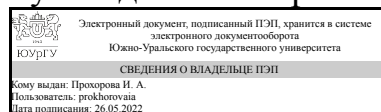


УТВЕРЖДАЮ:
Руководитель направления



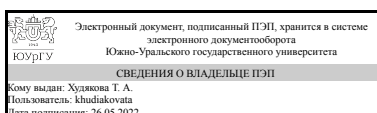
И. А. Прохорова

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.15 Информационная безопасность
для направления 09.03.03 Прикладная информатика
уровень Бакалавриат
форма обучения очная
кафедра-разработчик Цифровая экономика и информационные технологии

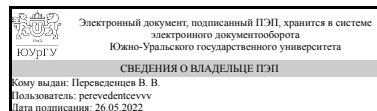
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика, утверждённым приказом Минобрнауки от 19.09.2017 № 922

Зав.кафедрой разработчика,
Д.ЭКОН.Н., доц.



Т. А. Худякова

Разработчик программы,
старший преподаватель



В. В. Переведенцев

1. Цели и задачи дисциплины

Цель дисциплины - изучение принципов обеспечения информационной безопасности государства, подходов к анализу угроз его информационной инфраструктуры и освоение дисциплинарных компетенций для решения задач защиты информации в информационных системах, а также формирование фундаментальных знаний в области информационной безопасности. Задачи дисциплины: - сформировать общее представление об информационной безопасности как о состоянии защищенности информационного ресурса сложной системы, понимание необходимости системного подхода к практической реализации такого состояния; - передать знания о порядке организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации; - сформировать навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

Краткое содержание дисциплины

Защищенность информационной среды организации — одно из основных условий ее эффективного функционирования. Комплекс мероприятий по обеспечению информационной безопасности информационной среды должен быть неотъемлемой частью системы управления любой организации. В настоящее время, персональные компьютеры (рабочие станции) пользователей, как правило, подключены к глобальной сети Интернет. Знания и умения пользователя по обеспечению информационной безопасности персонального компьютера, работающего в «агрессивной» сетевой среде, становятся одними из самых востребованных и необходимых. Данная дисциплина обеспечивает знакомство студента с теоретическими основами криптографии, инструментальными средствами и стандартами, поддерживающими разработку криптографического обеспечения информационных систем, практическими приемами защиты рабочих станций и серверов

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-2 Способен разрабатывать и адаптировать прикладное программное обеспечение	Знает: Знание современных законов, стандартов, методов и технологий в области защиты информации. Умеет: Использовать современные программно-аппаратные средства защиты информации. Находить потенциальные уязвимости в коде приложений. Имеет практический опыт: Владения современными методами и средствами обеспечения защиты информации.
ПК-4 Способен разрабатывать базы данных ИС с учетом требований информационной безопасности, осуществлять ведение базы данных и поддержку информационного обеспечения решения прикладных задач.	Знает: Принципы безопасного проектирования базы данных информационных систем. Умеет: Обосновывать экономическую оправданность информационной защиты. Имеет практический опыт: Оценки

защищенности базы данных информационных систем.

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.Ф.09 Высокоуровневые методы информатики и программирования, 1.Ф.04 Численные методы в компьютерных расчетах, 1.Ф.07 Теория, методы и средства параллельной обработки информации	1.Ф.23 Практикум по виду профессиональной деятельности, 1.Ф.13 Информационные системы управленческого учета

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

Дисциплина	Требования
1.Ф.04 Численные методы в компьютерных расчетах	Знает: Машинное представление целых чисел. Ошибки программирования, связанные с переполнением целочисленных переменных. Машинное представление действительных чисел. Точность представления действительных чисел. Неустойчивые алгоритмы. Численные методы, Численных методов решения скалярных уравнений и систем линейных уравнений, численных методов аппроксимации, методов численного дифференцирования и интегрирования, численных методов решения обыкновенных дифференциальных уравнений и уравнений в частных производных. Теоретическое обоснование вышеперечисленных методов, анализ их точности, условий применимости и других свойств., Стандарты представления чисел в ЭВМ; математический пакет программ с открытыми кодами GNU Octave, предназначенный для решения инженерных и экономических задач в специализированной вычислительной среде. Умеет: Применять численные методы для решения нелинейных уравнений, задач интерполирования, дифференцирования и интегрирования, обыкновенных дифференциальных уравнений. , Правильно выбирать численный метод, опираясь на анализ характера поставленной задачи и знание свойств соответствующих численных методов; анализировать точность (погрешность) полученного численного решения, в том числе давать рекомендации по возможности достижения требуемой точности; грамотно реализовывать расчетные формулы методов, используя алгоритмические языки

	<p>программирования или специальные средства математических пакетов прикладных программ., Правильно выбирать типы данных и математические методы при выполнении финансовых расчетов; применять встроенный язык программирования GNU Octave для решения инженерных и экономических задач. Имеет практический опыт: Оценки сложности алгоритмов; владения графическими средствами визуализации результатов решения прикладных задач., построения расчетных формул, анализа сходимости и точности методов; использования инструментальной базы для реализации численных методов на ПК., Применения численных методов при решении прикладных задач с учетом имеющихся вычислительных ресурсов и графических средств визуализации результатов решения инженерных и экономических задач.</p>
1.Ф.07 Теория, методы и средства параллельной обработки информации	<p>Знает: Архитектуру параллельных вычислительных систем. Методологию разработки параллельных алгоритмов. Основы оценки эффективности параллельных вычислительных систем. Умеет: Параллелизировать проекты в среде MS Visual Studio с поддержкой MPI. Имеет практический опыт: Применения стандартов OpenMP и MPI.</p>
1.Ф.09 Высокоуровневые методы информатики и программирования	<p>Знает: Способы тестирования программного обеспечения., Основные понятия реляционных баз данных., Способы и приёмы программирования приложений. Языки программирования С++ и С#. Умеет: Тестировать компоненты программного обеспечения ИС., Осуществлять ведение базы данных, используя возможности современных языков программирования., Разрабатывать и адаптировать прикладное программное обеспечение. Имеет практический опыт: Использования различных отладочных средств для тестирования программного обеспечения., Работы с различными системами управления базами данных, в частности, MS Access и MS SQL Server., Использования интегрированной среды разработки программных продуктов Microsoft Visual Studio.</p>

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 54,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра

		7
Общая трудоёмкость дисциплины	108	108
<i>Аудиторные занятия:</i>	48	48
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16
Лабораторные работы (ЛР)	0	0
<i>Самостоятельная работа (СРС)</i>	53,75	53,75
Совместная работа, организация взаимодействия команды на основе внешних решений	20,75	20.75
Работа в письменной форме с устным докладом	18	18
Подготовка к зачету	15	15
Консультации и промежуточная аттестация	6,25	6,25
Вид контроля (зачет, диф.зачет, экзамен)	-	зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Информационная безопасность и уровни ее обеспечения.	2	2	0	0
2	Криптографические способы защиты информации	6	4	2	0
3	Антивирусная защита	4	2	2	0
4	Информационная безопасность вычислительных сетей. Одноранговые сети, построение, безопасность, настройка маршрутизации	14	10	4	0
5	Доменные сети. построение, администрирование	10	6	4	0
6	Системы доступа, фаерволы, маршрутизация	12	8	4	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Основные понятия информационной безопасности. Классификация угроз. Классификация средств защиты информации. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности	2
2-3	2	Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Простые криптосистемы. Шифрование методом замены (подстановки). Одноалфавитная подстановка. Многоалфавитная одноконтурная обыкновенная подстановка. Таблицы Вижинера. Многоалфавитная одноконтурная монофоническая подстановка. Многоалфавитная многоконтурная подстановка. Шифрование методом перестановки. Простая перестановка. Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований.	4

		Комбинированные методы шифрования. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Общая схема алгоритма IDEA	
4	3	Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы	2
5-7	4	Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты. Уровень защиты рабочих станций и сетевых серверов. Уровень защиты почты. Уровень защиты шлюзов. Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети. Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Маршрутизация в сетях на основе TCP/IP	6
8-9	4	Цифровая подпись. Установление подлинности объекта. Управление ключами. Безопасность на прикладном уровне: PGP и S/MIME. Безопасность на транспортном уровне: SSL и TLS. Безопасность на сетевом уровне: IP SEC. Брандмауэры. Определение типов брандмауэров. Разработка конфигурации межсетевого экрана. Построение набора правил межсетевого экрана. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. Анализаторы системных вызовов. Анализаторы поведения приложений. Контроллеры целостности файлов. Сетевые IDS. Установка IDS. Определение целей применения IDS. Управление IDS	4
10-12	5	Доменная организация сетей	6
13-14	6	Системы обеспечения сервисов, серверы доступа, серверы приложений, доменная организация прав пользователей	4
15-16	6	Роутеры, оборудование предоставления доступа. Инструменты управления правами пользователей в доменной структуре	4

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	2	Настройка и проверка защищенности Internet коммуникаций. Использование и защита почтовых протоколов. Использование PGP и GPG для обеспечения конфиденциальности электронной почты и шифрования файлов. Использование PKI (инфраструктуры открытых ключей) для защиты электронной почты и web-коммуникаций	2
2	3	Компьютерные вирусы и информационная безопасность; Классификация компьютерных вирусов. Виды "вирусоподобных" программ; Утилиты скрытого администрирования. Особенности работы антивирусных программ; Классификация антивирусных программ; Правила защиты от компьютерных вирусов. Обнаружение загрузочного вируса; Обнаружение загрузочного вируса.	2
3	4	Конфигурирование VirtualBox, распределение студентов на рабочие группы	2
4	4	Настройка одноранговых сетей	2
5	5	Установка серверной ОС, настройка контроллера домена	2
6	5	Включение в домен серверов и рабочих станций	2
7-8	6	Настройка брандмауэров и фаерволов в тестовом домене. Настройка системы	4

		доступа к внешним для тестовой сети сервисам. Контроль трафика, ограничение доступа пользователей внутренней сети	
--	--	---	--

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
Совместная работа, организация взаимодействия команды на основе внешних решений	https://docs.google.com/	7	20,75
Работа в письменной форме с устным докладом	https://www.youtube.com/c/NETVN82 https://www.youtube.com/playlist?list=PLF27492BD5FCA29C0	7	18
Подготовка к зачету	Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с.; Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 108 с. ; Никифоров, С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2019. — 160 с. ; Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — 2-е изд., испр. — Санкт-Петербург : Лань, 2020. — 124 с.	7	15

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	7	Текущий контроль	Установка одноранговой сети	1	5	Группа делится на мини группы по 2 человека. Каждой подгруппе выдается индивидуальное задание, связанное с созданием виртуальной машины и одноранговой сети. При оценивании	зачет

					<p>результатов работы используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). 5 баллов выставляется если студент демонстрирует правильно созданную одноранговую сеть, проведено правильное конфигурирование виртуальных машин, правильно и четко отвечает на вопросы по работе, понимает и разбирается в терминах; 4 балла выставляется если студент демонстрирует правильно созданную одноранговую сеть, виртуальная машина сконфигурирована с ошибками, понимает и разбирается в терминах, отвечает на вопросы преподавателя с уточнением; 3 балла выставляется если студент демонстрирует созданную одноранговую сеть и виртуальную машину, но есть замечание по проделанной работе, правильно и четко отвечает на вопросы, понимает и разбирается в терминах; 2 балла выставляется если студент демонстрирует созданную одноранговую сеть, но есть замечание по проделанной работе, виртуальная машина сконфигурирована с замечаниями, на вопросы отвечает с уточнением; 1 балл выставляется если студент создал одноранговую сеть с грубыми ошибками, виртуальная машина сконфигурирована с замечаниями, на вопросы преподавателя отвечает с замечаниями; 0 баллов выставляется если студент не демонстрирует одноранговую сеть, виртуальная машина сконфигурирована неверно или не может ответить на вопросы преподавателя.</p>		
2	7	Текущий контроль	Установка виртуальной машины для стенда	1	5	<p>Группа делится на мини группы по 2 человека. Каждой подгруппе выдается индивидуальное задание, связанное с созданием виртуальной машины. При оценивании результатов работы используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). 5 баллов выставляется если студент демонстрирует правильно созданную сеть виртуальных машин, проведено правильное конфигурирование виртуальных машин, правильно и четко отвечает на вопросы по работе, понимает и разбирается в терминах; 4 балла выставляется если студент демонстрирует конфигурацию виртуальных машин с</p>	зачет

						ошибками, но при защите с помощью преподавателя исправляет их, понимает и разбирается в терминах, отвечает на вопросы преподавателя с уточнением; 3 балла выставляется если студент демонстрирует созданные виртуальные машины с ошибками, правильно и четко отвечает на вопросы, понимает и разбирается в терминах; 2 балла выставляется если студент демонстрирует созданную сеть виртуальных машин с ошибками и при защите не все ошибки может исправить, на вопросы отвечает с уточнением; 1 балл выставляется если студент создал сеть виртуальных машин с грубыми ошибками, на вопросы преподавателя отвечает с замечаниями; 0 баллов выставляется если студент не демонстрирует виртуальную машину или не может ответить на вопросы преподавателя.	
3	7	Текущий контроль	Защита доклада	1	6	Для подготовки к докладу студентам выдаются темы для самостоятельного изучения. Доклад по теме готовится индивидуально. Защита доклада сопровождается презентацией, ответами 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: - содержание: 2 балла – содержание полностью соответствует теме доклада, тема раскрыта полностью; 1 балл – содержание доклада не полностью соответствует теме и/или раскрыты не все аспекты темы; 0 баллов – содержание доклада не соответствует теме. - - оформление: 2 балла – презентация оформлена в соответствии с выданным заданием; 1 балл – в презентации выявлены недочеты; 0 баллов – студент неверно оформил презентацию или не выполнил задание. - срочность: 2 балла – доклад защищен в назначенный срок; 1 балл – доклад защищен на следующем занятии или консультации, после назначенного срока; 0 баллов – доклад защищен позднее, чем на следующем занятии или консультации.	зачет
4	7	Промежуточная аттестация	Зачет	-	15	Зачет проводится в устной форме. Каждому студенту выдается билет с 3 вопросами. Время на подготовку отводится 30 минут. За каждый вопрос	зачет

					выставляется баллы. Максимальный балл за вопрос - 5. 5 баллов - Грамотный полный (развернутый) ответ на теоретический вопрос; 4 балла - дан правильный, но краткий ответ на вопрос; 3 балла - дан в общем правильный ответ на вопрос, но с замечаниями; 2 балла - дан неполный ответ на вопрос, но на уточняющие вопросы отвечено; 1 балл - дан неправильный ответ на вопрос, но на уточняющие вопросы даны правильные ответы; 0 -баллов - ответ на вопрос не дан.
--	--	--	--	--	--

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	На зачете происходит оценивание знаний, умений и приобретенного опыта обучающихся по дисциплине "... " на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля. При недостаточной и/или не устраивающей студента величине рейтинга ему может быть предложено пройти собеседование с преподавателем по основным разделам дисциплины. В результате складывается совокупный рейтинг студента, который позволяет получить зачет по дисциплине, который проставляется в ведомость, зачетную книжку студента. Зачтено: Величина рейтинга обучающегося по дисциплине 60% и более. Не зачтено: Величина рейтинга обучающегося по дисциплине 0...59 %.	В соответствии с пп. 2.5, 2.6 Положения

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ			
		1	2	3	4
ПК-2	Знает: Знание современных законов, стандартов, методов и технологий в области защиты информации.	+	+	+	+
ПК-2	Умеет: Использовать современные программно-аппаратные средства защиты информации. Находить потенциальные уязвимости в коде приложений.	+	+	+	+
ПК-2	Имеет практический опыт: Владения современными методами и средствами обеспечения защиты информации.		+		+
ПК-4	Знает: Принципы безопасного проектирования базы данных информационных систем.	+	+	+	+
ПК-4	Умеет: Обосновывать экономическую оправданность информационной защиты.			+	+
ПК-4	Имеет практический опыт: Оценки защищенности базы данных информационных систем.	+			+

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

1. Олифер, В. Г. Компьютерные сети : принципы, технологии, протоколы [Текст] учеб. для вузов по направлению 552800 "Информатика и вычисл. техника" и по специальностям 220100 "Вычисл. машины, комплексы, системы и сети", 220200 "Автоматизир. системы обработки информ. и упр.", 220400 "Програм. обеспечение вычисл. техники и автоматизир. систем" В. Г. Олифер, Н. А. Олифер. - 3-е изд. - СПб. и др.: Питер, 2008. - 957 с. ил.

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. Назаров С.В. Администрирование локальных сетей Windows NT/2000/.NET. Учеб. пособие. 2-е изд., перераб. и доп. – М.: Финансы и статистика, 2008.

2. Цилькер Б.Я., Орлов С.А. Организация ЭВМ и систем. Учебник для вузов. – СПб.: Питер. 2007.

г) методические указания для студентов по освоению дисциплины:

1. Цилькер Б.Я., Орлов С.А. Организация ЭВМ и систем. Учебник для вузов. – СПб.: Питер. 2007.

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Методические пособия для самостоятельной работы студента	Электронно-библиотечная система издательства Лань	Баринов, В.В. Технологии разработки и создания компьютерных сетей на базе аппаратуры D-LINK. Учебное пособие для вузов. [Электронный ресурс] / В.В. Баринов, А.В. Благодаров, Е.А. Богданова, А.Н. Пылькин. — Электрон. дан. — М. : Горячая линия-Телеком, 2013. — 216 с. https://e.lanbook.com/book/11826
2	Основная литература	Электронно-библиотечная система издательства Лань	Чекмарев, Ю.В. Вычислительные системы, сети и телекоммуникации. [Электронный ресурс] — Электрон. дан. — М. : ДМК Пресс, 2009. — 184 с. — Режим доступа: http://e.lanbook.com/book/1146 — Загл. с экрана.
3	Основная литература	Электронно-библиотечная система издательства Лань	Платунова, С.М. Администрирование вычислительных сетей на базе MS Winsows Server 2008. Учебное пособие. [Электронный ресурс] — Электрон. дан. — СПб. : НИУ ИТМО, 2012. — 41 с. https://e.lanbook.com/book/70799
4	Дополнительная литература	Электронно-библиотечная система издательства Лань	Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-

			библиотечная система. — URL: https://e.lanbook.com/book/165837 (дата обращения: 22.01.2022). — Режим доступа: для авториз. пользователей.
5	Дополнительная литература	Электронно-библиотечная система издательства Лань	Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 108 с. — ISBN 978-5-8114-8370-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/175506 (дата обращения: 22.01.2022). — Режим доступа: для авториз. пользователей.
6	Дополнительная литература	Электронно-библиотечная система издательства Лань	Никифоров, С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2019. — 160 с. — ISBN 978-5-8114-4042-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114699 (дата обращения: 22.01.2022). — Режим доступа: для авториз. пользователей.
7	Дополнительная литература	Электронно-библиотечная система издательства Лань	Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2019. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/125739 (дата обращения: 22.01.2022). — Режим доступа: для авториз. пользователей.
8	Основная литература	Электронно-библиотечная система издательства Лань	Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — 2-е изд., испр. — Санкт-Петербург : Лань, 2020. — 124 с. — ISBN 978-5-8114-4404-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/133924 (дата обращения: 22.01.2022). — Режим доступа: для авториз. пользователей.
9	Основная литература	Образовательная платформа Юрайт	Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741 (дата обращения: 22.01.2022).

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)

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Зачет, диф. зачет	141 (3б)	Компьютерная техника с предустановленным программным обеспечением, проектор
Самостоятельная работа студента	141 (3б)	Компьютерная техника с предустановленным программным обеспечением, проектор
Практические занятия и семинары	141 (3б)	Компьютерная техника с предустановленным программным обеспечением, проектор
Лекции	141 (3б)	Компьютерная техника с предустановленным программным обеспечением, проектор