Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

Институт информационных технологий и радиоэлектроники
(Наименование института)

УТВЕРЖДАЮ:
Директор института
_____ А.А. Галкин
«26» августа 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ
(наименование дисциплины)

направление подготовки / специальность

10.03.01 «Информационная безопасность»
(код и наименование направления подготовки (специальности)

направленность (профиль) подготовки

**Безопасность автоматизированных систем
(по отраслям или в сфере профессиональной деятельности)**
(направленность (профиль) подготовки))

г. Владимир

2021

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Защита информации от утечки по техническим каналам» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО 3++ и учебного плана по направлению подготовки 10.03.01 «Информационная безопасность». В процессе подготовки обеспечивается формирование у студентов обобщенного представления об основных понятиях и технических средствах защиты информации. В ходе освоения дисциплины проводится ознакомление студентов с техническими каналами утечки информации, активными и пассивными методами защиты информации от утечек, средствами поиска закладок и аппаратурой несанкционированного съема информации по техническим каналам.

Задачей дисциплины «Защита информации от утечки по техническим каналам» является изучение: основ технических средств защиты информации, физических процессов формирования утечек информации по техническим каналам; технических характеристик и свойств аппаратуры защиты от утечек и поиска технических средств нелегального съема информации. Задачей дисциплины также является формирование: представлений о структуре, принципах функционирования и организации, технических характеристиках средств защиты информации; о физических основах формирования каналов утечки информации и средствах предотвращения утечек; о методах моделирования, проектирования, монтажа и настройки технических средств защиты информации. Задачей дисциплины также является овладение навыками практической деятельности в области моделирования и анализа технических средств защиты информации с использованием средств вычислительной техники, умение использовать соответствующее специализированное программное обеспечение.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Защита информации от утечки по техническим каналам» относится к обязательной части Блока Б1 (код Б1.О.04). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, лабораторных работ и самостоятельной работы. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции *(код, содержание индикатора)*	Результаты обучения по дисциплине	
ОПК4 Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	ЗНАЕТ: основные понятия, законы и модели электричества и магнетизма применительно к техническим средствам ЗИ; ЗНАЕТ основные понятия, законы и модели теории колебаний и волн, оптики, физики твердого тела, статистической физики и термодинамики применительно к техническим средствам ЗИ; ЗНАЕТ особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности УМЕЕТ использовать физические модели и	КР Тестовые вопросы

	ОПК-4.2.1	законы в постановке и решении прикладных задач в профессиональной деятельности	
ОПК 9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1.1 ОПК-9.1.2 ОПК-9.1.2 ОПК-9.1.2 ОПК-9.2.1 ОПК-9.2.2 ОПК-9.3.1 ОПК-9.3.2	ЗНАЕТ классификацию и количественные характеристики технических каналов утечки информации; ЗНАЕТ способы и средства защиты информации от утечки по техническим каналам; методы и средства контроля эффективности технической защиты информации; ЗНАЕТ технические характеристики и возможности аппаратуры защиты информации от утечки по техническим каналам и аппаратуры средств несанкционированного съема информации по техническим каналам; ЗНАЕТ организацию защиты информации от утечки по техническим каналам на объектах информатизации УМЕЕТ анализировать и оценивать угрозы утечки информации по техническим каналам на объекте информатизации; УМЕЕТ формировать комплекс мер по технической защите объекта информатизации от утечки информации по техническим каналам с учетом технической обоснованности и реализуемости ВЛАДЕЕТ методами и средствами технической защиты информации; ВЛАДЕЕТ методами расчета и инструментального контроля показателей технической защиты информации	КР Тестовые вопросы

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 10 зачетных единиц, 360 часов

Тематический план
форма обучения – очная

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	*в форме практической подготовки*		
1	Основные положения и теоретические основы инженерно-технической защиты информации.	6	1	2	-			1	
2	Средства и методы инженерно-технической защиты информации.	6	2	2	-	4			
3	Демаскирующие признаки объектов защиты.	6	3	2	-			1	
4	Основные демаскирующие признаки, характеризующие физические свойства сигналов.	6	4	2	-	4			
5	Основные свойства информации как предмета инженерно-технической защиты.	6	5	2	-			1	
6	Органы добывания информации. Роль разведки в деятельности государств и коммерческих структур.	6	6	2	-	4			Рейтинг-контроль №1
7	Оптические каналы утечки информации.	6	7	2	-			1	
8	Радиоэлектронные каналы утечки информации.	6	8	2	-	4			
9	Акустические каналы утечки информации.	6	9	2	-			1	
10	Составные акустоэлектрон. и акустооптические каналы утечки информации.	6	10	2	-	4			
11	Материально-вещественные каналы утечки информации	6	11	2	-			1	
12	Классификация методов и средств защиты информации от утечки по техническим каналам.	6	12	2	-	4			Рейтинг-контроль №2
13	Технические средства акустической разведки. Принципы функционирования и основные характеристики микрофонов	6	13	2	-			1	
14	Направленные микрофоны. Параболические и лазерные микрофоны. Микрофон- труба.	6	14	2	-	4			
15	Виды и типы акустических закладок	6	15	2	-			1	
16	Полуактивные закладки	6	16	2	-	4			

17	Средства радио-и РТ разведки и поисковые средства.	6	17	2	-			1	
18	Сканерные приемники. Анализаторы спектра.	6	18	2	-	4			Рейтинг-контроль №3
Всего за 6 семестр:		**108**		**36**	**-**	**36**		**9**	**Экзамен (27)**
1	Радиочастотомеры и интерсептеры.	7	1	2	2			6	
2	ПАК радиоконтроля. Радиопеленгаторы	7	2	2	2	4		6	
3	Средства видовой разведки. Средства ТВ наблюдения.	7	3	2	2			6	
4	Средства обнаружения видеокамер.	7	4	2	2	4		6	
5	Каналы утечки по линиям связи. Характеристики проводных линий связи.	7	5	2	2			6	
6	Технические средства защиты телефонных линий, принципы действия, характеристики, эффективность работы.	7	6	2	2	4		6	Рейтинг-контроль №1
7	Средства защиты мобильной связи и wi-fi	7	7	2	2			6	
8	Акустические и виброакустические каналы. Разборчивость акустической информации.	7	8	2	2	4		6	
9	Магнитные и электромагнитные каналы. Побочные электромагнитные излучения и наводки.	7	9	2	2			6	
10	Методы и средства акустической и виброакустической защиты объекта.	7	10	2	2	4		6	
11	Методика акустической и виброакустич. защиты помещения. Генераторы шума	7	11	2	2			6	
12	Противодействие электронным устройствам перехвата информации.	7	12	2	2	4		6	Рейтинг-контроль №2
13	Исследование ПЭМИН электронной техники и средств обработки информации.	7	13	2	2			6	
14	Средства фильтрации сигналов.	7	14	2	2	4		6	
15	Методы и средства экранирования	7	15	2	2			6	
16	Нелинейные локаторы. Методика поиска закладных устройств.	7	16	2	2	4		6	
17	Специальные проверки и специальные обследования помещений.	7	17	2	2			6	
18	Аттестация объектов информатизации	7	18	2	2	4		6	Рейтинг-контроль №3
Всего за 7 семестр:		**252**		**36**	**36**	**36**		**108**	**Экзамен (36)**
Наличие в дисциплине КП/КР		**ДА**							
Итого по дисциплине		**360**		**72**	**36**	**72**		**117**	**Экзамен (27) Экзамен (36) Курсовая работа**

Содержание лекционных занятий по дисциплине

6 семестр. Технические каналы утечки информации и средства несанкционированного съема информации

Тема 1. Основные положения и теоретические основы инженерно-технической защиты информации. Основные понятия, термины и определения. Предмет, цели, задачи и содержание курса инженерно-технической защиты информации. (ИТЗИ). Роль и место курса в подготовке специалистов по организации защиты информации в государственных и коммерческих структурах. Базовые знания, необходимые для изучения курса

Тема 2. Средства и методы инженерно-технической защиты информации. Структура системы инженерно-технической защиты информации на объекте информатизации. Защита **информации от утечек, непреднамеренного и несанкционированного воздействия на нее.**

Тема 3. Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков. Опознавательные признаки и признаки деятельности объектов. Видовые, сигнальные и вещественные признаки. Информативность признаков.

Тема 4. Основные демаскирующие признаки, характеризующие физические свойства сигналов. Особенность видовых признаков в видимом, ИК и радиодиапазонах электромагнитных волн. Основные признаки аналоговых и дискретных (импульсных) электрических сигналов.

Тема 5. Основные свойства информации как предмета инженерно-технической защиты. Классификация источников информации. Источники технической и экономической информации при научных исследованиях, разработке, производстве и эксплуатации продукции на различных этапах коммерческой деятельности. Виды носителей информации (физические поля, электрические сигналы и материальные тела). Способы записи информации на носитель и съема с них. Источники функциональных сигналов. Источники паразитных электромагнитных излучений и наводок (ПЭМИН).

Тема 6. Органы добывания информации. Роль разведки в деятельности государств и коммерческих структур. Структура органов разведки и ее виды. Разведка коммерческих структур. Принципы ведения разведки. Принципы идентификации и интерпретации признаков, обнаружения и распознавания объектов, измерение их характеристик. Возможности различных видов радиоэлектронной разведки. Классификация технических средств разведки по видам их носителей. Принципы комплексного использования технических средств разведки разных видов.

Тема 7. Оптические каналы утечки информации. Условия и особенности утечки информации. Структура канала утечки. Виды каналов утечки. Характеристики каналов утечки информации. Общая классификация технических каналов утечки информации. Структура и физические характеристики оптических каналов утечки информации. Возможности использования оптических каналов, влияние на них факторов среды распространения.

Тема 8. Радиоэлектронные каналы утечки информации. Структура и физические характеристики радиоэлектронных каналов утечки информации. Особенности распространения радиоволн. Источники радиоэлектронных каналов утечки информации. Классификация каналов связи. Основные технические показатели и характеристики каналов связи. Помехи и шумы в каналах связи. Радиосигналы, классификация сигналов, основные свойства и характеристики. Спектры сигналов. Модуляция гармонического высокочастотного сигнала. Манипуляция сигналов. АМ, ЧМ, ФМ. Импульсная модуляция сигналов, шумоподобные сигналы, цифровые сигналы. Теорем Котельникова.

Тема 9. Акустические каналы утечки информации. Акустический канал утечки информации. Основные термины, определения и технические характеристики акустических сигналов. Понятие разборчивости речи. Реверберация звука. Затухание акустической волны при прохождении элементов строительных конструкций. Звукоизоляция помещений.

Тема 10. Составные акустоэлектронные и акустооптические каналы утечки информации. Классификация технических каналов утечки акустической информации.

Тема 11. Материально-вещественные каналы утечки информации. Структура и источники материально-вещественного канала утечки информации. Основные принципы комплексирования каналов утечки информации.

Тема 12. Классификация методов и средств защиты информации от утечки по техническим каналам. Классификация программных средств защиты информации. Основные организационные и режимные мероприятия по защите выделенного помещения от утечки информации по техническим каналам.
Тема 13. Технические средства акустической разведки. Принципы функционирования и основные характеристики микрофонов. Защита акустического и акусто-вибрационно канала. Классификация технических средств акустической защиты. Средства пассивной акустической защиты, виброизоляция. Классификация микрофонов. Принципы функционирования и характеристики микрофонов: чувствительность, уровень собственного шума, направленность и т.д.
Тема 14. Направленные микрофоны. Параболические и лазерные микрофоны. Микрофон-труба. Принципы действия, технические характеристики, особенности эксплуатации.
Тема 15. Виды и типы акустических закладок. Акустические закладки. Классификация. Радиозакладки: стабилизированные и нестабилизированные, с управлением, с системой шифрования и скремблированием. Закладки с ИК- каналом передачи. Сетевые закладки. Телефонные закладки. Классификация. Способы подключения к линии. Основные термины, определения и технические характеристики средств защиты информации в проводных линиях связи. Основные способы защиты телефонных линий.
Тема 16. Полуактивные закладки. Принципы действия, технические характеристики, особенности эксплуатации.
Тема 17. Средства радио-и РТ разведки и поисковые средства. Радиочастотомеры и интерсептеры. Радиопеленгаторы. Состав комплекса пеленгации и его характеристики. Программно-аппаратные комплексы адио- и радиотехнической разведки. Структура и состав комплексов, характеристики и режим работы. Технические характеристики и термины радиопередающей аппаратуры. Специальные обозначения выражение единиц мощности в децибелах. Технические характеристики и термины антенно-фидерных устройств. Функции радиоконтроля. Средства контроля сотовой связи.
Тема 18. Сканерные приемники. Анализаторы спектра. Принцип действия и характеристики приемников. Режимы сканирования. Анализаторы спектра. Спектрограммы. Чувствительность и погрешность измерений.

7 семестр. Технические средства ЗИ от УИТК, методы ЗИ от УИТК
Тема 1. Радиочастотомеры и интерсептеры. Принципы действия, технические характеристики, особенности эксплуатации.
Тема 2. Программно-аппаратные комплексы радиоконтроля. Радиопеленгаторы. Принципы действия, технические характеристики, особенности эксплуатации.
Тема 3. Средства видовой разведки. Средства ТВ наблюдения. Средства фоторазведки. Фотокамеры. Закамуфлированные средства. Средства телевизионного наблюдения. Бинокли, монокуляры, подзорные трубы. Приборы ночного видения. Инфракрасные прожекторы. Портативные видеокамеры.
Тема 4. Средства обнаружения видеокамер. Принципы действия, технические характеристики, особенности эксплуатации.
Тема 5. Каналы утечки по линиям связи. Характеристики проводных линий связи. Основные термины, определения и технические характеристики средств защиты информации в проводных линиях связи. Основные способы защиты телефонных линий.
Тема 6. Технические средства защиты телефонных линий, принципы действия, характеристики, эффективность работы. Принципы действия, технические характеристики, особенности эксплуатации.
Тема 7. Средства защиты мобильной связи и wi-fi. Принципы действия, технические характеристики, особенности эксплуатации.
Тема 8. Акустические и виброакустические каналы. Разборчивость акустической информации. Методики расчетов возможности утечки информации по акустическому каналу.

Тема 9. Магнитные и электромагнитные каналы. Побочные электромагнитные излучения и наводки. Виды акустоэлектрических преобразований. Паразитные излучения и наводки. Классификация акустических радиопередающий закладных устройств. Методы ВЧ навязывания. Технические характеристики и термины радиоприемной аппаратуры.
Тема 10. Методы и средства акустической и виброакустической защиты объекта. Пространственное и линейное зашумление. Пассивные методы защиты речевой информации. Активные методы защиты речевой информации. Определение соответствия помещения требованиям выделенного помещения. Технические средства защиты.
Тема 11. Методика акустической и виброакустич. защиты помещения. Генераторы шума. Принципы действия, технические характеристики, особенности эксплуатации.
Тема 12. Противодействие электронным устройствам перехвата информации.
Тема 13. Исследование ПЭМИН электронной техники и средств обработки информации. Принципы действия, технические характеристики, особенности эксплуатации технических средств активной защиты от ПЭМИН.
Тема 14. Средства фильтрации сигналов. Типы фильтров, их технические характеристики способы применения и особенности эксплуатации.
Тема 15. Методы и средства экранирования. Основные термины, определения и технические характеристики средств защиты информации при утечке информации по электрической сети и цепям заземления. Виды заземления, типы и свойства экранирования. Развязывание информационных сигналов. Фильтрация сигналов. Разделительные трансформаторы. Свойства и характеристики фильтров. Проходные конденсаторы в фильтрах
Тема 16. Нелинейные локаторы. Методика поиска закладных устройств. Принципы действия, технические характеристики, особенности эксплуатации.
Тема 17. Специальные проверки и специальные обследования помещений.
Тема 18. Аттестация объектов информатизации. Назначение, порядок проведения, типы и методы проведения измерений.

Содержание лабораторных занятий по дисциплине

6 семестр
Лабораторная работа 1. Изучение средств блокирования работы мобильной связи. Изучение микрофонов;
Лабораторная работа 2. Исследование методики защиты проводных линий связи с помощью поискового прибора ST 031P «Пиранья»;
Лабораторная работа 3. Исследование методики защиты помещения от утечки по инфракрасному каналу с помощью поискового прибора ST 031P «Пиранья»;
Лабораторная работа 4. Исследование уровней акустических сигналов защищаемого помещения
Лабораторная работа 5. Исследование методики акустической и виброакустической защиты помещения с помощью поискового прибора ST 031P «Пиранья»;
Лабораторная работа 6. Исследование методики поиска закладных устройств нелинейным локатором «Родник-2К»;
Лабораторная работа 7. Исследование радиоэлектронной обстановки и радиоэлектронного канала утечки информации с помощью радиосканера «Icom IC-R1500».
Лабораторная работа 8. Расчет показателей защищенности конфиденциальной информации (расчет зоны R2) выделенного помещения с помощью программного комплекса «Гроза-К».
Лабораторная работа 9. Расчет показателей защищенности конфиденциальной информации (нормативных значений октавных соотношений «Сигнал/шум» при оценке защищенности выделенного помещения от утечки речевой конфиденциальной информации по электроакустическим каналам) с помощью программного комплекса «Гроза-К».

7 семестр
Лабораторная работа 1. Исследование радиоэлектронного канала утечки информации;

Лабораторные работы 2-3. Исследование методики проверки выполнения норм эффективности защиты речевой информации от утечки по акустическому каналу с помощью программно-аппаратного комплекса «Спрут-мини-А»;
Лабораторные работы 4-5. Исследование методики проверки выполнения норм эффективности защиты речевой информации от утечки по виброакустическому каналу с помощью программно-аппаратного комплекса «Спрут-мини-А»;
Лабораторные работы 6-7. Исследование методики проверки выполнения норм эффективности защиты речевой информации от утечки за счет электроакустических преобразований в ТСПИ с помощью программно-аппаратного комплекса «Спрут-мини-А»;
Лабораторная работа 8. Исследование методики защиты телефонных линий в помещении с помощью прибора проверки проводных линий «ULAN»;
Лабораторная работа 9. Исследование методики защиты телефонных линий в помещении с помощью прибора защиты телефонных переговоров «Прокруст 2000».

Содержание практических занятий по дисциплине

7 семестр
Тема 1. Средства обнаружения видеокамер.
Тема 2. Каналы утечки по линиям связи. Характеристики проводных линий связи.
Тема 3. Технические средства защиты телефонных линий, принципы действия, характеристики, эффективность работы.
Тема 4. Разборчивость акустической информации.
Тема 5. Магнитные и электромагнитные каналы. Побочные электромагнитные излучения и наводки.
Тема 6. Методы и средства акустической и виброакустической защиты объекта.
Тема 7. Методика акустической и виброакустич. защиты помещения. Генераторы шума
Тема 8. Исследование ПЭМИН электронной техники и средств обработки информации.

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

5.1. Текущий контроль успеваемости

6 семестр

Перечень вопросов к рейтинг-контролю №1

1. Перечислите цели защиты информации.
2. Перечислите задачи ИТЗИ.
3. Какие признаки объекта защиты называют демаскирующими?
4. Приведите классификацию демаскирующих признаков объекта защиты.
5. Охарактеризуйте видовые демаскирующие признаки.
6. Охарактеризуйте демаскирующие признаки сигналов.
7. Дайте классификацию сигналов.
8. Охарактеризуйте демаскирующие признаки веществ.
9. Какие демаскирующие признаки называются именными, чем они отличаются от других признаков?
10. Какие демаскирующие признаки называются прямыми, чем они отличаются от других признаков?
11. Какие демаскирующие признаки называются косвенными, чем они отличаются от других признаков?
12. Перечислите свойства информации как предмета инженерно-технической защиты.
13. Понятие шумоподобных сигналов.

14. Дайте определения понятиям модуляции и демодуляции сигналов. Опишите и нарисуйте, какие типы импульсно-манипулированных сигналов Вы знаете?
15. Какие типы и виды помех в каналах связи Вы знаете?
16. Классификация помех в каналах связи. Дайте определения мультипликативной и аддитивной помехам.
17. Какие виды носителей информации Вы знаете? Как осуществляется запись информации на носитель?
18. Перечислите основные источники функциональных сигналов.
19. Проведите классификацию источников опасных сигналов по их физическому происхождению.
20. Принцип действия электромагнитных, электродинамических и магнитострикционных акустоэлектрических преобразователей.
21. Принцип действия емкостных акустоэлектрических преобразователей. Принцип действия пьезоэлектрических акустоэлектрических преобразователей.
22. Типы угроз, создаваемых акустоэлектрическими преобразователями.
23. Назовите источники побочных высокочастотных излучений. Назовите источники побочных низкочастотных излучений.

Перечень вопросов к рейтинг-контролю №2

1. Типы угроз, создаваемых акустоэлектрическими преобразователями.
2. Назовите источники побочных высокочастотных излучений. Назовите источники побочных низкочастотных излучений.
3. Назовите типы паразитных связей в радиоэлектронных средствах и физические причины их возникновения.
4. Физические основы паразитных емкостных и индуктивных наводок в радиоэлектронных средствах.
5. Классификация технической разведки по способам добывания информации.
6. Классификация технической разведки по физической природе носителя информации.
7. Основные задачи органов коммерческой разведки.
8. Перечислите основные способы ведения разведки.
9. Перечислите основные этапы добывания информации при разведке.
10. Основные методы анализа и синтеза разведывательной информации.
11. Способы доступа к разведывательной информации.
12. Классификация наземных технических средств дистанционного добывания информации.
13. Классификация каналов утечки информации.
14. Структурная схема, физическая сущность и основные свойства оптического канала утечки информации.
15. Основные свойства акустического канала утечки информации.
16. Основные свойства радиоэлектронного канала утечки информации.
17. Основные свойства материально-вещественного канала утечки информации.
18. Основные свойства акустооптического канала утечки информации.
19. Основные свойства акусто-вибрационного канала утечки информации.
20. Структурная схема и физическая сущность акусто-радиоэлектронного канала утечки информации.
21. Комплексирование каналов утечки информации.
22. Назовите основные этапы проектирования систем инженерно-технической защиты информации.
23. Назовите основные типы моделирования систем инженерно-технической защиты информации.

Перечень вопросов к рейтинг-контролю №3

1. Комплексирование каналов утечки информации.

2. Назовите основные этапы проектирования систем инженерно-технической защиты информации.
3. Назовите основные типы моделирования систем инженерно-технической защиты информации.
4. Что включает в себя моделирование угроз информации (приведите примеры)?
5. Типы контроля эффективности инженерно-технической защиты информации.
6. Что включают в себя организационные меры контроля эффективности инженерно-технической защиты информации?
7. Что включают в себя технические меры контроля эффективности инженерно-технической защиты информации?
8. В чем отличие основных от вспомогательных технических средств и систем?
9. Дайте определение контролируемой зоны.
10. Назовите основные виды каналов утечки информации, обрабатываемой ТСПИ.
11. Покажите, на каких физических процессах ОТСС и ВТСС построены основные виды каналов утечки с информационных носителей.
12. Объясните физическую сущность возникновения побочных электромагнитных излучений.
13. Какие причины приводят к возникновению электрических каналов утечки информации?
14. Покажите, на каких физических процессах в помещениях и размещенных в них ОТСС и ВТСС построены основные виды утечки акустической информации из помещений.
15. Как создаются составные каналы утечки информации?
16. Приведите структуру комплекса средств перехвата радиосигналов.
17. Как реализуется метод «высокочастотного навязывания»?
18. Назовите основные виды каналов утечки информации, передаваемой по каналам связи.
19. Каким параметром определяется зона возможного перехвата информации?
20. Каковы основные акустические параметры речевых сигналов?
21. От чего зависит звукоизоляция основных строительных конструкций?

7 семестр

Перечень вопросов к рейтинг-контролю №1

1. Что является наиболее распространенными причинами снижения звукоизоляции строительных конструкций?
2. Какие элементы строительных конструкций наиболее опасны с точки зрения несанкционированного съема информации?
3. Чем обусловлены материально-вещественные каналы утечки информации?
4. Основные технические характеристики микрофонов.
5. Физические основы явления ребеверации звука.
6. Технические средства акустической и виброакустической защиты выделенного помещения.
7. Основные характеристики и принцип действия параболического микрофона.
8. Основные характеристики и принцип действия лазерных микрофонов.
9. Классификация акустических закладок.
10. Принцип действия полуактивных радиозакладок.
11. Классификация телефонных закладок.
12. Физический принцип действия бесконтактных телефонных закладок.
13. Назначение и основные технические характеристики сканерных приемников.
14. Основные типы организации сканирования радиочастот.
15. Назначение и основные технические характеристики анализаторов спектра.
16. Назначение и основные технические характеристики радиочастотомеров.
17. Назначение и основные технические характеристики интерсепторов.
18. Назначение и основные технические характеристики программно-аппаратных комплексов радиоконтроля.

Перечень вопросов к рейтинг-контролю №2

1. Основные характеристики радиопеленгаторов.

2. Основные характеристики антенно-фидерных устройств.
3. Технические средства контроля сотовой связи.
4. Технические характеристики средств фоторазведки.
5. Основные технические характеристики средств видеонаблюдения.
6. Системы слежения (наблюдения) за перемещением транспортных средств.
7. Способы обнаружения видеокамер и основные технические характеристики средств обнаружения видеокамер.
8. Классификация методов и средств поиска электронных устройств перехвата информации
9. Электростатическое экранирование технических средств
10. Магнитостатическое экранирование технических средств
11. Электромагнитное экранирование технических средств
12. Заземление технических средств
13. Электростатическое экранирование технических средств
14. Магнитостатическое экранирование технических средств
15. Электромагнитное экранирование технических средств
16. Заземление технических средств
17. Развязывание информационных сигналов
18. Фильтрация информационных сигналов
19. Пространственное зашумление
20. Линейное зашумление

Перечень вопросов к рейтинг-контролю №3

1. Пассивные методы защиты акустической (речевой) информации
2. Активные методы защиты акустической (речевой) информации
3. Характеристики и способы повышения звукоизоляции помещений
4. Виброакустическая маскировка
5. Методы и средства обнаружения и подавления диктофонов и акустических закладок.
6. Защита телефонных линий методами синфазной маскирующей низкочастотной (НЧ) помехи и высокочастотной маскирующей помехи
7. Защита телефонных линий методами ультразвуковой маскирующей помехи и повышения напряжения
8. Защита телефонных линий методами "обнуления" и низкочастотной маскирующей помехи
9. Защита телефонных линий компенсационным методом и методом "выжигания"
10. Специальная проверка и спецобследование помещений
11. Нелинейные локаторы. Методика поиска закладных устройств.
12. Специальные проверки и специальные обследования помещений.
13. Аттестация объектов информатизации

5.2. Промежуточная аттестация

6 семестр

Примерный перечень вопросов к экзамену

1. Перечислите цели защиты информации.
2. Перечислите задачи ИТЗИ.
3. Какие признаки объекта защиты называют демаскирующими?
4. Приведите классификацию демаскирующих признаков объекта защиты.
5. Охарактеризуйте видовые демаскирующие признаки.
6. Охарактеризуйте демаскирующие признаки сигналов.
7. Дайте классификацию сигналов.
8. Охарактеризуйте демаскирующие признаки веществ.
9. Какие демаскирующие признаки называются именными, чем они отличаются от других признаков?

10. Какие демаскирующие признаки называются прямыми, чем они отличаются от других признаков?
11. Какие демаскирующие признаки называются косвенными, чем они отличаются от других признаков?
12. Перечислите свойства информации как предмета инженерно-технической защиты.
13. Понятие шумоподобных сигналов.
14. Дайте определения понятиям модуляции и демодуляции сигналов. Опишите и нарисуйте, какие типы импульсно-манипулированных сигналов Вы знаете?
15. Какие типы и виды помех в каналах связи Вы знаете?
16. Классификация помех в каналах связи. Дайте определения мультипликативной и аддитивной помехам.
17. Какие виды носителей информации Вы знаете? Как осуществляется запись информации на носитель?
18. Перечислите основные источники функциональных сигналов.
19. Проведите классификацию источников опасных сигналов по их физическому происхождению.
20. Принцип действия электромагнитных, электродинамических и магнитострикционных акустоэлектрических преобразователей.
21. Принцип действия емкостных акустоэлектрических преобразователей. Принцип действия пьезоэлектрических акустоэлектрических преобразователей.
22. Типы угроз, создаваемых акустоэлектрическими преобразователями.
23. Назовите источники побочных высокочастотных излучений. Назовите источники побочных низкочастотных излучений.
24. Типы угроз, создаваемых акустоэлектрическими преобразователями.
25. Назовите источники побочных высокочастотных излучений. Назовите источники побочных низкочастотных излучений.
26. Назовите типы паразитных связей в радиоэлектронных средствах и физические причины их возникновения.
27. Физические основы паразитных емкостных и индуктивных наводок в радиоэлектронных средствах.
28. Классификация технической разведки по способам добывания информации.
29. Классификация технической разведки по физической природе носителя информации.
30. Основные задачи органов коммерческой разведки.
31. Перечислите основные способы ведения разведки.
32. Перечислите основные этапы добывания информации при разведке.
33. Основные методы анализа и синтеза разведывательной информации.
34. Способы доступа к разведывательной информации.
35. Классификация наземных технических средств дистанционного добывания информации.
36. Классификация каналов утечки информации.
37. Структурная схема, физическая сущность и основные свойства оптического канала утечки информации.
38. Основные свойства акустического канала утечки информации.
39. Основные свойства радиоэлектронного канала утечки информации.
40. Основные свойства материально-вещественного канала утечки информации.
41. Основные свойства акустооптического канала утечки информации.
42. Основные свойства акусто-вибрационного канала утечки информации.
43. Структурная схема и физическая сущность акусто-радиоэлектронного канала утечки информации.
44. Комплексирование каналов утечки информации.
45. Назовите основные этапы проектирования систем инженерно-технической защиты информации.

46. Назовите основные типы моделирования систем инженерно-технической защиты информации.
47. Комплексирование каналов утечки информации.
48. Назовите основные этапы проектирования систем инженерно-технической защиты информации.
49. Назовите основные типы моделирования систем инженерно-технической защиты информации.
50. Что включает в себя моделирование угроз информации (приведите примеры)?
51. Типы контроля эффективности инженерно-технической защиты информации.
52. Что включают в себя организационные меры контроля эффективности инженерно-технической защиты информации?
53. Что включают в себя технические меры контроля эффективности инженерно-технической защиты информации?
54. В чем отличие основных от вспомогательных технических средств и систем?
55. Дайте определение контролируемой зоны.
56. Назовите основные виды каналов утечки информации, обрабатываемой ТСПИ.
57. Покажите, на каких физических процессах ОТСС и ВТСС построены основные виды каналов утечки с информационных носителей.
58. Объясните физическую сущность возникновения побочных электромагнитных излучений.
59. Какие причины приводят к возникновению электрических каналов утечки информации?
60. Покажите, на каких физических процессах в помещениях и размещенных в них ОТСС и ВТСС построены основные виды утечки акустической информации из помещений.
61. Как создаются составные каналы утечки информации?
62. Приведите структуру комплекса средств перехвата радиосигналов.
63. Как реализуется метод «высокочастотного навязывания»?
64. Назовите основные виды каналов утечки информации, передаваемой по каналам связи.
65. Каким параметром определяется зона возможного перехвата информации?
66. Каковы основные акустические параметры речевых сигналов?
67. От чего зависит звукоизоляция основных строительных конструкций?

7 семестр

Примерный перечень вопросов к экзамену

1. Что является наиболее распространенными причинами снижения звукоизоляции строительных конструкций?
2. Какие элементы строительных конструкций наиболее опасны с точки зрения несанкционированного съема информации?
3. Чем обусловлены материально-вещественные каналы утечки информации?
4. Основные технические характеристики микрофонов.
5. Физические основы явления ребеверации звука.
6. Технические средства акустической и виброакустической защиты выделенного помещения.
7. Основные характеристики и принцип действия параболического микрофона.
8. Основные характеристики и принцип действия лазерных микрофонов.
9. Классификация акустических закладок.
10. Принцип действия полуактивных радиозакладок.
11. Классификация телефонных закладок.
12. Физический принцип действия бесконтактных телефонных закладок.
13. Назначение и основные технические характеристики сканерных приемников.
14. Основные типы организации сканирования радиочастот.
15. Назначение и основные технические характеристики анализаторов спектра.
16. Назначение и основные технические характеристики радиочастотомеров.
17. Назначение и основные технические характеристики интерсепторов.

18. Назначение и основные технические характеристики программно-аппаратных комплексов радиоконтроля.
19. Основные характеристики радиопеленгаторов.
20. Основные характеристики антенно-фидерных устройств.
21. Технические средства контроля сотовой связи.
22. Технические характеристики средств фоторазведки.
23. Основные технические характеристики средств видеонаблюдения.
24. Системы слежения (наблюдения) за перемещением транспортных средств.
25. Способы обнаружения видеокамер и основные технические характеристики средств обнаружения видеокамер.
26. Классификация методов и средств поиска электронных устройств перехвата информации
27. Электростатическое экранирование технических средств
28. Магнитостатическое экранирование технических средств
29. Электромагнитное экранирование технических средств
30. Заземление технических средств
31. Электростатическое экранирование технических средств
32. Магнитостатическое экранирование технических средств
33. Электромагнитное экранирование технических средств
34. Заземление технических средств
35. Развязывание информационных сигналов
36. Фильтрация информационных сигналов
37. Пространственное зашумление
38. Линейное зашумление
39. Пассивные методы защиты акустической (речевой) информации
40. Активные методы защиты акустической (речевой) информации
41. Характеристики и способы повышения звукоизоляции помещений
42. Виброакустическая маскировка
43. Методы и средства обнаружения и подавления диктофонов и акустических закладок.
44. Защита телефонных линий методами синфазной маскирующей низкочастотной (НЧ) помехи и высокочастотной маскирующей помехи
45. Защита телефонных линий методами ультразвуковой маскирующей помехи и повышения напряжения
46. Защита телефонных линий методами "обнуления" и низкочастотной маскирующей помехи
47. Защита телефонных линий компенсационным методом и методом "выжигания"
48. Специальная проверка и спецобследование помещений
49. Нелинейные локаторы. Методика поиска закладных устройств.
50. Специальные проверки и специальные обследования помещений.
51. Аттестация объектов информатизации

5.3. Самостоятельная работа обучающегося.

Примерные темы курсовой работы 7 семестр

Тема работы: «Моделирование технических каналов утечки информации на объекте, создание инженерно-технической защиты от НСД» по вариантам. Всего в методических рекомендациях по выполнению курсовой работы имеется 18 вариантов заданий.

Вопросы для выполнения в курсовой работе:

–Провести расстановку в защищаемом помещении мебели, ТСПИ, ОТСС и ВТСС;

–Скорректировать генплан территориального размещению объекта на местности;

–Структурирование информации на объекте, создание основных характеристик объекта защиты;

– Формирование путей физического проникновения злоумышленников на объект;
– Классификация возможных каналов утечки информации на объекте;

- Формирование модели получения информации по техническим каналам с объекта защиты;
- Расчет уровней акустического сигнала на строительных конструкциях;
- Выбор и описание тактико-технических характеристик устройств съема информации;
- Формирование модели защиты информации от утечки по техническим каналам с объекта защиты;
- Выбор и описание тактико-технических характеристик средств защиты информации;
- Изучить организацию и проведение обследований объектов на предмет состояния инженерно-технического укрепления, составление акта обследования состояния инженерно-технического укрепления объекта;
- Проектирование охранно-тревожной сигнализации объектов на основе оборудования ИСБ «Орион» НВП «Болид». На основании Р78.36.031-2013, изученного лекционного материала и примера составления проектной документации (выданного в электронном виде) составить по имеющимся вариантам (16шт) планировок:
  - структурную схему;
  - поэтажные планы сетей охранно-тревожной сигнализации (ОТС);
  - пояснительную записку;
  - расчет емкости резервного питания;
- спецификацию оборудования.

Примерные вопросы и задания для самостоятельной работы студентов 6 семестр

- Демаскирующие признаки объектов защиты информации
- Источники и носители конфиденциальной информации
- Органы добывания информации
- Принципы добывания и обработки информации
- Оптические каналы утечки информации
- Радиоэлектронные каналы утечки
- Акустические каналы утечки
- Утечка информации через ПЭМИН
- Способы доступа к конфиденциальной информации
- Моделирование каналов защиты и объектов утечки информации
- Технические средства акустической разведки
- Средства радиотехнической разведки
- Средства видовой разведки
- Методы поиска технических каналов утечки информации
- Методы акустической и виброакустической защиты
- Заземление и фильтрация сигналов
- Защита телефонных линий
- Противодействие электронным устройствам перехвата информации.

Примерные вопросы и задания для самостоятельной работы студентов 7 семестр

- Средства фильтрации сигналов. Методы и средства экранирования.
- Нелинейные локаторы. Методика поиска закладных устройств.
- Специальные проверки и специальные обследования помещений.
- Аттестация объектов информатизации
- Инженерно-техническое укрепление объектов
- Извещатели охранной сигнализации. Основные ТТД, правила установки и эксплуатации
- Организация централизованной охраны объектов. Системы передачи извещений
- Интегрированные системы и комплексы технических средств охраны и безопасности
- Организация эксплуатационно-технического обслуживания технических средств охраны и безопасности
- Основные понятия СКУД

- Методы и средства идентификации в СКУД
- Устройства преграждающие управляемые СКУД
- Основные термины, понятия и определения СВН
- Устройства управления и передачи видео изображений. Устройства регистрации видеоизображений

Фонд оценочных материалов (ФОМ) для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ
		Наличие в электронном каталоге ЭБС
Основная литература		
1. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам: Справочное пособие / Бузов Г.А. - Москва :Гор. линия-Телеком, 2015. - 586 с. ISBN 978-5-9912-0424-8	2015	https://znanium.com/catalog/product/895240
2. Рагозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации: учебное пособие / Рагозин Ю. Н. - Санкт-петербург : ИЦ Интермедия, 2019. - 216 с. - ISBN 978-5-4383-0182-0	2019	https://www.studentlibrary.ru/book/ISBN9785438301820.html
3. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ: Защита информации от утечки по техническим каналам. Основные понятия, термины, определения и характеристики : учеб. пособие / А. В. Тельный, Ю. М. Монахов ; под ред. проф. М. Ю. Монахова ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир: Изд-во ВлГУ, 2018. – 161 с. (Комплексная защита объектов информатизации. Кн. 26). – ISBN 978-5-9984-0875-5, №госрегистрации №0321803506	2018	http://dspace.www1.vlsu.ru/bitstream/123456789/7165/1/00792.pdf
4. Тельный А. В., Монахов Ю.М. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ: Аппаратура поиска каналов и устройств несанкционированного съема информации. Методики и рекомендации по применению технических средств защиты информации: учеб. пособие / А. В. Тельный, Ю. М. Монахов ; под ред. проф. М. Ю. Монахова ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир: Изд-во ВлГУ, 2018. 86 с. – (Комплексная защита объектов информатизации. Кн. 27). – ISBN 978-5-9984-0874-8, № госрегистрации № 0321803507.	2018	http://dspace.www1.vlsu.ru/bitstream/123456789/7185/1/00793.pdf
5. Тельный А. В. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ: Проектирование технических средств защиты территорий и объектов от несанкционированного доступа: учеб. пособие / А. В. Тельный; под ред. проф. М. Ю. Монахова ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2020. – 251 с. – (Комплексная защита объектов информатизации. Кн. 29). – ISBN 978-5-9984-1172-4	2020	http://dspace.www1.vlsu.ru/bitstream/123456789/8947/1/02160.pdf
Дополнительная 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. : 387-388	2021	https://biblioclub.ru/index.php?page=book&id=458285
2. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. - 2-е изд., перераб. и доп. - Москва : ИНФРА-М, 2021. - 256 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6.	2021	https://znanium.com/catalog/product/1178151
3. Рагозин, Ю. Н. Инженерно-техническая защита информации / Рагозин Ю. Н. - Санкт-петербург : ИЦ Интермедия, 2018. - 168 с. - ISBN 978-5-4383-0161-5.	2018	https://www.studentlibrary.ru/book/ISBN9785438301615.html

6.2. Периодические издания

1. Электронный журнал «Защита информации. Инсайд» ISSN 2413-3582, Режим доступа: http://inside-zi.ru/pages/about.html
2. Электронный журнал «Спецтехника и Связь», Режим доступа: http://www.st-s.su/
3. Электронный журнал «Системы безопасности связи и телекоммуникаций» –компания «Гротек», Москва [Электронный ресурс] // URL: http://sccs.intelgr.com/
4. Электронный научно-технический журнал «Специальная техника», Москва [Электронный ресурс] // URL: http://www.ess.ru/
5. Электронный журнал «БДИ» (Безопасность, Достоверность, Информация), С.-Петербург. [Электронный ресурс] // URL: http://asbgroup.ru/izdaniya/zhurnal-bdi/

6.3. Интернет-ресурсы

1. Сайт «Группа СТ» г. Санкт-Петербург [Электронный ресурс] // URL: http://spymarket.com/
2. Сайт «Группа компаний «Маском»» г.Москва [Электронный ресурс] // URL: http://www.mascom.ru/ (дата обращения: 13.06.2018).
3. Сайт ЗАО НПЦ Фирма "НЕЛК" г. Москва [Электронный ресурс] // URL: https://www.nelk.ru/
4. Сайт «НПО Защита информации» г. Москва [Электронный ресурс] // URL: http://www.sinf.ru/
5. Сайт компании «Проминформзащита» г. Москва [Электронный ресурс] // URL: http://www.profinfo.ru/
6. Сайт компании «Сюртель» г. Москва [Электронный ресурс] // URL: http://www.suritel.ru/
7. ЗАО ПФ «Элвира» Московская обл. г. Железнодорожный [Электронный ресурс] // URL: http://www.elvira.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Занятия проводятся в следующих аудиториях ВлГУ (корпус №2) по адресу г. Владимир, ул. Белоконской, д. 3.

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс

2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокруст 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3»,учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Рабочую программу составил _____ доцент кафедры ИЗИ Тельный А.В.
(ФИО, должность, подпись)

Рецензент
(представитель работодателя) Заместитель руководителя РАЦ ООО «ИнфоЦентр» _____ к.т.н. Вертилевский Н.В.
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ
Протокол № _____ от _____ года
Заведующий кафедрой д.т.н., профессор _____ /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена
на заседании учебно-методической комиссии направления 10.03.01 «Информационная безопасность»
Протокол № _____ от _____ года
Председатель комиссии д.т.н., профессор _____ /М.Ю. Монахов/
(ФИО, должность, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 20 22 / 20 23 учебный год
Протокол заседания кафедры № 14 от 28.06.22 года
Заведующий кафедрой д.т.н., профессор _____ /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный года
Протокол заседания кафедры № _____ от _____ года
Заведующий кафедрой _____

Рабочая программа одобрена на 20____ / 20____ учебный года
Протокол заседания кафедры № _____ от _____ года
Заведующий кафедрой _____

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

образовательной программы направления подготовки *10.03.01 «Информационная безопасность»*

Номер изменения	Внесены изменения в части/разделы рабочей программы	Исполнитель ФИО	Основание (номер и дата протокола заседания кафедры)
1			
2			

Заведующий кафедрой _____/ _____

Подпись *ФИО*