ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель направления

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 22.12.2022

А. Н. Соколов

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.34 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.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 22.12.2022

А. Н. Соколов

Разработчик программы,
д.пед.н., проф., профессор

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Астахова Л. В.
Пользователь: astakhovalv
Дата подписания: 22.12.2022

Л. В. Астахова

Челябинск

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

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.О.32 Программно-аппаратные средства защиты информации, ФД.02 Мониторинг информационной безопасности и активный поиск киберугроз, 1.О.29 Организационное и правовое обеспечение информационной безопасности	Не предусмотрены

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

Дисциплина	Требования
1.О.32 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.29 Организационное и правовое обеспечение информационной безопасности	Знает: 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, содержание основных нормативных правовых актов в сфере противодействия коррупции, 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: использовать систему организационных мер, направленных на защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами ФСБ России, ФСТЭК России, соблюдать требования антикоррупционного законодательства, воздерживаться от поведения, вызывающего сомнение в объективном и беспристрастном исполнении должностных (служебных) обязанностей, 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 организационно-распорядительных 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 основных нормативных правовых актов в сфере противодействия коррупции, работы с нормативными правовыми актами
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

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
		8
Общая трудоёмкость дисциплины	144	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

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
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	№ раздела	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 ПЕРСОНАЛОМ ОРГАНИЗАЦИИ	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 №ИСО/МЭК 27003-2012. – URL: http://docs.cntd.ru (дата обращения: 10.01. 2022). СТО БР ИББС-1.0-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. – М., 2014. Малюк, А. А. Защита информации в информационном обществе : учебное пособие / А. А. Малюк. — Москва : Горячая линия-Телеком, 2017. — 230 с. — ISBN 978-5-9912-0481-1. — Текст : электронный // Лань : электронно-библиотечная 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 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, 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.anti-malware.ru/analytics/Market_Analysis/Security-Awareness		
Экспертная оценка проблем УИБ	Абденов, А. Ж. Современные системы управления информационной безопасностью: учебное пособие / А. Ж. Абденов, Г. А. Дронова, В. А. Трушин. — Новосибирск: НГТУ, 2017. — 48 с. — ISBN 978-5-7782-3236-5. — Текст: электронный //	8	20

	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: электронно-библиотечная 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. – 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.		

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)

№ КМ	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 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 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 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 - 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 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 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 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 - 5.	
3	8	Текущий контроль	Оценка рисков ИБ организации по методике Microsoft	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 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 балла – полное соответствие требованиям , 1 балл – неполное соответствие, 0 баллов – несоответствие 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.	
4	8	Текущий контроль	ДОУИБ организации	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 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 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 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.	экзамен

						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 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 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 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.	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 балльно-рейтинговая 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; 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.	
7	8	Текущий контроль	Разработка Политики УИБ	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 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 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;	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	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 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 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 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 - 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 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 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 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 - 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 балльно-рейтинговая 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 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 контрольно-рейтинговые 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

Компетенции	Результаты обучения	№ КМ											
		1	2	3	4	5	6	7	8	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. 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. Методические указания по курсу "Управление информационной безопасностью" для студентов направления "Информационная безопасность"
2. УИБ_Лекционный материал
3. Астахова Л.В._УИБ_Управление рисками ИБ_Методическое пособие

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Методические указания по курсу "Управление информационной безопасностью" для студентов направления "Информационная безопасность"
2. УИБ_Лекционный материал
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 система издательства Лань	информационной безопасностью". Выпуск 2. [Электронный ресурс] / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 130 с. — Режим доступа: http://e.lanbook.com/book/5179 — Загл. с экрана.
2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 4. [Электронный ресурс] / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 214 с. — Режим доступа: http://e.lanbook.com/book/5181 — Загл. с экрана.
3	Дополнительная литература	Электронно-библиотечная система издательства Лань	Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1. [Электронный ресурс] / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 244 с. — Режим доступа: http://e.lanbook.com/book/5178 — Загл. с экрана.
4	Дополнительная литература	Электронно-библиотечная система издательства Лань	Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 5. [Электронный ресурс] / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 166 с. — Режим доступа: http://e.lanbook.com/book/5182 — Загл. с экрана.
5	Дополнительная литература	Электронно-библиотечная система издательства Лань	Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 3. [Электронный ресурс] / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2013. — 170 с. — Режим доступа: http://e.lanbook.com/book/5180 — Загл. с экрана.
6	Основная литература	Электронно-библиотечная система издательства Лань	Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401 — Режим доступа: для авториз. пользователей. (Раздел управления рисками ИБ)
7	Основная литература	Электронно-библиотечная система издательства Лань	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 — Режим доступа: для авториз. пользователей.
8	Основная литература	Электронно-библиотечная система издательства Лань	Абденов, А. Ж. Современные системы управления информационной безопасностью : учебное пособие / А. Ж. Абденов, Г. А. Дронова, В. А. Трушин. — Новосибирск : НГТУ, 2017. — 48 с. — ISBN 978-5-7782-3236-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118224 — Режим доступа: для авториз. пользователей.

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 "ГарантУралСервис"-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 (3б)	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 (3б)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+.