информационной безопасности.
	ПК-6.3 Определяет меры для защиты в информации в телекоммуникационных системах и сетях	***Знать:*** Назначение инструментальных средств обеспечения защиты информации телекоммуникационных систем. ***Уметь:*** Выделять требуемые характеристики средств обеспечения информационной	***Знать:*** Инструментальные средства обеспечения защиты информации телекоммуникационных систем. ***Уметь:*** осуществлять выбор средств обеспечения информационной безопасности телекоммуникационных систем.	***Знать:*** Полный спектр инструментальных средств обеспечения защиты информации телекоммуникационных систем. ***Уметь:*** осуществлять рациональный выбор средств обеспечения информационной безопасности

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
		безопасности телекоммуникационных систем. ***Владеть:*** Базовыми навыками эксплуатации телекоммуникационных приборов и средств защиты информации.	***Владеть:*** Навыками эксплуатации телекоммуникационных приборов и средств защиты информации.	телекоммуникационных систем. ***Владеть:*** Уверенными навыками эксплуатации телекоммуникационных приборов и средств защиты информации.
ПК-9 /завершающий	ПК-9.1 Выявляет сбои и отказы устройств и программ	***Знать:*** отдельные признаки возникновения сбоев и отказов при эксплуатации ТКС ***Уметь:*** под руководством в процессе эксплуатации фиксировать режимы работы ТКС, отличные от штатных ***Владеть:*** обнаружения части сбоев и отказов реальных ТКС	***Знать:*** основные признаки возникновения сбоев и отказов при эксплуатации ТКС ***Уметь:*** в процессе эксплуатации фиксировать режимы работы ТКС, отличные от штатных ***Владеть:*** обнаружения сбоев и отказов типовых ТКС	***Знать:*** различные, в том числе нетиповые признаки возникновения сбоев и отказов при эксплуатации ТКС ***Уметь:*** в процессе эксплуатации выявлять и фиксировать режимы работы ТКС, отличные от штатных ***Владеть:*** обнаружения сбоев и отказов сложных ТКС
	ПК-9.2 Восстанавливает работоспособность систем после сбоев и отказов устройств и программ	***Знать:*** знать номенклатуру регламентных работ по восстановлению работоспособности устройств и программ ***Уметь:***	***Знать:*** порядок проведения регламентных работ по восстановлению работоспособности устройств и программ ***Уметь:***	***Знать:*** знать цели и задачи регламентных работ по восстановлению работоспособности устройств и программ ***Уметь:***

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
		выполнять регламентные работы по восстановлению работоспособности устройств и программ ***Владеть):*** эксплуатации отдельных элементов программного и аппаратного обеспечения ТКС	оперативно выполнять регламентные работы по восстановлению работоспособности устройств и программ ***Владеть:*** эксплуатации программного и аппаратного обеспечения ТКС	выполнять точно и оперативно требуемые работы по восстановлению работоспособности устройств и программ ***Владеть:*** эксплуатации программного и аппаратного обеспечения ТКС в различных режимах работы
	ПК-9.3 Формулирует перечень действий для восстановления последствий сбоев и отказов	***Знать:*** назначение и классификацию программно-аппаратных средств ТКС; технические характеристики и правила эксплуатации средств восстановления последствий сбоев и отказов. ***Уметь:*** провести настройку ПО и оборудования ТКС. ***Владеть:*** навыками настройки, антивирусного ПО.	***Знать:*** назначение и классификацию программно-аппаратных средств ТКС; особенности функционирования ТКС; систем обнаружения сетевых атак, антивирусного ПО; технические характеристики и правила эксплуатации средств восстановления последствий сбоев и отказов. ***Уметь:*** проводить мониторинг безопасности АС; провести настройку ПО и оборудования	***Знать:*** назначение и классификацию программно-аппаратных средств ТКС; особенности функционирования ТКС; классификацию программных и аппаратных средств анализа защищённости ТКС, систем обнаружения сетевых атак, антивирусного ПО; технические характеристики и правила эксплуатации средств восстановления последствий сбоев и отказов. ***Уметь:***

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
			ТКС. ***Владеть:*** навыками настройки программных и аппаратных средств анализа защищённости ТКС, антивирусного ПО.	проводить мониторинг безопасности АС; обнаруживать уязвимые места в функционировании ПО и оборудования ТКС; провести настройку ПО и оборудования ТКС. ***Владеть:*** навыками настройки программных и аппаратных средств анализа защищённости ТКС, систем обнаружения сетевых атак, антивирусного ПО.
	ПК-9.4 Регистрирует сообщения об ошибках в сетевых устройствах и операционных системах	***Знать:*** номенклатуру ошибок в сетевых устройствах и операционных системах ***Уметь:*** в процессе эксплуатации фиксировать режимы работы сетевых устройств и операционных систем, отличные от штатных ***Владеть:*** навыками протоколирования	***Знать:*** основные признаки возникновения ошибок в сетевых устройствах и операционных системах ***Уметь:*** в процессе эксплуатации фиксировать режимы работы сетевых устройств и операционных систем, отличные от штатных ***Владеть:*** навыками	***Знать:*** методику выявления признаков возникновения ошибок в сетевых устройствах и операционных системах ***Уметь:*** в процессе эксплуатации обнаруживать и фиксировать режимы работы сетевых устройств и операционных систем, отличные

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
		отдельных сбоев и отказов реальных сетевых устройств и операционных систем	протоколирования сбоев и отказов реальных сетевых устройств и операционных систем	от штатных ***Владеть:*** навыками обнаружения и протоколирования сбоев и отказов реальных сетевых устройств и операционных систем
	ПК-9.5 Формирует отчёты по результатам работ системы мониторинга	***Знать:*** структуру журналов аудита информационной безопасности ***Уметь:*** под руководством использовать технические средства ведения журналов аудита информационной безопасности ***Владеть:*** навыками формирования журналов аудита информационной безопасности	***Знать:*** структуру и содержание журналов аудита информационной безопасности ***Уметь:*** использовать технические средства ведения журналов аудита информационной безопасности ***Владеть:*** навыками работы с журналами аудита информационной безопасности	***Знать:*** методику формирования журналов аудита информационной безопасности ***Уметь:*** выбирать и использовать технические средства ведения журналов аудита информационной безопасности ***Владеть:*** навыками анализа журналов аудита информационной безопасности
ПК-11 /завершающий	ПК-11.1 Определяет действия по обеспечению информационной безопасности на различных этапах жизненного цикла телекоммуникационной системы	***Знать:*** номенклатуру этапов жизненного цикла ТКС ***Уметь:*** исходя их ограниченного перечня угроз реализовывать технологии обеспечения	***Знать:*** характеристики различных этапов жизненного цикла ТКС ***Уметь:*** исходя их имеющегося перечня угроз реализовывать технологии обеспечения	***Знать:*** особенности различных этапов жизненного цикла ТКС ***Уметь:*** исходя их обширного перечня угроз реализовывать технологии обеспечения

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
		информационной безопасности ***Владеть:*** эксплуатации ТКС на отдельных этапах жизненного цикла	информационной безопасности ***Владеть:*** эксплуатации ТКС на основных этапах жизненного цикла	информационной безопасности ***Владеть:*** эксплуатации ТКС на различных этапах жизненного цикла
	ПК-11.2 Выбирает перечень реализуемых телекоммуникационной системой технологий для удовлетворения требований по информационной безопасности	***Знать:*** перечень реализуемых телекоммуникационной системой технологий для удовлетворения требований по информационной безопасности ***Уметь:*** соотносить отдельные технологии информационной безопасности существующим в ТКС уязвимостям ***Владеть:*** реализации базовых технологий информационной безопасности	***Знать:*** структуру реализуемых телекоммуникационной системой технологий для удовлетворения требований по информационной безопасности ***Уметь:*** соотносить основные технологии информационной безопасности существующим в ТКС уязвимостям ***Владеть:*** реализации основных технологий информационной безопасности	***Знать:*** структуру и особенности реализуемых телекоммуникационной системой технологий для удовлетворения требований по информационной безопасности ***Уметь:*** соотносить технологии информационной безопасности существующим в ТКС уязвимостям ***Владеть:*** реализации стека технологий информационной безопасности
	ПК-11.3 Оценивает результат применения штатных средств обеспечения информационной безопасности	***Знать:*** шкалы результативности применения штатных средств обеспечения информационной безопасности ***Уметь:*** использовать	***Знать:*** критерии результативности применения штатных средств обеспечения информационной безопасности ***Уметь:*** формулировать	***Знать:*** методику оценки результативности применения штатных средств обеспечения информационной безопасности ***Уметь:*** формулировать

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
		количественные критерии результативности применения штатных средств обеспечения информационной безопасности ***Владеть:*** навыками применения штатных средств обеспечения информационной безопасности	количественные критерии результативности применения штатных средств обеспечения информационной безопасности ***Владеть:*** навыками оценки результативности применения штатных средств обеспечения информационной безопасности	методы оценки результативности применения штатных средств обеспечения информационной безопасности ***Владеть:*** сформированными навыками оценки результативности применения различных средств обеспечения информационной безопасности
	ПК-11.4 Формулирует предложения по совершенствованию подсистем обеспечения информационной безопасности	***Знать:*** базовые технологии, направленные на повышение защищённости процессов обработки информации в ТКС ***Уметь:*** определять отдельные меры и технологии, направленные на повышение защищённости процессов обработки информации в конкретной ТКС ***Владеть:*** проведения отдельных процедур защиты	***Знать:*** основные технологии, направленные на повышение защищённости процессов обработки информации в ТКС ***Уметь:*** определять меры и технологии, направленные на повышение защищённости процессов обработки информации в конкретной ТКС ***Владеть:*** обеспечения процесса защиты информации в ТКС	***Знать:*** меры и технологии, направленные на повышение защищённости процессов обработки информации в ТКС ***Уметь:*** определять меры и технологии, направленные на повышение защищённости процессов обработки информации в сложных ТКС ***Владеть:*** обеспечения процесса защиты информации в сложных ТКС

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
		информации в ТКС		

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 форматирования	Оценочные средства		Описание шкал оценивания
				наимено-вание	№ заданий	
1	2	3	4	5	6	7
1	Понятия и определения технических средств охраны. Структура автоматизированной системы охраны	ПК-6, ПК-9, ПК-11	Лекция, СРС,практичес-кая работа	ВС КВЗПР в т.ч. для контроля результатов практической под-готовки	1-5 1-5	Согласно табл. 7.2
2	Варианты программно-аппаратной реализации ТСО	ПК-6, ПК-9, ПК-11	Лекция, СРС,практичес-кая работа	ВС КВЗПР	1-5 1-5	Согласно табл. 7.2
3	Методология разработки концепции комплексного обеспечения безопасности объектов охраны	ПК-6, ПК-9, ПК-11	Лекция, СРС,практичес-кая работа	ВС КВЗПР	1-5 1-5	Согласно табл. 7.2
4	Общий подход к категорированию объектов охраны	ПК-6, ПК-9, ПК-11	Лекция, СРС,практичес-кая работа	ВС КВЗПР	1-5 1-5	Согласно табл. 7.2

5	Классификация нарушителей информационной безопасности, угроз ИБ Классификация технических средств охраны, необходимых для построения комплексной системы защиты информации	ПК-6, ПК-9, ПК-11	Лекция, СРС, практическая работа	ВС КВЗПР в т.ч. для контроля результатов практической под-готовки	1-5 1-5	Согласно табл. 7.2
6	Классификация нарушителей информационной безопасности, угроз ИБ	ПК-6, ПК-9, ПК-11	Лекция, СРС,практичес-кая работа	ВС КВЗПР в т.ч. для контроля результатов практической под-готовки	1-5 1-5	Согласно табл. 7.2

СРС – самостоятельная работа студента, КВЗПР – контрольные вопросы для защиты практических работ, ВС – вопросы для собеседования

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для собеседования

Тема 1. Понятия и определения технических средств охраны. Структура автоматизированной системы охраны

1. Что такое технические средства охраны (ТСО)?
2. Назначение и цели ТСО.
3. Основные виды ТСО.
4. Дайте определение термину «Техническая безопасность».
5. Дайте определение термину «Компьютерная безопасность».
6. Что такое канал сигнализации? Как можно классифицировать ССОИ.

Контрольные вопросы для защиты практической работы №5:

1. Физические основы акустического канала утечки.
2. Способы пассивной защита акустического ТКУ КИ.
3. Способы активной защиты акустического ТКУКИ.
4. Как выбираются частоты сигнала при оценке защищенности акустического ТКУКИ?
5. Что такое октавная полоса звуковых частот?
6. Как образуется виброакустический ТКУКИ?

7. В чем состоят различия акустического и виброакустического сигналов утечки КИ?

Производственная задача для контроля результатов практической подготовки обучающихся на лабораторном занятии №1

1. составить по имеющимся вариантам планировок и техническому заданию поэтажные план-схемы оборудования СВН;
2. рассчитать углы обзора и фокусное расстояние каждой камеры; выбрать марки камер, кожухов, объективов, мультиплексоров и другого оборудования;
3. составить структурную схему СВН; составить краткое техническое описание оборудования и используемого ПО.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме экзамена. Экзамен проводится в виде компьютерного тестирования.

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

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

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

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

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

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

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в открытой форме:

В концепции обеспечения информационной безопасности предприятия определяются _____

Задание в закрытой форме:

Конфиденциальность – это..

a. защита от несанкционированного доступа к информации

b. программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

c. описание процедур

Задание на установление правильной последовательности,

Надиктовать тестовую информацию (с обязательным указанием номера точки, в которой производиться измерение, и расстояния до нее от центра антенны ЛГШ-104), расположить антенну ЛГШ-104 на столе; повторить измерения во всех 7 контрольных точках; Включить ЛГШ-104 и провести измерение среднего значения напряженности поля *E*; включить диктофоны на запись; переместить диктофоны на 15 см в заданную сторону от центра антенныЛГШ-104; поместить антенну прибора ЛГШ-104 на подставку, находящуюся под столом; повторить измерения.

Задание на установление соответствия:

1 Случайный нарушитель

2 Неподготовленный нарушитель

3 Подготовленный нарушитель

4 Осведомленный нарушитель

5 Сотрудник предприятия или охранник

А обладающий специальной подготовкой, имеющий сведения об организации системы охраны на объекте

Б обладающий специальной подготовкой, часто действующий в сговоре с осведомленным нарушителем (характерно для крупного предприятия).

Г проникающий на объект со специальной целью и предполагающий возможность охраны объекта, но не имеющий представления о системе охраны и принципах ее функционирования.

Д имеющий информацию о возможных методах обхода действующих средств охраны, прошедший соответствующую подготовку скрытно преодолевать зоны обнаружения средств из состава комплексной системы безопасности.

Е не знающий, что объект охраняется и не имеющий специальной цели проникновения на объект.

Компетентностно-ориентированная задача:

Рассчитать требуемое кол-во ГШ-1000 для зашумления помещения с ПК если его размеры следующие длина 20 м ширина 6 м.

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
1	2	3	4	5
Выполнение работы №1	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Выполнение работы №2	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Выполнение работы №3	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Выполнение работы №4	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Выполнение работы №5	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Выполнение работы №6	2	Выполнил, доля правильных ответов от 50% до 90%	4	Выполнил, доля правильных ответов более 90%
Собеседование по теме 1	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Собеседование по теме 2	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Собеседование по теме 3	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Собеседование по теме 4	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Собеседование по теме 5	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Собеседование по теме 6	2	Доля правильных ответов от 50% до 90%	4	Доля правильных ответов более 90%
Итого	24		48	

Посещаемость	0		16	
Экзамен	0		36	
Итого	24		100	

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

Каждый верный ответ оценивается следующим образом:

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

Максимальное количество баллов за тестирование –36 баллов.

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

8.1 Основная учебная литература

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

2. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : [16+] / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

8.2 Дополнительная учебная литература

3. Проскуряков, А. В. Компьютерные сети: основы построения компьютерных сетей и телекоммуникаций: учебное пособие / А. В. Проскуряков; Министерство науки и высшего образования Российской Федерации ; Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет» ; Инженерно-технологическая академия. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 202 с. : ил. - URL: http://biblioclub.ru/index.php?page=book&id=561238. (дата обращения 16.02.2023) . - Режим доступа: по подписке. – Текст : электронный.

4. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учебник для студентов вузов, обучающихся по направлению 552800 "Информатика и вычислительная техника" и по специальностям 220100 "Вычислительные машины, комплексы, системы и сети", 220200 "Автоматизированные системы обработки информации и управления" и 220400 "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Г. Олифер, Н. А. Олифер. - 5-е изд. - Санкт-Петербург : Питер, 2019. - 922 с. – Текст : непосредственный.

5. Спеваков, А. Г. Основы правового обеспечения информационной безопасности [Текст] : учебное пособие / А. П. Фисун. - Курск : ЮЗГУ, 2013 - Ч. 1 / Минобрнауки России, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Юго-Западный государственный университет". - 150 с.

6. Спеваков, А. Г. Основы правового обеспечения информационной безопасности [Текст] : учебное пособие / А. П. Фисун. - Курск : ЮЗГУ, 2013 - Ч. 2 / Минобрнауки России, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Юго-Западный государственный университет". - 303 с.

8.3 Перечень методических указаний

1) Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение [Электронный ресурс] : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Электрон. текстовые дан. (541 КБ). - Курск : ЮЗГУ, 2017. - 16 с. : ил., табл. - Библиогр.: с. 16. - Б. ц.

2) Определение показателей защищенности информации при несанкционированном доступе [Электронный ресурс] : методические указания по выполнению лабораторной работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: В. В. Карасовский, О. А. Демченко. - Электрон. текстовые дан. (342 КБ). - Курск : ЮЗГУ, 2017. - 7 с. : ил., табл. - Библиогр.: с. 7. - Б. ц.

3) Критерии оценки и выбора CASE-Средств : методические указания для выполнения лабораторных и практических работ студентами групп специальностей 02.03.03, 09.00.00, 10.00.00, 11.00.00, 12.03.04, 38.05.01, 45.03.03 / Юго-Зап. гос. ун-т ; сост. О. А. Демченко. - Электрон. текстовые дан. (298 КБ). - Курск : ЮЗГУ, 2022. - 11 с. - Загл. с титул. экрана. - Б. ц.

4) Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности [Электронный ресурс] : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Электрон. текстовые дан. (324 КБ). - Курск : ЮЗГУ, 2017. - 7 с. : ил., табл. - Библиогр.: с. 7. - Б. ц.

5) Исследование противодействия несанкционированной работе портативных звукозаписывающих устройств : [Электронный ресурс] : методические указания по выполнению практических работ по дисциплине «Технология обеспечения информационной безопасности объекта» для студентов специальности 10.00.00 / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Электрон. текстовые дан. (314 КБ). - Курск : ЮЗГУ, 2017. - 9 с. - Б. ц.

6) Исследование акустического и виброакустического каналов утечки информации : [Электронный ресурс] : методические указания по выполнению практических работ по дисциплине «Технология обеспечения информационной безопасности объекта» для студентов специальности 10.00.00 / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Электрон. текстовые дан. (321 КБ). - Курск : ЮЗГУ, 2017. - 12 с. - Б. ц.

9 Перечень ресурсов информационно-телекаммуникационной 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/

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Комплексная защита объектов информатизации» являются лекции и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

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

Изучение наиболее важных тем или разделов дисциплины завершают практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

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.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Комплексная защита объектов информатизации»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных

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

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Комплексная защита объектов информатизации» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Комплексная защита объектов информатизации» - 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";
- Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624- 192234;
- Windows 7, договор IT000012385;
- редактор двоичных файлов Free Hex Editor Neo, (Свободное ПО договор IT000012385, http://www.hhdsoftware.com/free-hex-editor),
- открытая среда разработки программного обеспечения Lazarus (Свободное ПО http://www.lazarus.freepascal.org/);
- система виброакустического зашумления «Шорох-2» (104.3009);
- виброакустический датчик КПВ-2 (104.3000);
- виброакустический датчик КПВ-7 (104.3002).

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

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10 шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран

на штативе; Мультимедиацентр: ноут бук ASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/ проектор inFocusIN24+.

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

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

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

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

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	Изме-нённых	Заменён ных	Аннули рованн ых	новых			