Директор института ИРИТ

_____Мякиньков А.В.

«03» июня 2024 г.

Лист актуализации рабочей программы дисциплины
«Б1.Б.41 Поиск уязвимостей в автоматизированных системах»
индекс по учебному плану, наименование

для подготовки **специалистов**
Направление: 10.05.03 «Информационная безопасность автоматизированных систем»
Направленность: Безопасность открытых информационных систем
Форма обучения: очная
Год начала подготовки: 2022
Курс 5
Семестр 9

В рабочую программу 2022 г. вносятся изменения:

1) Таблицу 7.2 читать в следующей редакции:

№	Наименование ЭБС	Ссылка к ЭБС
1	Консультант студента	http://www.studentlibrary.ru/
2	Лань	https://e.lanbook.com/
3	Юрайт	https://biblio-online.ru/
4	TNT-ebook	https://www.tnt-ebook.ru/

2) Пункт 9 читать в следующей редакции:

Для контактной и самостоятельной работы обучающихся выделены помещения, оснащённые компьютерной техникой с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации:

Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом образовательной программы, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес места нахождения помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом образовательной программы
Лаборатория информационной безопасности ВС и С №4407 учебного корпуса №4 для проведения учебных занятий **Оснащенность оборудованием и техническими средствами обучения:** 1. Сервер HP ProLiant ML150G6 – 1 шт. 2. Сервер Dell Rack 410 – 2 шт. 3. Сетевое хранилище Netgear – 2 шт. 4. Openflow-коммутаторы HP ProCurve 3500 – 2 шт. 5. Коммутаторы Русьтелетех PTT-A311 – 2 шт. 6. Коммутатор Zyxel ES-3124 – 1 шт. 7. Микрокомпьютеры Cubieboard – 20 шт.	603155, Нижегородская область, г. Нижний Новгород, ул. Минина, д. 24В

8. Мониторы – 1 шт. 9. Компьютеры AMD Phenom II X6 – 6 шт. 10. Компьютера Intel i7 – 5 шт. 11. Компьютер Intel i3 – 1 шт. 12. Моноблок Acer Core 2 – 1 шт. 13. Wi-Fi маршрутизатора TP-Link TP-ML3230 – 2 шт. 14. Мониторы – 1 шт. 15.Десктопные компьютерные станции с мониторами Dell 24" UltraSharp U2415 - 3 шт. 16.Web-камера Intel RealSense camera - 1 шт. Посадочных мест – 10 **Программное обеспечение:** 1. Dr.Web (С/н ZNFC-CR5D-5U3U-JKGP от 20.05.2024, до 30.05.25) 2. Распространяемое по свободной лицензии: ОС: Ubuntu 18.04.5 LTS, Apache OpenOffice, VScode, git, Anydesk	

Программа актуализирована для 2022 г. начала подготовки.

Разработчик (и): __Капранов С.Н., к.т.н., доцент_____
(ФИО, ученая степень, ученое звание)

«_15_»_05___2024г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБВСС _____ протокол № _9___ от «_15_» ___05___2024_г.

И.о. заведующий кафедрой _____Ляхманов Д.А.

Лист актуализации принят на хранение:

Заведующий выпускающей кафедрой ИБВСС _____«03» июня 2024 г.

Методический отдел УМУ:_____ «03» июня 2024 г.

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Нижегородский государственный технический университет
им. Р.Е. Алексеева» (НГТУ)

Учебно-научный институт радиоэлектроники и информационных технологий (ИРИТ)
(Полное и сокращенное название института, реализующего данное направление)

УТВЕРЖДАЮ:
Директор института:
_____ Мякиньков А.В.
подпись ФИО
22 апреля 2023г г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.41 Поиск уязвимостей в автоматизированных системах
(индекс и наименование дисциплины по учебному плану)
для подготовки специалистов

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

Направленность: Безопасность открытых информационных систем

Форма обучения: очная
Год начала подготовки 2022

Выпускающая кафедра ИБВСС

Кафедра-разработчик ИБВСС

Объем дисциплины 144/4
часов/з.е
Промежуточная аттестация Зачет

Разработчик: Капранов С.Н., к.т.н., доцент

Нижний Новгород

2023г

Рабочая программа дисциплины: разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по направлению подготовки «Информационная безопасность автоматизированных систем», утвержденного приказом МИНОБРНАУКИ РОССИИ от 26 ноября 2020 г. № 1457 на основании учебного плана, принятого УМС НГТУ

протокол от 20.04.2023г № 18.

Рабочая программа одобрена на заседании кафедры протокол от _01.04.2023_ № 4
Зав. кафедрой к.т.н, доцент Ляхманов Д.А. _____
(подпись)

Программа рекомендована к утверждению ученым советом института ИРИТ, Протокол от 21.04.2023_№_4

Рабочая программа зарегистрирована в УМУ, регистрационный № 10.05.03-б-41
Начальник МО _____ Н.Р. Булгакова

Заведующая отделом комплектования НТБ _____ Н.И. Кабанина
(подпись)

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ 6

1.1 Цель освоения дисциплины 6
1.2 Задачи освоения дисциплины (модуля) 6

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 6

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ) 7

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 9

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам 9
4.2 Содержание дисциплины, структурированное по темам 10

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ. 17

5.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности 17
5.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания 19

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 22

7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 23

7.1 Перечень информационных справочных систем 23
7.2 Перечень свободно распространяемого программного обеспечения 23
7.3 Перечень современных профессиональных баз данных и информационных справочных систем 24

8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ 24

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, НЕОБХОДИМОЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ 25

ТАБЛИЦА 9.1 - ОСНАЩЕННОСТЬ АУДИТОРИЙ И ПОМЕЩЕНИЙ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ 25

10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ 26

10.1 Общие методические рекомендации для обучающихся по освоению дисциплины, образовательные технологии 26
10.2 Методические указания для занятий лекционного типа 27
10.3Методические указания по освоению дисциплины на лабораторныхработах 27
10.4 Методические указания по самостоятельной работе обучающихся 27

11. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ 28

11.1 Типовые контрольные задания или иные +материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе текущего контроля успеваемости 28
11.1.1. Типовые задания для лабораторных работ 28
11.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе промежуточной аттестации по дисциплине 28
11.2.1. Защита курсового проекта/ работы 28
11.2.2. Зачет в 9 семестре для студентов очной формы. 28

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель освоения дисциплины

Целью освоения дисциплины является развитие компетенций в области проектирования и обеспечения функционирования информационных систем с применением инструментальных средств защиты информации.

1.2 Задачи освоения дисциплины (модуля)

Дисциплина «Поиск уязвимостей в автоматизированных системах» способствует подготовке студентов к решению следующих профессиональных задач:

1. Определение состава инструментальных средств защиты информации его применение при проектировании информационных систем.
2. Использование современных инструментальных средств защиты информации для обеспечения функционирования информационных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Поиск уязвимостей в автоматизированных системах» Б1.Б.41 включена в обязательный перечень дисциплин обязательной части образовательной программы вне зависимости от ее направленности (профиля). Дисциплина реализуется в соответствии с требованиями ФГОС, ОП ВО и УП, по направлению подготовки 10.05.03.

Дисциплина базируется на дисциплинах блока по информационной безопасности, предшествующими курсами, на которых непосредственно базируется дисциплина «Поиск уязвимостей в автоматизированных системах», являются:

- «Защита информации от утечек по техническим каналам»,
- «Основы информационной безопасности».

Дисциплина «Поиск уязвимостей в автоматизированных системах» является основополагающей для преддипломной практики и выполнения выпускной квалификационной работы.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)[1]

Дисциплина «Поиск уязвимостей в автоматизированных системах» формирует компетенцию ОПК-13 совместно с дисциплинами и практиками, указанными в таблице 3.1.

Таблица 3.1- Формирование компетенций дисциплинам

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки специалиста»										
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
ОПК-13 (Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем)											
Управление информационной безопасностью											
Поиск уязвимостей в автоматизированных системах											
Подготовка и защита ВКР											

Таблица 3.2- Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**			**Оценочные средства**	
					Текущего контроля	**Промежуточной аттестации**
ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ИОПК-13.2. Применяет методы пинтестинга для поиска и устранения уязвимостей систем защиты информации в открытых информационных системах	***Знать:*** – угрозы и уязвимости специфичные для различных типов открытых информационных систем; – основные атаки на открытые информационные системы; – каналы утечки информации;	***Уметь:*** – выполнять поиск информации об угрозах, уязвимостях и каналах утечки информации в открытых информационных систем; – проводить контрольные проверки работоспособности применяемых средств защиты информации;	***Владеть:*** – методами поиска уязвимостей и каналов утечки информации в открытых информационных системах различных типов.	Выполнение сквозного индивидуального задания – лабораторная работа – 10работ	Вопросы для устного собеседования – 20 вопросов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 4 зач.ед. 144 часа, распределение часов по видам работ семестрам представлено в таблице 4.1.

Таблица 4.1 - Распределение трудоёмкости дисциплины по видам работ по семестрам для студентов очного обучения

Вид учебной работы	**Трудоёмкость в час**	
		В т.ч. по семестрам
		9 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	**144**	**144**
1. Контактная работа:	**72**	**72**
1.1 Аудиторная работа, в том числе:	**68**	**68**
занятия лекционного типа (Л)	34	34
занятия семинарского типа (ПЗ-семинары, практ. Занятия и др)		
лабораторные работы (ЛР)	34	34
1.2 Внеаудиторная, в том числе	**4**	**4**
курсовая работа (проект) (КР/КП) (консультация, защита)		
текущий контроль, консультации по дисциплине	4	4
контактная работа на промежуточном контроле (КРА)		
2. Самостоятельная работа (СРС)	**72**	**72**
реферат/эссе (подготовка)		
расчётно-графическая работа (РГР) (подготовка)		
контрольная работа		
курсовая работа/проект (КР/КП) (подготовка)		
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиум и т.д.)	72	72
Подготовка к зачёту/ зачёту с оценкой	-	-

4.2 Содержание дисциплины, структурированное по темам

Таблица 4.2 -Содержание дисциплины, структурированное по темам для студентов очного обучения

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
Раздел 1. Понятие и назначение ИСЗИ										
ОПК-13- ИОПК-13.2.	**Тема 1.1** Понятие и назначение Инструментальных средств информационных систем защиты информации (ИСЗИ)	3				8	Подготовка к лекциям [6.1.1, 6.1.3], работа над сквозным индивидуальным заданием			
	Тема 1.2 Методология защиты информации как теоретический базис ИСЗИ. Системный анализ и системный подход. Основные системные представления	3				8	Подготовка к лекциям [6.1.1, 6.1.3], работа над сквозным индивидуальным заданием			
	Тема лабораторной работы: «Методы анализа защищенности сети»		3				Подготовка к лабораторной работе [6.1.10, 6.1.11]		3	

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
	Итого по 1 разделу	**6**	**3**		**1**	**16**				
Раздел 2. Принципы организации и этапы разработки ИСЗИ										
ОПК-13- ИОПК-13.2.	**Тема 2.1** Принципы построения ИСЗИ. Цели системного подхода к защите информации. Основные требования, предъявляемые к ИСЗИ	3				8	Подготовка к лекциям [6.1.1, 6.1.3], работа над сквозным индивидуальным заданием			
	Тема 2.1 Оценка угроз безопасности информации	3				6	Подготовка к лекциям [6.1.1, 6.1.3], работа над сквозным индивидуальным заданием			
	Тема 2.2 Источники дестабилизирующего воздействия на информацию	3				8	Подготовка к лекциям [6.1.1, 6.1.3], работа над сквозным			

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
							индивидуальным заданием			
	Тема 2.3 Причины, обстоятельства и условия дестабилизирующего воздействия на информацию со стороны технических средств, технологических процессов и природных явлений	3				8	Подготовка к лекциям [6.1.1, 6.1.3], работа над сквозным индивидуальным заданием			
	Тема лабораторной работы: «Установка ПО Virtualbox и ОС Windows 7, MS Office 2007»		6				Подготовка к лабораторной работе [6.1.10, 6.1.11]		6	
	Тема лабораторной работы: «Контроль защищенности сети с применением СПО		3				Подготовка к лабораторной работе [6.1.10, 6.1.11]		3	

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
	«Ревизор сети 3.0»»									
	Тема лабораторной работы: «Работа с анализатором сетевых пакетов Wireshark 2019»		3				Подготовка к лабораторной работе [6.1.10, 6.1.11]		3	
	Тема лабораторной работы: «Принципы работы средств защиты информации (СЗИ) от НСД»		3				Подготовка к лабораторной работе [6.1.10, 6.1.11]		3	
	Итого по 2 разделу	**12**	**15**		**1**	**30**				
Раздел 3. Определение потенциальных каналов и методов НСД и компонентов ИСЗИ										
ОПК-13- ИОПК-13.2.	**Тема 3.1** Методика выявления каналов несанкционированного доступа к информации (НСД).	3				6	Подготовка к лекциям [6.1.1, 6.1.3], работа над сквозным индивидуальным заданием			

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
	Тема 3.2. Определение возможных методов НСД	3				6	Подготовка к лекциям [6.1.1, 6.1.3], работа над сквозным индивидуальным заданием			
	Тема 3.3. Понятие модели объекта. Моделирование сетевых угроз как инструмент анализа объекта ИСЗИ	3				6	Подготовка к лекциям [6.1.1, 6.1.3], работа над сквозным индивидуальным заданием			
	Тема лабораторной работы: «Установка и настройка СЗИ от НСД «Dallas Lock 8.0»		3				Подготовка к лабораторной работе [6.1.10, 6.1.11]		3	
	Тема лабораторной работы: «Установка и настройка СЗИ от НСД «Secret Net Studio 8»		3				Подготовка к лабораторной работе [6.1.10, 6.1.11]		3	

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
	Тема лабораторной работы: «Установка и настройка МЭ «Vip Net Client 4.5»		3				Подготовка к лабораторной работе [6.1.11]		3	
	Итого по 3 разделу	**9**	**9**		**1**	**18**				
Раздел 4. Материально-техническое и нормативно-методическое обеспечение ИСЗИ										
ОПК-13- ИОПК-13.2.	**Тема 4.1.** Значение и состав нормативно-методического обеспечения. Порядок разработки и внедрения документов предприятия	3				4	Подготовка к лекциям [6.1.1, 6.1.3], работа над сквозным индивидуальным заданием			
	Тема 4.2. Цели планирования деятельности ИСЗИ. Принципы и способы планирования	4				4	Подготовка к лекциям [6.1.1, 6.1.3], работа над сквозным индивидуальным заданием			
	Тема лабораторной работы:		3				Подготовка к лабораторной		5	

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
	«Разработка пакета ОРД по защите информации предприятия »						работе [6.1.11]			
	Тема лабораторной работы: «Работа с СПО контроля защищенности «Терьер-3.0», «Фикс 2.02», Ревизор - 1XP»		4				Подготовка к лабораторной работе [6.1.11]		5	
	Итого по 4 разделу	**7**	**7**		**1**	**8**				
	Подготовка к зачету					18				
	Итого по дисциплине	**34**	**34**		**4**	**72**				

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.

5.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности

Для выполнения процедур оценивания составлен паспорт оценочных средств.

Таблица 5.1 - Паспорт оценочных средств (текущая аттестация)

Номер раздела	Наименование раздела дисциплины	**Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций**	**Лекционные занятия**		**Лабораторные работы**		**Самостоятельная работа**	
			Процедура оценивания	Наименование оценочных средств	Процедура оценивания	Наименование оценочных средств	Процедура оценивания	Наименование оценочных средств
1	Понятие и назначение ИСЗИ	ОПК-13- ИОПК-13.2.			Проверка выполнения заданий сквозной контрольной работы по темам раздела	Задание сквозной контрольной работы – программная реализация, анализ результатов лабораторной работы	Устный опрос по результатам самостоятельной работы	Вопросы по заданиям практической части
2	Принципы организации и этапы разработки ИСЗИ	ОПК-13- ИОПК-13.2.			Проверка выполнения заданий сквозной контрольной работы по темам раздела	Задание сквозной контрольной работы – программная реализация, анализ результатов лабораторной работы	Устный опрос по результатам самостоятельной работы	Вопросы по заданиям практической части
3	Определение потенциальных каналов и	ОПК-13- ИОПК-13.2.			Проверка выполнения заданий сквозной контрольной	Задание сквозной контрольной работы – программная реализация, анализ	Устный опрос по результатам самостоятельной работы	Вопросы по заданиям практической части

Номер раздела	Наименование раздела дисциплины	**Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций**	**Лекционные занятия**		**Лабораторные работы**		**Самостоятельная работа**	
			Процедура оценивания	Наименование оценочных средств	Процедура оценивания	Наименование оценочных средств	Процедура оценивания	Наименование оценочных средств
	методов НСД и компонентов ИСЗИ				работы по темам раздела	результатов лабораторной работы		
4	Материально-техническое и нормативно-методическое обеспечение ИСЗИ	ОПК-13- ИОПК-13.2.			Проверка выполнения заданий сквозной контрольной работы по темам раздела	Задание сквозной контрольной работы – программная реализация, анализ результатов лабораторной работы	Устный опрос по результатам самостоятельной работы	Вопросы по заданиям практической части

Комплект оценочных средств является неотъемлемой частью ФОС и хранится на кафедре «Информационная безопасность вычислительных систем и сетей».

5.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

При промежуточном контроле успеваемость студентов оценивается по четырехбальной системе «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Таблица 5.3–Критерии оценивания результата обучения по дисциплине и шкала оценивания

Код и наименование компетенции	**Код и наименовани индикатора достижения компетенции**	**Критерии оценивания результатов обучения**			
		Оценка **«неудовлетворительно»** / «не зачтено» 0-59% от max рейтинговой оценки контроля	Оценка **«удовлетворительно»** / «зачтено» 60-74% от max рейтинговой оценки контроля	Оценка **«хорошо» /** «зачтено» 75-89% от max рейтинговой оценки контроля	Оценка **«отлично» /** «зачтено» 90-100% от max рейтинговой оценки контроля
ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ИОПК-13.2. Применяет методы пинтестинга для поиска и устранения уязвимостей систем защиты информации в открытых информационных системах	Изложение учебного материала бессистемное, неполное, не освоены особенности применения программно-аппаратные средства защиты информации (ПАЗИ). Не знает показатели защищенности средств вычислительной техники (СВТ) от несанкционированного доступа (НСД), не умеет конфигурировать параметры системы защиты информации (СЗИ) в соответствии с ее эксплуатационной документацией (ЭД).	Фрагментарные, поверхностные знания особенностей применения ПАЗИ. Имеет представление о показателях защищенности СВТ от НСД, знает некоторые основные категории требований к ПАЗИ. Владеет некоторыми методами и средства контроля защищенности информации для различных подсистем защиты.	Знает особенности применения ПАЗИ, умеет конфигурировать параметры СЗИ в соответствии с ее ЭД, знает о показателях защищенности СВТ от НСД. Владеет навыками разработки архитектуры системы защиты информации открытой информационной системы.	Имеет глубокие знания всего материала структуры дисциплины, знает особенностей применения ПАЗИ, умеет конфигурировать параметры СЗИ в соответствии с ее ЭД, владеет методами и средства контроля защищенности информации для различных подсистем защиты.

Таблица 5.4 - Критерии оценивания

Оценка	Критерии оценивания
Высокий уровень «5» (отлично)	оценку **«отлично»** заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку **«хорошо»** заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый уровень «3» (удовлетворительно)	оценку **«удовлетворительно»** заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.
Минимальный уровень «2» (неудовлетворительно)	оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1. Зайцев, А. П. Технические средства и методы защиты информации : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. — 7-е изд., испр. — Москва : Горячая линия-Телеком, 2018. — 442 с. — ISBN 978-5-9912-0233-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111057

6.1.2. Потерпеев, Г. Ю. Безопасность операционных систем : учебное пособие / Г. Ю. Потерпеев, В. С. Нефедов, А. А. Криулин. — Москва : РТУ МИРЭА, 2021. — 93 с. — ISBN 978-5-7339-1393-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182416

6.2 Справочно-библиографическая литература

— *учебники и учебные пособия*

6.1.3. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : элек-тронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837

6.1.4. Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко. — Ставрополь : СКФУ, 2015. — 222 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155247

6.1.5. Мартынов, Л. М. Алгебра для криптографии : учебное пособие / Л. М. Мартынов. — Омск : ОмГУПС, [б. г.]. — Часть 3 — 2018. — 83 с. — ISBN 978-5-949-41189-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/129190

6.1.6. Онлайн-книга Руководство по языку программирования Java / https://metanit.com/java/tutorial/

6.1.7. Д. Раджпут Spring. Все паттерны проектирования / Пальчиковский В.В., Павлоградский В.В. – Питер. – 2014.- 320 с.

6.3 Перечень журналов по профилю дисциплины:

6.1.8. *Научно-технический и научно-производственный журнал Информационные технологии.* Журнал "Информационные технологии" (novtex.ru).

6.1.9. *Информационные ресурсы России. Российская ассоциация электронных библиотек.* Информационные Ресурсы России — Российская ассоциация электронных библиотек (aselibrary.ru).

6.1.10. Научно-технический журнал «Информационная безопасность». *Журнал «Информационная безопасность» - (itsec.ru)*

6.4 Методические указания, рекомендации и другие материалы к занятиям

Методические пособия и указания по выполнению лабораторных работ по дисциплине Информационные технологии в электронном варианте находятся на кафедре «Информационная безопасность вычислительных систем и сетей». Электронные варианты методических пособий и указаний по выполнению лабораторных работ отправляются на электронные адреса групп.

6.1.11. Инструментальные средства защиты информации [Электронные текстовые данные]: метод. указания к лаб. работам по дисциплине «Поиск уязвимостей в автоматизированных системах» для студентов направления 10.05.03 «Информационная безопасность автоматизированных систем» дневной формы обучения / НГТУ; Сост.: Р.А. Васильев, 2022, 124 с.

6.1.12. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных: метод. пособие для студентов направления 10.05.03 «Информационная безопасность автоматизированных систем» дневной формы обучения / НГТУ; Сост.: Р.А. Васильев, М.А. Степаненко. Н. Новгород, 2022, 146 с.

7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебный процесс по дисциплине обеспечен необходимым комплектом свободно распространяемого программного обеспечения (состав по дисциплине определен в настоящей РПД и подлежит обновлению при необходимости).

7.1 Перечень информационных справочных систем

Таблица 7.1 -Перечень электронных библиотечных систем

№	Наименование ЭБС	Ссылка к ЭБС
1	«Консультант студента - Электронная библиотека технического вуза»	http://www.studentlibrary.ru/
2	Лань	https://e.lanbook.com/
3	«Юрайт» (коллекция «Легендарные книги»)	https://urait.ru/
4	«Техэксперт» - «Нормы, правила, стандарты и законодательство России»	https://www.nntu.ru/frontend/web/ngtu/files/org_structura/library/resurvsy/tehekspert.pdf

7.2 Перечень свободно распространяемого программного обеспечения

Таблица 7.2 – Программное обеспечение, используемое студентами очного обучения

Программное обеспечение, используемое в университете на договорной основе	Программное обеспечение свободного распространения

Программное обеспечение, используемое в университете на договорной основе	Программное обеспечение свободного распространения
1. Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23 2. MATLAB R2008a DVD KIT-WIN & UNIX/MAC (№ лицензии 527840, № заказа 2035235 Softline от 05.05.2008). 3. Microsoft Windows 7 MSDN (подписка DreamSpark Premium, договор № Tr113003 от 25.09.14)	Adobe Acrobat Reader (https://acrobat.adobe.com/ru/ru/acrobat/pdf-reader.html) Linux (https://www.linux.com/) OpenOffice (FreeWare) https://www.openoffice.org/ru/ JDK 8 и выше (https://adoptopenjdk.net/) Фреймворк Java Spring 5 (https://spring.io/projects/spring-framework) Eclipse (https://www.eclipse.org/) Intellij Idea (https://www.jetbrains.com/ru-ru/idea/) git (https://git-scm.com/), github (https://github.com/) Maven (https://maven.apache.org/), Gradle (https://gradle.org/) Редактор блок-схем (https://app.diagrams.net/) ОС: Ubuntu 18.04.5 LTS, Apache OpenOffice, VScode, git, Anydesk Apache OpenOffice, ОС: Windows multiPoint Server 2011 Браузер Google Chrome, Браузер Mozilla Firefox, McAfee Security Scan

7.3 Перечень современных профессиональных баз данных и информационных справочных систем

В таблице7.4указан перечень профессиональных баз данных и информационных справочных систем, к которым обеспечен доступ (удаленный доступ). Данный перечень подлежит обновлению в соответствии с требованиями ФГОС ВО.

В данном разделе могут быть приведены ресурсы (ссылки на сайты), на которых можно найти полезную для курса информацию, в т.ч. статистические или справочные данные, учебные материалы, онлайн курсы и т.д.

Таблица 7.4– Перечень современных профессиональных баз данных и информационных справочных систем

№	Наименование профессиональной базы данных, информационно-справочной системы	Доступ к ресурсу (удаленный доступ с указанием ссылки/доступ из локальной сети университета)
1	2	3
1	База данных издательства Wiley	https://onlinelibrary.wiley.com/
2	База данных Polpred	http://www.polpred.com
3	Научная электронная библиотека ELIBRARY.RU	http://elibrary.ru
4	База данных стандартов и регламентов РОССТАНДАРТ	https://www.rst.gov.ru/portal/gost/home/standarts
5	Перечень профессиональных баз данных и информационных справочных систем	https://cyberpedia.su/21x47c0.html
6	Каталог паттернов проектирования	https://refactoring.guru/ru/design-patterns/catalog

8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице 8.1 указан перечень образовательных ресурсов, имеющих формы, адаптированные к ограничениям их здоровья, а также сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования. При заполнении таблицы может быть

использована информация, размещенная в подразделе «Доступная среда» специализированного раздела сайта НГТУ «Сведения об образовательной организации» https://www.nntu.ru/sveden/ovz/.

Таблица 8.1 - Образовательные ресурсы для инвалидов и лиц с ОВЗ

№	Перечень образовательных ресурсов, приспособленных для использования инвалидами и лицами с ОВЗ	Сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования
1	ЭБС «Консультант студента»	Версия для слабовидящих, прослушивание с помощью синтезатора речи
2	ЭБС «Лань»	Версия для слабовидящих, прослушивание с помощью синтезатора речи
3	«Юрайт» (коллекция «Легендарные книги»)	Версия для слабовидящих

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, НЕОБХОДИМОЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Учебные аудитории для проведения занятий по дисциплине, оснащены оборудованием и техническими средствами обучения

В таблице 9.1 перечислены:

- учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения;
- помещения для самостоятельной работы обучающихся, которые должны оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду НГТУ.

Таблица 9.1 - Оснащенность аудиторий и помещений для самостоятельной работы студентов по дисциплине

№	Наименование аудиторий и помещений для самостоятельной работы	Оснащенность аудиторий помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	1	2	3
1	Лаборатория программирования автоматизированных систем обработки информации и управления, мультимедийная аудитория № 4403 учебного корпуса № 4 для проведения для проведения учебных занятий и обеспечения практической подготовки обучающихся. 603155, Нижегородская область, г. Нижний Новгород, ул. Минина д.28В	1.Мультимедийный проектор Vivitek H 1180 - 1 шт. 2. Экран настенный LMP 100109 - 1 шт. 3. Сетевая купольная PTZ-камера AXIS M5014 4. Ноутбук Sony Vaio PCG-71812V - 1 шт. 5. Рабочие места, оснащенные комплектами терминалов доступа NComputing и мониторов ASUS -10шт. 6. Серверный компьютер на базе AMD Phenom II X6 – 2 шт. 7. Источник бесперебойного питания Ippon BP-PRO500 8. Рабочее место студента - 40.	1. Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23 до 28.05.24) 2. MATLAB R2008a DVD KIT-WIN & UNIX/MAC (№ лицензии 527840, № заказа 2035235 Softline от 05.05.2008). 3. Распространяемое по свободной лицензии: Apache OpenOffice, ОС: Windows multiPoint Server 2011
2	Лаборатория «Безопасности вычислительных сетей и систем» - аудитория № 4407 учебного корпуса № 4 для	1. Сервер HP ProLiant ML150G6 – 1 шт. 2. Сервер Dell Rack 410 – 2 шт. 3. Сетевое хранилище Netgear – 2 шт. 4. Openflow-коммутаторы HP ProCurve 3500 –	1.Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23 до 28.05.24) 2. Распространяемое по свободной лицензии: ОС: Ubuntu

	проведения учебных занятий и практической подготовки обучающихся. 603155, Нижегородская область, г. Нижний Новгород, ул. Минина д.28В	2 шт. 5. Коммутаторы Русьтелетех PTT-A311 – 2 шт. 6. Коммутатор Zyxel ES-3124 – 1 шт. 7. Микрокомпьютеры Cubieboard – 20 шт. 8. Мониторы – 1 шт. 9. Компьютеры AMD Phenom II X6 – 6 шт. 10. Компьютера Intel i7 – 5 шт. 11. Компьютер Intel i3 – 1 шт. 12. Моноблок Acer Core 2 – 1 шт. 13. Wi-Fi маршрутизатора TP-Link TP-ML3230 – 2 шт. 14. Мониторы – 1 шт. 15.Десктопные компьютерные станции с мониторами Dell 24" UltraSharp U2415 - 3 шт. 16.Web-камера Intel RealSense camera - 1 шт. 17. Рабочее место студента - 10	18.04.5 LTS, Apache OpenOffice, VScode, git, Anydesk
3	Помещение для самостоятельной работы обучающихся № 6545 учебно-лабораторного корпуса № 6 для проведения научно-исследовательской работы обучающихся, курсового и дипломного проектирования. 603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12	1. Рабочие места, оснащенные ПК на базеCore 2 Duo с мониторами – 5 шт. 2. Рабочее место преподавателя, оснащенное ПК на базе Intel Core i5 с монитором – 1 шт. 3. Доска интерактивная ScreenMedia-M. ПК подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета. 4. Посадочных мест - 12, шесть оснащены ПК. 5. Принтер Xerox Phaser 3300 MFP	1. Microsoft Windows 7 MSDN реквизиты договора - подписка (подписка DreamSpark Premium, договор № 0509/КМР от 15.10.18), 2. Бесплатное ПО: Пакет программ Open Office, True Conf, Браузер Google Chrome, Браузер Mozilla Firefox, Браузер Opera, McAfee Security Scan, Adobe Acrobat Reader DC

10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

10.1 Общие методические рекомендации для обучающихся по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При преподавании дисциплины «Поиск уязвимостей в автоматизированных системах», используются современные образовательные технологии, позволяющие повысить активность студентов при освоении материала курса и предоставить им возможность эффективно реализовать часы самостоятельной работы.

Весь лекционный материал курса сопровождается компьютерными презентациями, в которых наглядно преподносятся материал различных разделов курса и что дает возможность обсудить материал со студентами во время чтения лекций, активировать их деятельность при освоении материала. Электронные материалы лекций в период дистанционного обучения отправляются по электронной почте на адреса групп и могут быть получены до чтения лекций и проработаны студентами в ходе самостоятельной работы.

На лекциях, лабораторных занятиях реализуются интерактивные технологии, приветствуются вопросы и обсуждения, используется личностно-ориентированный подход, технология работы в малых группах, что позволяет студентам проявить себя, получить навыки самостоятельного изучения материала, выровнять уровень знаний в группе.

Все вопросы, возникшие при самостоятельной работе над домашним заданием подробно разбираются на лабораторных занятиях и лекциях. Проводятся индивидуальные и групповые консультации с использованием современных информационных технологий: электронная почта, мессенджеры, Zoom, Discord.

Инициируется активность студентов, поощряется задание любых вопросов по материалу, практикуется индивидуальный ответ на вопросы студента, рекомендуются методы успешного самостоятельного усвоения материала в зависимости от уровня его базовой подготовки.

Для оценки знаний, умений, навыков и уровня сформированности компетенции применяется традиционная система контроля и оценки успеваемости студентов в процессе текущего контроля.

Промежуточная аттестация проводится в форме зачета с учетом текущей успеваемости.

10.2 Методические указания для занятий лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины (Таблицы 4.4, 4.5, 4.6) . Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала. Материалы лекций являются опорной основой для подготовки обучающихся к лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

10.3Методические указания по освоению дисциплины на лабораторных работах

Подготовку к каждой лабораторной работе студент должен начать с ознакомления с планом занятия, который отражает содержание предложенной темы. Каждая выполненная работа с оформленным отчетом подлежит защите у преподавателя.

При оценивании лабораторных работ учитывается следующее:

- качество выполнения практической части работы и степень соответствия результатов работы заданным требованиям;
- качество оформления отчета по работе;
- качество устных ответов на контрольные вопросы при защите работы.

10.4 Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы, представленной в Разделе 6.

В процессе самостоятельной работы при изучении дисциплины студенты могут работать на компьютере в специализированных аудиториях для самостоятельной работы, указанных в Разделе 9. В аудиториях имеется доступ через информационно-телекоммуникационную сеть «Интернет» к электронной информационно-образовательной среде университета (ЭИОС) и электронной библиотечной системе (ЭБС), где в электронном виде располагаются учебные и учебно-методические материалы, которые могут быть использованы для самостоятельной работы при изучении дисциплины.

11. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

11.1 Типовые контрольные задания или иные +материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе текущего контроля успеваемости

Для текущего контроля знаний студентов по дисциплине проводится **комплексная оценка знаний,** включающая

- выполнение и защита лабораторных работ для студентов очной формы обучения;

11.1.1. Типовые задания для лабораторных работ

Типовые задания для лабораторных работ приведены в учебно-методических указания по проведению лабораторных работ.

11.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе промежуточной аттестации по дисциплине

11.2.1. Защита курсового проекта/ работы

Курсовая работа не предусмотрена учебным планом

11.2.2. Зачет в 9 семестре для студентов очной формы.

Типовые вопросы для промежуточной аттестации в форме зачета **для студентов очной формы обучения**

Вопросы, направленные на проверку компетенции ОПК-13:

1. Предмет защиты. Информация общедоступная и ограниченного доступа. Категории ценности информации.
2. Информация как объект права собственности. Назначение и задачи в сфере обеспечения информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной и коммерческой тайны.
3. Общие принципы обеспечения информационной безопасности (ИБ). Основные термины и определения. Угрозы безопасности информационных систем.
4. Классификация угроз безопасности: угрозы преднамеренные и случайные; каналы утечки информации прямые и косвенные; угрозы, обусловленные человеческим фактором, техническими средствами, форс-мажорными обстоятельствами.
5. Классификация методов и средств защиты информации. Службы защиты информации: обеспечение, аутентичности субъектов информационного взаимодействия, управление доступом, обеспечение секретности и конфиденциальности информации, обеспечение целостности информации.
6. Требования к защищенности информационных систем (ИС). Требования к защищенности ИС и к средствам защиты в соответствии с руководящим документом ФСТЭК «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации»
7. Общие сведения о защите ИС от Несанкционированного доступа (НСД). Принципы защиты информации от НСД Идентификация, аутентификация и авторизация.
8. Аутентификация субъекта. Парольные схемы защиты. Симметричные методы аутентификации.
9. Разграничение и контроль доступа к информации. Контроль и управление доступом средствами операционной системы.
10. Принципы работы и функциональные возможности ОС Windows 7
11. Принципы работы и функциональные возможности ПО VirtualBox
12. Принципы работы и функциональные возможности ПО Wireshark 2019

13. Принципы работы и функциональные возможности СЗИ от НСД «SecretNetStudio 8»
14. Принципы работы и функциональные возможности СЗИ от НСД «DallasLock 8.0»
15. Принципы работы и функциональные возможности МЭ «VipNetClient 4.5»
16. Принципы работы и функциональные возможности СПО «Терьер-3.0»
17. Принципы работы и функциональные возможности СПО «Фикс 2.02»
18. Принципы работы и функциональные возможности СПО «Ревизор – 1/2XP»
19. Принципы работы и функциональные возможности СПО «Ревизор сети»
20. Компьютерные Вирусы. Определения и свойства вирусов. Классификация вирусов. Классификация антивирусного ПО
21. Дискреционный метод организации разграничения доступа.
22. Мандатный метод организации разграничения доступа. Контроль целостности информации. Имитозащита информации.
23. Криптографические методы контроля целостности. Защищенные операционные системы. Средства защиты программного обеспечения от несанкционированной загрузки.
24. Защита информации на машинных носителях. Защита остатков информации.

В полном объеме оценочные средства имеются на кафедре «Информационная безопасность вычислительных систем и сетей». Оценочные средства могут быть получены по требованию.