

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 14:06:52

Уникальный программный ключ:

65ab2aa0d384efe8480e6a4c688eddbc475e411a

Аннотация к рабочей программе

дисциплины «Инженерно-техническая защита информации»

Цель преподавания дисциплины

Целью преподавания дисциплины «Инженерно-техническая защита 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 навыки по разработке и проектированию обустройства помещений объектов с повышенными требованиями к инженерно-технической защите

Компетенции, формируемые в результате освоения дисциплины

ПК-1 - способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе

криптографических) и технических средств защиты информации;

ПК-5 - способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

ПК-7 - способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;

ПК-9 - способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

Разделы дисциплины

Задачи инженерно-технической 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:

Декан факультета

фундаментальной и прикладной

(наименование ф-та полностью)

информатики



Т.А. Ширабакина

(подпись, инициалы, фамилия)

«01» 02 2017 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Инженерно-техническая защита информации

направление подготовки (специальность)

10.03.01

(шифр согласно ФГОС)

Информационная безопасность

и наименование направление подготовки (специальности)

Безопасность автоматизированных систем

наименование профиля, специализации или магистерской программы

форма обучения

очная

очная, очно-заочная, заочная

Курс – 2017

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность и на основании учебного плана направления 10.03.01 Информационная безопасность (профиль Безопасность автоматизированных систем), одобренного Учёным советом университета, протокол № 5 «30» 01 2017г.

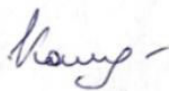
Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по направлению подготовки 10.03.01 Информационная безопасность на заседании кафедры информационной безопасности № «9» 1 февраля 2017г.

Зав. кафедрой ИБ



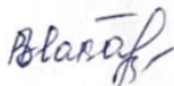
Таныгин М.О.

Разработчик программы
доцент кафедры ИБ



Калуцкий И.В.

Директор научной библиотеки

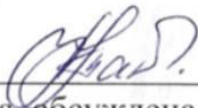


Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № «28» 06 2017г. на заседании кафедры себ

информационной №1
(наименование кафедры, дата, номер протокола)

Зав. кафедрой



Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № 5 «01» 30 2017г. на заседании кафедры 45 29.06.2018

№12
(наименование кафедры, дата, номер протокола)

Зав. кафедрой



Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № 5 «30» 01 2017г. на заседании кафедры 45 27.06.2018,

№11
(наименование кафедры, дата, номер протокола)

Зав. кафедрой



Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 «Информационная безопасность», одобренного Ученым советом университета протокол №9 «25» 03 2019г. на заседании кафедры ИБ ИИ от 30.06.2022г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 «Информационная безопасность», одобренного Ученым советом университета протокол №7 «25» 02 2020г. на заседании кафедры ИБ ИИ от 30.08.2022г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 «Информационная безопасность», одобренного Ученым советом университета протокол № « » 20 г. на заседании кафедры _____

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 «Информационная безопасность», одобренного Ученым советом университета протокол № « » 20 г. на заседании кафедры _____

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

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

1.1. Цель преподавания дисциплины

Целью преподавания дисциплины «Инженерно-техническая защита 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 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

Обучающиеся должны **знать:**

- основные демаскирующие признаки объектов защиты и носителей информации;
- технические каналы утечки информации;
- технические средства разведки;
- способы и средства защиты конфиденциальной информации;
- подсистемы комплексной системы охраны объектов;
- основы организации работ по инженерно-технической защите информации;
- основные руководящие документы в области инженерно-технической защиты информации.

уметь:

- моделировать объекты защиты;
- выявлять и оценивать угрозы безопасности информации на конкретных объектах;
- определять рациональные меры защиты на объектах и оценивать их эффективность;
- контролировать эффективность мер инженерно-технической защиты информации.

владеть:

- методами и средствами инженерной защиты и технической охраны объектов;
- методами расчета и инструментального контроля показателей защиты информации.

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПК-1 - способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-5 - способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

ПК-7 - способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;

ПК-9 - способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

2. Указание места дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам базовой части профессионального цикла (БЗ.В.ОД.2). Изучается на 4 курсе в 7 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 7 зачётных единиц, 252 часа.

Таблица 3.1 – Объём дисциплины по видам учебных занятий

Общая трудоемкость дисциплины	252
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	109,65
лекции	36
лабораторные занятия	18
практические занятия	54
экзамен	0,15
зачет	
курсовая работа (проект)	36
расчетно-графическая (контрольная) работа	
Аудиторная работа (всего):	108
в том числе:	
лекции	36
лабораторные занятия	18
практические занятия	54
Самостоятельная работа обучающихся (всего)	115,35
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 инженерно-технической защиты информации	Политика безопасности и определение задач инженерно-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 при передаче по каналам связи	Характеристики каналов утечки информации. Структура 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 скрывтия 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 (<i>по неделям семестра</i>)	Компетенции
		лек., час	№ лб.	№ пр.			
1	2	3	4	5	6	7	8
1.	Задачи инженерно-технической защиты информации	2	-	-	О-1,2 Д-1,2	С	ПК-1, ПК-5, ПК-7, ПК-9
2.	Угрозы информационной безопасности информации и объекты защиты	2	1	-	О-1,3 Д-3-6	КО	ПК-1, ПК-5, ПК-7, ПК-9
3.	Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков	4	-	-	О-1,3 Д-7-12	С	ПК-1, ПК-5, ПК-7, ПК-9
4.	Источники и носители информации	2	-	-	О-1,2 Д-1,3-15	С	ПК-1, ПК-5, ПК-7, ПК-9
5.	Принципы и способы добывания информации	2	-	-	О-2 Д-3,4	КО	ПК-1, ПК-5, ПК-7, ПК-9
6.	Основы противодействия техническим средствам разведки	4	2	-	О-2,3, Д-3-5	С	ПК-1, ПК-5, ПК-7, ПК-9
7.	Технические каналы утечки информации (электромагнитные каналы, электрические каналы, параметрические каналы, вибрационные каналы)	4	3	-	О-1,3, Д-12-21	КО	ПК-1, ПК-5, ПК-7, ПК-9
8.	Каналы утечки речевой информации	2	7	-	О-1 Д-2,4,6	С	ПК-1, ПК-5, ПК-7, ПК-9
9.	Каналы утечки информации при передаче по каналам связи	4	4	-	О-1,3, Д-3-6	КО	ПК-1, ПК-5, ПК-7, ПК-9

1	2	3	4	5	6	7	8
10.	Технические каналы утечки видовой информации	4	8	-	О-2,3, Д-12-21	С	ПК-1, ПК-5, ПК-7, ПК-9
11.	Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники	4	-	-	О-1,3, Д-3,4	С	ПК-1, ПК-5, ПК-7, ПК-9
12.	Звукоизоляция помещений	2	9	-			

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.	Изучение устройства и основных режимов работы универсального прибора для обнаружения устройств скрытого съема информации СМР-700	2
2.	Изучение методики обследования помещения с помощью РЧ-зонда	4
3.	Изучение методики обследования помещения с помощью ОНЧ-зонда и дополнительного входа	4
4.	Изучение методики проверки телефонных линий и обнаружения носимых радиопередатчиков	4
5.	Отделение полезного голоса от зашумляющего фона	4
Итого		18

Таблица 4.4 – Практические работы

№	Наименование лабораторной работы	Объем, час.
1.	Изучение программно-аппаратного комплекса «VНК-012GL»	12
2.	Изучение существующих каналов утечки информации	14
3.	Демаскирующие признаки объекта	14
4.	Оценка звукоизоляции помещений	14
Итого		54

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 инженерно-технической защиты информации. Задачи.	1-2 недели	6
2.	Угрозы информационной безопасности информации и объекты защиты.	2-3 недели	6
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	6
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	8
11.	Звукоизоляция помещений	15-18 недели	9,35
12.	Курсовое проектирование	3-17 недели	36
Итого			115,35

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

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

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

библиотекой университета:

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

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

кафедрой:

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

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

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объём, час.
1.	Выполнение работы №1 «Изучение устройства и основных режимов работы универсального прибора для обнаружения устройств скрытого съема информации СМР-700»	Выполнение студентом заданий с использованием универсального прибора для обнаружения устройств скрытого съема информации	2
2.	Выполнение работы №2 «Изучение методики обследования помещения с помощью РЧ-зонда»	Выполнение студентом интерактивных заданий с помощью оборудования для обнаружения скрытого съема информации	2

3.	Выполнение работы №3 «Изучение методики обследования помещения с помощью ОНЧ-зонда и дополнительного входа»	Выработка студентом практических навыков при обследовании помещения прибором для обнаружения устройств скрытого съема информации.	6
4.	Выполнение работы №4 «Изучение методики проверки телефонных линий и обнаружения носимых радиопередатчиков»	Выработка студентом практических навыков при проведении проверки телефонных линий и обнаружения носимых радиопередатчиков. Проверка телефонной линии на предмет наличия возможных закладных устройств.	6
5.	Выполнение работы №5 «Отделение полезного голоса от зашумляющего фона»	Выполнение студентом интерактивных заданий для освоения методики выделения полезного сигнала и удаления вредных шумов с помощью представленных программ	2
6.	Выполнение работы №6 «Изучение программно-аппаратного комплекса «VNK-012GL»	Выполнение студентом интерактивных заданий, связанных с подключением и настройкой программно-аппаратного комплекса.	6
7.	Выполнение работы №7 «Изучение существующих каналов утечки информации»	Выполнение студентом интерактивных заданий по определению и графическому отображению на эскизе помещения существующих технических каналов утечки информации.	6
8.	Выполнение работы №8 «Демаскирующие признаки объекта»	Выполнение студентом интерактивных заданий на освоение методики определения демаскирующих признаков объектов.	6
9.	Выполнение работы №9 «Оценка звукоизоляции помещений»	Выполнение студентом интерактивных заданий для проведения измерений по оценке звукоизоляции исследуемого помещения, с помощью специального оборудования.	2
	Итого		36

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
ПК-1 - способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.	Ознакомительная практика	Введение в криптографию; Аппаратные средства вычислительной техники; Криптографическ	Программно-аппаратные средства защиты информации; Инженерно-техническая защита

		<p>ие методы защиты информации;</p> <p>Безопасность сетей ЭВМ;</p> <p>Технические средства охраны;</p> <p>Системы контроля доступа и видеонаблюдения</p> <p>Технологическая практика</p>	<p>информации;</p> <p>Эксплуатационная практика;</p> <p>Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты</p>
<p>ПК-5 - способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;</p>		<p>Техническая защита информации;</p> <p>Технологическая практика</p>	<p>Инженерно-техническая защита информации;</p> <p>Эксплуатационная практика;</p> <p>Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты</p>
<p>ПК-7 - способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;</p>	<p>Патентование</p>	<p>Введение в криптографию;</p> <p>Криптографические методы защиты информации;</p> <p>Экология;</p> <p>Технологическая практика;</p> <p>Проектно-технологическая практика</p>	<p>Инженерно-техническая защита информации;</p> <p>Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты</p>

ПК-9 - способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;	Русский язык и культура речи; Ознакомительная практика	Программно-аппаратные средства защиты информации; Учебно-исследовательская работа студентов	Инженерно-техническая защита информации; Преддипломная практика; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
--	---	--	---

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
ПК-1 - способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	1. Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2. Качество освоенных обучающимся знаний, умений, навыков 3. Умение применять	Знать: - различные виды и носители информации. Уметь: - определять направления использования аппаратного и программного обеспечения определенного класса для решения служебных задач. Владеть	Знать: - различные виды и носители информации. - аппаратные средства вычислительной техники. Уметь: - определять направления использования аппаратного и программного обеспечения определенного	Знать: - различные виды и носители информации. - аппаратные средства вычислительной техники. - историю развития, состояние и тенденции развития вычислительной техники. Уметь: - определять

	знания, умения, навыки в типовых и нестандартных ситуациях	навыками: - навыками формирования требований по обеспечению надежности аппаратных средств вычислительной техники.	класса для решения служебных задач. - ориентироваться в особенностях применяемых микропроцессорных комплектов. Владеть навыками: - навыками формирования требований по обеспечению надежности аппаратных средств вычислительной техники. - методами и средствами выявления неисправностей автоматизированных систем.	направления использования аппаратного и программного обеспечения определенного класса для решения служебных задач. - ориентироваться в особенностях применяемых микропроцессорных комплектов. - использовать стандартные диагностические средства. Владеть навыками: - навыками формирования требований по обеспечению надежности аппаратных средств вычислительной техники. - методами и средствами выявления неисправностей автоматизированных систем. - осуществлять поиск наиболее эффективных путей обработки информации и (или) ее управления.
ПК-5 - способностью принимать участие в организации и сопровождении аттестации	1. Доля освоенных обучающимся знаний, умений, навыков от общего	Знать: - компьютерную систему, как объект информационного воздействия, критерии оценки	Знать: - компьютерную систему, как объект информационного воздействия, критерии оценки	Знать: - компьютерную систему, как объект информационного воздействия, критерии оценки ее защищенности и

<p>объекта информатизации по требованиям безопасности информации;</p>	<p>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>ее защищенности и методы обеспечения ее информационной безопасности.</p> <p>Уметь:</p> <ul style="list-style-type: none"> - выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; <p>Владеть навыками:</p> <ul style="list-style-type: none"> - методами определения источников и носителей защищаемой информации. 	<p>ее защищенности и методы обеспечения ее информационной безопасности.</p> <ul style="list-style-type: none"> - угрозы информационной безопасности. <p>Уметь:</p> <ul style="list-style-type: none"> - выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации. <p>Владеть навыками:</p> <ul style="list-style-type: none"> - методами определения источников и носителей защищаемой информации, демаскирующих признаков объектов и сигналов. 	<p>методы обеспечения ее информационной безопасности.</p> <ul style="list-style-type: none"> - угрозы информационной безопасности. - современные подходы к построению систем защиты информации. <p>Уметь:</p> <ul style="list-style-type: none"> - выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации. - анализировать общие характеристики систем защиты информации. <p>Владеть навыками:</p> <ul style="list-style-type: none"> - методами определения источников и носителей защищаемой информации, демаскирующих признаков объектов и сигналов. - методами описания и моделирования объекты защиты.
<p>ПК-7 - способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения</p>	<p>1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД</p>	<p>Знать:</p> <ul style="list-style-type: none"> - базовые принципы объектно-ориентированный анализ и проектирование особенности разработки программного 	<p>Знать:</p> <ul style="list-style-type: none"> - базовые принципы объектно-ориентированный анализ и проектирование особенности разработки программного 	<p>Знать:</p> <ul style="list-style-type: none"> - базовые принципы объектно-ориентированный анализ и проектирование особенности разработки программного

<p>информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;</p>	<p>2. Качество освоенных обучающимся знаний, умений, навыков</p> <p>3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях</p>	<p>обеспечения, ориентированного на повторное использование.</p> <p>Уметь:</p> <ul style="list-style-type: none"> - разрабатывать стандартные диаграммы на языке UML. <p>Владеть навыками:</p> <ul style="list-style-type: none"> - типовыми приемами проектирования. 	<p>обеспечения, ориентированного на повторное использование.</p> <ul style="list-style-type: none"> - основы унифицированного языка моделирования UML, понятие типового приема проектирования. <p>Уметь:</p> <ul style="list-style-type: none"> - разрабатывать стандартные диаграммы на языке UML. - применять типовые приемы проектирования в типовом контексте приложения. <p>Владеть навыками:</p> <ul style="list-style-type: none"> - типовыми приемами проектирования. - инструментариум для документирования проектных решений методами прямого и обратного проектирования. 	<p>обеспечения, ориентированного на повторное использование.</p> <ul style="list-style-type: none"> - основы унифицированного языка моделирования UML, понятие типового приема проектирования. - основные категории типовых приемов проектирования. <p>Уметь:</p> <ul style="list-style-type: none"> - разрабатывать стандартные диаграммы на языке UML. - применять типовые приемы проектирования в типовом контексте приложения. - анализировать причины, приводящие к перепроектированию - определять необходимые интерфейсы для программных классов и модулей. <p>Владеть навыками:</p> <ul style="list-style-type: none"> - типовыми приемами проектирования. - инструментариум для документирования проектных решений методами прямого и обратного проектирования.
<p>ПК-9 - способностью</p>	<p>1. Доля освоенных</p>	<p>Знать:</p> <ul style="list-style-type: none"> - источники 	<p>Знать:</p> <ul style="list-style-type: none"> - источники 	<p>Знать</p> <ul style="list-style-type: none"> - источники

<p>осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;</p>	<p>обучающимся знаниям, умениям, навыков от общего объема ЗУН, установленных в п.1.3 РПД</p> <p>2.Качество освоенных обучающимся знаниям, умениям, навыков</p> <p>3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях</p>	<p>научной информации по теме исследования.</p> <p>Уметь:</p> <ul style="list-style-type: none"> - выполнять поиск, сбор, обработку, анализ и систематизацию информации по теме исследования. - проводить формализацию и реализацию решения выбора процесса защиты информации. <p>Владеть навыками:</p> <ul style="list-style-type: none"> - библиографического поиска, с привлечением современных информационных технологий. - применения технических средств защиты информации. 	<p>научной информации по теме исследования.</p> <ul style="list-style-type: none"> - принципы организации информационных систем в соответствии с требованиями по защите информации. <p>Уметь:</p> <ul style="list-style-type: none"> - выполнять поиск, сбор, обработку, анализ и систематизацию информации по теме исследования. - проводить формализацию и реализацию решения выбора процесса защиты информации. <p>Владеть навыками:</p> <ul style="list-style-type: none"> - библиографического поиска, с привлечением современных информационных технологий. - применения технических средств защиты информации. 	<p>научной информации по теме исследования.</p> <ul style="list-style-type: none"> - принципы организации информационных систем в соответствии с требованиями по защите информации. - концепцию технологического процесса защиты информации в соответствии с правовыми нормативными актами и методическими документами. <p>Уметь:</p> <ul style="list-style-type: none"> - выполнять поиск, сбор, обработку, анализ и систематизацию информации по теме исследования. - проводить формализацию и реализацию решения выбора процесса защиты информации. - организовывать процесс защиты информации. <p>Владеть навыками:</p> <ul style="list-style-type: none"> - библиографического поиска, с привлечением современных информационных технологий. - применения технических средств защиты информации.
---	---	---	--	--

				администрирование систем и устройств защиты информации.
--	--	--	--	---

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 инженерно-технической защиты информации	ПК-1	Лекция, СРС	собеседование	1-2	Согласно табл.7.2
				контрольный опрос	1-1	
2.	Угрозы информационной безопасности информации и объекты защиты.	ПК-1, ПК-5	Лекция, СРС, лабораторная работа №1	собеседование	1-2	Согласно табл.7.2
				контрольный опрос	1-1	
3.	Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков.	ПК-5	Лекция, СРС	Собеседование	1-4	Согласно табл.7.2

				контрольный опрос		
4.	Источники и носители информации.	ПК-7	Лекция, СРС	собеседование	1-2	Согласно табл.7.2
				контрольный опрос		
5.	Принципы и способы добывания информации.	ПК-7, ПК-9	Лекция, СРС,	собеседование	1-2	Согласно табл.7.2
				контрольный опрос		
6.	Основы противодействия техническим средствам разведки.	ПК-5, ПК-7	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, параметрические каналы, вибрационные каналы).	ПК-1, ПК-5	Лекция, СРС, лабораторная работа №3,4	собеседование	1-4	Согласно табл.7.2
				контрольный опрос	1-3	
8.	Каналы утечки речевой информации.	ПК-7	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.	ПК-7	Лекция, СРС, лабораторная работа №6	собеседование	1-4	Согласно табл.7.2
				контрольный опрос	1-4	
10.	Технические каналы утечки видовой информации.	ПК-7, ПК-9	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.	ПК-1	Лекция, СРС	собеседование	1-4	Согласно табл.7.2
				контрольный опрос		
12.	Звукоизоляция помещений	ПК-1	Лекция, СРС, лабораторная работа №9	собеседование	1-2	Согласно табл.7.2
				контрольный опрос	1-9	

Промежуточная аттестация по дисциплине проводится в форме компьютерного теста из 15 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 зачета. Зачет 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

	Минимальный балл	Максимальный балл
--	------------------	-------------------

Форма контроля	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 зашумляющего 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	

Перечень тем для курсовой работы приведен в Приложении А.

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) Технические средства и методы защиты информации [Текст] : учебное пособие / под ред. А. П. Зайцева и А. А. Шелупанова. - Москва : Горячая линия - Телеком, 2012. - 616 с. : ил. - ISBN 978-5-9912-00 84-4

8.2. Дополнительная учебная литература

1) Торокин А. А. Инженерно-техническая защита информации [Текст] учебное пособие- М. : Гелиос АРВ, 2005. – 960 с. : ил.

2) Титов, А. А. Инженерно-техническая защита информации [Электронный ресурс] : учебное пособие / А. А. Титов. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. - 195 с.

3) Методы и средства инженерно-технической защиты информации [Электронный ресурс] : учебное пособие. - 2-е изд., стер. - Москва : Флинта, 2011. - 187 с. - (Организация и технология защиты информации). - ISBN 978-5-9765-1275-7

4) Бузов, Г. А. Защита от утечки информации по техническим каналам [Текст] : учебное пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. - М. : Горячая линия - Телеком, 2005. - 416 с. : ил. - ISBN 5-93517-204-6.

5) Меньшаков, Ю. К. Защита объектов и информации от технических средств разведки [Текст] : учебное пособие / Ю. К. Меньшаков. - М. : РГГУ, 2002. - 399 с. - ISBN 5-7281-0487-8.

8.3. Перечень методических указаний

1) Изучение устройства и основных режимов работы универсального прибора для обнаружения устройств скрытого съема информации СРМ-700 [Электронный ресурс] : 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. Калуцкий, И. И. Рудак, А. В. Тепикина. - Электрон. текстовые дан. (460 КБ). - Курск : ЮЗГУ, 2016. - 21 с. - Библиогр.: с. 21. - Б. ц.

2) Изучение методики обследования помещения с помощью РЧ-зонда [Электронный ресурс] : 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. Калуцкий, И. И. Рудак, А. В. Тепикина. - Электрон. текстовые дан. (212 КБ). - Курск : ЮЗГУ, 2016. - 13 с. - Библиогр.: с. 13. - Б. ц.

3) Изучение методики обследования помещения с помощью ОНЧ-зонда и дополнительного входа [Электронный ресурс] : 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. Калуцкий, И. И. Рудак, А. В. Тепикина. - Электрон. текстовые дан. (311 КБ). - Курск : ЮЗГУ, 2016. - 12 с. - Библиогр.: с. 12. - Б. ц.

4) Изучение методики проверки телефонных линий и обнаружения носимых радиопередатчиков [Электронный ресурс] : 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. Калуцкий, И. И. Рудак, А. В. Тепикина. - Электрон. текстовые дан. (211 КБ). - Курск : ЮЗГУ, 2016. - 12 с. - Библиогр.: с. 12. - Б. ц.

5) Изучение программно-аппаратного комплекса «VНК-012GL» [Электронный ресурс] : 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. Калуцкий, А. А. Кретов, С. Ю. Тарыгин. - Электрон. текстовые дан. (376 КБ). - Курск : ЮЗГУ, 2016. - 24 с. - Библиогр.: с. 24. - Б. ц.

6) Изучение существующих каналов утечки информации [Электронный ресурс]: методические указания к выполнению лабораторных и практических работ / Юго-Зап. гос. ун-т; сост. И.В. Калуцкий, Ю.А. Куденцова. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2017. 12 с.: ил. 0. Библиогр.: с. 12. - Б. ц.

7) Калуцкий И.В. Демаскирующие признаки объекта информации [Электронный ресурс]: методические указания к выполнению лабораторных и практических работ / Юго-Зап. гос. ун-т; сост. И.В. Калуцкий, Ю.А. Куденцова. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2017. 12 с.: ил. 3. Библиогр.: с. 12. . - Б. ц.

8) Оценка звукоизоляции помещений [Электронный ресурс] : 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. Калущкий, А. А. Кретов, С. Ю. Тарыгин. - Электрон. текстовые дан. (285 КБ). - Курск : ЮЗГУ, 2016. - 21 с. : ил. - Библиогр.: с. 21. - Б. ц.

9) Инженерно-техническая защита информации [Электронный ресурс]: методические указания к выполнению курсового проекта для студентов укрупненной группы специальностей 10.00.00/ Юго-Зап. гос. ун-т; сост.: И.В. Калущкий, Е.М. Чудненко, А.А. Чеснокова. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2017. 58 с.: ил. 1, табл. 17. Библиогр.: с. 56. - Б. ц

10) Аспекты технической защиты информации [Электронный ресурс] : 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. Калущкий, Е.М. Чудненко, А.А. Чеснокова – Курск : ЮЗГУ, 2017. 13 с : ил. 0, табл. 0. Библиогр.: с. 13. - Б. ц.

11) Отделение полезного голоса от зашумляющего фона [Электронный ресурс]: 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. Калущкий, А.А. Чеснокова – Курск : ЮЗГУ, 2018. 29 с : ил. 15, табл. 1. Библиогр.: с. 29. - Б. ц.

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, прочесть 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			

ПРИЛОЖЕНИЕ А Список тем курсовых работ

1. Организация защиты помещений от утечки по электро-магнитному и материально-вещественному каналу
2. Организация защиты помещений от утечки по вибро-акустическому и материально-вещественному каналу
3. Организация защиты помещений от утечки по оптическому и материально-вещественному каналу

Полный список вариантов заданий приведен в методических указаниях к выполнению курсового проекта (Калуцкий И.В. 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. Калуцкий, Е.М. Чудненко, А.А. Чеснокова, Курск, 2017. 58 с.: ил. 1, табл. 17. Библиогр.: с. 56.)