УТВЕРЖДАЮ:
Директор института ИРИТ

_____Мякиньков А.В.
«03» июня 2024 г.

Лист актуализации рабочей программы дисциплины
«Б1.В.ОД.3 Комплексная защита информации»
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) 1) Таблицу 7.1 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 «Программно-аппаратных средств и технической защиты информации» №6039 учебно-лабораторного корпуса №6 для проведения учебных занятий **Оснащенность оборудованием и техническими средствами обучения:** 1.Учебный лабораторный стенд "Блочное кодирование" – 1 шт. 2.Учебный лабораторный стенд "Основы криптографии" – 1 шт. 3.Учебный лабораторный стенд "Биометрическая аутентификация" – 2 шт. 4.Учебный лабораторный стенд "Доверенная загрузка (Соболь)" – 1	603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12

шт. 5.Учебный лабораторный стенд "Доверенная загрузка (Аккорд)" – 1 шт. 6.Учебный лабораторный стенд "Криптоконтейнеры и ЭЦП" – 2 шт. 7. Для ивалидов и лиц с ОВЗ: переносной радиокласс, клавиатура адаптированная 8. МФУ Brother LC 9. Посадочных мест - 16. **Программное обеспечение:** Распространяемое по свободной лицензии: 1.Операционная система Ubuntu Linux 20 2. GNS3 3. Snort 4. Wareshark 5. OpenVPN 6. Libre Office 7. OpenVPN 8. IP scanner	
Мультимедийная аудитория №6421 учебно-лабораторного корпуса №6 для проведения учебных занятий **Оснащенность оборудованием и техническими средствами обучения:** 1. Доска меловая – 1 шт. 3. Экран – 1 шт. 4. Мультимедийный проектор Epson X12 – 1 шт. 5. Компьютер PC MB Asus на чипсете Nvidia/AMDAthlonXII CPU 2.8Ggz/ RAM 4 Ggb/SVGAStandartGraphics +Ge-FORCE Nvidia GT210/HDD 250Ggb,SATAinterface, монитор 19”, с выходом на проектор. 6. Рабочее место студента - 30 7. Рабочее место для преподавателя – 1 шт. **Программное обеспечение:** 1. Windows 7 32 bit корпоративная; VL 49477S2 2. Adobe Acrobat Reader DC-Russian (беспл.) 3. Microsoft Office Professional Plus 2007 (лицензия № 42470655); 4. Dr.Web (С/н ZNFC-CR5D-5U3U-JKGP от 20.05.2024, до 30.05.25)	603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12

Программа актуализирована для 2022 г. начала подготовки.

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

«_17_»_05___2024г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБВСС протокол № _9___ от «_17_» ___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__”_____04_____2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ОД.3 Комплексная защита информации
(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

2023

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 _21.04.2023_ № __4____
Зав. кафедрой к.т.н, доцент Ляхманов Д.А. _____
(подпись)

Программа рекомендована к утверждению ученым советом института ИРИТ, Протокол от 21.05.2023_№_4_

Рабочая программа зарегистрирована в УМУ, регистрационный № 10.05.03-б-48
Начальник МО _____ Н.Р. Булгакова

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

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель освоения дисциплины

Целью освоения дисциплины является освоение дисциплинарных компетенций в области построения комплексных систем защиты на предприятиях различных форм собственности.

1.2 Задачи освоения дисциплины (модуля)

Дисциплина «Комплексная защита информации» способствует подготовке студентов к решению следующих профессиональных задач:

1. изучение целей и задач комплексного обеспечения информационной безопасности автоматизированных систем;
2. освоение принципов и этапов разработки КСЗИ в соответствии с международными стандартами и отечественными государственными и отраслевыми стандартами;
3. освоение технологии установления состава защищаемой информации и объектов защиты;
4. изучение методов оценки уязвимости защищаемой информации;
5. изучение параметров и структуры КСЗИ;
6. изучение состава мероприятий по обеспечению функционирования КСЗИ;
7. изучение структуры и методов управления КСЗИ;
8. изучение показателей эффективности КСЗИ и методики ее оценки

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Комплексная защита информации» Б1.В.ОД.3 включена в перечень вариативной части дисциплин (формируемой участниками образовательных отношений), направленный на углубление уровня освоения компетенций. Дисциплина реализуется в соответствии с требованиями ФГОС, ОП ВО и УП, по направлению подготовки 10.05.03.

Дисциплина базируется на дисциплине блока защиты информации «Основы информационной безопасности».

Дисциплина «Комплексная защита информации» является основополагающей для практик: практика по получению профессиональных умений и опыта профессиональной деятельности, преддипломная практика.

.

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

Дисциплина «Комплексная защита информации» формирует компетенцию ПК-2 совместно с дисциплинами и практиками, указанными в таблице 3.1

Дисциплинарная часть компетенции ПК-2 «Способен проводить разработку и анализ объектов информационной безопасности»: способен понимать и применять на практике методы построения комплексных систем защиты на предприятиях различных форм собственности

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*
ПК-2 (Способен проводить разработку и анализ объектов информационной безопасности)											
Анализ вредоносного программного обеспечения											
Защищенное администрирование информационных систем											
Комплексная защита информации											
Интеллектуальный анализ данных											
Разработка и эксплуатация автоматизированных систем в защищенном исполнении											
Основы построения защищенных компьютерных сетей											
Шаблоны проектирования программного обеспечения											
Методы проектирования программного обеспечения											
Проектно-технологическая практика											
Практика по получению опыта контрольно-аналитической деятельности											
Эксплуатационная практика											
Практика по получению умений и опыта профессиональной деятельности											
Преддипломная практика											
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**
ПК-2. Способен проводить разработку и анализ объектов информационной безопасности	ИПК-2.2. Выполняет анализ защищенности информационных систем	***Знать:*** – цели и задачи построения КСЗИ – общие принципы проектирования КСЗИ – принципы системы управления службы безопасности предприятия – факторы, влияющие на организацию КСЗИ – международные модели и стандарты проектирования КСЗИ – виды политик информационной безопасности – основные угрозы и уязвимости	***Уметь:*** – выявлять и оценивать источники угроз – выявлять способы дестабилизирующего воздействия на информацию – применять российскую и международную практику построения проблемно-ориентированных КСЗИ – организовать службу защиты информации в соответствии с нормативными правовыми актами, нормативными и методическими документами	***Владеть:*** – методами аудита информационной безопасности предприятий различных форм собственности; – методами построение процессов системы управления КСЗИ**.**	Набор индивидуальных заданий (лабораторных работ)	Вопросы для устного собеседования

		информационных систем – модели безопасности компьютерных систем – правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации – организационные меры по защите информации	органов государственной власти – реализовывать и проводить анализ политик информационной безопасности – оценивать риски информационной безопасности в отношении компьютерных систем – оформлять аналитический отчет по результатам проведенного анализа – разрабатывать предложения по устранению выявленных уязвимостей			

Освоение дисциплины причастно к ТФ С/03.7 (ПС 06.032 «Специалист по безопасности компьютерных систем и сетей»), решает задачу анализа комплексной безопасности компьютерных систем.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 4 зач. ед. 144 часов, 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**	
	Всего час.	**В т.ч. по семестрам**
		10 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.)	68	68
Подготовка к зачёту	4	4

4.2 Содержание дисциплины, структурированное по темам

Таблица 4.1 - 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. Сущность и задачи комплексной системы защиты информации										
ПК-2 - ИПК-2.2	**Тема 1.1** Классификация предприятий Структура предприятий Информационные технологии предприятий	1				1	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Тема 1.2 Понятие, цели и задачи КСЗИ Принципы организации и этапы разработки КСЗИ Факторы, влияющие на организацию КСЗИ Планирование функционирования КСЗИ	1				1	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			

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	**2**				**2**				
Раздел 2. Общие принципы проектирования КСЗИ										
ПК-2 - ИПК-2.2	**Тема 2.1** Определение и нормативное закрепление состава защищаемой информации Определение объектов защиты	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		
	Тема 2.2 Выявление и оценка источников угроз, способов и результатов дестабилизирующего воздействия на информацию Моделирование КСЗИ	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		
	Тема 2.3 Технологическое и организационное построение КСЗИ	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]		6	

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					
	Материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ Проектная документация КСЗИ									
	Итого по 2 разделу	**6**		**8**		**6**				
Раздел 3. Международная практика проектирования КСЗИ										
ПК-2 - ИПК-2.2	**Тема 3.1** Процессный подход к управлению сетевой и информационной инфраструктурой. Способы контроля и проверки процессов и систем	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Тема 3.2. Модель Деминга и ITIL Библиотека ITIL и	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		

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					
	подход ITSM Стандарт ГОСТ Р ИСО/МЭК 17799:2005 Подход COBIT Внедрение лучших практик ISO 17799, ITIL, cobit Подход Microsoft к управлению сетевой и информационной инфраструктурой Общие критерии безопасности информационных технологий									
	Итого по 3 разделу	**4**				**4**				
Раздел 4. Построение процессов системы управления информационной безопасности										
ПК-2 - ИПК-2.2	**Тема 4.1.** Понятие СУИБ. Классификация процессов управления	2				4	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			

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					
	информационной безопасности.									
	Тема 4.2. Подсистема управления инцидентами Подсистема управления информационными ресурсами и носителями конфиденциальной информации Подсистема управления доступом к информационным ресурсам и сервисам Подсистема управления конфигурациями и изменениями Подсистема управления персоналом	6				6	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		

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					
	Подсистема администрирования Построение системы антивирусной защиты Подсистема резервного копирования и восстановления Подсистема анализа защищённости Подсистема управления обновлениями Подсистема обращения с критичными технологиями									
	Тема 4.3. Документирование процессов СУИБ	2					Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Тема лабораторной работы: Настройка средств		6			5	Подготовка к лабораторной работе [6.1.1, 6.1.2,			

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					
	предотвращения утечки конфиденциальной информации						6.1.3]			
	Тема лабораторной работы: Настройка средств защиты и средств анализа защищенности web-приложений от типовых сетевых атак		6			5	Подготовка к лабораторной работе [6.1.1, 6.1.2, 6.1.3]		6	
	Тема лабораторной работы: Анализ сетевой защищенности		6			5	Подготовка к лабораторной работе [6.1.1, 6.1.2, 6.1.3]			
	Тема лабораторной работы: Безопасность корпоративной почтовой службы		6			5	Подготовка к лабораторной работе [6.1.1, 6.1.2, 6.1.3]			
	Тема лабораторной работы:		6			5	Подготовка к лабораторной			

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					
	Настройка штатных средств защиты ОС по требованиям защиты ПДн						работе [6.1.1, 6.1.2, 6.1.3]			
	Тема лабораторной работы: Комплексная защита от НСД		4			5	Подготовка к лабораторной работе [6.1.1, 6.1.2, 6.1.3]			
	Итого по 4 разделу	**10**	**34**		**4**	**40**				
Раздел 5. Управление КСЗИ в условиях чрезвычайных ситуаций										
ПК-2 - ИПК-2.2	**Тема 5.1.** Понятие и основные виды чрезвычайных ситуаций	1				1	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		
	Тема 5.2. Планирование обеспечения бесперебойной деятельности организации в случае нештатных ситуаций	1				1	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]		5	
	Итого по 5 разделу	**2**				**2**				
Раздел 6. Российская практика построения проблемно-ориентированных КСЗИ										
ПК-2 - ИПК-2.2	**Тема 6.1.**	1				1	Подготовка к	Разбор		

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					
	Проектирование защищенных ИСПДн						лекциям [6.1.1, 6.1.2, 6.1.3]	конкретных ситуаций		
	Тема 6.2. Проектирование банковских КСЗИ	1				1	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Итого по 6 разделу	**2**				**2**				
Раздел 7. Аудит информационной безопасности										
ПК-2 - ИПК-2.2	**Тема 7.1.** Общие положения Методика информационного обследования объектов аудита Инструментальная проверка защищенности информационной системы	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Тема 7.2. Аудит ИБ государственных структур	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Итого по 7 разделу	**4**				**4**				
Раздел 8. Построение политики безопасности предприятия										

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 8.1. Реализация общей политики информационной безопасности предприятия	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Тема 8.2. Реализация частных политик информационной безопасности автоматизированной системы	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Итого по 8 разделу	**4**				**4**				
	Подготовка к зачёту					**8**				
	Итого за семестр	**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

Перечень вопросов, выносимых на промежуточную аттестацию (зачет).

1) Дайте определение понятию комплексная система защиты информации.
2) На что направлена КСЗИ? каковы ее цели и задачи?
3) Какие существуют уровни мер защиты?
4) Перечислите принципы организации КСЗИ.
5) Перечислите этапы разработки КСЗИ.
6) Перечислите уровни Политики безопасности и их состав.
7) Перечислите состав логической цепочки, лежащей в основе моделирования процессов нарушения информационной безопасности.
8) Приведите примеры объективных уязвимостей.
9) Приведите примеры субъективных уязвимостей.
10) Приведите примеры случайных уязвимостей

Для выполнения процедур оценивания составлен паспорт оценочных средств.

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

Для оценки знаний, умений, навыков и формирования компетенции по дисциплине применяется традиционная система контроля и оценки успеваемости студентов.

При промежуточном контроле успеваемость студентов оценивается по системе «зачтено», «не зачтено».

Таблица 5.4 – 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
ПК-2. Способен проводить разработку и анализ объектов информационной безопасности	ИПК-2.2. Выполняет анализ защищенности информационных систем	Изложение учебного материала бессистемное, неполное, не освоены базовые принципы комплексной защиты информации; не во всех случаях правильно оперирует основными понятиями по защите информации; не отвечает на задаваемые вопросы	Фрагментарные, поверхностные знания базовых принципов по комплексной защите информации; не во всех случаях выполняет корректное сравнение систем обеспечения безопасности данных	Знает материал на достаточно хорошем уровне; представляет основные концепции комплексной защиты информации; подтверждает теоретические знания отдельными практическими примерами по защите информации; дает ответы на задаваемые вопросы	Имеет глубокие знания всего материала по комплексной защите информации; дает развернутые ответы на задаваемые вопросы; имеет собственные суждения о решении теоретических и практических вопросов по защите информации

Таблица 5.5 - 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 Комплексные системы защиты информации на предприятиях : учебное пособие / составители Д. С. Алексеев, О. В. Щекочихин. — Кострома : КГУ им. Н.А. Некрасова, 2021. — 167 с. — ISBN 978-5-8285-1164-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/201884

6.1.2. Буранова, М. А. Комплексная система защиты информации : учебное пособие / М. А. Буранова, Н. В. Киреева. — Самара : ПГУТИ, 2019. — 145 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223181.

6.2 Справочно-библиографическая литература

— *учебники и учебные пособия*

6.1.3. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/

6.3 Методические указания, рекомендации и другие материалы к занятиям

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

6.3.1. Комплексная защита информации [Электронные текстовые данные]: метод. указания к лаб. работе по дисциплине «Комплексная защита информации» для студентов направления подготовки специалиста 10.05.03 «Информационная безопасность автоматизированных систем» дневной формы обучения / НГТУ; Сост.: Д.А. Ляхманов. Н. Новгород, 2019.

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
-	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/)

7.3 Перечень современных профессиональных баз данных и информационных справочных систем

В таблице 7.4 указан 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/accenv/

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

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:

- зал электронно-информационных ресурсов (ауд. 2210 – 11 компьютеров, ауд. 6119 – 9 компьютеров);
- читальный зал открытого доступа (ауд. 6162 – 2 компьютера);
- ауд. 2303, 2202, оборудованные Wi-Fi.

Перечень материально-технического обеспечения, необходимого для реализации программы специалитета и проведения лабораторных работ для студентов очного обучения, включает в себя компьютерные классы

Ауд. 6039 кафедры «Информационная безопасность вычислительных систем и сетей» - лаборатория «Программно-аппаратных средств и технической защиты информации»

Оснащенность специализированной мебелью и техническими средствами обучения:

- рабочий стол – 1 шт.
- парта – 8 шт.
- стул – 17 шт.

Оборудование:

- учебный лабораторный стенд "Блочное кодирование" – 1 шт.
- учебный лабораторный стенд "Основы криптографии" – 1 шт.
- учебный лабораторный стенд "Биометрическая аутентификация" – 2 шт.
- учебный лабораторный стенд "Доверенная загрузка (Соболь)" – 1 шт.
- учебный лабораторный стенд "Доверенная загрузка (Аккорд)" – 1 шт.
- учебный лабораторный стенд "Криптоконтейнеры и ЭЦП" – 2 шт.

Пакеты ПО (лицензионое)

- MaxPatrol 8

Пакеты, распространяемые по свободной лицензии

- NESSUS
- Snort Security Kit
- Kali Linux v2018
- Linux Ubuntu 2020
- Сетевой снифер Wireshark
- JetBrains IntellijIdea Community

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

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	Мультимедийная учебная аудитория № 6421 учебно-лабораторного корпуса № 6 для проведения учебных занятий. 603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12	1. Доска меловая – 1 шт. 3. Экран – 1 шт. 4. Мультимедийный проектор Epson X12 – 1 шт. 5. Компьютер PC MB Asus на чипсете Nvidia/AMDAthlonXII CPU 2.8Ggz/ RAM 4 Ggb/SVGAStandartGraphics +Ge-FORCE Nvidia GT210/HDD 250Ggb,SATAinterface, монитор 19”, с выходом на проектор. 6. Рабочее место студента - 74 7. Рабочее место для преподавателя – 1 шт.	1. Windows 7 32 bit корпоративная; VL 49477S2 2. Adobe Acrobat Reader DC-Russian (беспл.) 3. Microsoft Office Professional Plus 2007 (лицензия № 42470655); 4. Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23 до 28.05.24)
2	Лаборатория «Программно-аппаратные средства и техническая защита	1.Учебный лабораторный стенд "Блочное кодирование" – 1 шт. 2.Учебный лабораторный стенд "Основы	Распространяемое по свободной лицензии: 1.Операционная система

	информации» - учебная аудитория № 6039 учебно-лабораторного корпуса № 6 для проведения учебных занятий и практической подготовки обучающихся. 603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12	криптографии" – 1 шт. 3.Учебный лабораторный стенд "Биометрическая аутентификация" – 2 шт. 4.Учебный лабораторный стенд "Доверенная загрузка (Соболь)" – 1 шт. 5.Учебный лабораторный стенд "Доверенная загрузка (Аккорд)" – 1 шт. 6.Учебный лабораторный стенд "Криптоконтейнеры и ЭЦП" – 2 шт. 7. МФУ Brother LC 8. Посадочных мест - 16.	Ubuntu Linux 20 2. GNS3 3. Snort 4. Wareshark 5. OpenVPN 6. Libre Office 7. Splunk 8. Zeek Network Security Monitor 9. Security Onion 10. OpenVPN 11. IP scanner 12. Nemesis 13. Eyercap
3	Компьютерный класс № 1 - Помещение для самостоятельной работы обучающихся № 6543 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 студента, оснащенные ПК на базе Intel Core i5 с мониторами – 8 шт. 2. Рабочие места студента, оснащенные ПК на базеCore 2 Duo с мониторами –2 шт. 3. Рабочее место преподавателя, оснащенное ПК на базе Intel Core i5 с монитором – 1 шт. 4. Проектор Accer, проекционный экран – 1 шт. ПК подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета 5. Принтер HP LaserJet 1200 – 1 шт.	1. Microsoft Windows 7 MSDN реквизиты договора - 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, AutoCAD2013

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 «Комплексная защита информации», 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 балльно-рейтинговая 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.

10.3 Методические 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 освоению дисциплины на курсовой работе

Курсовая работа не предусмотрена учебным планом.

10.5 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**;

Варианты заданий для лабораторных работ приведены в учебно-методическом пособии 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

Зачет для студентов очной формы обучения в 9 семестре

Типовые вопросы для промежуточной аттестации в форме зачета для студентов очной формы обучения
Вопросы, направленные на проверку компетенции ПК-2:

1. Дайте определение понятию комплексная система защиты информации.
2. На что направлена КСЗИ? каковы ее цели и задачи?
3. Какие существуют уровни мер защиты?
4. Перечислите принципы организации КСЗИ.
5. Перечислите этапы разработки КСЗИ.
6. Перечислите уровни Политики безопасности и их состав.
7. Перечислите состав логической цепочки, лежащей в основе моделирования процессов нарушения информационной безопасности.
8. Приведите примеры объективных уязвимостей.
9. Приведите примеры субъективных уязвимостей.
10. Приведите примеры случайных уязвимостей.
11. Перечислите типы источников угроз.
12. Какие существуют методы реализации угроз?
13. Какие существуют потенциальные каналы и методы несанкционированного доступа к информации?
14. Какие роли (должности), как правило, должны быть созданы для кадрового обеспечения функционирования КСЗИ?
15. Что должна отражать модель нарушителя?
16. Перечислите существующие виды обеспечения КСЗИ.
17. Дайте определение понятию «процесс». Какова цель процессного подхода?
18. Какие преимущества имеет процессный подход?
19. Что представляет собой цикл Деминга и модель PDSA?
20. Какова связь между циклом Деминга и библиотекой ITIL?
21. Какие группы процессов выделяет ITIL?
22. Какие принципы лежат в основе ITSM?
23. Перечислите уровни зрелости согласно CMMI.
24. Опишите сущность стандарта ISO/IEC 17799 и применения модели PDSA к процессам СУИБ/СМЗИ.
25. Назовите основной принцип модели управления ИТ согласно CobiT.
26. Каким правилам стоит следовать при внедрении лучших практик ITIL, CobiT, ISO/IEC 17799.
27. На чем основан подход Microsoft (MSM) к управлению сетевой и информационной инфраструктурой? В чем заключается характерное отличие MSM от ITIL?

28. Что определяет стандарт ГОСТ Р ИСО/МЭК 15408?
29. На какие государственные службы возложены полномочия контроля и надзора в области обеспечения безопасности персональных данных? Каковы функции данных гос. служб в рамках указанных полномочий?
30. Что должно быть обеспечено в ИСПДн в части защиты ПДн?
31. Какие нормативно-методические документы, которые регламентируют вопрос защиты ПДн?
32. Дайте определение категорий персональных данных.
33. Назовите этапы проведения классификации ИСПДн.
34. Какие характеристики ИСПДн используются при классификации ИСПДн?
35. Решение каких задач обеспечивает базовая модель угроз безопасности ПДн?
36. На чем основано выявление частных угроз безопасности ИСПДн?
37. Какие параметры используются при определении актуальности угрозы ИСПДн?
38. Приведите пример технических решений обеспечения безопасности ПДн.
39. Назовите принципы обеспечения ИБ банковских организаций.
40. Перечислите этапы проектирования СМЗИ банковской организации.
41. Приведите примеры требований стандарта PCI DSS.
42. На кого возлагается ликвидация ЧС согласно требованиям российского законодательства о действиях в нештатных ситуациях.
43. Что необходимо иметь на случай возникновения ЧС?
44. Каковы выгоды от составления детального плана обеспечения бесперебойной деятельности предприятия?
45. Перечислите варианты технических решений восстановления деятельности после бедствия.
46. Какие функции должны быть запланированы (учтены в плане) на случай ЧС?
47. Назовите стадии планирования обеспечения бесперебойной деятельности

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