

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 выполнять работы по обеспечению информационной безопасности автоматизированных систем на всех этапах их жизненного цикла (ПК-5).

Способен определять уровень защищённости автоматизированных систем (ПК-7).

Способен выполнять задачи по выявлению уязвимых узлов автоматизированной системы (ПК-8).

Способен собирать, анализировать и систематизировать информацию по зафиксированным инцидентам информационной безопасности (ПК-10).

Разделы дисциплины

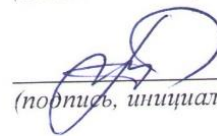
Понятия и определения технических средств охраны. Структура автоматизированной системы охраны. Варианты программно-аппаратной реализации ТСО. Методология разработки концепции комплексного обеспечения безопасности объектов охраны. Общий подход к категорированию объектов охраны. Классификация нарушителей 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 10.03.01 Информационная безопасность*(цифр согласно ФГОС и наименование направления подготовки (специальности))*направленность (профиль, специализация) «Безопасность автоматизирован-
ных систем в сфере информационных и коммуникационных технологий»*наименование направленности (профиля, специализации)*

форма обучения

очная*(очная, очно-заочная, заочная)*

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», 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 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий» на заседании кафедры информационной безопасности №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 пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета протокол № « » 20 г., на заседании кафедры _____.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

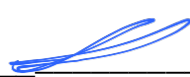
Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым 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 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета протокол № 9 «22» 03 204 г. на заседании кафедры *информационной безопасности*
протокол № 12 «24» 06 2024 г.

Зав. кафедрой _____

 Марухленко А.А.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета протокол № 9 «31» 03 2025 г. на заседании кафедры *информационной безопасности*
протокол № 12 «24» 06 2025 г.

Зав. кафедрой _____

 Марухленко А.А.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета протокол № « » 20 г. на заседании кафедры *информационной безопасности*
протокол № « » 20 г.

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий», одобренного Ученым советом университета протокол № « » 20 г. на заседании кафедры *информационной безопасности*
протокол № « » 20 г.

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-5	Способен выполнять работы по обеспечению информационной безопасности автоматизированных систем на всех этапах их жизненного цикла	ПК-5.1 Проверяет соответствие внедряемых решений и средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности	Знать: -реализуемую политику безопасности; -основные характеристики программных и технических средств разработки ПО;

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			<p>-особенности проверки внедряемых решений и средств для обеспечения информационной безопасности;</p> <p>Уметь:</p> <ul style="list-style-type: none"> -строить модели формирования решений для обеспечения информационной безопасности; -находить возможные решения и средства информационной безопасности; -анализировать возможные несоответствия внедряемых решений. <p>Владеть:</p> <ul style="list-style-type: none"> -навыком выбора соответствующего решения/ средства для обеспечения информационной безопасности; -навыками разработки средств обеспечения информационной безопасности; -навыками определения соответствия выбранных средств реализуемой политики безопасности.
		<p>ПК-5.2 Восстанавливает работоспособность автоматизированных систем после инцидентов информационной безопасности</p>	<p>Знать:</p> <ul style="list-style-type: none"> -особенности автоматизированных систем; -виды инцидентов информационной безопасности; -особенности восстановления автоматизированных систем после

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			<p>инцидентов информационной безопасности.</p> <p>Уметь:</p> <ul style="list-style-type: none"> - определять причину возникновения инцидента информационной безопасности; - анализировать предметную область и создавать декларативное описание задачи; - применять принципы выявления ключевых параметров работы автоматизированной системы; <p>Владеть:</p> <ul style="list-style-type: none"> - приемами анализа полноты и корректности ключевых параметров эксплуатации автоматизированных систем; - навыком определения вида инцидента; - навыком восстановления работоспособности автоматизированной системы.
		<p>ПК-5.3 Проводит операции вывода защищённых автоматизированных систем из эксплуатации</p>	<p>Знать:</p> <ul style="list-style-type: none"> - содержание и порядок выполнения работ на стадиях создания автоматизированных систем в защищенном исполнении; - технологии повышения защищенности автоматизированных систем из эксплуатации; - особенности вывода защищённых

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			автоматизированных систем из эксплуатации. Уметь: - выполнять определять характер угрозы и масштабы последствий; -проектировать регламент защищенного взаимодействия компонентов автоматизированных систем; -минимизировать последствия ущерба за счет интеграции средств защиты. Владеть: - навыками разработки компонентов автоматизированных систем; - навыками обеспечения совместимого взаимодействия отдельных модулей; -навыками вывода защищённых автоматизированных систем из эксплуатации.
ПК-7	Способен определять уровень защищённости автоматизированных систем	ПК-7.1 Формулирует целевые показатели функционирования защищенных автоматизированных систем	Знать: - критерии оценки защищенности автоматизированной системы; - регламент информирования персонала автоматизированной системы о выявленных инцидентах; - регламент учета выявленных инцидентов; - основные криптографические методы, алгоритмы,

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной	Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций
код компетенции	наименование компетенции		
			<p>протоколы, используемые для обеспечения защиты информации в автоматизированных системах.</p> <p>Уметь:</p> <ul style="list-style-type: none"> - определять источники и причины возникновения инцидентов; - формулировать целевые показатели функционирования защищённых автоматизированных систем; - проводить оценку защищенности автоматизированных систем с помощью типовых программных средств; - рассчитывать и проводить инструментальный контроль показателей эффективности защиты информации; <p>Владеть:</p> <ul style="list-style-type: none"> - навыками определения источников и причин возникновения инцидентов; - навыками расчёта целевых показателей защищённых автоматизированных систем.
		ПК-7.2 Анализирует уязвимости автоматизированных систем в соответствии с нормативными документами	<p>Знать:</p> <ul style="list-style-type: none"> - нормативные документы; - особенности анализа уязвимости, автоматизированные

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			<p>систем;</p> <ul style="list-style-type: none"> - основные виды уязвимости автоматизированных систем. <p>Уметь:</p> <ul style="list-style-type: none"> - анализировать уязвимости автоматизированных систем в соответствии с требованиями; - минимизировать количество потенциальных несоответствий. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками установки директив, определяющих работу автоматизированных систем; - навыками проведения анализа нормативных документов; - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных.
		<p>ПК-7.3 Формулирует угрозы информационной безопасности исходя из выявленных характеристик автоматизированной системы</p>	<p>Знать:</p> <ul style="list-style-type: none"> -основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; -основы шифрования потоков данных; - основы использования средств защиты информации. <p>Уметь:</p> <ul style="list-style-type: none"> -организовать

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			<p>безопасную работу в масштабе вычислительной сети;</p> <ul style="list-style-type: none"> - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на программном уровне. <p>Владеть:</p> <ul style="list-style-type: none"> -навыками установки программных средств защиты; -навыками оценки защищенности информационной системы с учетом возможных угроз.
ПК-8	Способен выполнять задачи по выявлению уязвимых узлов автоматизированной системы	ПК-8.1 Разрабатывает методическую, техническую, рекомендательную и отчетную документацию по анализу защищенности автоматизированной системы	<p>Знать:</p> <ul style="list-style-type: none"> -содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; -основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; -основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах; нормативно-правовые акты в области информационной

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной	Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций
код компетенции	наименование компетенции		
			<p>безопасности и защиты информации.</p> <p>Уметь:</p> <ul style="list-style-type: none"> -анализировать программные, архитектурно-технические и схмотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации -разрабатывать методическую, техническую, рекомендательную и отчётную документацию по анализу защищённости автоматизированной системы; -контролировать эффективность принятых мер по защите информации в автоматизированных системах. <p>Владеть:</p> <ul style="list-style-type: none"> -навыками анализ компонентов автоматизированных систем; -навыками разработки документации.
		<p>ПК-8.2</p> <p>Осуществляет подбор программных средств тестирования защищённости автоматизированной системы в зависимости от</p>	<p>Знать:</p> <ul style="list-style-type: none"> -принципы построения и функционирования систем и сетей передачи информации; -основные угрозы безопасности

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
		предъявляемым к ней требованиям	<p>информации и модели нарушителя в автоматизированных системах;</p> <ul style="list-style-type: none"> - основные меры по защите информации в автоматизированных системах - принципы построения средств защиты информации от утечки по техническим каналам; - основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах; - технические каналы утечки информации; - технические средства контроля эффективности мер защиты информации <p>Уметь:</p> <ul style="list-style-type: none"> - анализировать основные узлы и устройства современных автоматизированных систем; - применять действующую нормативную базу в области обеспечения безопасности информации; - контролировать безотказное функционирование технических средств защиты информации - составлять методики тестирования систем защиты информации

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			автоматизированных систем - подбирать программные средства тестирования систем защиты информации автоматизированных систем. Владеть: - навыками установки программных средств защиты; - навыками оценки защищенности информационной системы с учетом возможных угроз. - навыками анализа основных узлов и устройств современных автоматизированных систем.
		ПК-8.3 Использует средств инструментального анализа защищённости программных и аппаратных платформ узлов автоматизированной системы	Знать: - принципы построения компьютерных систем и сетей; - формальные модели безопасности компьютерных систем и сетей; - принципы построения систем обнаружения компьютерных атак; - методы обработки данных мониторинга безопасности компьютерных систем и сетей; - порядок создания и структура отчета, создаваемого по результатам проверок; - способы обнаружения и нейтрализации последствий вторжений

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			<p>в компьютерные системы;</p> <ul style="list-style-type: none"> - криптографические протоколы. <p>Уметь:</p> <ul style="list-style-type: none"> -формализовывать задачу управления безопасностью автоматизированных систем; -применять инструментальные средства проведения мониторинга защищенности автоматизированных систем; -применять методы анализа защищенности компьютерных систем и сетей; -структурировать аналитическую информацию для включения в отчет. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками выполнения анализа защищенности; - навыками составления отчетов по результатам проверок.
		<p>ПК-8.4 Проводит контроль защищённости и функционирования программно-аппаратных и технических средств автоматизированной системы</p>	<p>Знать:</p> <ul style="list-style-type: none"> -основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности информации; -способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			<p>информации; -принципы построения систем защиты информации. Уметь: -классифицировать и оценивать угрозы безопасности информации для объекта информатизации; -разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; -разрабатывать политики безопасности информации автоматизированных систем; -применять действующую законодательную базу в области обеспечения защиты информации Владеть: -навыками оценки информационных рисков; -навыками экспертизы состояния защищенности информации автоматизированных систем; -навыками обоснования критериев эффективности функционирования защищенных автоматизированных систем.</p>

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной	Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций
код компетенции	наименование компетенции		
ПК-10	Способен собирать, анализировать и систематизировать информацию по зафиксированным инцидентам информационной безопасности	ПК-10.3 Формулирует правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности	<p>Знать: правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности.</p> <p>Уметь: Формулировать правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности</p> <p>Владеть: навыками разработки мер защиты информации, правил применения мер защиты информации, направленных на устранение причин возникновения инцидентов информационной безопасности.</p>

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 бакалавриата 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий». Дисциплина изучается на 4 курсе в 8 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 5 зачётных единицы, 180 часов

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоёмкость дисциплины	180
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	90
в том числе:	
лекции	36
практические занятия	54
Самостоятельная работа обучающихся (всего)	61,85
Контроль (подготовка к экзамену)	27
Контактная работа по промежуточной аттестации (всего АттКР)	1,15
в том числе:	
зачет	не предусмотрен
зачет с оценкой	не предусмотрен
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- методическ ие материалы	Формы текущего контроля успеваемости (<i>по неделям семестра</i>)	Компетенц ии
		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-5, ПК-7, ПК-8, ПК-10
2	Варианты программно-аппаратной реализации ТСО	6	2	У 1-6, МУ 1-6	С, ЗПР (2-6)	ПК-5, ПК-7, ПК-8, ПК-10
3	Методология разработки концепции комплексного обеспечения безопасности объектов охраны	6	3	У 1-6, МУ 1-6	С, ЗПР (7-9)	ПК-5, ПК-7, ПК-8, ПК-10

1	2	3	4	5	6	7
4	Общий подход к категорированию объектов охраны	6	4	У 1-6, МУ 1-6	С, ЗПР (10-12)	ПК-5, ПК-7, ПК-8, ПК-10
5	Классификация нарушителей информационной безопасности, угроз ИБ	6	5	У 1-6, МУ 1-6	С, ЗПР (13-15)	ПК-5, ПК-7, ПК-8, ПК-10
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-5, ПК-7, ПК-8, ПК-10
	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
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
6	Исследование акустического и виброакустического каналов утечки информации	10
	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	1-3 неделя	9,85

	охраны. Структура автоматизированной системы охраны		
2	Варианты программно-аппаратной реализации ТСО	4-7 неделя	10
3	Методология разработки концепции комплексного обеспечения безопасности объектов охраны	8-11 неделя	14
4	Общий подход к категорированию объектов охраны	12-15 неделя	14
5	Классификация нарушителей информационной безопасности, угроз ИБ и технических средств охраны	16-18 неделя	14
Итого			61.85

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 экзамену;
 - 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	Объем, 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.	Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности	Разбор конкретных ситуаций	2
4.	Исследование противодействия несанкционированной работе портативных звукозаписывающих устройств	Разбор конкретных ситуаций	2
5.	Исследование акустического и виброакустического каналов утечки информации	Разбор конкретных ситуаций	2
Итого			12

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-5 Способен выполнять работы по обеспечению информационной безопасности автоматизированных систем на всех этапах их жизненного цикла	Методы защиты программного обеспечения	Комплексная защита объектов информатизации Производственная преддипломная практика	
ПК-7 Способен определять уровень защищённости автоматизированных систем	Комплексная защита объектов информатизации Производственная преддипломная практика		
ПК-8 Способен выполнять задачи по выявлению уязвимых узлов	Комплексная защита объектов информатизации Производственная преддипломная практика		

автоматизированной системы		
ПК-10 Способен собирать, анализировать и систематизировать информацию по зафиксированным инцидентам информационной безопасности	Системы охраны и инженерной защиты информации	Комплексная защита объектов информатизации

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-5 /завершающий	ПК-5.1 Проверяет соответствие внедряемых решений и средств для обеспечения информационной безопасности требованиям реализуемой политики безопасности	Знать: -основные характеристики программных и технических средств разработки ПО; Уметь: - строить модели формирования решений для обеспечения информационной безопасности; - анализировать возможные несоответствия внедряемых решений. Владеть): -навыками	Знать: -реализуемую политику безопасности; -особенности проверки внедряемых решений и средств для обеспечения информационной безопасности; Уметь: -находить возможные решения и средства информационной безопасности; -анализировать возможные несоответствия	Знать: - реализуемую политику безопасности; -основные характеристики программных и технических средств разработки ПО; - особенности проверки внедряемых решений и средств для обеспечения информационной безопасности; Уметь: - строить модели формирования решений для

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 («удовлетворитель но»)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
		разработки средств обеспечения информационной безопасности; -навыками определения соответствия выбранных средств реализуемой политики безопасности.	внедряемых решений. Владеть: - навыком выбора соответствующего решения/ средства для обеспечения информационной безопасности; -навыками определения соответствия выбранных средств реализуемой политики безопасности.	обеспечения информационной безопасности; -находить возможные решения и средства информационной безопасности; - анализировать возможные несоответствия внедряемых решений. Владеть: - навыком выбора соответствующего решения/ средства для обеспечения информационной безопасности; -навыками разработки средств обеспечения информационной безопасности; -навыками определения соответствия выбранных средств реализуемой политики безопасности.
	ПК-5.2 Восстанавливает работоспособност ь автоматизированн ых систем после инцидентов информационной	Знать: -особенности автоматизированн ых систем; - виды инцидентов информационной безопасности; Уметь:	Знать: - виды инцидентов информационной безопасности; -особенности восстановления автоматизированн ых систем после	Знать: -особенности автоматизированн ых систем; - виды инцидентов информационной безопасности; -особенности

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 («удовлетворитель но»)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	безопасности	<p>-определять причину возникновения инцидента информационной безопасности;</p> <p>-применять принципы выявления ключевых параметров работы автоматизированной системы;</p> <p>Владеть):</p> <p>-навыком определения вида инцидента;</p> <p>-навыком восстановления работоспособности и автоматизированной системы.</p>	<p>инцидентов информационной безопасности.</p> <p>Уметь:</p> <p>- анализировать предметную область и создавать декларативное описание задачи;</p> <p>-применять принципы выявления ключевых параметров работы автоматизированной системы;</p> <p>Владеть:</p> <p>-навыком определения вида инцидента;</p> <p>-навыком восстановления работоспособности автоматизированной системы.</p>	<p>восстановления автоматизированных систем после инцидентов информационной безопасности.</p> <p>Уметь:</p> <p>-определять причину возникновения инцидента информационной безопасности;</p> <p>-анализировать предметную область и создавать декларативное описание задачи;</p> <p>-применять принципы выявления ключевых параметров работы автоматизированной системы;</p> <p>Владеть:</p> <p>-приемами анализа полноты и корректности ключевых параметров эксплуатации автоматизированных систем;</p> <p>-навыком определения вида инцидента;</p> <p>-навыком восстановления работоспособности</p>

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 («удовлетворитель но»)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
				автоматизированно й системы.
	ПК-5.3 Проводит операции вывода защищённых автоматизированн ых систем из эксплуатации	Знать: - содержание и порядок выполнения работ на стадиях создания автоматизированн ых систем в защищенном исполнении; -особенности вывода защищённых автоматизированн ых систем из эксплуатации. Уметь: - минимизировать последствия ущерба за счет интеграции средств защиты. Владеть: -навыками обеспечения совместимого взаимодействия отдельных модулей; -навыками вывода защищённых автоматизированн ых систем из эксплуатации.	Знать: -технологии повышения защищенности автоматизированн ых систем из эксплуатации; -особенности вывода защищённых автоматизированн ых систем из эксплуатации. Уметь: -выполнять определять характер угрозы и масштабы последствий; - проектировать регламент защищенного взаимодействия компонентов автоматизированн ых систем; Владеть: -навыками разработки компонентов автоматизированн ых систем; - навыками вывода защищённых автоматизированн ых систем из эксплуатации.	Знать: -содержание и порядок выполнения работ на стадиях создания автоматизированн ых систем в защищенном исполнении; -технологии повышения защищенности автоматизированн ых систем из эксплуатации; -особенности вывода защищённых автоматизированн ых систем из эксплуатации. Уметь: -выполнять определять характер угрозы и масштабы последствий; -проектировать регламент защищенного взаимодействия компонентов автоматизированн ых систем; - минимизировать последствия ущерба за счет интеграции

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 («удовлетворитель но»)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
				<p>средств защиты.</p> <p>Владеть:</p> <ul style="list-style-type: none"> -навыками разработки компонентов автоматизированных систем; -навыками обеспечения совместимого взаимодействия отдельных модулей; - навыками вывода защищённых автоматизированных систем из эксплуатации.
ПК-7 /завершающий	ПК-7.1 Формулирует целевые показатели функционирования защищенных автоматизированных систем	<p>Знать: перечень реализуемых телекоммуникационной системой технологий для удовлетворения требований по информационной безопасности</p> <p>Уметь: соотносить отдельные технологии информационной безопасности существующим в ТКС уязвимостям</p> <p>Владеть: реализации базовых технологий</p>	<p>Знать: структуру реализуемых телекоммуникационной системой технологий для удовлетворения требований по информационной безопасности</p> <p>Уметь: соотносить основные технологии информационной безопасности существующим в ТКС уязвимостям</p> <p>Владеть: реализации основных технологий</p>	<p>Знать: структуру и особенности реализуемых телекоммуникационной системой технологий для удовлетворения требований по информационной безопасности</p> <p>Уметь: соотносить технологии информационной безопасности существующим в ТКС уязвимостям</p> <p>Владеть: реализации стека технологий информационной</p>

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 («удовлетворитель но»)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
		информационной безопасности	информационной безопасности	безопасности
	ПК-7.2 Анализирует уязвимости автоматизированн ых систем в соответствии с нормативными документами	<p>Знать:</p> <ul style="list-style-type: none"> - нормативные документы; - основные виды уязвимости автоматизированн ых систем. <p>Уметь:</p> <ul style="list-style-type: none"> - минимизировать количество потенциальных несоответствий. <p>Владеть:</p> <ul style="list-style-type: none"> - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных. 	<p>Знать:</p> <ul style="list-style-type: none"> - особенности анализа уязвимости автоматизированн ые систем; - основные виды уязвимости автоматизированн ых систем. <p>Уметь:</p> <ul style="list-style-type: none"> - анализировать уязвимости автоматизированн ых систем в соответствии с требованиями; <p>Владеть:</p> <ul style="list-style-type: none"> - навыками установки директив, определяющих работу автоматизированн ых систем; - технологией ведения протокола работы системы с выводом промежуточных результатов обработки данных. 	<p>Знать:</p> <ul style="list-style-type: none"> - нормативные документы; - особенности анализа уязвимости автоматизированн ые систем; - основные виды уязвимости автоматизированн ых систем. <p>Уметь:</p> <ul style="list-style-type: none"> - анализировать уязвимости автоматизированн ых систем в соответствии с требованиями; - минимизировать количество потенциальных несоответствий. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками установки директив, определяющих работу автоматизированн ых систем; - навыками проведения анализа нормативных документов; - технологией ведения протокола работы системы с

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 («удовлетворитель но»)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
				выводом промежуточных результатов обработки данных.
	ПК-7.3 Формулирует угрозы информационной безопасности исходя из выявленных характеристик автоматизированн ой системы	<p>Знать:</p> <ul style="list-style-type: none"> - основы шифрования потоков данных; - основы использования средств защиты информации. <p>Уметь:</p> <ul style="list-style-type: none"> - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; <p>Владеть:</p> <ul style="list-style-type: none"> - навыками оценки защищенности информационной системы с учетом возможных угроз. 	<p>Знать:</p> <ul style="list-style-type: none"> - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; - основы шифрования потоков данных; - основы использования средств защиты информации. <p>Уметь:</p> <ul style="list-style-type: none"> - организовать безопасную работу в масштабе вычислительной сети; - интегрировать средства защиты на программном уровне. <p>Владеть):</p> <ul style="list-style-type: none"> - навыками установки программных средств защиты; 	<p>Знать:</p> <ul style="list-style-type: none"> - основы работы в режиме пошаговой отладки передачи конфиденциальных данных в информационной системе; - основы шифрования потоков данных; - основы использования средств защиты информации. <p>Уметь:</p> <ul style="list-style-type: none"> - организовать безопасную работу в масштабе вычислительной сети; - выводить сообщения в случае возникновения нештатных ситуаций работы информационной системы; - интегрировать средства защиты на программном уровне. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками установки

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 («удовлетворитель но»)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
				программных средств защиты; - навыками оценки защищенности информационной системы с учетом возможных угроз.
ПК-8 /завершающи й	ПК-8.1 Разрабатывает методическую, техническую, рекомендательну ю и отчётную документацию по анализу защищённости автоматизированн ой системы	Знать: перечень угроз, на нейтрализацию которых направлены отдельные меры по защите информации Уметь: проводить отдельные мероприятия по обеспечению информационной безопасности в логически структурированн е последовательност и Владеть: использования отдельных технологий обеспечения информационной безопасности в ТКС	Знать: перечень угроз, на нейтрализацию которых направлена та или иная мера по защите информации Уметь: последовательно проводить отдельные мероприятия по обеспечению информационной безопасности в логически структурированн е последовательност и Владеть: использования типовых технологий обеспечения информационной безопасности в ТКС	Знать: методики определения угроз, на нейтрализацию которых направлена та или иная мера по защите информации Уметь: объединять отдельные мероприятия по обеспечению информационной безопасности в логически структурированн е последовательност и Владеть: использования разнообразных технологий обеспечения информационной безопасности в ТКС
	ПК-8.2 Осуществляет подбор программных	Знать: номенклатуру этапов работ по оценке уровня	Знать: последовательност ь работ по оценке уровня	Знать: методику и принципы оценки уровня

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 («удовлетворитель но»)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	средств тестирования защищённости автоматизированной системы в зависимости от предъявляемым к ней требованиям	защищённости автоматизированных системы Уметь: проводить оценку отдельных характеристик защищённости автоматизированной системы Владеть: навыками оценки отдельных характеристик автоматизированных систем	защищённости автоматизированных систем Уметь: проводить оценку уровня защищённости автоматизированной системы Владеть: навыками контроля уровня защищённости автоматизированных систем	защищённости автоматизированной системы. Уметь: проводить оценку уровня защищённости сложной и нетиповой автоматизированной системы Владеть: навыками контроля уровня защищённости сложной и нетиповой автоматизированной системы
	ПК-8.3 Использует средств инструментального анализа защищённости программных и аппаратных платформ узлов автоматизированной системы	Знать: отдельные уязвимости защищённости автоматизированных систем и угрозы автоматизированных систем Уметь: использовать инструментальные средства выявления уязвимостей защищённости автоматизированных систем Владеть: навыками выявления типовых	Знать: уязвимости защищённости автоматизированных систем и угрозы автоматизированных систем Уметь: с помощью инструментальных средств выявлять уязвимости защищённости автоматизированных систем Владеть: навыками выявления уязвимостей защищённости автоматизированных систем	Знать: уязвимости защищённости автоматизированных систем и угрозы автоматизированных систем и методики их выявления Уметь: выявлять уязвимости защищённости автоматизированных систем комбинацией различных методов и средств Владеть: навыками выявления уязвимостей

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 («удовлетворитель но»)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
		уязвимостей защищённости автоматизированн ых систем		защищённости автоматизированн ых систем, в том числе и не описанных в специализированн ых справочниках
	ПК-8.4 Проводит контроль защищённости и функционирова ния программно- аппаратных и технических средств автоматизированн ой системы	Знать: отдельные уязвимости защищённости телекоммуникаци онных систем и сетей и угрозы автоматизированн ых систем Уметь: использовать инструментальные средства выявления уязвимостей защищённости телекоммуникаци онных систем и сетей Владеть: навыками выявления типовых уязвимостей защищённости автоматизированн ых систем	Знать: уязвимости защищённости телекоммуникацио нных систем и сетей и угрозы автоматизированн ых систем Уметь: с помощью инструментальных средств выявлять уязвимости защищённости телекоммуникацио нных систем и сетей Владеть: навыками выявления уязвимостей защищённости автоматизированн ых систем	Знать: уязвимости защищённости телекоммуникацио нных систем и сетей и угрозы автоматизированн ых систем и методики их выявления Уметь: выявлять уязвимости защищённости телекоммуникацио нных систем и сетей комбинацией различных методов и средств Владеть: навыками выявления уязвимостей защищённости автоматизированн ых систем, в том числе и не описанных в специализированн ых справочниках
ПК-10 /завершающи й	ПК-10.3 Формулирует правила применения мер	Знать: основные правила применения мер защиты	Знать: правила применения мер защиты	Знать: в полной мере правила применения мер

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
	защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности	информации. Уметь: формулировать основные правила применения мер защиты информации. Владеть: применения базовых мер защиты информации, направленных на устранение причин инцидентов информационной безопасности.	информации. Уметь: формулировать основные правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности. Владеть: применения мер защиты информации, направленных на устранение причин инцидентов информационной безопасности.	защиты информации. Уметь: в полной мере формулировать расширенный список правил применения мер защиты информации, направленных на устранение причин возникновения инцидентов информационной безопасности. Владеть: в полной мере применения мер защиты информации, направленных на устранение причин инцидентов информационной безопасности.

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
				наименование	№ заданий	
1	2	3	4	5	6	7
1	Понятия и определения технических средств охраны. Структура автоматизированной системы охраны	ПК-5, ПК-7, ПК-8, ПК-10	Лекция, СРС, практическая работа	ВС КВЗПР	1-5 1-5	Согласно табл. 7.2
2	Варианты программно-аппаратной реализации ТСО	ПК-5, ПК-7, ПК-8, ПК-10	Лекция, СРС, практическая работа	ВС КВЗПР	1-5 1-5	Согласно табл. 7.2
3	Методология разработки концепции комплексного обеспечения безопасности объектов охраны	ПК-5, ПК-7, ПК-8, ПК-10	Лекция, СРС, практическая работа	ВС КВЗПР	1-5 1-5	Согласно табл. 7.2
4	Общий подход к категорированию объектов охраны	ПК-5, ПК-7, ПК-8, ПК-10	Лекция, СРС, практическая работа	ВС КВЗПР	1-5 1-5	Согласно табл. 7.2
5	Классификация нарушителей информационной безопасности, угроз ИБ	ПК-5, ПК-7, ПК-8, ПК-10	Лекция, СРС, практическая работа	ВС КВЗПР	1-5 1-5	Согласно табл. 7.2
6	Классификация технических средств охраны,	ПК-5, ПК-7, ПК-8,	Лекция, СРС, практическая работа	ВС КВЗПР	1-5 1-5	Согласно табл. 7.2

	необходимых для построения комплексной системы защиты информации	ПК-10				
--	--	-------	--	--	--	--

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 5. Классификация нарушителей информационной безопасности, угроз ИБ

1. Внутренние и внешние нарушители
2. Причины и мотивы нарушений
3. Перечень угроз, оценки вероятностей их реализации
4. Модели нарушителей, служащие основой для анализа риска реализации угроз
5. Виды техники, предназначенные для использования силами охраны с целью повышения эффективности обнаружения нарушителя и обеспечения контроля доступа на объект охраны

Контрольные вопросы для защиты практической работы №1:

1. Какие части документа относятся к вопросам защиты информации?
2. Что такое CISQ?
3. Что показывают комментарии к данному документу?
4. Как менялся текст нормативного акта с момента его создания по настоящее время?
5. Анализ методик и технологий управления рисками.
6. Раскройте качественные методики управления рисками.
7. Какие количественные методики управления рисками вы знаете?
8. Опишите метод CRAMM.

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 закрытой форме:

Количественный состав службы безопасности зависит, прежде всего от

- a. Типа циркулирующей в ней конфиденциальной информации
- b. От возможностей фирмы
- c. Нормативных документов регуляторов
- d. Численности штата

Задание в открытой форме:

... критерии предъявляются к действиям разработчика системы, документам для оценивания и работе самой организации. Включают требования доверия к мерам к СЗИ в информационных системах, а также к их разработке и эксплуатации.

Задание на установление правильной последовательности,

Надиктовать тестовую информацию (с обязательным указанием номера точки, в которой производится 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 антенны ЛГШ-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-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Федеральная служба безопасности [официальный сайт]. Режим доступа: <http://www.fsb.ru/>

2. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: <http://fstec.ru/>

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 лекций, 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 закрепления освоенного материала является конспектирование, без которого немислима 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
	Изменённых	Заменённых	Аннулированных	Новых			