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: Буслаева О. С.
Пользователь: buslaevaos
Дата подписания: 09.06.2025

О. С. Буслаева

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.11 Введение в информационную безопасность
для направления 38.03.05 Бизнес-информатика
уровень Бакалавриат
форма обучения очная
кафедра-разработчик Цифровая экономика и информационные технологии

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 38.03.05 Бизнес-информатика, утверждённым приказом Минобрнауки от 29.07.2020 № 838

Зав.кафедрой разработчика,
д.экон.н., доц.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Худякова Т. А.
Пользователь: khudiakovata
Дата подписания: 09.06.2025

Т. А. Худякова

Разработчик программы,
старший преподаватель

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Переведенцев В. В.
Пользователь: perevedentcevvv
Дата подписания: 06.06.2025

В. В. Переведенцев

Челябинск

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 выполнять работы по проектированию, созданию (модификации) и внедрению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы	Знает: последствия слабой защищенности информационных систем; принципы безопасного проектирования информационных систем на стадиях жизненного цикла; методы сбора данных для проектирования безопасных информационных систем; безопасные техники программирования Умеет: отстаивать позицию важности обеспечения информационной безопасности разрабатываемых информационных систем; определять потенциальные уязвимости и пути по их устранению; формировать входные данные для анализа защищенности информационных систем; находить потенциальные уязвимости в коде приложений

	Имеет практический опыт: оценки защищенности информационных систем на этапах проектирования; использования инструментов тестирования программ
ПК-5 Способен готовить технико-экономическое обоснование проектов по совершенствованию и регламентации бизнес-процессов и ИТ-инфраструктуры предприятия	Знает: основы безопасности информационных систем Умеет: источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации классифицировать и оценивать угрозы информационной безопасности для объекта информатизации Имеет практический опыт: оценки защищенности программных прототипов решения прикладных задач; разработки документации для заказчика по совершенствованию ИС

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.Ф.03 Управление ИТ-инфраструктурой, 1.Ф.15 Проектирование информационных систем, 1.Ф.08 Практикум по видам профессиональной деятельности	1.О.15 Управление проектами внедрения информационных систем

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

Дисциплина	Требования
1.Ф.03 Управление ИТ-инфраструктурой	Знает: современные инструменты и методы управления организацией, в том числе методы планирования деятельности, распределения поручений, контроля исполнения, принятия решений; программные средства и платформы инфраструктуры информационных технологий организаций; современные стандарты информационного взаимодействия систем, основы управления изменениями; оценка (прогнозирование) бюджетов и графиков метод аналогов, экспертные оценки; источники информации, необходимой для профессиональной деятельности; Умеет: собирать и анализировать документацию, полученную от заказчика для решения профессиональных задач; разрабатывать и утверждать регламентную документацию для заказчика по предлагаемым решениям; , разрабатывать регламентные документы; Имеет

	практический опыт: описания бизнес-процессов на основе исходных данных; установки прикладного ПО, необходимого для функционирования ИС в соответствии с заданием;, разработки регламентов управления изменениями согласование и утверждение регламентов управления изменениями; ведения истории изменений базовых элементов конфигурации ИС в соответствии с трудовым заданием;
1.Ф.08 Практикум по видам профессиональной деятельности	Знает: предметную область автоматизации; методы верификации требований к информационной системе; правила деловой переписки, структуру и основные правила разработки презентаций разрабатываемых информационных систем, стандарты и протоколы, используемые для интеграции бизнес-модулей и компонентов в корпоративных информационных системах; современные стандарты информационного взаимодействия систем Умеет: анализировать функциональные и нефункциональные требования к информационной системе; анализировать исходные данные; документировать процессы создания информационных систем на стадиях жизненного цикла, проводить презентации, переговоры, публичные выступления; организовывать эффективные презентации разрабатываемых информационных систем с учетом аудитории, которой представляется презентация, анализировать исходные данные в рамках выполнения работ по созданию (модификации) и сопровождению информационных систем; разрабатывать технологии обмена данными в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению информационными системами Имеет практический опыт: выявления первоначальных требований заказчика к ИС; сбора исходных данных у заказчика; разработки моделей бизнес-процессов; составления технической документации проектов автоматизации и информатизации прикладных процессов, применения соответствующего прикладного программного обеспечения для разработки презентаций; проведения переговоров с заинтересованными лицами, применения различных технологий и инструментов для интеграции; проведения тестирования и отладки модулей и компонент
1.Ф.15 Проектирование информационных систем	Знает: методики описания и средства моделирования бизнес-процессов предприятия заказчика, технологии обследования предприятия, сущность процессного подхода при моделировании бизнес-процессов; технологии

	канонического, автоматизированного и типового проектирования информационных систем; технологии моделирования бизнес-процессов и ИТ инфраструктуры предприятий; возможности типовой ИС, методологии и методы проектирования ИС; отраслевую нормативную техническую документацию Умеет: проводить обследование предприятия; разрабатывать документацию для проектирования информационных систем, применять технологии и методы сбора данных при проведении обследования предприятий и методологии моделирования бизнес-процессов; выполнять технико-экономическое обоснование проектов; применять методологии и методы автоматизированного и типового проектирования информационных систем, выполнять технико-экономического обоснования проектов методологии и методы автоматизированного и типового проектирования ИС; Имеет практический опыт: описания бизнес-процессов; разработки модели бизнес-процессов, выявления первоначальных требований заказчика к ИС; назначения и распределения ресурсов, выполнения технико-экономического обоснования проектов навыками работы с инструментальными средствами, реализующими методологию и методы моделирования данных и бизнес процессов

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 2 з.е., 72 ч., 36,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		7
Общая трудоёмкость дисциплины	72	72
Аудиторные занятия:	32	32
Лекции (Л)	16	16
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	35,75	35,75
Работа в письменной форме с устным докладом	10	10
Совместная работа, организация взаимодействия команды на основе внешних решений	12,75	12.75
Подготовка к зачету	13	13
Консультации и промежуточная аттестация	4,25	4,25
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 . Антивирусная защита	8	4	4	0
3	Информационная безопасность вычислительных сетей. Одноранговые сети, построение, безопасность, настройка маршрутизации. Доменные сети. построение, администрирование	8	4	4	0
4	Системы доступа, фаерволы, маршрутизация	14	6	8	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	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. Комбинированные методы шифрования. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Общая схема алгоритма IDEA	2
3	2	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
4	3	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	2

5	3	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	2
6-7	4	Доменная организация сетей. Системы обеспечения сервисов, серверы доступа, серверы приложений, доменная организация прав пользователей	4
8	4	Роутеры, оборудование предоставления доступа. Инструменты управления правами пользователей в доменной структуре	2

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	2	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	3	Конфигурирование VirtualBox для для проведения лабораторных работ, распределение студентов на рабочие группы	4
5	4	Настройка одноранговых сетей	2
6	4	Установка серверной ОС, настройка контроллера домена	2
7	4	Включение в домен серверов и рабочих станций.	2
8	4	Настройка брандмауеров и фаерволов в тестовом домене. Настройка системы доступа к внешним для тестовой сети сервисам. Контроль трафика, ограничение доступа пользователей внутренней сети	2

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
Работа в письменной форме с устным докладом	https://www.youtube.com/c/NETVN82 https://www.youtube.com/playlist?list=PLF27492BD5FCA29C0	7	10

Совместная работа, организация взаимодействия команды на основе внешних решений	https://docs.google.com/	7	12,75
Подготовка к зачету	Краковский, Ю. М. Методы и средства защиты информации : учебное пособие для вузов / Ю. М. Краковский. — Санкт-Петербург : Лань, 2024. — 272 с.; Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. ; Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с.	7	13

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 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	зачет

						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.	
2	7	Текущий контроль	Установка виртуальной машины для стенда	1	5	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 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 созданныую 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.	зачет

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	Текущий контроль	Тестирование	1	20	Тест состоит из 20 вопросов, позволяющих оценить сформированность компетенций. На ответы отводится 10 минут. Правильный ответ на вопрос соответствует 1 баллу. Неправильный ответ на вопрос соответствует 0 баллов	зачет
5	7	Проме-жуточная аттестация	Зачет	-	15	Зачет проводится в устной форме. Каждому студенту выдается билет с 3 вопросами. Время на подготовку отводится 30 минут. За каждый вопрос 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.	зачет

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 "Информационная безопасность" 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	5
ПК-2	Знает: последствия слабой защищенности информационных систем; принципы безопасного проектирования информационных систем на стадиях жизненного цикла; методы сбора данных для проектирования безопасных информационных систем; безопасные техники программирования	+	+	+	+	+
ПК-2	Умеет: отстаивать позицию важности обеспечения информационной безопасности разрабатываемых информационных систем; определять потенциальные уязвимости и пути по их устранению; формировать входные данные для анализа защищенности информационных систем; находить потенциальные уязвимости в коде приложений	+	+		+	+
ПК-2	Имеет практический опыт: оценки защищенности информационных систем на этапах проектирования; использования инструментов тестирования программ	+	+			+
ПК-5	Знает: основы безопасности информационных систем	+	+	+	+	+
ПК-5	Умеет: источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации классифицировать и оценивать угрозы информационной безопасности для объекта информатизации	+	+	+	+	+
ПК-5	Имеет практический опыт: оценки защищенности программных прототипов решения прикладных задач; разработки документации для заказчика по совершенствованию ИС	+	+			+

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. 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. Переведенцев В.В. Методические указания по дисциплине "Введение в информационную безопасность". Челябинск, ЮУрГУ, 2025
2. Цилькер Б.Я., Орлов С.А. Организация ЭВМ и систем. Учебник для вузов. – СПб.: Питер. 2007.

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Переведенцев В.В. Методические указания по дисциплине "Введение в информационную безопасность". Челябинск, ЮУрГУ, 2025

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
2	Основная литература	Образовательная платформа Юрайт	Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544290 (дата обращения: 10.07.2024).
6	Дополнительная литература	Образовательная платформа Юрайт	Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544029 (дата обращения: 10.07.2024).
7	Дополнительная литература	Образовательная платформа Юрайт	Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/555950 (дата обращения: 10.07.2024).
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	141 (3б)	Компьютерная техника с предустановленным программным обеспечением, проектор
Самостоятельная работа студента	141 (3б)	Компьютерная техника с предустановленным программным обеспечением, проектор
Лекции	141 (3б)	Компьютерная техника с предустановленным программным обеспечением, проектор
Практические занятия и семинары	141 (3б)	Компьютерная техника с предустановленным программным обеспечением, проектор