Приложение 3

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФГБОУ ВО «ИГУ»

Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ

Декан _____ Буднев Н.М.

«20» апреля 2023 г.

Рабочая программа дисциплины

Наименование дисциплины **Б1.В.04 Основы построения и функционирования технических средств защиты информации**

Направление подготовки **10.03.01 Информационная безопасность**

Направленность (профиль) подготовки **Техническая защита информации**

Квалификация выпускника **бакалавр**

Форма обучения **очная**

Согласовано с УМК физического факультета

Протокол №38 от «18» апреля 2023 г.

Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 7 от «27» февраля 2023 г.

И.О. зав. кафедрой _____ Колесник С.Н.

Иркутск 2023 г.

Содержание

I. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ (МОДУЛЯ):

Учебная дисциплина «Основы построения и функционирования технических средств защиты информации» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует фундаментализации образования, формирование знаний в области технической защиты информации и навыков применения средств технической защиты информации в профессиональной деятельности.

Цели освоения учебной дисциплины:

1) развитие у студентов социально-личностных качеств: коммуникативности, организованности, ответственности, трудолюбия, целеустремленности;

2) формирование профессиональных знаний, навыков и умений в области технической защиты информации;

3) формирование практических навыков при работе со средствами технической защиты информации.

Задачи освоения учебной дисциплины**:**

1) формирование профессиональных знаний, навыков и умений по установке, настройке, эксплуатации и поддержании в работоспособном состоянии технических средств защиты информации с учетом установленных требований; изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

2) участие в проведении аттестации объектов, помещений, технических средств, систем, программ алгоритмов на предмет соответствия требованиям защиты информации;

3) получение навыков сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

4) совершенствование системы управления информационной безопасностью.

II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Основы построения и функционирования технических средств защиты информации» является базовой дисциплиной профессионального цикла. Дисциплина является вводной в проблематику технической защиты информации. Взаимосвязь данной дисциплины через компетенции отражена в рабочем учебном плане и матрице компетенций. Дисциплина опирается на знания, полученные в ходе изучения дисциплин «Математический анализ», «Информатика», «Аппаратные средства вычислительной техники», «Электричество, магнетизм и волновая оптика», «Электротехника» которая должна быть освоена полностью и студенты должны владеть навыками применения методов технической защиты информации.

Дисциплина является предшествующей для таких дисциплин профессионального цикла

как «Основы управления информационной безопасностью», «Техническая защита объектов критической информационной инфраструктуры», «Аттестация объектов информатизации», а так же для учебной и производственной практики и итоговой государственной аттестации. Изучение данной дисциплины позволяет приобрести первичные навыки, необходимые для изучения принципов обеспечения безопасности автоматизированных систем.

III. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенции ПК-4 в соответствии с ФГОС ВО и ОП ВО по данному направлению подготовки (специальности) 10.03.01 Информационная безопасность

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
ПК-4 Способен использовать основные принципы построения и функционирования технических средств защиты информации	ИДК$_{ПК4.1}$ Применяет основные принципы построения и функционирования технических средств защиты информации	***Знать:*** - основные программно-аппаратные и технические средства защиты информации, применяемые на объектах информатизации;; - основные характеристики программно-аппаратных и технических средств защиты информации, применяемых на объектах информатизации; - особенности и возможности применения программно-аппаратных и технических средств защиты информации, применяемых на объектах информатизации для выявления и нейтрализации технических каналов утечки информации (ТКУИ). ***Уметь:*** - подготавливать к работе технические средства защиты информации, применяемые на объектах информатизации;; - проводить установку, настройку технических средств защиты информации, применяемых на объектах информатизации; - определять неисправности технических средств защиты информации, применяемых на объектах информатизации в

		соответствии с инструкцией по эксплуатации данных средств; ***Владеть:*** - навыками настройки технических средств защиты информации, применяемых на объектах информатизации;. - навыками проведения контроля работоспособности и неисправности технических средств защиты информации, применяемых на объектах информатизации в соответствии с инструкцией по эксплуатации данных средств.

IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетных единицы, 108 часов,
Форма промежуточной аттестации: зачет

4.1 Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов

№ п/н	Раздел дисциплины/тема	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся, практическую подготовку и трудоемкость (в часах)				Форма текущего контроля успеваемости/ Форма промежуточной аттестации (по семестрам)
					Контактная работа преподавателя с обучающимися			Самостоятельная работа (в том числе, внеаудиторная СР, КСР)	
					Лекция	лабораторное занятие	Консультация		
1	2	3	4	5	6	7	8	9	10
1	Тема 1. Введение. Объекты информационной защиты.	6	13		4	4		5	
2	Тема 2. Структура, классификация и основные характеристики технических каналов утечки информации.	6	18		6	6		6	Защита ЛР

3	Тема 3. Побочные электромагнитные излучения и наводки, электромагнитные излучения средств вычислительной техники.	6	14		4	4		6	Защита ЛР
4	Тема 4. Технические средства доступа, перехвата и съема информации.	6	18		6	6		6	Защита ЛР
5	Тема 5. Способы и средства защиты речевой информации от утечки по каналам связи и скрытие объектов наблюдения.	6	18		6	6	1	6	Защита ЛР
6	Тема 6. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки.	6	18		6	6		6	Защита ЛР

4.2. План внеаудиторной самостоятельной работы (в том числе КСР) обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
1	Тема 1. Введение. Объекты информационной защиты.	Работа с учебником, справочной литературой, конспектом	1 нед.	5		Конспект, рекомендуемая литература
2	Тема 2. Структура, классификация и основные характеристики технических каналов утечки информации.		2-4 нед.	6	Защита ЛР	

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
3	Тема 3. Побочные электромагнитные излучения и наводки, электромагнитные излучения средств вычислительной техники.		5-7 нед	6		
4	Тема 4. Технические средства доступа, перехвата и съема информации.		8-10 нед.	6		
5	Тема 5. Способы и средства защиты речевой информации от утечки по каналам связи и скрытие объектов наблюдения.		11-13 нед.	6		
6	Тема 6. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки.		14-17 нед	6		
Общий объем самостоятельной работы по дисциплине (час)				**35**		
Из них объем самостоятельной работы с использованием электронного обучения и дистанционных образовательных технологий (час)				**0**		

4.3. Содержание учебного материала

Тема 1. Введение. Объекты информационной защиты.

Основные понятия**.** Классификация угроз безопасности информации. Информационные системы и необходимость их защиты.

Тема 2. Структура, классификация и основные характеристики технических каналов утечки информации.

Основные элементы канала реализации угроз безопасности информации. Классификация ТКУИ. ТКУИ, обрабатываемой техническими средствами. Схема ТКУИ.

Тема 3. Побочные электромагнитные излучения и наводки, электромагнитные излучения средств вычислительной техники.

Основные понятия и законы электромагнитных полей (ЭМП). Электромагнитные излучения систем средств вычислительной техники. Информативность побочных электромагнитных излучений и наводок (ПЭМИН). Паразитные связи и наводки.

Тема 4. Технические средства доступа, перехвата и съема информации.

Способы перехвата речевой информации. Классификация закладных устройств. Устройства съема информации с телефонной линии.

Тема 5. Способы и средства защиты речевой информации от утечки по каналам связи и скрытие объектов наблюдения.

Методы и способы защиты персональных данных от утечки по техническим каналам. Пассивные и активные методы и способы защиты каналов утечки информации. Состав пассивных и активных средств защиты технических каналов утечки информации. Генераторы акустического шума.

Тема 6. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки. Методы и способы защиты информации, обрабатываемой в технических средствах передачи информации. Методы борьбы с утечками через ПЭМИН. Генераторы линейно-пространственного зашумления. Экранирование и компенсация информативных полей. Заземление технических средств.

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

№ п/н	№ раздела и темы	Наименование семинаров, практических илабораторных работ	Трудоемкость (час.)		Оценочные средства	Формируемые компетенции (индикаторы)*
			Всего часов	Из них практическая подготовка		
1	2	3	4	5	6	7
1	Т1	Введение. Объекты информационной	4		Защита ЛР	ПК4

		защиты.				
2	Т2	Структура, классификация и основные характеристики технических каналов утечки информации.	6		Защита ЛР	
3	Т3	Побочные электромагнитные излучения и наводки, электромагнитные излучения средств вычислительной техники.	4		Защита ЛР	
4	Т4	Технические средства доступа, перехвата и съема информации.	6		Защита ЛР	
5	Т5	Способы и средства защиты речевой информации от утечки по каналам связи и скрытие объектов наблюдения.	6		Защита ЛР	
6	Т6	Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки.	6			

4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СРС)

№ п/п	Тема	Задание	Формируемая компетенция	ИДК
1	2	3	4	5
1	Введение. Объекты информационной защиты.	Осмысление материала лекций. Подготовка к защите Лр1.	ПК4	$ИДК_{ПК4.1}$
2	Структура, классификация и основные характеристики технических каналов утечки информации.	Осмысление материала лекций. Подготовка к защите Лр2.		
3	Побочные электромагнитные излучения и наводки, электромагнитные излучения средств вычислительной техники.	Осмысление материала лекций. Подготовка к защите Лр3.		
4	Технические средства доступа, перехвата и съема информации.	Осмысление материала лекций. Подготовка к защите Лр4.		
5	Способы и средства защиты речевой информации от утечки по каналам связи и скрытие объектов наблюдения.	Осмысление материала лекций. Подготовка к защите Лр5.		
	Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки.			

4.4. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа бакалавров – индивидуальная учебная деятельность, осуществляемая без непосредственного руководства преподавателя, в ходе которой бакалавр активно воспринимает, осмысливает полученную информацию, решает теоретические и практические задачи, готовится к защите лабораторных работ.

На самостоятельную работу выносятся следующие вопросы по темам дисциплины:

Тема 1. Введение. Объекты информационной защиты.

Тема 2. Структура, классификация и основные характеристики технических каналов утечки информации.

Тема 3. Побочные электромагнитные излучения и наводки, электромагнитные излучения средств вычислительной техники.

Тема 4. Технические средства доступа, перехвата и съема информации.

Тема 5. Способы и средства защиты речевой информации от утечки по каналам связи и скрытие объектов наблюдения.

Тема 6. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки.

4.4. Примерная тематика курсовых работ (проектов)

не предусмотрено

V. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Электронная информационно-образовательная среда университета обеспечивает доступ к электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочей программе дисциплины (модуля).

Библиотечный фонд укомплектован печатными зданиями из расчета не менее 0,25 экземпляра каждого из изданий на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль).

Обучающимся обеспечен доступ к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей).

1. Фрязинов, А. В. Практикум по дисциплине "Защита персональных данных, автоматизация управленческой деятельности". Раздел 1 [Текст] : учеб.-практ. пособие / А. В. Фрязинов ; Иркут. гос. ун-т, Фак. сервиса и рекламы, Каф. прикл. информатики и документоведения. - Иркутск : Изд-во ИГУ, 2018. - 65 с.

2. Техническая защита информации: учебное пособие / Раков А. С., Маслов О. Н., Губарева О. Ю., Почепцов А. О., Гуреев В. О. Поволжский государственный университет телекоммуникаций и информатики, 2020. – 96с. https://e.lanbook.com/book/255575.

3. Глухарев М.Л., Исаева М.Ф. Технические средства защиты информации: Учебное пособие. Петербургский государственный университет путей сообщения Императора Александра I, 2018. – 55 с. https://e.lanbook.com/book/111736.

VI.МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Учебно-лабораторное оборудование:

Аудитория 317 – лаборатория, оснащенная лабораторным оборудованием, в том числе, для проведения лабораторных работ по дисциплине «Цифровые системы передачи информации». NI ELVIS.

6.2. Программное обеспечение:

1. Windows 7 Professional. Номер Лицензии Microsoft 60642086. Бессрочно.

2. ABBY PDF Transformer 3.0 Пакет из 10 неименных лицензий Per Seat (10лиц.) EDU. Код позиции: AT30-1S1P10-102 Котировка № 03-165-11 от 23.11.2011. Бессрочно.
3. Microsoft OfficeProPlus 2013 RUS OLP NL Acdmc. Контракт № 03-013-14 от 08.10.2014.Номер Лицензии Microsoft 45936786. Бессрочно.

6.3. Технические и электронные средства:
Мультимедийный проектор, экран (по необходимости), меловая или маркерная доска.

VII.ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

На лекциях используются активные методы обучения (компьютерных симуляций, разбор конкретных ситуаций). Лабораторные работы проводятся с использованием ПЭВМ, специализированных лабораторных стендов с последующей защитой.

VIII.ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Текущий контроль реализуется при защите лабораторных работ ЛР1-ЛР5. Текущий контроль направлен на выявление сформированности компетенции ПК-7.

Контроль качества освоения дисциплины (модуля) включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация проводятся в целях установления соответствия достижений обучающихся требованиям образовательной программы к результатам обучения и формирования компетенций.

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки.

Для реализации текущего контроля используется балльно-рейтинговая система оценки, принятая в университете.

За посещение одного вида занятия дается 0,5 балла (42 занятия (Л+ ЛР)*0,5 балла = 21 балл),лабораторные работы (ЛР) – 75 баллов (5*ЛР*15 баллов=75 баллов). 4 балла преподаватель может добавить за досрочную защиту лабораторных работ.

Параметры оценочного средства для защиты лабораторных работ ЛР1-ЛР5

Критерии оценки	Оценка / баллы			
	Отлично 11-15 баллов	Хорошо 6-10 балла	Удовлетв. 1-5 балла.	Неудовл. 0 баллов
Выполнение заданий	Полностью и корректно оформлен отчет, сделаны выводы. При защите показано всестороннее и глубокое знание материала.	В целом отчет оформлен корректно, сделаны выводы, но имеются незначительные недостатки. При защите студент показывает понимает материала, приводит примеры, но	Отчет оформлен полностью. Имеются замечания по оформлению, выводы сделаны не полностью. При защите - суждения поверхностны, содержат ошибки, примеры не приводятся, ответы на дополнительные	Отчет не оформлен. Отчет оформлен со значительными замечаниями, выводы не полные, при защите студент с трудом формулирует свои мысли, не приводит примеры, не дает ответа на дополнительные вопросы

		испытывает затруднения с выводами, однако достаточно полно отвечает на дополнительные вопросы.	вопросы не уверенные.	.

Вопросы к практическим занятиям (12 тем). Представляют собой перечень вопросов, проверяющих знание теоретического лекционного материала и тем, вынесенных на самостоятельную проработку:

Пз. 1 1. Демаскирующие признаки объектов защиты.
2. Классификация демаскирующих признаков.

Пз. 2 Конфиденциальная информация и её носители.

Пз. 3 1. Демаскирующие признаки аналоговых сигналов.
2. Демаскирующие признаки цифровых сигналов.

Пз. 4 1. Состав и характеристики технических каналов утечки информации.
2. Какие демаскирующие признаки сигналов позволяют выявить наличие закладного устройства в помещении?

Пз. 5 1. Что представляют собой ПЭМИН?
2. Характеристики аппаратуры перехвата и регистрации ПЭМИН.

Пз.6 1. Технические средства выявления демаскирующих признаков.
2. Методика и порядок проведения исследований по выявлению демаскирующих признаков.

Пз.7 1. Каким образом организуется процесс перехвата и восстановление информации ПЭМИН?
2. Какие характеристики СВТ используются при настройке аппаратуры перехвата ПЭМИН?

Пз. 8 1. Каким образом организуется процесс перехвата и восстановление речевой информации?
2. В чем заключается принцип формирования акустического канала утечки информации?

Пз. 9 Каким образом организуется процесс перехвата и восстановление видовой информации?

Пз. 10 1. Аппаратура акустической защиты речевой информации. Проблемы применения.
2. Принципы построения генераторов акустического и вибрационного шумов.

Пз. 11
1. Активные и пассивные средства защиты от ПЭМИН.
2. Подавление ПЭМИН с помощью генераторов линейно-пространственного зашумления.

Пз. 12
1. Принципы построения и функционирования программно-аппаратных комплексов.

2. Основные технические характеристики программно-аппаратных комплексов.
3. Порядок проведения исследований с помощью многофункциональных комплексов.

Форма промежуточного контроля – зачет. Зачет выставляется по итогам изучения дисциплины в течение семестра при условии положительных результатов защиты всех лабораторных работ, предусмотренных программой.

Промежуточная аттестация направлена на проверку сформированности компетенций ПК-4и проводится в форме зачета. Для реализации промежуточного контроля используется балльно-рейтинговая система оценки, принятая в университете.

Зачет выставляется по сумме балов, полученных при изучении дисциплины.

Усвоение бакалавром изучаемой дисциплины максимально оценивается 100 баллами. Из них 90 баллов обучающийся может набрать в течение семестра и от 0 до 10 баллов могут быть даны в качестве «премиальных» баллов за активные формы работы, высокое качество выполненных лабораторных и т.д.

Перечень теоретических вопросов к зачету

1 Скрытие речевой информации в каналах связи
2 Энергетическое скрытие акустических информативных сигналов
3 Скрытие речевой информации в каналах связи.
4 Способы и средства обнаружения закладных устройств
5 Классификация средств обнаружения и локализации закладных устройств
6 Средства обнаружения излучений закладных устройств
7 Сканирующие радиоприемники
8 Средства обнаружения неизлучающих закладок
9 Принцип действия нелинейного локатора.
10 Нелинейный локатор «Катран». Назначение, состав, основные характеристики, режимы работы.
11 Многофункциональные комплекты для выявления каналов утечки информации
12 Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «ПКУ-6М»
13 Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «Пиранья»
14 Комплекс RS turbo
15. Радиотехнические системы передачи информации.
16. Радиолокационная система охраны периметра и территории объектов.
17. Классификация помех.
18. Естественные аддитивные помехи.
19. Искусственные аддитивные помехи.
20. Мультипликативные помехи.
21. Особенности частотных диапазонов.
22. Распространение радиоволн.
23. Диапазоны волн (частот).
24 Подавление опасных сигналов акустоэлектрических преобразователей телефонных линиях
4.25 Пассивные методы защиты от утечки информации по акустоэлектрическому каналу
4.26 Активные методы защиты от утечки информации по акустоэлектрическому каналу
4.27 Экранирование как пассивный способ защиты от утечек по техническим каналам

4.28 Заземление технических средств и подавление информационных сигналов в цепях заземления.

Параметры оценочного средства для аттестации в форме зачета.

Итоговый семестровый рейтинг	Академическая оценка
0-59 баллов	«не зачтено»
60-100 баллов	«зачтено»

Материалы для проведения текущего и промежуточного контроля знаний студентов:

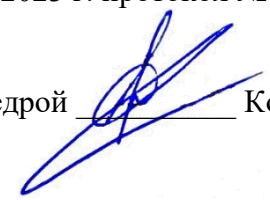
№	Вид контроля	Контролируемые темы (разделы)	Контролируемые компетенции/ индикаторы
1	**2**	**3**	**4**
1	Защита лабораторных работ	Т1-Т6	ПК-4.

_____ профессор Ерохин В.В.

(подпись) (занимаемая должность) (Ф.И.О.)

Программа составлена в соответствии с требованиями ФГОС ВО и учитывает рекомендации ОПОП по направлению и профилю подготовки 10.03.01 Информационная безопасность.

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники
«27» февраля 2023 г. протокол № 7



И.О. зав. кафедрой _____ Колесник С.Н.