УТВЕРЖДАЮ:
Директор института ИРИТ

_____Мякиньков А.В.
3 июня 2024 г.

Лист актуализации рабочей программы дисциплины
«Б1.Б.40 Управление информационной безопасностью»
индекс по учебному плану, наименование

для подготовки бакалавров/ **специалистов**/ магистров
Направление: 10.05.03 «Информационная безопасность автоматизированных систем»
Направленность: Безопасность открытых информационных систем
Форма обучения: очная
Год начала подготовки: 2022

Курс 4
Семестр 8

В рабочую программу 2022г вносятся изменения:
1) Табл.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) П.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.

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 №	603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12

42470655); 4. Dr.Web (С/н ZNFC-CR5D-5U3U-JKGP от 20.05.2024, до 30.05.25)	

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 _____03.06. 2024г.

Методический отдел УМУ:___ _____03.06. 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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.40 Управление информационной безопасностью
(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 с оценкой

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 20.04.2023 №18.

Рабочая программа одобрена на заседании кафедры протокол от 01.04.2023г № 4.
Зав. кафедрой к.т.н, доцент Ляхманов Д.А. _____
(подпись)

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

Рабочая программа зарегистрирована в УМУ, регистрационный № 10.05.03-б-40
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 развитие компетенций в области анализа информационной безопасности в организациях.

1.2 Задачи освоения дисциплины (модуля)

Дисциплина «Управление информационной безопасностью» способствует подготовке студентов к решению следующих профессиональных задач:

1. Оценка рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем
2. Организация мер по защите информации
3. Формирование политик безопасности компьютерных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Управление информационной безопасностью» Б1.Б.40 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 относиться к дисциплинам математического блока программы специалитета и базируется на дисциплине «Математика».

Дисциплина «Управление информационной безопасностью» является основополагающей для прохождения практики: преддипломная.

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

Дисциплина «Управление информационной безопасностью» формирует компетенцию ОПК-5.1, ОПК-13, ОПК-14 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-5.1 (Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем)											
Управление информационной безопасностью											
Государственный экзамен											

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											

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-14 (Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений)											
Технологии и методы программирования											
Управление информационной безопасностью											
Разработка и эксплуатация автоматизированных систем в защищенном исполнении											
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-5.1. Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	ИОПК-5.1.1. Разрабатывает и анализирует политику информационной безопасности организации (предприятия) ИОПК-5.1.2. Разрабатывает и анализирует частные политики информационной безопасности автоматизированных систем хранения, обработки и передачи информации	***Знать:*** – Стандарты нормативные документы в области управления ИБ; – классификацию информационных ресурсов открытых информационных систем;	***Уметь:*** – идентифицировать информационные ресурсы организации; – разрабатывать мероприятия по снижению уровня информационных рисков для открытых информационных систем.	***Владеть:*** – методами организации системы управления информационной безопасности на предприятии;	Набор индивидуальных заданий (1-4) (лабораторных работ)	Набор экзаменационных билетов
ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ИОПК-13.1. Применяет методы анализа рисков информационной безопасности для поиска уязвимостей в открытых информационных системах	***Знать:*** – стандарты и нормативные документы в области управления ИБ – методы анализа информационных рисков –	***Уметь:*** -рассчитывать уровень информационных рисков – разрабатывать мероприятия по снижению уровня информационных рисков для открытых информационных систем.	***Владеть:*** – методами идентификации и снижения рисков на предприятии	Набор индивидуальных заданий (1-4) (лабораторных работ)	Набор экзаменационных билетов
ОПК-14. Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите	ИОПК-14.1. Применяет методы управления инцидентами информационной безопасности и непрерывности бизнеса	***Знать:*** – методы управления инцидентами информационной безопасности в открытых ин-	***Уметь:*** - идентифицировать инциденты информационной безопасности в открытых информационных	***Владеть:*** – методами реагирования на инциденты информационной безопасности в от-	Набор индивидуальных заданий (1-4) (лабораторных работ)	Набор экзаменационных билетов

информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	при эксплуатации открытых информационных систем.	формационных системах	системах	крытых информационных системах		

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

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

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

Вид учебной работы	Трудоёмкость в час	
	Всего час.	В т.ч. по семестрам
		8 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)	34	34
лабораторные работы (ЛР)		
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.)	50	50
Подготовка к зачёту с оценкой	22	22

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. Основы управления информационной безопасности										
ОПК-5.1.-ИОПК-5.1.1. ОПК-5.1.-ИОПК-5.1.2. ОПК-13 - ИОПК-13.1. ОПК-14 - ИОПК-14.1.	**Тема 1.1** Стандарты в области управления ИБ	2				2	Подготовка к лекциям [6.1.1]			
	Тема 1.2 Система управления ИБ в организации	2				2	Подготовка к лекциям [6.1.1]			
	Тема 1.3 Процессный подход в рамках управления ИБ	2				2	Подготовка к лекциям [6.1.1]			
	Тема 1.4Работа с процессами системы управления ИБ в организации	2				2	Подготовка к лекциям [6.1.1]			
	Тема 1.5Инвентаризация информационных ресурсов и их классификация	4		6	1	12	Подготовка к лекциям [6.1.1] работа над сквозным индивидуальным заданием	Разбор конкретных ситуаций		
	Итого по 1 разделу	**12**		**6**	**1**	**20**				
Раздел 2. Основы управления рисками информационной безопасности										
ОПК-5.1.-ИОПК-5.1.1. ОПК-5.1.-ИОПК-5.1.2. ОПК-13 - ИОПК-13.1. ОПК-14 - ИОПК-14.1.	**Тема 2.1** Основные этапы системы управления рисками	4				2	Подготовка к лекциям [6.1.1]	Разбор конкретных ситуаций		
	Тема 2.2 Идентификация угроз	4		6	1	5	Подготовка к лекциям [6.1.2, 6.1.4, 6.1.5], работа над сквозным индивидуальным заданием	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					
	Тема 2.3 Методы идентификации рисков	2		22	1	5	Подготовка к лекциям [6.1.2, 6.1.4, 6.1.5], работа над сквозным индивидуальным заданием	Разбор конкретных ситуаций		
	Тема 2.4Методы обработки рисков	2				4	Подготовка к лекциям [6.1.1]			
	Тема 2.5Мониторинг и пересмотр рисков	2				2	Подготовка к лекциям [6.1.1]			
	Тема 2.6Документальное обеспечение системы управления рисков	2				2	Подготовка к лекциям [6.1.1]			
	Итого по 2 разделу	**18**		**28**	**2**	**20**				
Раздел 3. Управление инцидентами информационной безопасности										
ОПК-5.1.-ИОПК-5.1.1. ОПК-5.1.-ИОПК-5.1.2. ОПК-13 - ИОПК-13.1. ОПК-14 - ИОПК-14.1.	**Тема 3.1**Событие и инцидент ИБ	2				**4**	Подготовка к лекциям [6.1.3]	Разбор конкретных ситуаций		
	Тема 3.2Система управления инцидентами ИБ	2			**1**	**2**	Подготовка к лекциям [6.1.3]			
	Тема 3.3Методы реагирования на инциденты ИБ	2				**4**	Подготовка к лекциям [6.1.3]			
	Итого по 3 разделу	**6**			**1**	**10**				
	Подготовка к зачету с оценкой (контроль)					**22**				
	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

Для выполнения процедур оценивания составлен паспорт оценочных средств.

Перечень вопросов, выносимых на промежуточную аттестацию (зачет с оценкой)

1. Стандарты в области управления ИБ
2. Система управления ИБ в организации
3. Процессный подход в рамках управления ИБ
4. Работа с процессами системы управления ИБ в организации
5. Инвентаризация информационных ресурсов и их классификация
6. Основные этапы системы управления рисками
7. Идентификация угроз
8. Методы идентификации рисков
9. Методы обработки рисков
10. Мониторинг и пересмотр рисков
11. Документальное обеспечение системы управления рисков
12. Событие и инцидент ИБ
13. Система управления инцидентами ИБ
14. Методы реагирования на инциденты ИБ

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 четырехбалльной системе «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Таблица 5.1–Критерии оценивания результата обучения по дисциплине и шкала оценивания

Код и наименование компетенции	**Код и наименование 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-5.1. Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	ИОПК-5.1.1. Разрабатывает и анализирует политику информационной безопасности организации (предприятия) ИОПК-5.1.2. Разрабатывает и анализирует частные политики информационной безопасности автоматизированных систем хранения, обработки и передачи информации	Изложение учебного материала бессистемное, неполное, не освоеныбазовые принципы методов анализа рисков; не во всех случаях правильно оперирует основными понятиями организационных методов защиты информации; не отвечает на задаваемые вопросы	Фрагментарные, поверхностные знания базовых принципы методов анализа рисков; не во всех случаях находит правильные ответы на задаваемые вопросы по управлению инцидентами ИБ	Знает на достаточно хорошем уровне методы анализа рисков и управления инцидентами ИБ; представляет основные концепции организации системы управления информационной безопасности на предприятии; подтверждает теоретические знания отдельными практическими примерами по анализу рисков ИБ; дает ответы на задаваемые вопросы	Имеет глубокие знания методов анализа рисков и управления инцидентами ИБ; дает развернутые ответы на задаваемые вопросы; имеет собственные суждения о решении теоретических и практических вопросов, связанных с организацией системы управления информационной безопасности на предприятии
ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ИОПК-13.1. Применяет методы анализа рисков информационной безопасности для поиска уязвимостей в открытых информационных системах	Изложение учебного материала бессистемное, неполное, не освоеныбазовые принципы методов анализа рисков; не во всех случаях правильно оперирует основными понятиями организационных методов защиты информации; не отвечает на задаваемые вопросы	Фрагментарные, поверхностные знания базовых принципы методов анализа рисков; не во всех случаях находит правильные ответы на задаваемые вопросы по управлению инцидентами ИБ	Знает на достаточно хорошем уровне методы анализа рисков и управления инцидентами ИБ; представляет основные концепции организации системы управления информационной безопасности на предприятии; подтверждает теоретические знания отдельными практическими примерами по анализу рисков ИБ;	Имеет глубокие знания методов анализа рисков и управления инцидентами ИБ; дает развернутые ответы на задаваемые вопросы; имеет собственные суждения о решении теоретических и практических вопросов, связанных с организацией системы управления информационной безопасности на пред-

				дает ответы на задаваемые вопросы	приятии
ОПК-14. Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	ИОПК-14.1. Применяет методы управления инцидентами информационной безопасности и непрерывности бизнеса при эксплуатации открытых информационных систем.	Изложение учебного материала бессистемное, неполное, не освоеныбазовые принципы методов анализа рисков; не во всех случаях правильно оперирует основными понятиями организационных методов защиты информации; не отвечает на задаваемые вопросы	Фрагментарные, поверхностные знания базовых принципы методов анализа рисков; не во всех случаях находит правильные ответы на задаваемые вопросы по управлению инцидентами ИБ	Знает на достаточно хорошем уровне методы анализа рисков и управления инцидентами ИБ; представляет основные концепции организации системы управления информационной безопасности на предприятии; подтверждает теоретические знания отдельными практическими примерами по анализу рисков ИБ; дает ответы на задаваемые вопросы	Имеет глубокие знания методов анализа рисков и управления инцидентами ИБ; дает развернутые ответы на задаваемые вопросы; имеет собственные суждения о решении теоретических и практических вопросов, связанных с организацией системы управления информационной безопасности на предприятии

Таблица 5.2 - Критерии оценивания

Оценка	Критерии оценивания
Высокиий 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 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.

6.1.2 Петренко, С. А. Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. — Москва : ДМК Пресс, 2009. — 394 с. — ISBN 5-94074-246-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/40021.

6.1.3 Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. — Ставрополь : СКФУ, 2017. — 86 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155146.

6.2 Справочно-библиографическая литература

— *учебники и учебные пособия*

6.1.4Риск-контроллинг информационной и экономической безопасности : монография / Г. И. Золотарева, С. В. Филько, И. В. Филько, И. В. Федоренко. — Красноярск : СибГУ им. академика М. Ф. Решетнёва, 2018. — 192 с. — ISBN 978-5-86433-759-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/147582.

6.1.5Коробулина, О. Ю. Риск-модели информационной безопасности : учебное пособие / О. Ю. Коробулина. — Санкт-Петербург : ПГУПС, 2014. — 26 с. — ISBN 978-5-7641-0605-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/64390.

6.3Методические указания, рекомендации и другие материалы к занятиям

Методические указания по выполнению практических работ по дисциплине Управление информационной безопасностью 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 Управление информационной безопасностью [Электронные текстовые данные]: метод. указания к практическим работам по дисциплине «Управление информационной безопасностью» для студентов направления подготовки 10.05.03 «Информационная безопасность автоматизированных систем» дневной формы обучения / НГТУ; Сост.: С.Н. Капранов. Н.Новгород, 2021.

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	Лань	https://e.lanbook.com/
2	Юрайт	https://biblio-online.ru/

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/)
	Microsoft Visual Studio 2017 Community Edition (https://visualstudio.microsoft.com/ru/vs/community/)

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 стандартов и регламентов РОССТАНДАРТ	https://www.rst.gov.ru/portal/gost/home/standarts
2	Перечень профессиональных баз данных и инфор-	https://cyberpedia.su/21x47c0.html

	мационных справочных систем	
3	Каталог паттернов проектирования	https://refactoring.guru/ru/design-patterns/catalog

8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице8.1 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»	озвучка книг и увеличение шрифта
2	ЭБС «Лань»	специальное мобильное приложение - синтезатор речи, который воспроизводит тексты книг и меню навигации
3	ЭБС «Юрайт»	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

1. ***Ауд. 4403 кафедры «Информатика и системы управления» - лаборатория Программирования АСО и У***

Компьютеры, оснащенные необходимым оборудованием, техническими и электронными средствами обучения и контроля знаний студентов:

- 10 АРМ (терминалов);
- мультимедийный проектор Vivitek H 1180,
- экран настенный LMP 100109,
- сетевая купольная PTZ-камера AXIS M5014.

Пакеты ПО (лицензионное):

- Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23
- MATLAB R2008a DVD KIT-WIN & UNIX/MAC (№ лицензии 527840, № заказа 2035235 Softline от 05.05.2008).

Пакеты ПО (распространяемое по свободной лицензии):

- Apache OpenOffice;
- Eclipse (https://www.eclipse.org/)
- git (https://git-scm.com/)

– Microsoft Visual Studio 2017 Community Edition (https://visualstudio.microsoft.com/ru/vs/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	Оснащенностьаудиторий помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	1	2	3
1	**6421** учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации; г. Нижний Новгород, Казанское ш., 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 +GeFORCE 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)
	6543 компьютерный класс - помещение для СРС, курсового проектирования (выполнения курсовых работ), г. Нижний Новгород, Казанское ш., 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 «Управление информационной безопасностью», 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-рейтинговаясистема контроля и оценки успеваемости студентов в процессе текущего контроля.

Промежуточная аттестация проводится в форме зачета с оценкой 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 занятиях семинарского типа – или практические

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

Практические (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- получение умений и навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;
- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Приводятся конкретные методические указания для обучающихся по выполнению реферата или эссе, требования к их оформлению, порядок сдачи

Примерная тематика рефератов

1. Анализ видов и последствий отказов (EMEA)
2. Структурированные и полуструктурированные интервью
3. Метод Дельфи
4. Контрольные списки
5. Первичный анализ опасностей (PHA)
6. Исследование опасностей и работоспособности (HAZOP)
7. Анализ опасностей и критических контрольных точек (HACCP)
8. Оценка риска со стороны внешней среды
9. Анализ видов и последствий отказов (FMEA)
10. Дерево отказов (неисправностей FTA)
11. «Мозговой штурм»
12. Анализ причин и последствий
13. Причинно-следственный анализ
14. Анализ защитного слоя (анализ уровней защиты LOPA)
15. Сопровождение (техническое обслуживание), нацеленное на надежность
16. Марковские цепи
17. Метод Монте-Карло
18. Сети и статистика Байеса
19. Анализ галстук-бабочка
20. Индексы рисков
21. Матрица последствий/ вероятностей

10.4Методические указания по освоению дисциплины на курсовой работе

Курсовая работа не предусмотрена учебным планом.

10.5Методические 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 вРазделе 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 рефератов

Примерная тематика рефератов

1. Анализ видов и последствий отказов (EMEA)
2. Структурированные и полуструктурированные интервью
3. Метод Дельфи
4. Контрольные списки
5. Первичный анализ опасностей (PHA)
6. Исследование опасностей и работоспособности (HAZOP)
7. Анализ опасностей и критических контрольных точек (HACCP)
8. Оценка риска со стороны внешней среды
9. Анализ видов и последствий отказов (FMEA)
10. Дерево отказов (неисправностей FTA)
11. «Мозговой штурм»
12. Анализ причин и последствий
13. Причинно-следственный анализ
14. Анализ защитного слоя (анализ уровней защиты LOPA)
15. Сопровождение (техническое обслуживание), нацеленное на надежность
16. Марковские цепи
17. Метод Монте-Карло
18. Сети и статистика Байеса
19. Анализ галстук-бабочка
20. Индексы рисков
21. Матрица последствий/ вероятностей

Варианты заданий для рефератов приведены в учебно-методическом пособии по проведению практических 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 с оценкой для студентов очной формы обучения в 8 семестре.

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

Вопросы, направленные на проверку компетенции ОПК-5-1, ОПК-14:

1. Стандарты в области управления ИБ
2. Система управления ИБ в организации
3. Процессный подход в рамках управления ИБ
4. Работа с процессами системы управления ИБ в организации

5. Инвентаризация информационных ресурсов и их классификация
6. Основные этапы системы управления рисками
7. Идентификация угроз
8. Методы идентификации рисков
9. Методы обработки рисков
10. Мониторинг и пересмотр рисков
11. Документальное обеспечение системы управления рисков
12. Событие и инцидент ИБ
13. Система управления инцидентами ИБ
14. Методы реагирования на инциденты ИБ

Вопросы, направленные на проверку компетенции ОПК-5-1, ОПК-13:

1. Основные этапы системы управления рисками
2. Идентификация угроз
3. Методы идентификации рисков
4. Методы обработки рисков
5. Мониторинг и пересмотр рисков
6. Документальное обеспечение системы управления рисков

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

УТВЕРЖДАЮ:
Директор института ИРИТ

___Мякиньков А.В.__
“____”_____2022 г.

Лист актуализации рабочей программы дисциплины
«Б1.Б.40 Управление информационной безопасностью»
индекс по учебному плану, наименование

для подготовки **специалистов**
Направление: {шифр – название} 10.05.03. Информационная безопасность автоматизированных систем
Направленность: Безопасность открытых информационных систем
Форма обучения очная
Год начала подготовки: 2022

Курс 4
Семестр 8
В рабочую программу не вносятся изменения. Программа актуализирована для 2022 г. начала подготовки.

Разработчик (и): __Капранов С.Н., к.т.н., доцент_____
(ФИО, ученая степень, ученое звание)
«__»_____20__г.
Рабочая программа пересмотрена и одобрена на заседании кафедры ИБВСС
_____ протокол № _____ от «__» _____20__ г.

Заведующий кафедрой _____

Лист актуализации принят на хранение:

Заведующий выпускающей кафедрой ИБВСС _____ «__» _____ 20__ г.

Методический отдел УМУ:_____ «__» _____ 20__ г.

_____