

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Таныгин Максим Олегович

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

Дата подписания: 14.11.2023 14:29:31

Уникальный программный ключ:

65ab2aa0d384efe8480e6a4c688eddbc475e411a

Аннотация к рабочей программе

дисциплины «Системы охраны и инженерной защиты информации»

Цель преподавания дисциплины

Целью преподавания дисциплины «Системы охраны и инженерной защиты информации» является ознакомление студентов с источниками и носителями информации, изучение физических принципов возникновения технических каналов утечки информации, способов и методик их выявления, оценки степени опасности, методов и средств защиты.

Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

- получить знания о демаскирующих признаках объектов;
- получить знания о технических каналах утечки информации и методиках их выявления;
- получить знания о методах защиты информации от утечек по радиоканалу;
- получить знания о методах защиты информации от утечек по вибро-акустическому каналу;
- получить знания о методах защиты информации от утечек по каналу ПЭМИН;
- получить знания о методах защиты информации от утечек по оптическому каналу;
- получить знания о средствах и охраны и методах их применения на объектах информатизации;
- получить навыки по разработке и проектированию обустройства помещений объектов с повышенными требованиями к инженерно-технической защите.

Компетенции, формируемые в результате освоения дисциплины

Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде (УК-3);

Способен реализовывать политики безопасности с использованием инструментальных средств обеспечения информационной безопасности (ПК-2);

Способен организовывать работы по обеспечению информационной безопасности в автоматизированных системах (ПК-9);

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

Разделы дисциплины

Задачи курса «Системы охраны и инженерной защиты информации». Угрозы информационной безопасности информации и объекты защиты. Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков. Источники и носители информации. Принципы и способы добывания информации. Основы противодействия техническим средствам разведки. Технические каналы утечки информации (электромагнитные каналы, электрические каналы, параметрические каналы, вибрационные каналы). Каналы утечки речевой информации. Каналы утечки информации при передаче по каналам связи. Технические каналы утечки видовой информации. Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники. Звукоизоляция помещений.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:

И.о. декана факультета

фундаментальной и прикладной

информатики

(наименование факультета полностью)

 М.О. Таныгин

(подпись, инициалы, фамилия)

« 31 » 08 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Системы охраны и инженерной защиты информации

(наименование дисциплины)

ОПОП ВО 10.03.01 Информационная безопасность

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

направленность (профиль, специализация) «Безопасность автоматизированных систем» (по отрасли или в сфере профессиональной деятельности)»

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 (по отрасли или в сфере профессиональной деятельности)», одобренного Ученым советом университета (протокол № 6 «26» 02 2021 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 (по отрасли или в сфере профессиональной деятельности)» на заседании кафедры информационной безопасности № 1 «30» 08 2021 г.

Зав. кафедрой  Таныгин М.О.

Разработчик программы
к.т.н., доцент  Калущий И.В.
(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 (по отрасли или в сфере профессиональной деятельности)», одобренного Ученым советом университета протокол № 6 «26» 02 2021 г., на заседании кафедры ИБ ИИ от 30.06.22 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой  Таныгин М.О.

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 (по отрасли или в сфере профессиональной деятельности)», одобренного Ученым советом университета протокол № 9 «27» 02 2023 г., на заседании кафедры

ИБ информационном ИИ от 30.08.2023

(наименование кафедры, дата, номер протокола)

Зав. кафедрой 

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

1.1. Цель преподавания дисциплины

Целью преподавания дисциплины «Системы охраны и инженерной защиты информации» является ознакомление студентов с источниками и носителями информации, изучение физических принципов возникновения технических каналов утечки информации, способов и методик их выявления, оценки степени опасности, методов и средств защиты.

1.2. Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

- получить знания о демаскирующих признаках объектов;
- получить знания о технических каналах утечки информации и методиках их выявления;
- получить знания о методах защиты информации от утечек по радиоканалу;
- получить знания о методах защиты информации от утечек по вибро-акустическому каналу;
- получить знания о методах защиты информации от утечек по каналу ПЭМИН;
- получить знания о методах защиты информации от утечек по оптическому каналу;
- получить знания о средствах и охраны и методах их применения на объектах информатизации;
- получить навыки по разработке и проектированию обустройства помещений объектов с повышенными требованиями к инженерно-технической защите

1.3. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

<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>		
УК-3	Способен осуществлять социальное взаимодействие и	УК-3.2 При реализации своей роли в команде учитывает	Знать: - свою роль в социальном взаимодействии и командной работе, исходя из стратегии

<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>		
	реализовывать свою роль в команде	особенности поведения других членов команды	сотрудничества для достижения поставленной цели; - стандарты, нормы и правила работы в команде; - анализ последствий/ рисков, как следствие личных действий. Уметь: -учитывать особенности поведения и интересы других участников; - обосновывать выбор стандартов, норм и правил разработки ПО при работе в команде; - анализировать возможные последствия личных действий в социальном взаимодействии и командной работе; Владеть (или Иметь опыт деятельности): -навыками обмена информацией, знаниями и опытом с членами команды, применяя соответствующие методы защиты ПО; - навыком оценки идеи других членов команды для достижения поставленной цели; - нормами и установленными правилами командной работы;
		УК-3.4 Осуществляет обмен информацией, знаниями и опытом с членами команды, оценивает идеи других членов команды для достижения поставленной цели	Знать Особенности обмена информацией и знаниями с членами команды. Уметь: проводить оценку вклада каждого члена команды при достижении общей цели. Владеть (или Иметь опыт деятельности): методами оценки эффективности работы каждого члена команды.
ПК-2	Способен реализовывать политики	ПК-2.1 Формулирует критерии безопасности	Знать: требования действующих стандартов и рекомендаций, определяющих критерии оценки

<p>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</p>		<p>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</p>	<p>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</p>
код компетенции	наименование компетенции		
	<p>безопасности с использованием инструментальных средств обеспечения информационной безопасности</p>	<p>обработки информации в автоматизированных системах</p>	<p>безопасности АС и этапы анализа рисков и угроз безопасности и уязвимости АС; классификацию общих критериев, пути организации общих критериев; требования к разработке должностных инструкций; порядок эксплуатации программно-аппаратных средств защиты АС; основные принципы построения политики безопасности; методы и способы защиты информации в АС, методы анализа угроз и оценки рисков информационной безопасности АС.</p> <p>Уметь: применять требования действующих стандартов и рекомендаций для обеспечения безопасности обработки информации в АС; разрабатывать служебную и техническую документацию; применять средства защиты информации в соответствии с заданными требованиями к АС; проводить анализ информационных рисков.</p> <p>Владеть: навыками применения требования действующих стандартов и рекомендаций для обеспечения безопасности обработки информации в АС; разработки служебной и технической документации; программных средств защиты информации, разработки архитектуры сетевой защиты.</p>
		<p>ПК-2.2 Выполняет мероприятия для реализации политики информационной безопасности</p>	<p>Знать: виды угроз и каналы утечки информации, состав, структуру, требования и принципы построения политики безопасности; модели и типы политик безопасности; состав,</p>

<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>технические характеристики и правила эксплуатации программно-аппаратных средств АС; основные элементы политики безопасности, методы управления доступом, средства идентификации и аутентификация, анализа регистрационной информации; требования к технической, должностной и эксплуатационной документации; требования к уровням надёжности (безопасности); основные виды сетевых атак.</p> <p>Уметь: проводить анализ угроз, рисков, разрабатывать документацию пользователя, администратора сети, применять тестовые программы, разрабатывать архитектуры АС, разрабатывать политики безопасности; применять средства защиты информации в АС, проводить анализ защищенности АС, применять антивирусные программные комплексы, настраивать режимы работы межсетевых экранов.</p> <p>Владеть: навыками разработки документации пользователя, администратора сети, разработки и применения тестовых программ, описания архитектуры, описания политики безопасности; защиты информации в компьютерных системах, навыками анализа защищенности АС, применения антивирусных программных комплексов, настройки режимов работы межсетевых экранов.</p>

<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, соотношенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
		ПК-2.3 Определяет состав средств, необходимый для управления автоматизированными системами и средствами их защиты от НСД	<p>Знать: требования руководящих документов по защите АС от НСД; классификацию средств и АС по уровню защищенности от НСД; требования к защищенности АС; показатели и классы защищенности межсетевых экранов от НСД к информации; классификацию ПО СЗИ, требования руководящих документов к составу и содержанию документаций и испытаний ПО СЗИ; механизмы управления ключами, шифрованием, администрирования управления доступом, аутентификацией, маршрутизацией; задачи и методы управления системой защиты АС; типы, состав, назначение, способы применения современных систем управления защитой АС; принципы организации управления безопасностью АС; функции управления правами доступа пользователей АС, информационным каталогом, правилами политики безопасности; цели, задачи и порядок проведения аудита безопасности АС; программные средства мониторинга безопасности АС; состав, характеристики серверного, пользовательского и сетевого оборудования АС; показатели защищенности средств вычислительной техники от несанкционированного доступа, классы защищенности автоматизированных систем.</p> <p>Уметь: проводить анализ</p>

<p>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</p>		<p>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</p>	<p>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</p>
код компетенции	наименование компетенции		
			<p>защищенности локальной вычислительной сети, определять текущее состояние оборудования АС; применять программно-аппаратные средства ЗИ в АС; классифицировать программные продукты управления в соответствии с задачами АС, подбирать конфигурацию системы управления безопасности АС; проводить анализ информационных рисков.</p> <p>Владеть: навыками определения задач АС, классификации оборудования АС (серверов, АРМ, рабочих станций, сетевое оборудование), установки ПО серверной и клиентской части, настройки систем управления доступом, эксплуатации программных средств мониторинга и управления средствами безопасности АС, определения уязвимых мест АС и выбора средств защиты от НСД.</p>
ПК-9	Способен организовывать работы по обеспечению информационной безопасности в автоматизированных системах	ПК-9.1 Формулирование правил работы персонала со средствами защиты информации	<p>Знать: правила работы персонала со средствами защиты информации;</p> <p>Уметь: формулировать правил работы персонала со средствами защиты информации;</p> <p>Владеть (или Иметь опыт деятельности): -навыками разработки правил обращения и эксплуатации средств защиты информации.</p>
		ПК-9.2 Распределяет обязанности и полномочия	<p>Знать: обязанности и полномочия персонала, обслуживающего</p>

<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>		
		персонала, обслуживающего защищенную автоматизированную систему	защищенную автоматизированную систему. Уметь: распределять и обосновывать обязанности и полномочия персонала, обслуживающего защищенную автоматизированную систему; Владеть (или Иметь опыт деятельности): -навыками организации процесса обслуживания средств и систем защиты автоматизированных систем коллективом специалистов.
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	Знать: правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности. Уметь: - формулировать правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности Владеть (или Иметь опыт деятельности): -навыками разработки мер защиты информации, правил применения мер защиты информации, направленных на устранение причин возникновения инцидентов информационной безопасности.

2. Указание места дисциплины в структуре образовательной программы

Дисциплина « Системы охраны и инженерной защиты информации» входит в вариативную часть блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы бакалавриата 10.03.01. Информационная безопасность профиль «Безопасность автоматизированных систем». Дисциплина изучается на 3 курсе в 6 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 единиц, 180 часов.

Таблица 3.1 – Объём дисциплины по видам учебных занятий

Общая трудоёмкость дисциплины	180
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	81,15
лекции	32
лабораторные занятия	48
практические занятия	-
экзамен	1,15
зачет	
курсовая работа (проект)	-
расчетно-графическая (контрольная) работа	
Аудиторная работа (всего):	108
в том числе:	
лекции	32
лабораторные занятия	48
практические занятия	
Самостоятельная работа обучающихся (всего)	71,85
Контроль/экз (подготовка к экзамену)	27

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

4.1 Содержание дисциплины

Таблица 4.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Задачи курса «Системы	Политика безопасности и определение задач инженерно-

	охраны и инженерной защиты информации»	технической защиты информации. Общие принципы инженерно-технической защиты информации.
2.	Угрозы информационной безопасности информации и объекты защиты	Виды угроз безопасности информации, защищаемой техническими средствами. Виды потенциальных угроз безопасности информации. Преднамеренные и случайные воздействия на источники информации. Утечка информации и ее особенности. Подходы к оценке уровня угрозы. Факторы, влияющие на возможность реализации угроз.
3.	Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков	Опознавательные признаки и признаки деятельности объектов. Видовые, сигнальные и вещественные демаскирующие признаки. Информативность признаков. Понятие о признаковых структурах. Основные видовые демаскирующие признаки объектов наблюдения. Основные признаки, характеризующие физические и химические свойства материальных тел. Понятие о демаскирующих объектах, сигналах и веществах.
4.	Источники и носители информации	Понятие об источниках, носителях и получателях информации. Классификация источников информации. Виды носителей информации. Способы записи информации на различные виды носителей. Виды модуляции (манипуляции) сигналов. Характеристики модулированных сигналов. Принципы съема информации путем демодуляции (детектирования).
5.	Принципы и способы добывания информации	Основные принципы добывания и обработки информации техническими средствами. Структура органов управления, добывания и информационной работы. Видовая и комплексная обработка данных и сведений. Принципы идентификации и интерпретации, обнаружения и распознавания объектов, измерения характеристик демаскирующих признаков. Методы синтеза информации. Пути автоматизации процессов добывания и обработки информации.
6.	Основы противодействия техническим средствам разведки	Способы комплексного использования злоумышленниками технических каналов утечки информации.
7.	Технические каналы утечки информации (электромагнитные каналы, электрические каналы, параметрические каналы, вибрационные каналы)	Характеристики каналов утечки информации. Структура технических каналов утечки информации. Отличия технического канала утечки информации от канала связи. Виды технических каналов утечки информации. Типовая структура технического канала утечки информации. Основные характеристики технических каналов утечки информации.
8.	Каналы утечки речевой информации	Акустические каналы утечки информации. Структура акустического канала утечки информации. Отражение и поглощение акустических волн в среде распространения. Понятие о реверберации и влияние времени реверберации на разборчивость речи. Способы увеличения протяженности акустического канала утечки информации.
9.	Каналы утечки информации	Характеристики каналов утечки информации. Структура

	при передаче по каналам связи	каналов утечки информации при передаче по каналам связи. Отличия технического канала утечки информации от канала связи. Виды каналов утечки информации. Основные характеристики утечки информации при передаче по каналам связи.
10.	Технические каналы утечки видовой информации	Типовая структура технического канала утечки информации. Основные характеристики технических каналов утечки информации. Способы комплексного использования злоумышленниками технических каналов утечки информации.
11.	Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники	Виды доступа к источникам информации (физический контакт и дистанционный доступ). Принципы доступа к источникам информации, обрабатываемой средствами вычислительной техники. Классификация и характеристики средств съема информации с носителей.
12.	Звукоизоляция помещений	Методы энергетического скрывания акустических сигналов: звукоизоляция и звукопоглощение. Классификация, сущность и параметры звукоизоляции ограждений, кабин, акустических экранов, глушителей. Способы повышения звукоизоляции окон и дверей. Основные звукопоглощающие материалы и способы их применения.

Таблица 4.2 – Содержание дисциплины и ее методическое обеспечение

№ п/ п	Раздел (тема) дисциплины	Виды деятельности			Учебно- методич еские материа лы	Формы текущего контроля успеваем ости (по неделям семестра)	Компетенции
		лек., час	№ лб.	№ пр.			
1	2	3	4	5	6	7	8
1.	Задачи курса «Системы охраны и инженерной защиты информации»	2	-	-	О-1,2 Д-1,2	С	УК-3.2, УК-3.4, ПК-2.1, ПК-2.2, ПК-10.3
2.	Угрозы информационной безопасности информации и объекты защиты	2	1	-	О-1,3 Д-3-6	КО	ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.2
3.	Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков	4	-	-	О-1,3 Д-7-12	С	ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.2
4.	Источники и носители информации	2	-	-	О-1,2 Д-1,3-15	С	ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.2
5.	Принципы и способы добывания информации	2	-		О-2 Д-3,4	КО	УК-3.2, ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.1, ПК-9.2, ПК-10.3

1	2	3	4	5	6	7	8
6.	Основы противодействия техническим средствам разведки	4	2	-	О-2,3, Д-3-5	С	УК-3.2, УК-3.4, ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.1, ПК-9.2, ПК-10.3
7.	Технические каналы утечки информации (электромагнитные каналы, электрические каналы, параметрические каналы, вибрационные каналы)	4	3	-	О-1,3, Д-12-21	КО	УК-3.2, УК-3.4, ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.1, ПК-9.2, ПК-10.3
8.	Каналы утечки речевой информации	2	7	-	О-1 Д-2,4,6	С	УК-3.2, УК-3.4, ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.1, ПК-9.2, ПК-10.3
9.	Каналы утечки информации при передаче по каналам связи	4	4	-	О-1,3, Д-3-6	КО	УК-3.2, ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.1, ПК-9.2, ПК-10.39
10.	Технические каналы утечки видовой информации	4	8	-	О-2,3, Д-12-21	С	УК-3.2, ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.1, ПК-9.2, ПК-10.3
11.	Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники	4	-	-	О-1,3, Д-3,4	С	ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.2

Э – экзамен, КР – курсовая работа; КП – курсовой проект, К – контрольная работа, З – зачет, С – собеседование, СР – семестровая работа, Кл – коллоквиум, КО – контрольный опрос, МК – автоматизированный программированный контроль (машинный контроль).

4.2. Лабораторные работы и практические занятия

Таблица 4.3 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1.	Демаскирующие признаки объекта	4
2.	Изучение существующих каналов утечки информации	4
3.	Изучение устройства и основных режимов работы универсального прибора для обнаружения устройств скрытого съема информации СМР-700	4
4.	Изучение методики обследования помещения с помощью РЧ-зонда	4
5.	Изучение методики обследования помещения с помощью ОНЧ-	4

	зонда и дополнительного входа	
6.	Изучение методики проверки телефонных линий и обнаружения носимых радиопередатчиков	4
7.	Изучение программно-аппаратного комплекса «VНК-012GL»	4
8.	Отделение полезного голоса от зашумляющего фона	4
Итого		32

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Сущность предмета «Системы охраны и инженерной защиты информации». Задачи.	1-2 недели	6
2.	Угрозы информационной безопасности информации и объекты защиты.	2-3 недели	7,85
3.	Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков.	3-4 недели	6
4.	Источники и носители информации.	5-6 недели	6
5.	Принципы и способы добывания информации.	6-8 недели	8
6.	Основы противодействия техническим средствам разведки.	8-9 недели	8
7.	Технические каналы утечки информации (электромагнитные каналы, электрические каналы, параметрические каналы, вибрационные каналы).	9-10 недели	8
8.	Каналы утечки информации при передаче по каналам связи.	11-12 недели	8
9.	Технические каналы утечки видовой информации.	12-14 недели	8
10.	Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники.	14-15 недели	6
Итого			71,85

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

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

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

библиотекой университета:

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

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

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала за счёт выкладки на сайт кафедры ИБ в интернете (адрес http://www.swsu.ru/structura/up/fivt/k_ib/index.php);

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

– путем разработки вопросов к экзамену

– методических указаний к выполнению лабораторных работ.

типографией университета:

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

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

Темы курсовых работ приведены в приложении А.

6. Образовательные технологии. Технологии использования воспитательного потенциала дисциплины

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 05 апреля 2017 г. №301 реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. Удельный вес занятий, проводимых в интерактивных формах, составляет 24.9% от аудиторных занятий согласно УП. Средствами промежуточного контроля успеваемости студентов являются защита лабораторных работ, опросы на практических занятиях по темам лекций.

Проведение занятий в интерактивной форме учебным планом не предусмотрено.

Технологии использования воспитательного потенциала дисциплины

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

обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

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

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

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

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

7. Фонд оценочных средств для проведения промежуточной аттестации

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

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
УК-3.2 При реализации своей роли в команде учитывает особенности поведения других членов команды		Безопасность систем баз данных Системы охраны и инженерной защиты информации	Методы защиты программного обеспечения Подготовка к процедуре защиты и защита выпускной

			квалификационной работы
УК-3.4 Осуществляет обмен информацией, знаниями и опытом с членами команды, оценивает идеи других членов команды для достижения поставленной цели		Безопасность систем баз данных Системы охраны и инженерной защиты информации	Методы защиты программного обеспечения Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК-2.1 Формулирует критерии безопасности обработки информации в автоматизированных системах		Системы охраны и инженерной защиты информации	Защита информационных процессов в компьютерных системах Производственная технологическая практика Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК-2.2 Выполняет мероприятия для реализации политики информационной безопасности		Системы охраны и инженерной защиты информации	Защита информационных процессов в компьютерных системах Производственная технологическая практика Подготовка к процедуре защиты и защита выпускной квалификационной работы

ПК-2.3 Определяет состав средств, необходимый для управления автоматизированными системами и средствами их защиты от НСД		Системы охраны и инженерной защиты информации	Защита информационных процессов в компьютерных системах Производственная технологическая практика Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК-9.1 Формулирование правил работы персонала со средствами защиты информации		Системы охраны и инженерной защиты информации Организация и управление службой защиты информации Работа с конфиденциальной информацией	Производственная преддипломная практика Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК-9.2 Распределяет обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему		Системы охраны и инженерной защиты информации Организация и управление службой защиты информации Работа с конфиденциальной информацией	Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК-10.3 Формулирует правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности		Системы охраны и инженерной защиты информации	Комплексная защита объектов информатизации Подготовка к процедуре защиты и защита выпускной квалификационной

			ой работы
--	--	--	-----------

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

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

Таблица 7.2 – Критерии освоения компетенций

Наименование компетенции	Показатели оценивания компетенций	Критерии освоения		
		Удовлетворительно	Хорошо	Отлично
УК-3.2 При реализации своей роли в команде учитывает особенности поведения других членов команды	<p>1. Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД</p> <p>2. Качество освоенных обучающимся знаний, умений, навыков</p> <p>3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях</p>	<p>Знать основы социального взаимодействия.</p> <p>Уметь: Применять основы социального взаимодействия.</p> <p>Владеть (или Иметь опыт деятельности): Практическими основами социального взаимодействия.</p>	<p>Знать Методы социального взаимодействия.</p> <p>Уметь: Применять принципы социального взаимодействия.</p> <p>Владеть (или Иметь опыт деятельности): Практическими навыками социального взаимодействия.</p>	<p>Знать Методы социального взаимодействия и методы воздействия на членов команды.</p> <p>Уметь: Применять принципы социального взаимодействия.</p> <p>Владеть (или Иметь опыт деятельности): Практическими навыками социального взаимодействия с элементами воздействия на членов группы.</p>
УК-3.4 Осуществляет обмен информацией,	1. Доля освоенных обучающимся знаний,	Знать Особенности обмена информацией и	Знать Методы коммуникаций обмена информацией и	Знать Методы и средства коммуникаций обмена

<p>знаниями и опытом с членами команды, оценивает идеи других членов команды для достижения поставленной цели</p>	<p>умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД</p> <p>2.Качество освоенных обучающимся знаний, умений, навыков</p> <p>3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях</p>	<p>знаниями с членами команды.</p> <p>Уметь: проводить оценку вклада каждого члена команды при достижении общей цели.</p> <p>Владеть (или Иметь опыт деятельности): методами оценки эффективности работы каждого члена команды.</p>	<p>знаниями с членами команды.</p> <p>Уметь: проводить оценку вклада каждого члена команды при достижении общей цели.</p> <p>Владеть (или Иметь опыт деятельности): методами оценки эффективности работы каждого члена команды.</p>	<p>информацией и знаниями с членами команды.</p> <p>Уметь: проводить оценку и мотивацию вклада каждого члена команды при достижении общей цели.</p> <p>Владеть (или Иметь опыт деятельности): методами оценки эффективности и мотивации работы каждого члена команды.</p>
<p>ПК-2.1 Формулирует критерии безопасности обработки информации в автоматизированных системах</p>	<p>1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД</p> <p>2.Качество освоенных обучающимся знаний, умений, навыков</p> <p>3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях</p>	<p>Знать: базовые принципы обработки информации.</p> <p>Уметь: выделять признаки для формулирования критериев безопасности обработки информации.</p> <p>Владеть навыками: реализации базовых мер защиты информации в автоматизированных системах.</p>	<p>Знать: принципы обеспечения безопасности обработки информации в автоматизированных системах.</p> <p>Уметь: формулировать основные критерии безопасности обработки информации в автоматизированных системах</p> <p>Владеть навыками: классификации мер безопасности при обработке информации в автоматизированных системах по базовым</p>	<p>Знать: в полной мере принципы и меры обеспечения безопасности обработки информации в автоматизированных системах.</p> <p>Уметь: в полной мере формулировать критерии безопасности обработки информации в автоматизированных системах</p> <p>Владеть навыками: в полной мере классифицировать меры и средства обеспечения безопасности при обработке информации в</p>

			критериям.	автоматизированны х системах по расширенным критериям.
ПК-2.2 Выполняет мероприятия для реализации политики информацион ной безопасности	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленны х в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартны х ситуациях	Знать: базовые модели разграничения доступа. Уметь: применять базовые модели разграничения доступа. Владеть навыками: реализации базовых моделей разграничения доступа штатными средствами операционных систем.	Знать: основные модели разграничения доступа и политики информационно й безопасности. Уметь: реализовывать основные модели разграничения доступа и базовые политики информационно й безопасности. Владеть навыками: внедрения основных моделей политик информационно й безопасности.	Знать в полной мере модели разграничения доступа и политики информационной безопасности Уметь: в полной мере реализовывать модели разграничения доступа и политики информационной безопасности на объектах информатизации. Владеть навыками: внедрения моделей разграничения доступа и политик информационной безопасности на объектах информатизации различного уровня секретности.
ПК-9.1 Формулирован ие правил работы персонала со средствами защиты информации	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленны х в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение	Знать: основные правила работы со средствами защиты информации. Уметь: применять базовые правила работы с штатными средствами защиты информации. Владеть навыками: формулирования основных правил работы со	Знать: правила работы со средствами защиты информации. Уметь: применять правила работы со средствами защиты информации различных производителей. Владеть навыками: формулирования перечня правил	Знать в полной мере правила работы со средствами защиты информации. Уметь: в полной мере применять правила работы со средствами защиты информации различных производителей. Владеть навыками: формулирования расширенного перечня правил

	применять знания, умения, навыки в типовых и нестандартных ситуациях	средствами защиты информации.	обращения и работы со средствами защиты информации.	обращения и работы со средствами защиты информации.
ПК-9.2 Распределяет обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему	<p>знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД</p> <p>2.Качество освоенных обучающимся знаний, умений, навыков</p> <p>3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях</p>	<p>Знать: основные обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систем.</p> <p>Уметь: выполнять базовые процедуры по обслуживанию автоматизированных систем.</p> <p>Владеть навыками: обслуживания защищенных автоматизированных систем не в полной мере.</p>	<p>Знать: обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систем.</p> <p>Уметь: выполнять базовые процедуры по обслуживанию защищенных автоматизированных систем.</p> <p>Владеть навыками: распределения обязанностей персонала, обслуживающего защищенную автоматизированную систему.</p>	<p>Знать в полной мере обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систем.</p> <p>Уметь: в полной мере выполнять расширенные процедуры по обслуживанию защищенных автоматизированных систем.</p> <p>Владеть навыками: в полной мере распределения обязанностей и полномочий персонала, обслуживающего защищенную автоматизированную систему</p>
ПК-10.3 Формулирует правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности	<p>знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД</p> <p>2.Качество освоенных обучающимся знаний, умений, навыков</p>	<p>Знать: основные правила применения мер защиты информации.</p> <p>Уметь: формулировать основные правила применения мер защиты информации.</p> <p>Владеть</p>	<p>Знать: правила применения мер защиты информации.</p> <p>Уметь: формулировать основные правила применения мер защиты информации, направленные на</p>	<p>Знать в полной мере правила применения мер защиты информации.</p> <p>Уметь: в полной мере формулировать расширенный список правил применения мер защиты информации,</p>

	3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	навыками: применения базовых мер защиты информации, направленных на устранение причин инцидентов информационной безопасности.	устранение причин возникновения инцидентов информационно й безопасности. Владеть навыками: применения мер защиты информации, направленных на устранение причин инцидентов информационно й безопасности.	направленных на устранение причин возникновения инцидентов информационной безопасности. Владеть навыками: 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 образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				Наименование	№№ заданий	
1	2	3	4	5	6	7
1.	Задачи курса «Системы охраны инженерной защиты информации»	УК-3.2, УК-3.4, ПК-2.1, ПК-2.2, ПК-10.3 ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.2	Лекция, СРС	собеседование	1-2	Согласно табл.7.2
				контрольный опрос	1-1	
2.	Угрозы информационной безопасности объектов защиты.	ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.2 ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.2	Лекция, СРС, лабораторная работа №1	собеседование	1-2	Согласно табл.7.2
				контрольный опрос	1-1	

3.	Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков.	УК-3.2, ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.1, ПК-9.2, ПК-10.3 УК-3.2, УК-3.4, ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.1, ПК-9.2, ПК-10.3	Лекция, СРС	Собеседование	1-4	Согласно табл.7.2
				контрольный опрос		
4.	Источники и носители информации.	УК-3.2, УК-3.4, ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.1, ПК-9.2, ПК-10.3 УК-3.2, УК-3.4, ПК-2.1, ПК-2.2,	Лекция, СРС	собеседование	1-2	Согласно табл.7.2
				контрольный опрос		
5.	Принципы и способы добывания информации.	УК-3.2, ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.1, ПК-9.2, ПК-10.39 УК-3.2, ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.1, ПК-9.2, ПК-10.3	Лекция, СРС,	собеседование	1-2	Согласно табл.7.2
				контрольный опрос		
6.	Основы противодействия техническим средствам разведки.	ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.2 УК-3.2, УК-3.4, ПК-2.1, ПК-2.2, ПК-10.3	Лекция, СРС, лабораторная работа №2	собеседование	1-4	Согласно табл.7.2
				контрольный опрос	1-2	
7.	Технические каналы утечки информации (электромагнитные каналы, электрические каналы, параметрическ	ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.2 ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.2	Лекция, СРС, лабораторная работа №3,4	собеседование	1-4	Согласно табл.7.2

	ие каналы, вибрационные каналы).			контрольный опрос	1-3	
8.	Каналы утечки речевой информации.	ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.2 УК-3.2, ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.1, ПК-9.2, ПК-10.3	Лекция, СРС, лабораторная работа №5	собеседование	1-2	Согласно табл.7.2
				контрольный опрос	1-7	
9.	Каналы утечки информации при передаче по каналам связи.	УК-3.2, УК-3.4, ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.1, ПК-9.2, ПК-10.3 УК-3.2, УК-3.4, ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.1, ПК-9.2, ПК-10.3	Лекция, СРС, лабораторная работа №6	собеседование	1-4	Согласно табл.7.2
				контрольный опрос	1-4	
10.	Технические каналы утечки видовой информации.	УК-3.2, УК-3.4, ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.1, ПК-9.2, ПК-10.3 УК-3.2, ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.1, ПК-9.2, ПК-10.39	Лекция, СРС, лабораторная работа №7.8	собеседование	1-4	Согласно табл.7.2
				контрольный опрос	1-8	
11.	Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники.	УК-3.2, ПК-2.1, ПК-2.2, ПК-2.3, ПК-9.1, ПК-9.2, ПК-10.3	Лекция, СРС	собеседование	1-4	Согласно табл.7.2
				контрольный опрос	1-9	

Промежуточная аттестация по дисциплине проводится в форме компьютерного теста из 20 вопросов по различным темам курса. Для текущего контроля используются тестовые задания - закрытой (с выбором одного или нескольких правильных ответов).

Умения, навыки и компетенции проверяются с помощью задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

Примеры типовых контрольных заданий для текущего контроля

Задания

1. Взять три произвольных объекта и описать их демаскирующие признаки в соответствии с классификацией.
2. Для аудитории в которой проходят практические занятия, нарисовать план-схему помещения с мебелью, оборудованием, коммуникациями и отобразить на плане все технические каналы утечки информации, опишите механизмы их реализации.

Типовые задания для промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме экзамена. Экзамен проводится в форме тестирования (бланкового).

Для тестирования используются контрольно-измерительные материалы (КИМ) – 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 (%).

Для проверки знаний используются вопросы и задания в закрытой форме (с выбором одного или нескольких правильных ответов).

Умения, навыки и компетенции проверяются с помощью 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.

7.4. Рейтинговый контроль изучения учебной дисциплины

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

- Положение П 02.016–2018 «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* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Выполнение работы №1 «Изучение устройства и основных режимов работы универсального прибора для обнаружения устройств скрытого съема информации СМР-700»	2	Работа выполнена, но не защищена	5	Работа выполнена, защищена
Выполнение работы №2 «Изучение методики обследования помещения с помощью РЧ-зонда»	3	Работа выполнена, но не защищена	6	Работа выполнена, защищена
Выполнение работы №3 «Изучение методики обследования помещения с помощью ОНЧ-зонда и дополнительного входа»	3	Работа выполнена, но не защищена	5	Работа выполнена, защищена
Выполнение работы №4 «Изучение методики проверки телефонных линий и обнаружения носимых радиопередатчиков»	3	Работа выполнена, но не защищена	6	Работа выполнена, защищена
Выполнение работы №5 «Отделение полезного голоса от шумящего фона»	3	Работа выполнена, но не защищена	6	Работа выполнена, защищена
Выполнение работы №6 «Изучение программно-аппаратного комплекса «VНК-012GL»	2	Работа выполнена, но не защищена	5	Работа выполнена, защищена
Выполнение работы №7 «Оценка защищенности речевой информации»	2	Работа выполнена, но не защищена	5	Работа выполнена, защищена

Выполнение работы №8 «Настройка активной системы защиты речевой информации»	3	Работа выполнена, но не защищена	5	Работа выполнена, защищена
Выполнение работы №9 «Оценка звукоизоляции помещений»	3	Работа выполнена, но не защищена	5	Работа выполнена, защищена
Итого	24		48	

Промежуточная аттестация выставляется с учётом требований Положения о балльно-рейтинговой системе ЮЗГУ, в качестве критериев выставления промежуточной аттестации используются: посещаемость студентом лекций, практических занятий, качество выполнения заданий, степень глубины проработки материала, а также вопросы для собеседования и бланковое тестирование.

Перечень билетов к экзамену приведён в учебно-методическом комплексе дисциплины. Экзаменационный билет содержит 20 вопросов. Каждый вопрос оценивается в 1,8 балла, итоговая максимальная оценка 36 баллов. Итоговая сумма баллов за ответ на экзамене в случае дробного результата округляется в большую сторону. Для получения положительной оценки студенту необходимо набрать не менее 24 баллов за отдельные виды деятельности и не менее 50 баллов в сумме (с учётом баллов за посещаемость и премиальных баллов деканата). Итоговая оценка выставляется в зависимости от набранной студентом в течение семестра и на экзамене суммы баллов в соответствии с Положением о балльно-рейтинговой системе ЮЗГУ.

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

8.1. Основная учебная литература

1) Сагдеев, К. М. Физические основы защиты информации : учебное пособие / К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2015. – 394 с. : ил. – URL: <https://biblioclub.ru/index.php?page=book&id=458285> (дата обращения: 28.08.2021). – Режим доступа: по подписке. – Библиогр.: с. 387-388. – Текст : электронный.

2) Денисова, Е. В. Автономные информационные системы обнаружения скрытых объектов : учебное пособие / Е. В. Денисова, В. Н. Легкий ; ред. В. Н. Опарин. – Новосибирск : Новосибирский государственный технический университет, 2012. – 128 с. – URL: <https://biblioclub.ru/index.php?page=book&id=228582> (дата обращения: 28.08.2021). – Режим доступа: по подписке. – ISBN 978-5-7782-1961-8. – Текст : электронный.

8.2. Дополнительная учебная литература

3) Титов, А. А. Инженерно-техническая защита информации : учебное пособие / А. А. Титов. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. - 195 с. – URL: <http://biblioclub.ru/index.php?page=book&id=208567> (дата обращения: 28.08.2021). – Режим доступа: по подписке. – Текст : электронный.

4) Бузов, Г. А. Защита от утечки информации по техническим каналам : учебное пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. - М. : Горячая линия - Телеком, 2005. - 416 с. – Текст : непосредственный.

5) Меньшаков, Ю. К. Защита объектов и информации от технических средств разведки : учебное пособие / Ю. К. Меньшаков. - М. : РГГУ, 2002. - 399 с. – Текст : непосредственный.

8.3.Перечень методических указаний

1) Изучение устройства и основных режимов работы универсального прибора для обнаружения устройств скрытого съема информации СРМ-700 : методические указания по выполнению лабораторных и практических работ по дисциплине «Инженерно-техническая защита информации» для студентов специальностей 10.05.02, 10.05.03, 10.03.01, 10.04.01 / Юго-Зап. гос. ун-т ; сост.: И. В. Калущкий, И. И. Рудак, А. В. Тепикина. - Курск : ЮЗГУ, 2016. - 21 с. – Текст : электронный.

2) Изучение методики обследования помещения с помощью РЧ-зонда : методические указания по выполнению лабораторных и практических работ по дисциплине «Инженерно-техническая защита информации» для студентов специальностей и направлений подготовки 10.05.02, 10.05.03, 10.03.01, 10.04.01 / Юго-Зап. гос. ун-т ; сост.: И. В. Калущкий, И. И. Рудак, А. В. Тепикина. - Курск : ЮЗГУ, 2016. - 13 с. – Текст : электронный.

3) Изучение методики обследования помещения с помощью ОНЧ-зонда и дополнительного входа : методические указания по выполнению лабораторных и практических работ по дисциплине «Инженерно-техническая защита информации» для студентов специальностей 10.05.02, 10.05.03, 10.03.01, 10.04.01 / Юго-Зап. гос. ун-т ; сост.: И. В. Калущкий, И. И. Рудак, А. В. Тепикина. - Курск : ЮЗГУ, 2016. - 12 с. – Текст : электронный.

4) Изучение методики проверки телефонных линий и обнаружения носимых радиопередатчиков : методические указания по выполнению лабораторных и практических работ по дисциплине «Инженерно-техническая защита информации» для студентов специальностей и направлений подготовки 10.05.02, 10.05.03, 10.03.01, 10.04.01 / Юго-Зап. гос. ун-т ; сост.: И. В. Калущкий, И. И. Рудак, А. В. Тепикина. - Курск : ЮЗГУ, 2016. - 12 с. – Текст : электронный.

5) Изучение программно-аппаратного комплекса «VНК-012GL» : методические указания по выполнению лабораторных и практических работ по дисциплинам: «Инженерно-техническая защита информации», «Техническая защита информации» для студентов специальностей и направлений подготовки 10.05.02,

10.05.03, 10.03.01, 10.04.01 / Юго-Зап. гос. ун-т ; сост.: И. В. Калущий, А. А. Кретов, С. Ю. Тарыгин. - Курск : ЮЗГУ, 2016. - 24 с. – Текст : электронный.

6) Изучение существующих каналов утечки информации : методические указания к выполнению лабораторной и практической работы по дисциплинам «Инженерно-техническая защита информации», «Техническая защита информации» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 / Юго-Зап. гос. ун-т; сост.: И. В. Калущий, Ю. А. Куденцова. - Курск : ЮЗГУ, 2017. - 12 с. – Текст : электронный.

7) Демаскирующие признаки объекта : методические указания по выполнению лабораторной и практической работы по дисциплинам «Инженерно-техническая защита информации», «Техническая защита информации» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 / Юго-Зап. гос. ун-т ; сост.: И. В. Калущий, Ю. А. Куденцова. - Курск : ЮЗГУ, 2017. - 12 с. – Текст : электронный.

8) Оценка звукоизоляции помещений : методические указания по выполнению лабораторных и практических работ по дисциплинам: «Инженерно-техническая защита информации», «Техническая защита информации» для студентов специальностей и направлений подготовки 10.05.02, 10.05.03, 10.03.01, 10.04.01 / Юго-Зап. гос. ун-т ; сост.: И. В. Калущий, А. А. Кретов, С. Ю. Тарыгин. - Курск : ЮЗГУ, 2016. - 21 с. – Текст : электронный.

9) Инженерно-техническая защита информации : методические указания к выполнению курсового проекта для студентов укрупненной группы специальностей 10.00.00/ Юго-Зап. гос. ун-т; сост.: И. В. Калущий, Е. М. Чудненко, А. А. Чеснокова. - Курск : ЮЗГУ, 2017. - 58 с. – Текст : электронный.

10) Аспекты технической защиты информации : методические указания к самостоятельной работе по дисциплинам «Инженерно-техническая защита информации», «Техническая защита информации» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 / Юго-Зап. гос. ун-т ; сост.: И. В. Калущий, Е. М. Чудненко, А. А. Чеснокова. – Курск : ЮЗГУ, 2017. - 13 с. – Текст : электронный.

11) Отделение полезного голоса от зашумляющего фона : методические указания к выполнению лабораторной работы по дисциплинам «Инженерно-техническая защита информации», «Техническая защита информации» для студентов укрупненной группы специальностей 10.00.00/ Юго-Зап. гос. ун-т ; сост.: И. В. Калущий, А. А. Чеснокова. – Курск : ЮЗГУ, 2018. - 29 с. – Текст : электронный.

9. Перечень ресурсов информационно-телекоммуникационной сети Интернет

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 «Инженерно-техническая защита информации» являются лекции и практические занятия. Студент не имеет права пропускать занятия без уважительных причин.

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

Изучение наиболее важных тем или разделов дисциплины завершают практические занятия, которые обеспечивают:

- контроль подготовленности студента; закрепление учебного материала;
- приобретение опыта 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.

Лабораторному 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 лабораторным и практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Инженерно-техническая защита информации»: 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 и справочной документации 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 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 «Инженерно-техническая защита информации» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Инженерно-техническая защита информации» - 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)

- 1) Libreoffice (Бесплатная, GNU General Public License) - <https://ru.libreoffice.org/> ;
- 2) Microsoft Office 2016 Лицензионный договор №S0000000722 от 21.12.2015 г. С ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»;
- 3) Операционная система Windows, договор IT000012385;
- 4) Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234;
- 5) Sony Sound Forge (демо-версия) - <https://www.sonycreativesoftware.com/> ;
- 6) Adobe Audition (Бесплатная пробная версия) - <https://creative.adobe.com/ru/products/download/audition> .

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) Компьютер NORBEL C239264Ц-AMD/2x8Gb/2TB/DVDRW/LCD 20";

- Система виброакустического зашумления «Шорох-2», виброакустический датчик КПВ-2, акустический излучатель OMS -2000
- Подавитель «жучков» и беспроводных видеокамер “BigHunter Spy”
- Комбинированный поисковый прибор “D008”
- Универсальный поисковый прибор "СРМ-700"
- Лазерный дальномер Mettrod 60
- Генератор шума Соната-С1

Для проведения промежуточной аттестации необходимо следующее

материально-техническое оборудование:

1. Проекционный экран на штативе; Мультимедиа центр: ноутбук ASUS X50VL PMD-T2330/1471024Mb/160Gb/ сумка/ проектор inFocus IN24

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			