ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.38 ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИХ КАНАЛАМ

Направление подготовки (специальность) 10.03.01 Информационная безопасность

Профиль подготовки (специализация) 10.03.01 Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)

Квалификация выпускника бакалавр

Форма обучения очная

1. Цели освоения дисциплины

-формирование у студентов знаний по основам инженерно-технической защиты информации, а также навыков и умения в применении знаний для конкретных условий;

- развитие в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.

2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.О.38 Защита информации от утечки по технических каналам относится к обязательной части учебного плана. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Защита информации от утечки по технических каналам» является основополагающей, представлен в таблице 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенция	Дисциплина
УК-2	Русский язык и культура речи Моделирование систем Теория функции комплексного переменного Основы радиотехники Прикладные компьютерные программы WEB- технологии Программно-аппаратные средства защиты информации Дискретная математика
ОПК-3	Техническая защита информации Программно-аппаратные средства защиты информации
ОПК-4	Сетевые технологии
ОПК-9	Техническая защита информации Методы и средства криптографической защиты информации Производственная технологическая практика
ОПК-11	Дискретная математика Производственная технологическая практика

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенция	Дисциплина
УК-2	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра)
ОПК-3	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра)
ОПК-4	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра)
ОПК-9	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра)
ОПК-11	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра)

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 3.1 – Взаимосвязь планируемых результатов обучения по дисциплине и планируемых результатов освоения образовательной программы

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине (модулю)
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 Формулирует в рамках поставленной цели проекта совокупность взаимосвязанных задач, обеспечивающих ее достижение. Определяет ожидаемые результаты решения выделенных задач	*Знать:* Установку, монтаж и настройки технических средств защиты информации *Уметь:* Применять технические средства для криптографической защиты информации конфиденциального характера *Владеть:* Возможностью технического обслуживания технических средств защиты информации
	УК-2.2 Проектирует решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений	*Знать:* Номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам *Уметь:* Применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами *Владеть:* Навыками формирования и реализации политики информационной безопасности на защищаемом объекте
	УК-2.3 Решает конкретные задач проекта заявленного качества и за установленное время	*Знать:* Принципы организации информационной безопасности автоматизированных систем в соответствии с требованиями по защите информации *Уметь:* Пользоваться нормативными документами по противодействию технической разведке *Владеть:* Методами и средствами технической защиты информации

УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.4 Публично представляет результаты решения конкретной задачи проекта	*Знать:* Возможности технических средств перехвата информации *Уметь:* Анализировать и оценивать угрозы информационной безопасности объекта *Владеть:* Методами установки и настройки криптографических и технических средств защиты информации
ОПК-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-3.1 Проводит работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от утечки по техническим каналам	*Знать:* Принципы устройства и функционирования средств криптографической и технической защиты информации *Уметь:* Применять технические средства для криптографической защиты информации конфиденциального характера *Владеть:* Методами установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты

ОПК-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-3.2 Проводит работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа	*Знать:* Принципы организации информационной безопасности автоматизированных систем в соответствии с требованиями по защите информации *Уметь:* Производить установку и настройку программно-технических средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами *Владеть:* Методикой контроля защищенности информации от несанкционированного доступа
	ОПК-3.3 Проводит контроль эффективности защиты информации от утечки по техническим каналам	*Знать:* Технические каналы утечки информации *Уметь:* Применять технические средства для защиты информации в условиях применения устройств обработки и передачи данных *Владеть:* Применением основных типов технических средств защиты информации

ОПК-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-3.4 Проводит контроль эффективности защиты информации от несанкционированного доступа	*Знать:* Устранение выявленных неисправностей программно-технических средств защиты информации от несанкционированного доступа и при необходимости организация их ремонта с привлечением производителей этих средств *Уметь:* Производить установку и настройку программно-технических средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами *Владеть:* Навыками испытания программно-технических средств защиты информации от несанкционированного доступа
ОПК-4 Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1 Проводит организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;	*Знать:* Особенности организационного сопровождения разработки, отладки, модификации и поддержки информационных технологий и систем *Уметь:* Проводить организационное сопровождение разработки, отладки, модификации и поддержки информационных технологий и систем *Владеть:* Навыками проведения мероприятий организационного обеспечения информационной безопасности в процессе сопровождения разработки, отладки, модификации поддержки информационных технологий и систем

ОПК-4 Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-4.2 Способен администрировать операционные системы, системы управления базами данных, вычислительные сети	*Знать:* Администрирование локальных вычислительных сетей и принимать меры по устранению возможных сбоев *Уметь:* Администрировать сетевые ресурсы в информационных системах *Владеть:* Сбором данных для анализа использования и функционирования программно-технических средств компьютерных сетей
	ОПК-4.3 Выполняет работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	*Знать:* Основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации *Уметь:* выбирать, устанавливать и настраивать аппаратные средства защиты информации от несанкционированного доступа и соответствующее программное обеспечение *Владеть:* Основными методами, способами и средствами защиты информации от несанкционированного доступа

ОПК-4 Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-4.4 Осуществляет диагностику и мониторинг систем защиты автоматизированных систем	*Знать:* Типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа *Уметь:* Осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак *Владеть:* Установкой, настройкой программных средств защиты информации в автоматизированной системе
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1 Применяет математические модели и решает задачи криптографического преобразования при решении задач защиты информации	*Знать:* Математические методы, необходимые для решения задач защиты информации *Уметь:* Использовать типовые математические методы и модели для решения задач *Владеть:* Подходами к решению стандартных математических задач, выполнению расчетов математических величин, применению математических методов обработки экспериментальных данных

ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.2 Определяет и анализирует технические каналы утечки информации	*Знать:* Каналы утечки информации и методы их оценки *Уметь:* Изучать и анализировать характеристики и особенности применения основных приборов и оборудования, используемых для выявления каналов утечки информации *Владеть:* Расчетом контролируемой зоны, в пределах которой могут происходить утечки информации
	ОПК-9.3 Проводит работы по установке и настройке средств технической защиты информации	*Знать:* Основные принципы действия и характеристики технических средств физической защиты *Уметь:* Применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом *Владеть:* Навыками проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации

ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-11.1 Проводит испытания по оценки защищенности объектов информатизации на основе существующих методик ФСТЭК	*Знать:* Определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации *Уметь:* Прорабатывать общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России, модели угроз безопасности информации, разрабатываемые ФСТЭК России *Владеть:* Методиками для определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях, отнесенных к государственным и муниципальным информационным системам, информационным системам персональных данных, значимым объектам критической информационной инфраструктуры Российской Федерации
	ОПК-11.2 Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	*Знать:* Основные понятия и методы математической статистики *Уметь:* Использовать математические методы и модели для решения прикладных задач *Владеть:* Методами количественного анализа процессов обработки, поиска и передачи информации

ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-11.3 Принимает участие в проведении экспериментальных исследований системы защиты информации	*Знать:* Основные алгоритмы и типовые модели, используемые при решении практических задач с помощью аппарата теории вероятностей, математической статистики *Уметь:* Логически мыслить, подбирать формулы, соответствующие типам задач *Владеть:* Навыками использования математических моделей теории вероятностей и математической статистики

4. Объем дисциплины

Объем дисциплины Б1.О.38 Защита информации от утечки по технических каналам составляет 3 зачетных(ые) единиц(ы) (ЗЕ), (108 академических часов), распределение объёма дисциплины на контактную работу обучающихся с преподавателем (КР) и на самостоятельную работу обучающихся (СР) по видам учебных занятий и по периодам обучения представлено в таблице 4.1.

Таблица 4.1 – Распределение объема дисциплины по видам учебных занятий и по периодам обучения, академические часы

Вид учебной работы	Итого КР	Итого СР	Семестр №8	
			КР	СР
Лекции (Л)	24		24	
Лабораторные работы (ЛР)	12		12	
Практические занятия (ПЗ)	12		12	
Семинары(С)				
Курсовое проектирование (КП)	2		2	
Самостоятельная работа		54		54
Промежуточная аттестация	4		4	
Наименование вида промежуточной аттестации	x	x	КР	
Всего	54	54	54	54

5. Структура и содержание дисциплины

Структура и содержание дисциплины представлены в таблице 5.1.

Таблица 5.1 – Структура и содержание дисциплины

Наименование тем	Семестр	Объем работы по видам учебных занятий, академические часы									Коды формируемых компетенций, код индикатора достижения компетенции
		Лекции	Лабораторная работа	Практические занятия	Семинары	Курсовое проектирование	Индивидуальные домашние задания (контрольные работы)	Самостоятельное изучение вопросов	Подготовка к занятиям	Промежуточная аттестация	
Тема 1. Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Представление сил и средств защиты информации в виде системы	8	2		2				4			УК-2.1, УК-2.2, УК-2.3, УК-2.4, ОПК-3.1, ОПК- 3.2, ОПК-3.3, ОПК-3.4, ОПК- 4.1
Тема 2. Системный подход к защите информации Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации	8	2		2				4			ОПК-4.2, ОПК- 4.3, ОПК-4.4, ОПК-9.1, ОПК- 9.2, ОПК-9.3, ОПК-11.1, ОПК- 11.2, ОПК-11.3, УК-2.1, УК-2.2, УК-2.3

Тема 3. Распространение сигналов в технических каналах утечки информации Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в светопроводах. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи	8	2	2					4			ОПК-3.2, ОПК- 3.3, ОПК-3.4, ОПК-4.1, ОПК- 4.2, ОПК-4.3, ОПК-4.4, ОПК- 9.1, ОПК-9.2
Тема 4. Особенности информации как предмета защиты. Свойства информации, влияющие на ее безопасность. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ	8	2		2				4			ОПК-9.3, ОПК- 11.1, ОПК-11.2, ОПК-11.3, ОПК- 9.1, ОПК-9.2
Тема 5. Моделирование случайных величин. Законы распределения случайных величин. Статистические оценки и их точность. Аппроксимация результатов статистического моделирования	8	2	2					4			УК-2.2, ОПК- 9.1, ОПК-4.2, ОПК-11.2, ОПК- 11.1, ОПК-11.3

Тема 6. Основные понятия теории случайных процессов, их классификация и основные характеристики. Марковские процессы с дискретными состояниями. Марковские процессы с дискретными состояниями и непрерывным временем. Стационарные случайные процессы	8	2	2					4			УК-2.4, ОПК- 4.1, ОПК-9.1, ОПК-11.2
Тема 7. Моделирование инженерно-технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты	8	2	2					4			УК-2.3, ОПК- 11.2, ОПК-11.3, УК-2.2, ОПК- 3.4, ОПК-9.1, УК-2.1
Тема 8. Задачи защиты информации ТКС в условиях конфликта. Понятие конфликта. Способы разрешения конфликта в ТКС	8	2	2					4			УК-2.1, УК-2.2, УК-2.3, ОПК- 3.4, ОПК-4.2, ОПК-9.3, ОПК- 11.1, ОПК-11.2, ОПК-11.3

Тема 9. Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности инженерно-технической защиты информации. Виды зон контроля. Требования по защите информации от утечки по техническим каналам. Виды технического контроля	8	2	2					4			ОПК-3.2, ОПК- 3.3, ОПК-3.4, ОПК-9.2, ОПК- 9.3, УК-2.1, ОПК-4.1
Тема 10. Методические рекомендации по оценке эффективности защиты информации. Способы оценки эффективности охраны объектов защиты. Оценка эффективности защиты видовых признаков объектов наблюдения	8	2		2				6			УК-2.1, ОПК- 3.2, ОПК-3.3, ОПК-3.4, ОПК- 4.2
Тема 11. Основные задачи, структура и характеристика государственной системы противодействия технической защите. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации	8	2		2				6			ОПК-3.1, ОПК- 3.2, УК-2.1, УК- 2.2, ОПК-4.1, ОПК-3.3, ОПК- 3.4

Тема 12. Физические основы защиты информации от технических разведок. Классификация средств технических разведок по виду носителя. Типовые задачи технических разведок. Принципы действия аппаратуры технических разведок. Классификация методов и средств защиты информации от технических разведок	8	2		2				6			УК-2.1, ОПК- 3.2, УК-2.2, ОПК-3.4, ОПК- 3.3, ОПК-3.1, ОПК-4.1, ОПК- 4.3, ОПК-4.2, ОПК-9.1, ОПК- 11.2
Контактная работа	8	24	12	12		2				4	x
Самостоятельная работа	8							54			x
Объем дисциплины в семестре	8	24	12	12				54		4	x
Всего по дисциплине		24	12	12		2		54		4	

5.2. Темы курсовых работ (проектов)

1. Комплексный подход к построению технической защиты информации на объекте информатизации.

2. Основные положения и принципы построения технической защиты информации.

3. Анализ демаскирующих признаков, методы и способы защиты демаскирующих признаков на объекте защиты.

4. Модель поведения внешнего нарушителя на этапах реализации угроз безопасности информации, методы и способы противодействия от утечки информации по техническим каналам.

5. Модель поведения инсайдера на этапах реализации угроз безопасности информации, методы и способы противодействия от утечки информации по техническим каналам.

6. Условия и факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации.

7. Условия и субъективные факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации.

8. Методы защиты видовых демаскирующих признаков от технических средств разведок.

9. Методы защиты сигнальных демаскирующих признаков от технических средств разведок.

10. Методы защиты радиосигналов от перехвата техническими средствами разведок.

11. Методы защиты электрических сигналов от перехвата техническими средствами разведок.

12. Методы защиты материальных и вещественных демаскирующих признаков от технических средств разведок.

13. Технические средства наблюдения в видимом и ИК диапазонах за объектом защиты, методы и средства противодействия средствам наблюдения.

14. Технические средства наблюдения в радио диапазонах за объектом защиты,

методы и средства противодействия средствам наблюдения.

15. Технические средства перехвата конфиденциальной информации передаваемой по линии связи, методы и средства противодействия перехвата конфиденциальной информации.

16. Методы и технические средства съема конфиденциальной речевой информации с использованием вторичных переизлучателей.

17. Методы и технические средства съема конфиденциальной речевой информации с использованием опто-волоконных линий связи.

18. Методы и технические средства съема конфиденциальной речевой информации с использованием средств высокочастотного навязывания.

19. Технические средства подслушивания, методы и средства противодействия средствам подслушивания.

20. Технические средства анализа демаскирующих признаков веществ, методы и средства нейтрализации (утилизации) отходов производства.

21. Технические средства контроля, обнаружения, уничтожение закладных устройств, порядок проведения ЗПМ.

22. Технические средства контроля, обнаружения, уничтожение закладных устройств, в слаботочных линиях связи, порядок проведения ЗПМ.

23. Технические средства контроля, обнаружения, уничтожение закладных устройств в телефонных линиях связи, порядок проведения ЗПМ.

24. Технические средства контроля, обнаружения, уничтожение закладных устройств, в электросетях, цепях заземления, порядок проведения ЗПМ.

25. Способы и средства контроля и порядок проведения ЗПМ в защищаемых помещений на отсутствие закладных устройств.

26. Моделирование вербального объекта защиты, возможных угроз безопасности информации для оптических каналов утечки информации в видимом и ИК диапазонах, разработка способов, методов и технических средств защиты информации.

27. Математические методы моделирования для вербального объекта защиты от возможных угроз безопасности информации для акустических каналов утечки информации.

28. Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустических каналов утечки информации, разработка методов и технические средств защиты информации.

29. Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустикорадиоэлектронных каналов утечки информации, разработка методов и технических средств защиты информации.

30. Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустико-оптических каналов утечки информации, разработка методов и технических средств защиты информации.

31. Моделирование вербального объекта защиты, где производится обработка информации с использованием СВТ (АС), возможных угроз безопасности информации и технических каналов утечки информации, разработка методов и технических средств защиты информации.

32. Порядок проведения аттестационных испытаний по требованиям безопасности информации на примере вербального объекта информатизации.

33. Порядок проведения работ по созданию системы защиты информации для вербального объекта информатизации.

34. Организационные методы контроля эффективности защиты информации на примере вербального объекта информатизации.

5.3. Темы индивидуальных домашних заданий (контрольных работ)

Данный вид работы не предусмотрен учебным планом

5.4 Вопросы для самостоятельного изучения по очной форме обучения

№ п.п.	Наименования темы	Наименование вопросов	Объем, академические часы
1	Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно- технической защиты информации. Представление сил и средств защиты информации в виде системы	Особенности инженерно-технической защиты информации. Комплексная защита информации.	4
2	Системный подход к защите информации Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации	Утечка информации. Возможные способы утечки информации, их характеристика. Технические каналы утечки информации и их классификация.	4
3	Распространение сигналов в технических каналах утечки информации Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в светопроводах. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи	Возможные способы распространения акустических, оптических сигналов и радиосигналов.	4
4	Особенности информации как предмета защиты. Свойства информации, влияющие на ее безопасность. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ	Понятие информации, ее свойства: конфиденциальность, целостность и доступность.	4

5	Моделирование случайных величин. Законы распределения случайных величин. Статистические оценки и их точность. Аппроксимация результатов статистического моделирования	Понятие случайных величин	4
6	Основные понятия теории случайных процессов, их классификация и основные характеристики. Марковские процессы с дискретными состояниями. Марковские процессы с дискретными состояниями и непрерывным временем. Стационарные случайные процессы	Классификация случайных процессов	4
7	Моделирование инженерно-технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты	Какие выделяют основные этапы при проектировании системы инженерно-технической защиты информации	4
8	Задачи защиты информации ТКС в условиях конфликта. Понятие конфликта. Способы разрешения конфликта в ТКС	Какие есть способы разрешения конфликта в ТКС	4
9	Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности инженерно- технической защиты информации. Виды зон контроля. Требования по защите информации от утечки по техническим каналам Виды технического контроля	Какие существуют основные методы и способы контроля эффективности инженерно-технической защиты информации	4
10	Методические рекомендации по оценке эффективности защиты информации. Способы оценки эффективности охраны объектов защиты. Оценка эффективности защиты видовых признаков объектов наблюдения	Какие способы оценки эффективности охраны объектов защиты наиболее эффективны	6

11	Основные задачи, структура и характеристика государственной системы противодействия технической защите. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации	Какие выделяют основные документы по защите информации и противодействия технической разведке	6
12	Физические основы защиты информации от технических разведок. Классификация средств технических разведок по виду носителя. Типовые задачи технических разведок. Принципы действия аппаратуры технических разведок. Классификация методов и средств защиты информации от технических разведок	По каким признакам классифицируют методы и средства защиты информации от технических разведок	6
		Всего	54

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система.

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1. Петров, Ю. В. Моделирование случайных величин : учебное пособие / Ю. В. Петров, С. Н. Аникин, С. А. Юхно. — Санкт-Петербург : БГТУ "Военмех" им. Д.Ф. Устинова, 2020. — 89 с. — ISBN 978-5-907324-03-9. — Текст : электронный // Лань : электронно-библиотечная система.
2. Гутова, С. Г. Основы теории случайных процессов : учебно-методическое пособие / С. Г. Гутова, О. Н. Инденко, Е. С. Чернова. — Кемерово : КемГУ, 2020. — 159 с. — ISBN 978-5-8353-2869-7. — Текст : электронный // Лань : электронно-библиотечная система.

6.3 Методические материалы для обучающихся по освоению дисциплины

Тематическое содержание дисциплины

7. Требования к материально-техническому и учебно-методическому содержанию дисциплины

7.1 Учебные аудитории для проведения учебных занятий по дисциплине

Занятия лекционного типа проводятся в учебной аудитории для проведения занятий лекционного типа с набором демонстрационного оборудования, обеспечивающие тематические иллюстрации, укомплектованной специализированной мебелью и техническими средствами обучения.

Занятия семинарского типа проводятся в учебных аудиториях для проведения занятий семинарского типа, укомплектованных специализированной мебелью и техническими средствами обучения.

Консультации по дисциплине проводятся в учебных аудиториях для групповых и индивидуальных консультаций, укомплектованных специализированной мебелью и техническими средствами обучения.

Текущий контроль и промежуточная аттестация проводится в учебных аудиториях для текущего контроля и промежуточной аттестации, укомплектованных специализированной мебелью и техническими средствами обучения.

Самостоятельная работа студентов проводится в помещениях для самостоятельной работы, укомплектованных специализированной мебелью и техническими средствами обучения. Учебное оборудование хранится и обслуживается в помещениях для хранения и профилактического обслуживания учебного оборудования.

7.2 Перечень оборудования и технических средств обучения по дисциплине

Занятия лекционного типа проводятся в аудитории, оборудованной мультимедиа-проектором, компьютером и учебной доской.

7.3 Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1. JoliTest (JTRun, JTEditor, TestRun)
2. MS Office

7.4 Современные профессиональные базы данных и информационно-справочные системы

1. Консультант +

Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине представлены в Приложении 6.

Программа разработана в соответствии с Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

Разработал(и):

Заведующий кафедрой,к.т.н. _____ Урбан Владимир Александрович

Рабочая программа рассмотрена и одобрена на заседании кафедры Техносферной и информационной безопасности, протокол № 6 от 17.01.2021 г.

Зав. кафедрой _____ Урбан Владимир Александрович

Программа рассмотрена и утверждена на заседании Ученого совета Института управления рисками и комплексной безопасности, протокол № 4 от 22.02.2021 г.

Директор Института управления рисками и комплексной безопасности _____ Яковлева Евгения Васильевна

Дополнения и изменения

в рабочей программе дисциплины Б1.О.38 Защита информации от утечки по технических каналам на 2021 - 2022 учебный год.

В программу вносятся следующие изменения: без изменений

Рабочая программа рассмотрена и одобрена на заседании кафедры Техносферной и информационной безопасности, протокол № 6 от 17.09.2021 г.

Зав. кафедрой _____ Урбан Владимир Александрович