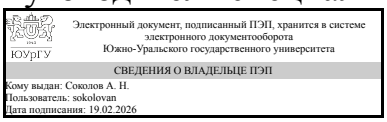
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель специальности



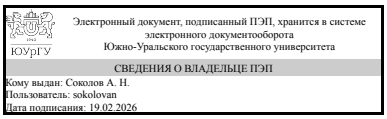
А. Н. Соколов

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.35 Информационная безопасность открытых систем
для специальности 10.05.03 Информационная безопасность автоматизированных систем
уровень Специалитет
форма обучения очная
кафедра-разработчик Защита информации

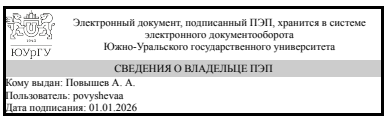
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 26.11.2020 № 1457

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



А. Н. Соколов

Разработчик программы,
доцент



А. А. Повышев

Челябинск

1. Цели и задачи дисциплины

Целью дисциплины является: изучение технологий, методов и средств создания защищенных открытых информационных систем (ИС) . Задачами дисциплины являются: - привитие обучаемым основ культуры обеспечения информационной безопасности (ИБ) в ОИС; - формирование у обучаемых понимания основ построения защищенных ОИС; - ознакомление обучаемых с основными уязвимостями, угроза ИБ и сетевыми атаками, ха-рактерными для современных ОИС; - обучение различным подходам и методам обеспечения ИБ ОИС.

Краткое содержание дисциплины

Дисциплина содержит разделы, посвященные нормативному обеспечению ИБОС, основным угрозам и уязвимостям ИБОС, различным подходам, методам и средствам обеспечения ИБОС.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	Знает: риски подсистем защиты информации автоматизированных систем и экспериментальные методы их оценки Умеет: анализировать и оценивать угрозы информационной безопасности автоматизированных систем Имеет практический опыт: анализа информационной инфраструктуры автоматизированных систем
ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	Знает: принципы формирования политики информационной безопасности в автоматизированных системах Умеет: разрабатывать частные политики информационной безопасности автоматизированных систем Имеет практический опыт: управления процессами обеспечения безопасности автоматизированных систем

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.О.33 Безопасность операционных систем, 1.О.32 Безопасность сетей электронных вычислительных машин	ФД.02 Мониторинг информационной безопасности и активный поиск киберугроз, 1.О.34 Безопасность систем баз данных, 1.О.41 Управление информационной безопасностью, 1.О.37 Контроль защищенности автоматизированных систем, 1.О.47 Измерительная аппаратура контроля защищенности объектов информатизации,

	1.О.28 Защита информации от утечки по техническим каналам, 1.О.36.02 Эксплуатация автоматизированных систем в защищенном исполнении

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

Дисциплина	Требования
1.О.32 Безопасность сетей электронных вычислительных машин	Знает: методы администрирования вычислительных сетей, методы проектирования вычислительных сетей Умеет: администрировать вычислительные сети; реализовывать политику безопасности вычислительной сети, проектировать вычислительные сети Имеет практический опыт: администрирования локальных вычислительных сетей с учетом требований по обеспечению информационной безопасности, эксплуатации локальных вычислительных сетей
1.О.33 Безопасность операционных систем	Знает: устройство и принципы работы операционных систем, структуру и возможности подсистем защиты операционных систем семейств UNIX и Windows, методы администрирования и принципы работы операционных систем семейств UNIX и Windows Умеет: использовать средства управления работой операционной системы; формулировать политику безопасности операционных систем семейств UNIX и Windows, настраивать политику безопасности операционных систем семейств UNIX и Windows Имеет практический опыт: установки операционных систем семейств Windows и Unix, администрирования операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч., 74,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		6
Общая трудоёмкость дисциплины	144	144
Аудиторные занятия:	64	64
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды	0	0

аудиторных занятий (ПЗ)		
Лабораторные работы (ЛР)	32	32
Самостоятельная работа (СРС)	69,5	69,5
Экспертная оценка проблемы ИБОС	57,5	57.5
Моделирование документационного обеспечения процессов ИБОС	12	12
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	Нормативные и концептуальные основы ИБОС	10	2	0	8
2	Атаки по уровням иерархической системы OSI и защита от них	14	6	0	8
3	Комплексное обеспечение ИБОС	20	12	0	8
4	Средства обеспечения ИБОС	20	12	0	8

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Нормативные и концептуальные основы ИБОС	2
2	2	Атаки по уровням иерархической системы OSI и защита от них	4
3	2	Атаки на беспроводные устройства	2
4	3	Комплексное обеспечение ИБОС: аутентификация, управление доступом, неотказуемость	4
5	3	Комплексное обеспечение ИБОС: конфиденциальность, целостность	2
6	3	Документационное сопровождение ИБОС: общие подходы	4
7	3	Документационное сопровождение обеспечения отдельных направлений ИБОС	2
8	4	Средства обеспечения ИБОС	4
9	4	Обеспечение сетевой безопасности	4
10	4	Инструментальные средства аудита ИБОС	4

5.2. Практические занятия, семинары

Не предусмотрены

5.3. Лабораторные работы

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во часов
1	1	Нормативные и концептуальные основы ИБОС в России	4
2	1	Нормативные и концептуальные основы ИБОС за рубежом	4
3	2	Моделирование угроз ИБОС	4
4	2	Технологии обеспечения ИБОС с помощью DLP-систем	4

5	3	Аутентификация	4
6	3	Управление доступом к файловым ресурсам	4
7	4	Технологические процессы внедрения средств обеспечения ИБОС	4
8	4	Разработка политики ИБОС	4

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Экспертная оценка проблемы ИБОС	Климентьев, К. Е. Введение в защиту компьютерной информации: учебное пособие / К. Е. Климентьев. — Самара : Самарский университет, 2020. — 183 с. — ISBN 978-5-7883-1526-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/189043 (дата обращения: 23.01.2022). — Режим доступа: для авториз. пользователей. (все разделы) Семь безопасных информационных технологий : учебник / А. В. Барабанов, А. В. Дорофеев, А. С. Марков, В. Л. Цирлов ; под редакцией А. С. Маркова. — Москва : ДМК Пресс, 2017. — 224 с. — ISBN 978-5-97060-494-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/97352 (дата обращения: 23.01.2022). — Режим доступа: для авториз. пользователей. (Глава 2, 3)	6	57,5
Моделирование документационного обеспечения процессов ИБОС	Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184 (дата обращения: 23.01.2022). — Режим доступа: для авториз. пользователей.(Все разделы и Приложения) Пугин, В. В. Защита информации в компьютерных информационных системах: учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299 (дата обращения: 23.01.2022). — Режим доступа: для авториз. пользователей. (п.1.3) Вострецова Е.В. Основы информационной безопасности: учебное	6	12

	пособие. – Екатеринбург: Изд-во Урал. ун-та, 2019.- 204 с. (раздел 7) Шаньгин, В. Ф. Информационная безопасность : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2014. — 702 с. — ISBN 978-5-94074-768-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/50578 (дата обращения: 20.01.2022). — Режим доступа: для авториз. пользователей. (Глава 2)		

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	6	Текущий контроль	Информационное моделирование процессов обеспечения ИБОС	10	7	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы. 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 -	экзамен

						неполное соответствие, 0 баллов - несоответствие. Срок представления пояснительной записки: курсовая работа представлена в установленный срок - 1 балл; с нарушением срока - 0 баллов. Максимальное количество баллов -7. Весовой коэффициент мероприятия – 10.	
2	6	Текущий контроль	Оценка уязвимостей и рисков ИБОС с помощью MSAT	10	7	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопрос, представленные в задании. 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 пояснительной записки: курсовая работа представлена в установленный срок - 1 балл; с нарушением срока - 0 баллов. Максимальное количество баллов -7. Весовой коэффициент мероприятия – 10.	экзамен
3	6	Текущий контроль	Использование NGFW: идентификация пользователей и политики безопасности.	5	7	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы.	экзамен

			Настройка параметров аутентификации ОС WINDOWS 10			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 пояснительной записки: курсовая работа представлена в установленный срок - 1 балл; с нарушением срока - 0 баллов. Максимальное количество баллов -7. Весовой коэффициент мероприятия – 5.	
4	6	Текущий контроль	Использование NGFW: политики сети, настройка политик в UserGate. Управление доступом к файловым ресурсам.	5	7	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы. 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	экзамен

						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 пояснительной записки: курсовая работа представлена в установленный срок - 1 балл; с нарушением срока - 0 баллов. Максимальное количество баллов -7. Весовой коэффициент мероприятия – 5.	
5	6	Текущий контроль	Использование NGFW: идентификация пользователей и политики безопасности. Разработка Политики ИБОС	15	7	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задаются 2 вопроса). 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 – 15.	экзамен
6	6	Текущий	Экспертная оценка	15	7	Защита задания осуществляется	экзамен

		контроль	проблем ИБОС			индивидуально. Студентом предоставляется презентация и выступление. Оценивается качество содержания, оформления, правильность выводов, ответы на вопросы и 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 – 15.	
10	6	Текущий контроль	Тестирование	5	10	Тестирование осуществляется студентом индивидуально. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) По окончании изучения дисциплины проводится тестирование, при котором студенту предлагается выбрать правильный ответ на заданный вопрос. Всего необходимо ответить на 10 вопросов в течение 10 минут. Каждый правильный ответ - 1 балл. Максимальное количество баллов –	экзамен

						10. Весовой коэффициент мероприятия – 5.	
12	6	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
13	6	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 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	экзамен

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	В соответствии с пп. 2.5, 2.6 Положения

	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	

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ							
		1	2	3	4	5	6	10	12	13
ОПК-13	Знает: риски подсистем защиты информации автоматизированных систем и экспериментальные методы их оценки	+	+	+	+	+	+	+	+	+
ОПК-13	Умеет: анализировать и оценивать угрозы информационной безопасности автоматизированных систем	+	+	+	+	+	+	+	+	+
ОПК-13	Имеет практический опыт: анализа информационной инфраструктуры автоматизированных систем		+	+	+	+	+	+	+	+
ОПК-15	Знает: принципы формирования политики информационной безопасности в автоматизированных системах	+	+	+	+	+	+	+	+	+
ОПК-15	Умеет: разрабатывать частные политики информационной безопасности автоматизированных систем	+	+	+	+	+	+	+	+	+
ОПК-15	Имеет практический опыт: управления процессами обеспечения безопасности автоматизированных систем		+	+	+	+	+	+	+	+

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. 1. Защита информации. Инсайд ,информ.-метод. журн. ,Изд. дом "Афина"
2. 2. Защита информации. Конфидент / Ассоц. защиты информ. "Конфидент" : информ.-метод. журн
3. 3. БДИ: Безопасность. Достоверность. Информация рос. журн. о безопасности бизнеса и личности ООО "Журн. "БДИ" журнал"
4. 4. Безопасность информационных технологий ,12+ ,М-во образования и науки Рос. Федерации, Моск. инж.-физ. ин-т (гос. ун-т), ВНИИПВТИ
5. 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. Управление риском

г) методические указания для студентов по освоению дисциплины:

1. ИБОС_Лекционный материал
2. Астахова Л.В. Методическое пособие по курсу ИБОС

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. ИБОС_Лекционный материал
2. Астахова Л.В. Методическое пособие по курсу ИБОС

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	ЭБС издательства Лань	Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. — 2-е изд., испр. и доп. — Москва : Горячая линия-Телеком, 2017. — 338 с. — ISBN 978-5-9912-0328-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111049 (дата обращения: 11.10.2025). — Режим доступа: для авториз. пользователей.
2	Основная литература	ЭБС издательства Лань	Бондарев, В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие / В. В. Бондарев. — 2-е изд. — Москва : МГТУ им. Баумана, 2018. — 250 с. — ISBN 978-5-7038-4899-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/172839 (дата обращения: 11.10.2025). — Режим доступа: для авториз. пользователей.
3	Основная литература	ЭБС издательства Лань	Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. — 2-е изд. — Москва : ДМК Пресс, 2017. — 434 с. — ISBN 978-5-97060-435-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/93278 (дата обращения: 11.10.2025). — Режим доступа: для авториз. пользователей.
4	Дополнительная литература	ЭБС издательства Лань	Мельников, Д. А. Информационная безопасность открытых систем : учебник / Д. А. Мельников. — 2-е изд. — Москва : ФЛИНТА, 2014. — 448 с. — ISBN 978-5-9765-1613-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/48368 (дата обращения: 11.10.2025). — Режим доступа: для авториз. пользователей.
5	Дополнительная литература	ЭБС издательства Лань	Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам : учебное пособие / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов, Э. Р. Газизова ; под редакцией А. А. Шелупанова [и др.]. — 2-е изд., стер. — Москва : Горячая линия-Телеком, 2012. — 550 с. — ISBN 978-5-9912-0257-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5114 (дата обращения: 11.10.2025). — Режим доступа: для авториз. пользователей.
6	Дополнительная литература	ЭБС издательства	Ворона, В. А. Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов. — Москва : Горячая линия-

		Лань	Телеком, 2018. — 272 с. — ISBN 978-5-9912-0059-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111037 (дата обращения: 11.10.2025). — Режим доступа: для авториз. пользователей.

Перечень используемого программного обеспечения:

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

Перечень используемых профессиональных баз данных и информационных справочных систем:

1. -База данных polpred (обзор СМИ)(бессрочно)
2. -База данных ВИНИТИ РАН(бессрочно)
3. EBSCO Information Services-EBSCOhost Research Databases(28.02.2017)
4. ООО "ГарантУралСервис"-Гарант(31.12.2022)

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	615 (3)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows 10, MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+.
Лабораторные занятия	626 (3)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows 10, MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, UserGate 7