ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:

Руководитель направления

Электронный документ, подписанный ПЭП, хранится в системе электронного документооброта Южно-Уральского государственного университета СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП Кому выдан: Соколов А. Н. Пользователь: sokolovan Пата подписания: 40 но. 2023

А. Н. Соколов

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.35 Основы управления информационной безопасностью для направления 10.03.01 Информационная безопасность уровень Бакалавриат форма обучения очная кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утверждённым приказом Минобрнауки от 17.11.2020 № 1427

Зав.кафедрой разработчика, к.техн.н., доц.

Разработчик программы, к.техн.н., доц., заведующий кафедрой

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота ЮжрГУУ (Южн.) Уральского государственного университета СВДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП Кому выдан: Соколов А. Н. Пользователь: sokolovan Дата подписание: 04 06 2023

А. Н. Соколов

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборога Южно-Уральского государственного университета СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП Кому выдан: Соколов А. Н. Нользователь sokolovan Дата подписания о 40 6 2023

А. Н. Соколов

1. Цели и задачи дисциплины

Дисциплина имеет целью изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии. Задачами дисциплины являются: - приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность; - формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности.

Краткое содержание дисциплины

Изучение дисциплины "Основы управления информационной безопасностью" является одной из завершающих стадий прикладной подготовки бакалавров в области обеспечения информационной безопасности. Ее освоение должно обеспечить интеграцию полученных ранее знаний в области методов и средств защиты информации с материалами по правовым и организационно-управленческим аспектам информационной безопасности, способность обучаемых применить приобретенные умения и навыки в профессиональной деятельности.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения	Планируемые результаты
ОП ВО (компетенции)	обучения по дисциплине
	Знает: основные документы по стандартизации в сфере управления ИБ; принципы формирования
	политики информационной безопасности в
ОПК-5 Способен применять нормативные	автоматизированных системах; требования
правовые акты, нормативные и методические	информационной безопасности при
	эксплуатации автоматизированной системы
защите информации в сфере профессиональной	Умеет: формировать политики информационной
деятельности	безопасности организации, выполнять полный
	объем работ, связанных с реализацией частных
	политик информационной безопасности
	автоматизированной системы
	Знает: основные угрозы безопасности
	информации и модели нарушителя объекта
	информатизации; цели и задачи управления
ОПК-10 Способен в качестве технического	информационной безопасностью, основные
специалиста принимать участие в формировании	•
политики информационной безопасности,	управления информационной безопасностью;
организовывать и поддерживать выполнение	принципы формирования политики
комплекса мер по обеспечению информационной	±. ±
безопасности, управлять процессом их	информатизации;
реализации на объекте защиты	Умеет: разрабатывать модели угроз и модели
	нарушителя объекта информатизации; оценивать
	информационные риски объекта
	информатизации

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин,	Перечень последующих дисциплин,
видов работ учебного плана	видов работ
1.О.33 Программно-аппаратные средства защиты	
информации,	
ФД.02 Мониторинг информационной	U а пратиомотрония
безопасности и активный поиск киберугроз,	Не предусмотрены
1.О.30 Организационное и правовое обеспечение	
информационной безопасности	

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
ФД.02 Мониторинг информационной безопасности и активный поиск киберугроз	Знает: организационную структуру и функциональную часть автоматизированных систем; методы и средства реализации удаленных сетевых атак на автоматизированные системы, методы мониторинга информационной безопасности и средства реализации удаленных сетевых атак на автоматизированные системы Умеет: осуществлять управление и администрирование защищенных автоматизированных систем; разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем, осуществлять диагностику и мониторинг систем защиты автоматизированных систем Имеет практический опыт: разработки политик информационной безопасности автоматизированных систем
1.О.33 Программно-аппаратные средства защиты информации	Знает: программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях Умеет: конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности Имеет практический опыт: проектирования системы защиты объекта информатизации от утечек информации за счет несанкционированного доступа
1.О.30 Организационное и правовое обеспечение информационной безопасности	Знает: содержание основных нормативных правовых актов в сфере противодействия коррупции, систему стандартов и нормативных правовых актов уполномоченных федеральных органов исполнительной власти по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации; систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по аттестации объектов информатизации и

сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях, основы правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; основные понятия и характеристику основных отраслей права. применяемых в профессиональной деятельности организации;основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; статус и порядок работы основных правовых информационно-справочных систем;основы организации и деятельности органов государственной власти в Российской Федерации Умеет: соблюдать требования антикоррупционного законодательства, воздерживаться от поведения, вызывающего сомнение в объективном и беспристрастном исполнении должностных (служебных) обязанностей, использовать систему организационных мер, направленных на защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ России, ФСТЭК России, применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав;анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационнораспорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; формулировать основные

требования информационной безопасности при эксплуатации автоматизированной системы; формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации Имеет практический опыт: применения
Имеет практический опыт: применения
основных нормативных правовых актов в сфере
противодействия коррупции, работы с нормативными правовыми актами

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч., 82,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах Номер семестра	
Общая трудоёмкость дисциплины	144	8 144	
Аудиторные занятия:	72	72	
Лекции (Л)	36	36	
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	36	36	
Лабораторные работы (ЛР)	0	0	
Самостоятельная работа (СРС)	61,5	61,5	
МОДЕЛИРОВАНИЕ ПОДСИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ, СВЯЗАННОЙ С ПЕРСОНАЛОМ ОРГАНИЗАЦИИ	41,5	41.5	
Экспертная оценка проблем УИБ	20	20	
Консультации и промежуточная аттестация	10,5	10,5	
Вид контроля (зачет, диф.зачет, экзамен)	-	экзамен	

5. Содержание дисциплины

№	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
раздела		Всего	Л	П3	ЛР
1 1	Базовые понятия и подходы к управлению информационной безопасностью	6	2	4	0
2	Международные и российские стандарты по УИБ	8	6	2	0
3	Политика ИБ организации	12	6	6	0
4	Система управления информационной безопасностью организации (СУИБ)	12	6	6	0
5	Ресурсное обеспечение СУИБ	12	6	6	0
6	Контроль и проверка процессов УИБ	12	6	6	0
7	Документационное обеспечение СУИБ	10	4	6	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Базовые понятия и подходы к управлению информационной безопасностью	2
2	2	Стандарты ИСО серии 27000	4
3	2	Отраслевые стандарты по ИБ	2
4	3	Политика ИБ организации	4
5	3	Организационные основы политики ИБ	2
6	4	Управление рисками ИБ	4
7	4	Управление инцидентами ИБ	2
8	5	Техническое обеспечение УИБ	2
9	5	Организационное и кадровое обеспечение СУИБ	4
10	6	Контроль и проверка процессов УИБ	4
11	6	Инструментальные средства проверки СУИБ	2
12	7	Документационное обеспечение СУИБ	4

5.2. Практические занятия, семинары

№ занятия	№ Наименование или краткое содержание практического занятия, семинара		Кол- во часов
1	1	Базовые понятия и подходы к управлению информационной безопасностью	4
2	2	Международные и российские стандарты ИСО по УИБ, отраслевые стандарты	2
4	3	Политика ИБ	4
5	3	Политика ИБ в организациях разных типов и видов	2
6	4	Система управления информационной безопасностью организации (СУИБ): структура и требования	4
7	4	Подсистемы СУИБ	2
8	5	Организационное и кадровое обеспечение СУИБ	4
9	5	Техническое обеспечение СУИБ	2
10	6	Контроль процессов УИБ	2
11	6	Проверка процессов УИБ	4
12	7	Документационное обеспечение СУИБ: определение состава	2
13	7	Документационное обеспечение СУИБ: разработка	4

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС						
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол- во часов			
МОДЕЛИРОВАНИЕ ПОДСИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ, СВЯЗАННОЙ С	ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной	8	41,5			

безопасности, ГОСТ Р от 15 ноября 2012 года № МСО/МХ 27003-29012 — URL: http://docs.enid.ru (дата обращения: 10.01. 2022). СТО БУ ИББС-1.0-2014. Обеспечение информационной безопасности ортапизаций банковской системы Российской Федерации. Общее подожения — № 2014. Малюк. А. А. Защита информации в информационном обществе: учебное пособие / А. А. Малюк. — Москва: Торячая лиция: Гслеком, 2017. — 230 с. — ISBN 978-5-9912-0481-1. — Текст: знектронный // Лань: знектронно-библиотчиная система. — URL: https://el.lanbook.com/book/11078 (дата обращения: 27.01.2022). — Режим доступа: для авториз. пользователей. (Лт.13). Астакова, // В. Сотрудиим организации как субъект управления её информационной безопасностью // Л. В. Астакова // Научнотехническая информации. Серия 1: Организация и методика информационной работы. — 2020. — № 5. С. 11-17. — DOI 10.36535/0548-0019-2020-05-2. Астакова, Л. В. Валидность методик оценки угроз информационной безопасность теоторик оценки угроз информационной организации // Л. В. Астакова // Научно-техническая информационной работы. — 2020. — № 5. С. 11-17. — DOI 10.3653/0548-0019-2020-05-2. Астакова, Л. В. Валидность методик оценки угроз информационной работы. — 2020. — № 1. — С. 18. — DOI 10.3653/0548-0019-2020-05-2. Астакова, Л. В. Траниформации // Л. В. Астакова // Научно-техническая информационной работы. — 2020. — № 1. — С. 18. — DOI 10.3653/0548-0019-2020-10-11. Астакова, Л. В. Траниформация стратетических моделей управления человиським угрозами информационной безопасности предприятия как императив шифровой индустурии // Л. В. Астакова // Научно-техническая информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.3653/0548-0019-2021-04-1. Астакова, Л. В. Целевая комплексность программы повышения осведомленности огрудников об информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.3653/0548-0019-2021-04-1. Астакова, Л. В. Целевая комплексность программы повышения осведомленности по ИБ (Security Awareness)// Зикстронный ресурс] URL: https://www.antimalware.ru/analytics/Market_Analysis/				
родер.) СТО БР ИББС-1.0-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обице положения. — М., 2014. Малюк, А. А. Запита информацион информационном обществе: учебное пособие / А. А. Малюк. — Москва: Торячая линия-Телеком, 2017. — 230 с. — ISBN 978-5-9912-0481-1. — Текст: электронный // Лань: электроннобиблиотечная система. — URL: https://e.lanbook.com/book/111078 (дата обращения: 27.01.2022). — Режим доступа: для автория: пользователей. (Гл. 13). Астахова, Л. В. Сотрудник организации как субъект управления се информационной безопасностью / Л. В. Астахова // Научнотехническая информациия. Серия 1: Организация и методика информационной работы. — 2020. — № 5. — С. 11-17. — DOI 10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидность методик оценки утроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информационной безопасности организации / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 6. — С. 1-1. — DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления стратегических моделей управления стратегическим игродика информационной безопасности предприятия как императив дифровой индустрии / Л. В. Астахова // Научно-техническая информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2020-11-1. Астахова, С. А. Бесенастнов // Информация информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения о сведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесенастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36525/VSTU 2021.24. 2006. Обзор рышка сервисов повышения осведомленности по ИБ (Security/Awareness) (Электронный ресуре). — VBL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness		года №ИСО/MЭК 27003-2012. – ŪRL:		
информационной безопасности организаций банковской системы Российской Федерации. Общие положения. — М., 2014. Малюк, А. А. Запцита информации в информационном обществе: учесбное пособие / А. А. Малюк. — Москва: Горячая липия-Телеком, 2017. — 230 с. — ISBN 978-5-9912-0481-1. — Текет: электроппий / Лапы: электроппобиблиотечная система. — URL: https://el.anbook.com/book/11078 (дата обращения: 27.01.2022). — Режим доступа: для авториз. пользователей. (Тл. 13). Астахова / Л. В. Сотрудник организации как субъект управления её информационной безопасностью / Л. В. Астахова // Научнотехническая информация. Серия 1: Организации и методика информационной работы. — 2020. — № 5. — С. 11-17. — DOI 10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидность методик оценки утроз информационной безопасностию горганизации / Л. В. Астахова // Научно-техническая информационной безопасности организации / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной безопасности организации / Л. В. Астахова // Научно-техническая информация и методика информация серия 1: Организация и методика информация и методика информация (Серия 1: Организация и методика информация организация и методика информация организация и методика информационной безопасности предприятия как императив информация объемова повышения осведомленности сотрудников об информация и методика информация и серия (Серия 1: Организация и методика информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность портраммы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастной // Информация и безопасность — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.242.206. Обзор рынка сервисов повышения осведомленности от по ИБ (Security) Амагелева // Делева информационной системы управления н				
банковской системы Российской Федерации. Обписи положения. — М., 2014. Малюк, А. А. Защита информации в информационном обществе: учебное пособие / А. А. Малюк. — Москва: Торячая линия-Телеком, 2017. — 230 с. — ISBN 978-5-9912-0481-1. — Текет: электронный // Лаги.: электроннобиблиотечная система. — URL: https://e.lanbook.com/book/111078 (дата обращения: 27.01.2022). — Режим доступа: для авториз. пользователей. (Тл.13). Астакова, Л. В. Сотрудник ортанизации как субъект управления её информационной безопасностью / Л. В. Астакова // Научно-техническая информация. Серия 1: Ортанизация и метолика информационной работы. — 2020. — № 5. — С. 11-17. — DOI 10.36535/0548-0019-2020-05-2. Астакова, Л. В. Валидность методик опенки угроз информационной безопасности ортанизации / Л. В. Астакова // Научно-техническая информационной безопасности ортанизации / Л. В. Астакова // Научно-техническая информационной безопасности ортанизации / Л. В. Астакова // Научно-техническая информационной безопасности ортанизации / Л. В. Астакова // Научно-техническая информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019-2020-11-1. Астакова, Л. В. Транеформация стратегических мудерами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астакова // Научно-техническая информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астакова, Л. В. Целсвая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астакова, С. А. Бесчастнов // Информация по безопасность. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астакова, С. А. Бесчастнов // Информационной работы. — 2021. — № 4. — С. 2. 7. — 2. 2. 2. — 2. 2. 2. — 2. 2. 2. 0. 6. Обаро рынка сервисов повышения осведомленности по ИБ (Security Mayencess) Электронный ресурс] URL: https://www.anti-malware.ru/analytics/Market_Analysis/Security-Awareness				
Обпице положения. — М., 2014. Малюк, А. А. Защита информации в информационном обществе: учебное пособие / А. А. Малюк, — Москва: Горячая липия-Телеком, 2017. — 230 с. — ISBN 978-5-9912-0481-1. — Текет: электронный // Лагь: электронно-библиотечная система. — URL: https://e.lanbook.com/book/111078 (дата обращения: 27.01.2022). — Режим доступа: ушя затория, пользователей. (Гл. 13). Астахова // Л. В. Астахова // Научнотехническая информации к Серия I: Организация и к субъект управления её информационной безопасностью // Л. В. Астахова // Научнотехническая информации Серия I: Организация и методика информационной работы. — 2020. — № 5. — С. 11-17. — DOI 10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидиость методик оценки угроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информации. Серия I: Организация и методика информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Транеформация стратегических моделей управления неловеческим итрогами информационной безопасности предприятия как императив информационной индустрии // Л. В. Астахова // Научно-техническая информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2020-11-1. Астахова // Научно-техническая информационной оработы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова // Научно-техническая информационной оработы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, С. А. Бесчастнов // Информация и безопасность порагнизации // Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность организации // Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность организации // Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность организации // Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность организации // Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность организации // Л. В. Астахова, С. А. Бесчастнов // Информация информация и безопасность организации // Л. В. Астахова, С. А. Бесчастнов //		1 1		
Запшта информации в информационном обществе : учебное пособие / А. А. Малюк. — Москва : Горячая липия—Телеком, 2017. — 230 с. — ISBN 978-5-9912-0481-1. — Текет : электрошый // Лаш. : электрошьобиблиотечная система. — URL: https://e.lanbook.com/book/111078 (дата обращения: 27 01 2022). — Режим доступа: для авториз. пользователей. (Гл.13). Астахова, Л. В. Сотрудник организации как субъект управления се информационной безопасностью / Л. В. Астахова // Научнотехническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 5. — С. 11-17. — DOI 10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидность методик оценки угроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информационной безопасности организации / Л. В. Астахова // Ваучно-техническая информационной даботы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Трансформация стратсгических моделей управления человеческими угрозами информационной безопасности предприятия как императив информация индустрами / Л. В. Астахова // Научно-техническая информационной безопасности предприятия как императив информация информационной безопасности порадриятия как императив информации / Л. В. Астахова // Научно-техническая информационной обезопасности порадриятия как императив пиформации информационной безопасности организации / Л. В. Астахова, С. А. Вечастнов // Информация и безопасность — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Д. В. Целевая комплексность портраммы повышения осведомленности сотрудников об информации/ Л. В. Астахова, С. А. Вечастнов // Информация и безопасность — 2021. — Т. 24. — 0. 2. — С. 231-238. — DOI 10.36622/VSTU.2021. 24. 20.06. Обзор рынка сервисов повышения осведомленности системы управления информационной безопасности по ИК (Security Awareness)]электронный ресурс]. — URL: thtys://www.anti-malwarc.ru/analytics/Market_Analysis/Security - Awareness		±		
обществе: учебное пособис? А. А. Малюк. — Москва: Горячая линия-Телеком, 2017. — 230 с. — ISBN 978-5-9912-0481-1. — Текет: электроппый // Лапа: электроппо- библиотечная система. — URL: https://c.lanbook.com/book/III078 (дата обращения: 27.01.2022). — Режим доступа: для авториз. пользователей. (Гл.13). Астахова, Л. В. Сотрудник организации как субъскт управлетия се информационной безопасностью /Л. В. Астахова // Научно- техническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 5. — С. 11-17. — DOI 10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидность методик оценки угроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019- 2020-11-1. Астахова, Л. В. Трансформация стратетических моделей управления человеческим угрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной безопасности предприятия как императив пифровой индустрии / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплекеность программы повышения осведомленности сотрудников об информационной безопасности организации // Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность организации // Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность организации // Л. В. Астахова, С. А. Бесчастнов // Информация и безопасности организации // Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность организации // Л. В. Остакова, С. А. Бесчастнов // Информация но безопасности организации // Л. В. Остакова, С. А. Бесчастнов // Информационной Безопасности по ИК (Security Awareness)				
— Москва : Горячая лиция-Телском, 2017. — 230 с. — ISBN 978-5-9912-0481-1. — Текст : электронный // Лань : электронно- библиотечная система. — URL: https://с.lanbook.com/book/111078 (дата обращения: 77.01.2022). — Режим доступа: для автория. пользователей. (Гл.13). Астахова, Л. В. Сотрудник организации как субъект управления сё информационной безопасностью / Л. В. Астахова // Научно- техническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 5. — С. 11-17. — DOI 10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидность методик оценки угроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019- 2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив инфоровой индустрии / Л. В. Астахова // Научно-техническая информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целсвая комплексность программы повышения оведомленность программы повышения оведомленность согрудников об информационной безопасность организации / Л. В. Астахова, Л. В. Целсвая комплексность программы повышения оведомленность портраммы повышения оведомленность портраммы повышения оведомленность портраммы повышения оведомленность портраммы повышения оведомленность по МБ (Security Awareness) [Электронный ресурс] URL: https://www.anti- malware.ru/analytics/Market_Analysis/Security -Awareness Абделов, А. Ж. Современные системы управления информационной безопасность организация информационной безопасность образованносты по ИБ (Security Awareness) [Электронный ресурс] URL: https://www.anti- malware.ru/analytics/Market_Analysis/Security -Awareness		* * *		
— 230 с. — ISBN 978-5-9912-0481-1. — Текет : электроппый // Лапь : электроппо- библиотечная система. — URL: https://e.lanbook.com/book/111078 (дата обращения: 27.01.2022). — Режим доступа: для авториз. пользователей. (Тл.13). Астахова, Л. В. Сотрудник организации как субъект управления её информационной безопасностью / Л. В. Астахова // Научно- техническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 5. — С. 11-17. — DOI 10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидность методик оценки угроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019- 2020-11-1. Астахова // В. Трапсформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив пифровой индустрии / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасность организации / Л. В. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасность — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (Security-Awareness) Электронный ресурс] URL: https://www.anti- malware.ru/analytics/Market_Analysis/Security -Awareness Абленов, А. Ж. Современные системы управления информационной безопасность — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (Security-Awareness) Электронный ресурс] URL: https://www.anti- malware.ru/analytics/Market_Analysis/Security -Awareness				
библиотечная система. — URL: https://e.lanbook.com/book/111078 (дата обращелия: 27.01.2022). — Режим доступа: для авториз. пользователей. (Гл.13). Астахова, Л. В. Сотрудник организации как субъект управления её информационной безопасностью / Л. В. Астахова // Научнотехническая информация. Серия 1: Организация и мстодика информационной работы. — 2020. — № 5. — С. 11-17. — DOI 10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидность методик оценки угроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информационной безопасности организации / Л. В. Астахова // Научно-техническая информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив пифровой индустрии / Л. В. Астахова // Научно-техническая информации (Серия 1: Организация и мстодика информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информационной сезопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информационной пресурс] URL: https://www.antimalvare.ru/analytics/Market_Analysis/Security -Awarencess Абденов, А. Ж. Современные системы управления информационной		<u> </u>		
https://e.lanbook.com/book/111078 (дата обращения: 27.01.2022). — Режим доступа: для авториз. пользователей. (Гл. 13). Астахова, Л. В. Сотрудник организации как субъект управления её информациолной безопасностью / Л. В. Астахова // Научпотехническая информация. Серия 1: Организация и методика информациолной работы. — 2020. — № 5. — С. 11-17. — DOI 10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидность методик оценки утроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информационной безопасности организация и методика информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческими утрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информационной оработы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информацион об об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.242.006. Обзор рынка сервисов повышения осведомленности по ИБ (SecurityAwareness)]-Олектронный ресурс] URL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness		Текст : электронный // Лань : электронно-		
обращения: 27.01.2022). — Режим доступа: для автория. пользователей. (Гл.13). Астахова, Л. В. Сотрудник организации как субъект управления её информационной безопасностью / Л. В. Астахова // Научнотехническая информация. Серия 1: Организация и методика информациолной работы. — 2020. — № 5. — С. 11-17. — DOI 10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидность методик оценки угроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информации Серия 1: Организация и методика информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019-2020-11-1. Астахова // Врагения человеческим угрозами информация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информациа. Серия 1: Организация и методика информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.206. Обзор рынка есрвисов повышения осведомленности по ИБ (Security Awareness) Электронный ресурс]. — URL: https://www.antimalware.ru/analytics/Market_Analysis/Security - Awareness		библиотечная система. — URL:		
для авториз. пользователей. (Гл.13). Астахова, Л. В. Сотрудник организации как субъект управления её информационной безопасностью / Л. В. Астахова // Научнотехническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 5. — С. 11-17. — DOI 10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидность методик оценки угроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информационной позопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (Security-Awareness) [Электронный ресурс]. — URL: https://www.antimalware.ru/analytics//Market_Analysis/Security-Awareness		https://e.lanbook.com/book/111078 (дата		
Астахова, Л. В. Сотрудник организации как субъект управления её информационной безопасностью / Л. В. Астахова // Научнотехническая информация. Серия 1: Организация и методика информационной работы. − 2020. − № 5. − С. 11-17. − DOI 10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидность методик оценки угроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информационной работы. − 2020. − № 11. − С. 1-8. − DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информация. Серия 1: Организация и методика информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информационной работы. − 2021. − № 4. − С. 1-7. − DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. − 2021. − Т. 24. − № 2. − С. 231-238. − DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness) [Электронный ресуре]. • URL: https://www.antimalware.ru/analytics/Market_Analysis/Security - Awareness Абденов, А. Ж. Современные системы управления информационной		обращения: 27.01.2022). — Режим доступа:		
субъект управления сё информационной безопасностью / Л. В. Астахова // Научнотехническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 5. — С. 11-17. — DOI 10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидность методик оценки угроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информационной безопасности организации и методика информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив щифровой индустрии / Л. В. Астахова // Научно-техническая информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность протраммы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (SecurityAwareness)]Электроный ресурс]. — URL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness		· · · · · · · · · · · · · · · · · · ·		
безопасностью / Л. В. Астахова // Научно- техническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 5. — С. 11-17. — DOI 10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидность методик оценки угроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019- 2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (Security Аwareness) [Электронный ресурс]. — URL: https://www.anti- malware.ru/analytics/Market_Analysis/Security - Аwareness Абденов, А. Ж. Современные системы управления информационной безопасностие управления информационной управления объема управления объема управления объема управления объема управления объ		, 1, 1		
техническая информация. Серия 1: Организация и методика информационной работы. – 2020. – № 5. – С. 11-17. – DOI 10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидность методик оценки угроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информация. Серия 1: Организация и методика информационной работы. – 2020. – № 11. – С. 1-8. – DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив шифровой индустрии / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. – 2021. – № 4. – С. 1-7. – DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. – 2021. – Т. 24. – № 2. – С. 231-238. – DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (SecurityAwareness)[Электронный ресурс]. – URL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness Абденов, А. Ж. Современные системы управления информационной безопасности.		1 7 2		
Организация и методика информационной работы. — 2020. — № 5. — С. 11-17. — DOI 10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидность методик оценки угроз информационной безопасности организации / Л. В. Астахова / Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.242.006. Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness) [Электронный ресурс] URL: https://www.antimalware.ru/analytics/Market_Analysis/Security -Awareness		•		
работы. — 2020. — № 5. — С. 11-17. — DOI 10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидность методик оценки угроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (SecurityAwareness)[Электронный ресурс] URL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness		1 1		
10.36535/0548-0019-2020-05-2. Астахова, Л. В. Валидность методик оценки угроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (SecurityAwareness)[Электронный ресурс] URL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness		= = =		
В. Валидность методик оценки угроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness) [Электронный ресурс] URL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness		*		
информационной безопасности организации / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness) [Электронный ресурс] URL: https://www.antimalware.ru/analytics/Market_Analysis/Security - Awareness				
Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness)[Электронный ресурс]. — URL: https://www.antimalware.ru/analytics/Market_Analysis/Security - Awareness		· ·		
информация. Серия 1: Организация и методика информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческимм угрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness) [Электронный ресурс] URL: https://www.antimalware.ru/analytics/Market_Analysis/Security - Awareness				
методика информационной работы. — 2020. — № 11. — С. 1-8. — DOI 10.36535/0548-0019- 2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческих моделей управления цифровой индустрии / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness)] Электронный ресурс] URL: https://www.anti- malware.ru/analytics/Market_Analysis/Security -Awareness Абденов, А. Ж. Современные системы управления информационной		1		
— № 11. — С. 1-8. — DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (SecurityAwareness)[Электронный ресурс]. — URL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness Абденов, А. Ж. Современные системы управления информационной		1 1 1		
2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информацио. Серия 1: Организация и методика информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness)[Электронный ресурс] URL: https://www.antimalware.ru/analytics/Market_Analysis/Security - Awareness Абденов, А. Ж. Современные системы управления информационной безопасность из учровное пособие / А. Ж.				
стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.3653/50548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness) [Электронный ресурс] URL: https://www.antimalware.ru/analytics/Market_Analysis/Security - Awareness Абденов, А. Ж. Современные системы управления информационной безопасность у управления информационной безопасность у управления информационной				
человеческими угрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness) [Электронный ресурс]. — URL: https://www.antimalware.ru/analytics/Market_Analysis/Security - Awareness Абденов, А. Ж. Современные системы управления информационной безопасность по управления информационной безопасность по управления информационной безопасность по управления информационной управления информационной безопасность по управления информационной безопасность по управления информационной управления информационной управления информационной безопасность по управления информационной управлени				
безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness) [Электронный ресурс] URL: https://www.antimalware.ru/analytics/Market_Analysis/Security - Awareness Абденов, А. Ж. Современные системы управления информационной безопасностью учебие пособие / А. Ж.				
цифровой индустрии / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (SecurityAwareness)[Электронный ресурс]. — URL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness Абденов, А. Ж. Современные системы управления информационной безопасность от учебное пособие / А. Ж.				
Научно-техническая информация. Серия 1: Организация и методика информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (SecurityAwareness)[Электронный ресурс]. — URL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness Абденов, А. Ж. Современные системы управления информационной безопасности в управления информационной		1		
Организация и методика информационной работы. — 2021. — № 4. — С. 1-7. — DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (SecurityAwareness)[Электронный ресурс]. — URL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness Абденов, А. Ж. Современные системы управления информационной безопасности от умебиле пособие / А. Ж.		7 -		
работы. – 2021. – № 4. – С. 1-7. – DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. – 2021. – Т. 24. – № 2. – С. 231-238. – DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (SecurityAwareness)[Электронный ресурс] URL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness				
10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. − 2021. − Т. 24. − № 2. − С. 231-238. − DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (SecurityAwareness)[Электронный ресурс]. − URL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness Абденов, А. Ж. Современные системы управления информационной безопасность от умебное пособие / А. Ж.				
В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (SecurityAwareness)[Электронный ресурс] URL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness Абденов, А. Ж. Современные системы управления информационной безопасность ю; умебное пособие / А. Ж.		<u>+</u>		
повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness) [Электронный ресурс]. — URL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness Абденов, А. Ж. Современные системы управления информационной безопасность ю; унеброе пособие / А. Ж.		· ·		
об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness) [Электронный ресурс]. — URL: https://www.antimalware.ru/analytics/Market_Analysis/Security—Awareness Абденов, А. Ж. Современные системы управления информационной		_ · · · · · · · · · · · · · · · · · · ·		
организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (SecurityAwareness)[Электронный ресурс]. — URL: https://www.antimalware.ru/analytics/Market_Analysis/Security—Awareness Абденов, А. Ж. Современные системы управления информационной безопасностью; ушебное пособие / А. Ж.		1.5		
Бесчастнов // Информация и безопасность. — 2021. — Т. 24. — № 2. — С. 231-238. — DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (SecurityAwareness)[Электронный ресурс] URL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness Абденов, А. Ж. Современные системы управления информационной безопасностью: унебное пособие / А. Ж.		* *		
2021. – Т. 24. – № 2. – С. 231-238. – DOI 10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (SecurityAwareness)[Электронный ресурс] URL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness Абденов, А. Ж. Современные системы управления информационной безопасностью: унебыре пособие / А. Ж		1 /		
10.36622/VSTU.2021.24.2.006. Обзор рынка сервисов повышения осведомленности по ИБ (SecurityAwareness)[Электронный ресурс] URL: https://www.antimalware.ru/analytics/Market_Analysis/Security-Awareness Абденов, А. Ж. Современные системы управления информационной				
сервисов повышения осведомленности по ИБ (SecurityAwareness)[Электронный ресурс] URL: https://www.anti-malware.ru/analytics/Market_Analysis/Security -Awareness Абденов, А. Ж. Современные системы управления информационной				
ИБ (SecurityAwareness)[Электронный ресурс] URL: https://www.anti-malware.ru/analytics/Market_Analysis/Security -Awareness Абденов, А. Ж. Современные системы управления информационной безопасностью: унебыре пособие / А. Ж				
ресурс] URL: https://www.anti-malware.ru/analytics/Market_Analysis/Security -Awareness Абденов, А. Ж. Современные системы управления информационной		<u> </u>		
malware.ru/analytics/Market_Analysis/Security -Awareness Абденов, А. Ж. Современные системы управления информационной безопасностью: унебное пособие / А. Ж		, , , , , , , , , , , , , , , , , , , ,		
-Awareness Абденов, А. Ж. Современные системы управления информационной		F		
управления информационной		1 = 7		
управления информационной		Абденов, А. Ж. Современные системы		
баропрационно и ущебила поробил / А. Ж		•		
Экспертная оценка проблем УИБ	Экспертиза опенка проблем VIAE	безопасностью: учебное пособие / А. Ж.	Q	20
Абденов, Г. А. Дронова, В. А. Трушин. —	экспертная оценка проолем у ив		O	20
Новосибирск: НГТУ, 2017. — 48 с. — ISBN				
978-5-7782-3236-5. — Текст: электронный //		978-5-7782-3236-5. — Текст: электронный //		

Лань: электронно-библиотечная система. -URL: https://e.lanbook.com/book/118224 (дата обращения: 23.09.2021). — Режим доступа: для авториз. пользователей. 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: электроннобиблиотечная система. — URL: https://e.lanbook.com/book/155146 (дата обращения: 20.01.2022). — Режим доступа: для авториз. пользователей. Основы управления информационной безопасностью Текст учеб. пособие для вузов по направлениям (специальностям) 090000 "Информ. безопасность" А. П. Курило и др. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2016. - 243 с. ил. Васильева И. Н. Управление информационной безопасностью : учебное пособие / И. Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2014. -82 с. Астахова, Л. В. Валидность методик оценки угроз информационной безопасности организации / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. – 2020. – № 11. -C. 1-8. – DOI 10.36535/0548-0019-2020-11-1. Астахова, Л. В. Трансформация стратегических моделей управления человеческими угрозами информационной безопасности предприятия как императив цифровой индустрии / Л. В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. – 2021. – № 4. – С. 1-7. – DOI 10.36535/0548-0019-2021-04-1. Астахова, Л. В. Целевая комплексность программы повышения осведомленности сотрудников об информационной безопасности организации / Л. В. Астахова, С. А. Бесчастнов // Информация и безопасность. -2021. – T. 24. – № 2. – C. 231-238. – DOI 10.36622/VSTU.2021.24.2.006.

6. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

6.1. Контрольные мероприятия (КМ)

№ KM	Се- местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи- тыва- ется в ПА
1	8	Текущий контроль	Информационное моделирование проблем УИБ	8	7	Защита выполненного практического задания осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество содержания, оформления, правильность выводов и ответы на вопросы, своевременность представления. При оценивании результатов мероприятия используется балльнорейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Показатели оценивания: Соответствие требованиям к структуре и содержанию работы: 2 балла — полное соответствие требованиям; Соответствие требованиям к оформлению работы: 2 балла — полное соответствие требованиям, 1 балл — неполное соответствие требованиям к оформлению работы: 2 балла — полное соответствие требованиям к полное соответствие требованиям к оформлению работы: 2 балла — полное соответствие, 0 баллов — несоответствие, 1 балл — неполное соответствие, 1 балл — неполное соответствие, 0 баллов — несоответствие. Срок представленияработы: работа представлена в установленный срок — 1 балл; с нарушением срока — 0 баллов. Максимальное количество баллов — 7. Весовой коэффициент мероприятия — 8.	экзамен
2	8	Текущий контроль	Выбор методики оценки рисков ИБ	5	7	Защита выполненного практического задания осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество содержания, оформления, правильность выводов и ответы на вопросы, своевременность представления.	экзамен

						При оценивании результатов мероприятия используется балльнорейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Показатели оценивания: Соответствие требованиям к структуре и содержанию работы: 2 балла — полное соответствие требованиям; Соответствие требованиям; Соответствие требованиям к оформлению работы: 2 балла — полное соответствие требованиям к оформлению работы: 2 балла — полное соответствие требованиям к оформлению работы: 2 балла — полное соответствие требованиям к полноте, логичности и правильности ответов на вопросы и/или выводов: 2 балла - полное соответствие, 1 балл - неполное соответствие, 1 балл - неполное соответствие, 0 баллов - несоответствие. Срок представления работы: работа представлена в установленный срок - 1 балл; с нарушением срока - 0	
3	8	Текущий контроль	Оценка рисков ИБ организации по методике Microsoft	5	7	баллов. Максимальное количество баллов -7. Весовой коэффициент мероприятия -5. Защита выполненного практического задания осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество содержания, оформления, правильность выводов и ответы на вопросы, своевременность представления. При оценивании результатов мероприятия используется балльнорейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Показатели оценивания: Соответствие требованиям к структуре и содержанию работы: 2 балла — полное соответствие требованиям; Соответствие требованиям; Соответствие требованиям к оформлению работы: 2 балла —	экзамен

						полное соответствие требованиям, 1	
						балл – неполное соответствие, 0	
						баллов – несоответствие	
						требованиям;	
						Соответствие требованиям к	
						полноте, логичности и правильности	
						ответов на вопросы и/или выводов: 2	
						балла - полное соответствие, 1 балл -	
						неполное соответствие, 0 баллов -	
						несоответствие.	
						Срок представленияработы: работа	
						представлена в установленный срок	
						- 1 балл; с нарушением срока - 0	
						баллов.	
						Максимальное количество баллов -7.	
						Весовой коэффициент мероприятия -	
						5.	
1						Защита выполненного практического	
						задания осуществляется	
						индивидуально. Студентом	
						предоставляется оформленный	
						отчет. Оценивается качество	
						содержания, оформления,	
						правильность выводов и ответы на	
						вопросы, своевременность	
						представления.	
						При оценивании результатов	
						мероприятия используется балльно-	
						рейтинговая система оценивания	
						результатов учебной деятельности	
						обучающихся (утверждена приказом	
						ректора от 24.05.2019 г. № 179)	
						Показатели оценивания:	
						Соответствие требованиям к	
						структуре и содержанию работы: 2	
		Текущий				балла – полное соответствие	
4	8	-	ДОУИБ организации	5	7	требованиям, 1 балл – неполное	экзамен
		контроль				соответствие, 0 баллов –	
						несоответствие требованиям;	
						Соответствие требованиям к	
						оформлению работы: 2 балла –	
						полное соответствие требованиям, 1	
						балл – неполное соответствие, 0	
						баллов – несоответствие	
						требованиям;	
						Соответствие требованиям к	
						полноте, логичности и правильности	
						ответов на вопросы и/или выводов: 2	
						балла - полное соответствие, 1 балл -	
						неполное соответствие, 0 баллов -	
						несоответствие, о осляюв	
						Срок представления работы: работа	
						представлена в установленный срок	
						- 1 балл; с нарушением срока - 0	
						- 1 балл, с нарушением срока - 0 баллов.	
						Максимальное количество баллов -7.	

						Весовой коэффициент мероприятия - 5.	
5	8	Текущий контроль	Количественная оценка рисков ИБ	5	7	Защита выполненного практического задания осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество содержания, оформления, правильность выводов и ответы на вопросы, своевременность представления. При оценивании результатов мероприятия используется балльнорейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Показатели оценивания: Соответствие требованиям к структуре и содержанию работы: 2 балла — полное соответствие требованиям; Соответствие требованиям к оформлению работы: 2 балла — полное соответствие требованиям; Соответствие требованиям к оформлению работы: 2 балла — полное соответствие требованиям к оформлению работы: 2 балла — полное соответствие, 0 баллов — несоответствие, 1 балл — неполное соответствие, 1 балл — неполное соответствие, 0 баллов — несоответствие. Срок представленияработы: работа представлена в установленный срок — 1 балл; с нарушением срока - 0 баллов. Максимальное количество баллов — 7. Весовой коэффициент мероприятия — 5.	экзамен
6	8	Текущий контроль	Разработка организационных и инструментальных средств повышения осведомленности сотрудников организации в области ИБ	15	7	Защита выполненного практического задания осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество содержания, оформления, правильность выводов и ответы на вопросы, своевременность представления. При оценивании результатов мероприятия используется балльнорейтинговая система оценивания результатов учебной деятельности	экзамен

						обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Показатели оценивания: Соответствие требованиям к структуре и содержанию работы: 2 балла — полное соответствие требованиям, 1 балл — неполное соответствие, 0 баллов — несоответствие требованиям; Соответствие требованиям к оформлению работы: 2 балла — полное соответствие требованиям, 1 балл — неполное соответствие, 0 баллов — несоответствие требованиям к полное соответствие требованиям; Соответствие требованиям к полноте, логичности и правильности ответов на вопросы и/или выводов: 2 балла - полное соответствие, 1 балл - неполное соответствие, 0 баллов - несоответствие. Срок представления работы: работа представлена в установленный срок - 1 балл; с нарушением срока - 0 баллов. Максимальное количество баллов -7.	
						Весовой коэффициент мероприятия - 15. Защита выполненного практического	
7	8	Текущий контроль	Разработка Политики УИБ	5	7	задания осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество содержания, оформления, правильность выводов и ответы на вопросы, своевременность представления. При оценивании результатов мероприятия используется балльнорейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Показатели оценивания: Соответствие требованиям к структуре и содержанию работы: 2 балла — полное соответствие требованиям; Соответствие требованиям к оформлению работы: 2 балла — полное соответствие требованиям к оформлению работы: 2 балла — полное соответствие требованиям к оформлению работы: 2 балла — полное соответствие требованиям , 1 балл — неполное соответствие, 0 баллов — несоответствие, 0 баллов — несоответствие, 0 баллов — несоответствие требованиям;	экзамен

						Соответствие требованиям к полноте, логичности и правильности ответов на вопросы и/или выводов: 2 балла - полное соответствие, 1 балл - неполное соответствие, 0 баллов - несоответствие. Срок представленияработы: работа представлена в установленный срок - 1 балл; с нарушением срока - 0 баллов. Максимальное количество баллов -7. Весовой коэффициент мероприятия - 5.	
8	8	Текущий контроль	Зарубежные технологии средства УИБ	7		Защита выполненного практического задания осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество содержания, оформления, правильность выводов и ответы на вопросы, своевременность представления. При оценивании результатов мероприятия используется балльнорейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Показатели оценивания: Соответствие требованиям к структуре и содержанию работы: 2 балла — полное соответствие требованиям; Соответствие требованиям; Соответствие требованиям к оформлению работы: 2 балла — полное соответствие требованиям к оформлению работы: 2 балла — полное соответствие требованиям к оформлению работы: 2 балла — полное соответствие, 0 баллов — несоответствие требованиям к полное соответствие требованиям к полное соответствие, 0 баллов — несоответствие, 0 баллов — несоответствие, 0 баллов — несоответствие, 1 балл — неполное соответствие, 1 балл — неполное соответствие, 1 балл — неполное соответствие, 1 балл — несоответствие. Срок представления работы: работа представлена в установленный срок — 1 балл; с нарушением срока - 0 баллов. Максимальное количество баллов -7. Весовой коэффициент мероприятия -7.	экзамен
9	8	Текущий контроль	Экспертная оценка проблем УИБ	10	7	Защита выполненного практического задания осуществляется	экзамен

						индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество содержания, оформления, правильность выводов и ответы на вопросы, своевременность представления. При оценивании результатов мероприятия используется балльнорейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Показатели оценивания: Соответствие требованиям к структуре и содержанию работы: 2 балла — полное соответствие требованиям; Соответствие требованиям к оформлению работы: 2 балла — полное соответствие требованиям к оформлению работы: 2 балла — полное соответствие требованиям , 1 балл — неполное соответствие, 0 баллов — несоответствие требованиям к оформлению работы: 2 балла — полное соответствие, 0 баллов — несоответствие, 0 баллов — несоответствие, 0 баллов — несоответствие, 0 баллов несоответствие, 0 баллов несоответствие, 0 баллов неполное соответствие, 0 баллов неполное соответствие, 0 баллов несоответствие. Срок представления работы: работа представлена в установленный срок - 1 балл; с нарушением срока - 0 баллов. Максимальное количество баллов -7. Восорой колофурматия	
						Весовой коэффициент мероприятия - 10.	
10	8	Текущий контроль	Моделирование подсистемы СУИБ	35	7	Защита выполненного практического задания осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество содержания, оформления, правильность выводов и ответы на вопросы, своевременность представления. При оценивании результатов мероприятия используется балльнорейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Показатели оценивания: Соответствие требованиям к	экзамен

						структуре и содержанию работы: 2 балла — полное соответствие требованиям, 1 балл — неполное соответствие, 0 баллов — несоответствие требованиям; Соответствие требованиям к оформлению работы: 2 балла — полное соответствие требованиям, 1 балл — неполное соответствие, 0 баллов — несоответствие требованиям; Соответствие требованиям; Соответствие требованиям; Соответствие требованиям к полноте, логичности и правильности ответов на вопросы и/или выводов: 2 балла - полное соответствие, 1 балл - неполное соответствие, 0 баллов - несоответствие. Срок представления работы: работа представлена в установленный срок - 1 балл; с нарушением срока - 0 баллов. Максимальное количество баллов -7. Весовой коэффициент мероприятия - 35.	
11	8	Бонус	Бонус	-	15	Выступление с докладом на международной научной конференции и/или публикация материалов в сборнике конференции - 15 баллов. Выступление с докладом на Всероссийской студенческой научной конференции и/или публикация материалов в сборнике конференции - 10 баллов. Выступление с докладом на ежегодной студенческой научной конференции ЮУрГУ (секция Защита информации) - 7 баллов. Посещаемость занятий 70% - 3 балла.	экзамен
12	8	Проме- жуточная аттестация	экзамен	-	0	На экзамене происходит оценивание учебной деятельности обучающихся по дисциплине на основе полученных оценок за контрольнорейтинговые мероприятия текущего контроля и бонусов. При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Оценка за экзамен складывается из результатов текущего контроля по дисциплине в течение семестра и бонусных	экзамен

		баллов. Студент может повысить оценку за контрольно-рейтинговые мероприятия на экзамене. Экзамен может проводиться в дистанционном формате в режиме видеоконференции в "Электронном ЮУрГУ""в соответствии с регламентом, утвержденном	
		приказом ректора ЮУРГУ от 21.04.2020 № 80	

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
экзамен	Оценка за экзамен складывается из результатов текущего контроля по дисциплине в течение семестра и бонусных баллов. Студент может повысить оценку на экзамене, доработав результаты выполнения мероприятий текущего контроля. Экзамен может проводиться в дистанционном формате в режиме видеоконференции в "Электронном ЮУрГУ""в соответствии с регламентом, утвержденном приказом ректора ЮУРГУ от 21.04.2020 № 80	В соответствии с пп. 2.5, 2.6 Положения

6.3. Паспорт фонда оценочных средств

1/	D	№ KM										
Компетенции	Результаты обучения					56	5 7	78	9	10	11	12
ОПК-5	Знает: основные документы по стандартизации в сфере управления ИБ; принципы формирования политики информационной безопасности в автоматизированных системах; требования информационной безопасности при эксплуатации автоматизированной системы	+	+	-+-	+	+ -		-	-+-	+	+	+
ОПК-5	Умеет: формировать политики информационной безопасности организации; выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы		+	+	+	+		-+	+	+	+	+
ОПК-10	Знает: основные угрозы безопасности информации и модели нарушителя объекта информатизации; цели и задачи управления информационной безопасностью, основные документы по стандартизации в сфере управления информационной безопасностью; принципы формирования политики информационной безопасности объекта информатизации;	+	-		+	+	+++	++	+	+	+	+
ОПК-10	Умеет: разрабатывать модели угроз и модели нарушителя объекта информатизации; оценивать информационные риски объекта информатизации				+	+		+	+	+	+	+

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

- в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:
 - 1. Защита информации. Инсайд ,информ.-метод. журн. ,Изд. дом "Афина"
 - 2. Защита информации. Конфидент / Ассоц. защиты информ. "Конфидент" : информ.-метод. журн
 - 3. БДИ: Безопасность. Достоверность. Информация рос. журн. о безопасности бизнеса и личности ООО "Журн. "БДИ" журнал"
 - 4. Безопасность информационных технологий ,12+ ,М-во образования и науки Рос. Федерации, Моск. инж.-физ. ин-т (гос. ун-т), ВНИИПВТИ
 - 5. Вестник УрФО : Безопасность в информационной сфере ,Юж.-Урал. гос. ун-т; ЮУрГУ
 - 6. 6. Информационные ресурсы России
 - 7. Информационное общество
 - 8. 8. Информационное право
 - 9. 9. Информационные процессы и системы
 - 10. 10. Информационные ресурсы России
 - 11. 11. Кадровое дело
 - 12. 12. Управление персоналом
 - 13. 13. Управление риском
- г) методические указания для студентов по освоению дисциплины:
 - 1. УИБ_Лекционный материал
 - 2. Методические указания по курсу "Управление информационной безопасностью" для студентов направления "Информационная безопасность"
 - 3. Астахова Л.В._УИБ_Управление рисками ИБ_Методическое пособие

из них: учебно-методическое обеспечение самостоятельной работы студента:

- 1. УИБ_Лекционный материал
- 2. Методические указания по курсу "Управление информационной безопасностью" для студентов направления "Информационная безопасность"
- 3. Астахова Л.В._УИБ_Управление рисками ИБ_Методическое пособие

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Дополнительная	Электронно-	Милославская, Н.Г. Серия «Вопросы управление

	литература	библиотечная	информационной безопасностью". Выпуск 2. [Электронный
		система	ресурс] / Н.Г. Милославская, М.Ю. Сенаторов, А.И.
		издательства	Толстой. — Электрон. дан. — М. : Горячая линия-Телеком,
		Лань	2012. — 130 с. — Режим доступа:
			http://e.lanbook.com/book/5179 — Загл. с экрана.
		Электронно-	Милославская, Н.Г. Серия «Вопросы управление
	T.	олсктронно- библиотечная система	информационной безопасностью". Выпуск 4. [Электронный
2	Дополнительная		ресурс] / Н.Г. Милославская, М.Ю. Сенаторов, А.И.
	литература	издательства	Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 214 с. — Режим доступа:
		Лань	http://e.lanbook.com/book/5181 — Загл. с экрана.
-			Курило, А.П. Основы управления информационной
		Электронно-	безопасностью. Серия «Вопросы управление
		библиотечная	информационной безопасностью". Выпуск 1. [Электронный
3	Дополнительная	система	ресурс] / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов,
	литература	издательства	А.И. Толстой. — Электрон. дан. — М.: Горячая линия-
		Лань	Телеком, 2012. — 244 c. — Режим доступа:
			http://e.lanbook.com/book/5178 — Загл. с экрана.
		Электронно-	Милославская, Н.Г. Серия «Вопросы управление
		библиотечная	информационной безопасностью". Выпуск 5. [Электронный
4	Дополнительная	система издательства	ресурс] / Н.Г. Милославская, М.Ю. Сенаторов, А.И.
	питература		Толстой. — Электрон. дан. — М.: Горячая линия-Телеком,
		Лань	2012. — 166 с. — Режим доступа:
\vdash			http://e.lanbook.com/book/5182 — Загл. с экрана.
		Электронно-	Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 3. [Электронный
	Дополнительная	библиотечная	ресурс] / Н.Г. Милославская, М.Ю. Сенаторов, А.И.
5	питепатупа	система	Толстой. — Электрон. дан. — М.: Горячая линия-Телеком,
	1 31	издательства	2013. — 170 с. — Режим доступа:
		Лань	http://e.lanbook.com/book/5180 — Загл. с экрана.
			Краковский, Ю. М. Методы защиты информации: учебное
		Электронно-	пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб.
	Основная	библиотечная	— Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-
6	литература	система	8114-5632-1. — Текст: электронный // Лань: электронно-
		издательства Лань	библиотечная система. — URL:
		иань	https://e.lanbook.com/book/156401 — Режим доступа: для авториз. пользователей. (Раздел управления рисками ИБ)
-			Пелешенко, В. С. Менеджмент инцидентов
			информационной безопасности защищенных
		Электронно-	автоматизированных систем управления: учебное пособие /
7	Основная	библиотечная	В. С. Пелешенко, С. В. Говорова, М. А. Лапина. —
'	литература	система	Ставрополь : СКФУ, 2017. — 86 с. — Текст : электронный //
		издательства Лань	Лань: электронно-библиотечная система. — URL:
		D IMILD	https://e.lanbook.com/book/155146 — Режим доступа: для
\vdash			авториз. пользователей.
			Абденов, А. Ж. Современные системы управления
		Электронно-	информационной безопасностью: учебное пособие / А. Ж.
8	Основная	библиотечная	Абденов, Г. А. Дронова, В. А. Трушин. — Новосибирск : НГТУ, 2017. — 48 с. — ISBN 978-5-7782-3236-5. — Текст :
0	литература	система издательства	электронный // Лань : электронно-библиотечная система.
		Лань	URL: https://e.lanbook.com/book/118224 — Режим доступа:
			для авториз. пользователей.
	1	1	p

Перечень используемого программного обеспечения:

1. Microsoft-Project(бессрочно)

- 2. Microsoft-Windows(бессрочно)
- 3. Microsoft-Office(бессрочно)
- 4. ФГАОУ ВО "ЮУрГУ (НИУ)"-Портал "Электронный ЮУрГУ" (https://edu.susu.ru)(бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

- 1. -База данных polpred (обзор СМИ)(бессрочно)
- 2. ООО "Гарант Урал Сервис" Гарант (31.12.2022)
- 3. -База данных ВИНИТИ РАН(бессрочно)

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Практические занятия и семинары	913 (36)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows XP, MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; MSAT; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2, DLP Staffcop
Лекции	912 (36)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: OC Windows XP, MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+.