ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Заведующий выпускающей кафедрой

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколинский Л. Б.
Пользователь: leonid.sokolinsky
Дата подписания: 25.06.2024

Л. Б. Соколинский

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.П0.07 Программирование защищенных интеллектуальных систем
для направления 02.03.02 Фундаментальная информатика и информационные технологии
уровень Бакалавриат
профиль подготовки Интеллектуальные системы
форма обучения очная
кафедра-разработчик Системное программирование

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии, утверждённым приказом Минобрнауки от 23.08.2017 № 808

Зав.кафедрой разработчика,
д.физ.-мат.н., проф.

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколинский Л. Б.
Пользователь: leonid.sokolinsky
Дата подписания: 25.06.2024

Л. Б. Соколинский

Разработчик программы,
старший преподаватель

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Никольская К. Ю.
Пользователь: nikolskaiaki
Дата подписания: 22.06.2024

К. Ю. Никольская

Челябинск

1. Цели и задачи дисциплины

Формирование у обучаемых знаний в области теоретических основ информационной безопасности (ИБ) и защиты информации (ЗИ), умений и навыков практического обеспечения ее защиты, безопасного использования программных средств в системах защиты информации (СЗИ) в вычислительных системах и сетях (ВСС). Цель изучения дисциплины достигается путем решения следующих задач: изучение теоретических положений ИБ, ее средств и методов, особенностей их использования в ВСС, перспектив развития в информационных технологий (ИТ), предметной и смежных с ней областях; повышения уровня профессиональной культуры и исполнительской дисциплины бакалавров, понимание необходимости использования СЗИ в ВВС, в профессиональной деятельности по специальности; освоения основные средств и методов обеспечения ИБ, методик их результативного использования; изучения технических и программно-аппаратных средств ЗИ, их основных характеристик; приобретения умений и навыков работы с СЗИ.

Краткое содержание дисциплины

Дисциплина посвящена изучению существующих технологий и программно-аппаратных средств защиты компьютерных сетей. В содержание дисциплины входят четыре основные направления: компьютерные вирусы и средства антивирусной защиты; стандарты защищенности информации в компьютерных системах; блокчейн; машинное обучение в задачах информационной безопасности и др. В ходе изучения дисциплины студенты получают знания о современных технологиях защиты информации. Также студенты учатся разбираться с многообразием законодательных актов Российской Федерации и международных стандартах в области защиты информации.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-3 Способен выявлять требования к программному обеспечению для покрытия тестами, проводить оценку соответствия системы техническому заданию	Знает: основные регламенты и стандарты по проведению тестирования программного обучения на предмет уязвимостей, законы по информационной безопасности Умеет: основные регламенты и стандарты по проведению тестирования программного обучения на предмет уязвимостей, законы по информационной безопасности Имеет практический опыт: разработки протоколов тестирования и наборов тестов для проведения тестирования программного обеспечения на предмет уязвимостей
ПК-4 Способен участвовать в организации подготовительных мероприятий по реализации проектов, а также участвовать в реализации и сопровождении проекта	Знает: основную нормативно-правовую базу в области информационной безопасности Умеет: разрабатывать подходы, согласно действующих норм, для создания безопасных информационных систем Имеет практический опыт: применения

	стандартов в области информационной безопасности

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Информационные системы, Программная инженерия	Не предусмотрены

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

Дисциплина	Требования
Информационные системы	Знает: основные справочные системы и достоверные источники информации о конфигурировании в системе 1С:Предприятие и прочих ERP-системах, основы устройства и администрирования программного обеспечения информационных систем, в том числе систем управления предприятием класса ERP, типовых решений фирмы 1С и сферу их применения, основные этапы разработки и средства разработки информационных систем, средства разработки в составе систем класса ERP на примере системы SAP ERP, основные объекты системы программ 1С:Предприятие и особенности их использования Умеет: осуществлять поиск информации в справочных информационных системах, ее хранение, обработку и анализ, представлять полученную информацию в нужном формате, выполнять установку системы программ 1С:Предприятие и производить предварительную настройку установленного программного обеспечения, создавать пользователей с различными правами доступа к объектам, задавать роли для групп пользователей, создавать собственную конфигурацию в файл-серверном варианте, формулировать и отлаживать запросы к созданной базе данных, а также программный код на встроенном языке системы программ 1С:Предприятие Имеет практический опыт: работы со справочной информацией по платформе 1С:Предприятие, выполнять установку системы программ 1С:Предприятие и производить предварительную настройку установленного программного обеспечения, создавать пользователей с различными правами доступа к объектам, задавать роли для групп пользователей, создания для системы программ 1С:Предприятие конфигурации "с нуля", описания и определения событий, происходящих

	в ней
Программная инженерия	Знает: этапы разработки программного обеспечения, способы выявления и формализации требований заказчика, методы и средства проектирования программного обеспечения Умеет: выявлять ключевые требования заказчика и описывать их на языке uml , применять UML для описания требований к программе и описания архитектуры программной системы Имеет практический опыт: составления диаграммы вариантов использования системы и плана тестирования программного обеспечения, анализа предметной области, а также проектирования и реализации приложения

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 56,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	48	48
Лекции (Л)	24	24
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	24	24
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	51,5	51,5
Подготовка к экзамену	30	30
Изучение дополнительного материала по применению методов машинного обучения в задачах информационной безопасности	21,5	21.5
Консультации и промежуточная аттестация	8,5	8,5
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	Правовая защита информации	2	2	0	0
2	Угрозы и меры защиты информации	8	2	6	0
3	Свободное ПО и типы лицензий	2	2	0	0
4	Компьютерные вирусы	2	2	0	0
5	Защита информации в компьютерных сетях	8	2	6	0
6	Введение в защиту информации на современном предприятии	2	2	0	0

7	Управление данными и технологии ИИ в задачах защиты информации	2	2	0	0
8	Современный SOC	2	2	0	0
9	Управление угрозами, уязвимостями и рисками кибербезопасности	2	2	0	0
10	Криптография и ее место в защите информации сегодня	8	2	6	0
11	Современные системы защиты информации	2	2	0	0
12	Безопасность и доверие систем искусственного интеллекта в защите информации	8	2	6	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Правовая защита информации	2
2	2	Угрозы и меры защиты информации	2
3	3	Свободное ПО и типы лицензий	2
4	4	Компьютерные вирусы	2
5	5	Защита информации в компьютерных сетях	2
6	6	Введение в защиту информации на современном предприятии	2
7	7	Управление данными и технологии ИИ в задачах защиты информации	2
8	8	Современный SOC	2
9	9	Управление угрозами, уязвимостями и рисками кибербезопасности	2
10	10	Криптография и ее место в защите информации сегодня	2
11	11	Современные системы защиты информации	2
12	12	Безопасность и доверие систем искусственного интеллекта в защите информации	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	2	Парольная защита	2
2-3	2	Разграничение доступа	4
4-6	5	Анализ сетевого трафика методами машинного обучения	6
7	10	Шифрование-расшифрование	2
8-9	10	Частотный анализ шифров	4
10-12	12	Компьютерное зрение в задачах биометрии	6

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
Подготовка к экзамену	Краковский, Ю. М. Методы защиты	8	30

	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. Режим доступа: для авториз. пользователей.		
Изучение дополнительного материала по применению методов машинного обучения в задачах информационной безопасности	Чио, К. Машинное обучение и безопасность : руководство / К. Чио, Д. Фримэн ; перевод с английского А. В. Снастина. — Москва : ДМК Пресс, 2020. — 388 с. — ISBN 978-5-97060-713-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131707. — Режим доступа: для авториз. пользователей.	8	21,5

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	Проме-жуточная аттестация	Итоговое тестирование	-	40	Экзамен проводится в виде компьютерного тестирования. Тест содержит 40 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 1 балл. За каждый неправильный ответ - 0 баллов.	экзамен
2	8	Текущий контроль	Тестирование по усвоению материала 1 раздела "Правовая защита информации"	2	2	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	экзамен
3	8	Текущий контроль	Тестирование по усвоению материала 2 раздела "Угрозы и меры защиты информации"	2	2	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	экзамен
4	8	Текущий контроль	Тестирование по усвоению материала 3 раздела "Свободное ПО и типы	2	2	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте	экзамен

			лицензий"			начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	
5	8	Текущий контроль	Тестирование по усвоению материала 4 раздела "Компьютерные вирусы"	2	2	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	экзамен
6	8	Текущий контроль	Тестирование по усвоению материала 5 раздела "Защита информации в компьютерных сетях"	2	2	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	экзамен
7	8	Текущий контроль	Тестирование по усвоению материала 6 раздела "Введение в защиту информации на современном предприятии"	2	2	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	экзамен
8	8	Текущий контроль	Тестирование по усвоению материала 7 раздела "Управление данными и технологии ИИ в задачах защиты информации"	2	2	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	экзамен
9	8	Текущий контроль	Тестирование по усвоению материала 8 раздела "Современный SOC"	2	2	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	экзамен
10	8	Текущий контроль	Тестирование по усвоению материала 9 раздела "Управление угрозами, уязвимостями и рисками кибербезопасности"	2	2	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	экзамен
11	8	Текущий контроль	Тестирование по усвоению материала 10 раздела "Криптография и ее место в защите информации сегодня"	5	5	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	экзамен
12	8	Текущий контроль	Тестирование по усвоению материала 11 раздела "Современные системы защиты информации"	5	5	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	экзамен

13	8	Текущий контроль	Тестирование по усвоению материала 12 раздела "Безопасность и доверие систем искусственного интеллекта в защите информации"	5	5	Проводится в виде компьютерного тестирования. Тест содержит 5 равнозначных вопросов. За каждый правильный ответ в тесте начисляется 0,4 балла. За каждый неправильный ответ - 0 баллов.	экзамен
14	8	Текущий контроль	Практическая работа 1 "Парольная защита"	5	5	Защита практической работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задаются 5 вопросов). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Общий балл при оценке складывается из следующих показателей: 5 баллов - работа выполнена правильно, студент ответил на все вопросы и отчет сформирован согласно требованиям. 4 балла - работа выполнена правильно, студент не ответил на 1 вопрос и отчет сформирован согласно требованиям. 3 балла - работа выполнена правильно, студент не ответил на 2 вопроса и отчет сформирован согласно требованиям. 2 балла - работа выполнена правильно, студент не ответил на 4 вопроса или отчет сформирован с нарушениями требований. 1 балл - работа выполнена правильно, студент не ответил на 5 вопросов и отчет сформирован с нарушениями требований. 0 баллов - работа не выполнена.	экзамен
15	8	Текущий контроль	Практическая работа 2 "Разграничение доступа"	5	5	Защита практической работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задаются 5 вопросов). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания	экзамен

						результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Общий балл при оценке складывается из следующих показателей: 5 баллов - работа выполнена правильно, студент ответил на все вопросы и отчет сформирован согласно требованиям. 4 балла - работа выполнена правильно, студент не ответил на 1 вопрос и отчет сформирован согласно требованиям. 3 балла - работа выполнена правильно, студент не ответил на 2 вопроса и отчет сформирован согласно требованиям. 2 балла - работа выполнена правильно, студент не ответил на 4 вопроса или отчет сформирован с нарушениями требований. 1 балл - работа выполнена правильно, студент не ответил на 5 вопросов и отчет сформирован с нарушениями требований. 0 баллов - работа не выполнена.	
16	8	Текущий контроль	Практическая работа 3 "Анализ сетевого трафика методами машинного обучения"	5	5	Защита практической работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задаются 5 вопросов). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Общий балл при оценке складывается из следующих показателей: 5 баллов - работа выполнена правильно, студент ответил на все вопросы и отчет сформирован согласно требованиям. 4 балла - работа выполнена правильно, студент не ответил на 1 вопрос и отчет сформирован согласно требованиям. 3 балла - работа выполнена правильно, студент не ответил на 2 вопроса и отчет сформирован	экзамен

						согласно требованиям. 2 балла - работа выполнена правильно, студент не ответил на 4 вопроса или отчет сформирован с нарушениями требований. 1 балл - работа выполнена правильно, студент не ответил на 5 вопросов и отчет сформирован с нарушениями требований. 0 баллов - работа не выполнена.	
17	8	Текущий контроль	Практическая работа 4 "Шифрование-расшифрование"	5	5	Защита практической работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задаются 5 вопросов). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Общий балл при оценке складывается из следующих показателей: 5 баллов - работа выполнена правильно, студент ответил на все вопросы и отчет сформирован согласно требованиям. 4 балла - работа выполнена правильно, студент не ответил на 1 вопрос и отчет сформирован согласно требованиям. 3 балла - работа выполнена правильно, студент не ответил на 2 вопроса и отчет сформирован согласно требованиям. 2 балла - работа выполнена правильно, студент не ответил на 4 вопроса или отчет сформирован с нарушениями требований. 1 балл - работа выполнена правильно, студент не ответил на 5 вопросов и отчет сформирован с нарушениями требований. 0 баллов - работа не выполнена.	экзамен
18	8	Текущий контроль	Практическая работа 5 "Частотный анализ текста"	5	5	Защита практической работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задаются 5 вопросов). При оценивании результатов	экзамен

						мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Общий балл при оценке складывается из следующих показателей: 5 баллов - работа выполнена правильно, студент ответил на все вопросы и отчет сформирован согласно требованиям. 4 балла - работа выполнена правильно, студент не ответил на 1 вопрос и отчет сформирован согласно требованиям. 3 балла - работа выполнена правильно, студент не ответил на 2 вопроса и отчет сформирован согласно требованиям. 2 балла - работа выполнена правильно, студент не ответил на 4 вопроса или отчет сформирован с нарушениями требований. 1 балл - работа выполнена правильно, студент не ответил на 5 вопросов и отчет сформирован с нарушениями требований. 0 баллов - работа не выполнена.	
19	8	Текущий контроль	Практическая работа 6 "Компьютерное зрение в задачах биометрии"	5	5	Защита практической работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задаются 5 вопросов). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Общий балл при оценке складывается из следующих показателей: 5 баллов - работа выполнена правильно, студент ответил на все вопросы и отчет сформирован согласно требованиям. 4 балла - работа выполнена правильно, студент не ответил на 1 вопрос и отчет сформирован согласно требованиям. 3 балла - работа выполнена	экзамен

						правильно, студент не ответил на 2 вопроса и отчет сформирован согласно требованиям. 2 балла - работа выполнена правильно, студент не ответил на 4 вопроса или отчет сформирован с нарушениями требований. 1 балл - работа выполнена правильно, студент не ответил на 5 вопросов и отчет сформирован с нарушениями требований. 0 баллов - работа не выполнена.	

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
экзамен	При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (Положение о БРС утверждено приказом ректора от 24.05.2019 г. № 179, в редакции приказа ректора от 10.03.2022 г. No 25-13/09). Процедура прохождения промежуточной аттестации осуществляется согласно Положению о текущем контроле успеваемости и промежуточной аттестации (приказ ректора от 27.02.2024 № 33-13/09). Оценка за дисциплину формируется на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля следующим образом: • Отлично: Величина рейтинга обучающегося по дисциплине 85…100 %. • Хорошо: Величина рейтинга обучающегося по дисциплине 75…84 %. • Удовлетворительно: Величина рейтинга обучающегося по дисциплине 60…74 %. • Неудовлетворительно: Величина рейтинга обучающегося по дисциплине 0…59 %. Если студент согласен с оценкой, полученной по результатам текущего контроля, то он может в день, предшествующий промежуточной аттестации дать свое согласие на автомат в личном кабинете. В случае явки студента на промежуточную аттестацию, давшего свое согласие на автомат в личном кабинете, студент имеет право пройти мероприятия текущего контроля по дисциплине на промежуточной аттестации для улучшения своего рейтинга в день ее проведения. Снижение оценки в этом случае запрещено. Если студент не дал согласия в личном кабинете, то он может согласиться с оценкой лично на промежуточной аттестации в день ее проведения. Если студент не согласен с оценкой, то он имеет право пройти контрольно-рейтинговые мероприятия на промежуточной аттестации для улучшения своего рейтинга в день ее проведения. Фиксация результатов учебной деятельности по дисциплине проводится в день промежуточной аттестации на основе согласия студента, данного им в личном кабинете. При отсутствии согласия в журнале дисциплины фиксация результатов происходит при личном присутствии студента. Если студент не дал согласие в личном кабинете и не явился на промежуточную аттестацию – ему выставляется «неявка».	В соответствии с пп. 2.5, 2.6 Положения

	Промежуточная аттестация проводится в форме тестирования. Тестирование проводится в системе edu.susu.ru. Тест содержит 40 вопросов, на выполнение теста дается 60 минут. В этом случае оценка за дисциплину рассчитывается на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля и промежуточной аттестации.	

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
ПК-3	Знает: основные регламенты и стандарты по проведению тестирования программного обучения на предмет уязвимостей, законы по информационной безопасности	+	+									+								
ПК-3	Умеет: основные регламенты и стандарты по проведению тестирования программного обучения на предмет уязвимостей, законы по информационной безопасности	+		+			+	+	+	+		+		+	+					
ПК-3	Имеет практический опыт: разработки протоколов тестирования и наборов тестов для проведения тестирования программного обеспечения на предмет уязвимостей	+													+	+	+			
ПК-4	Знает: основную нормативно-правовую базу в области информационной безопасности	+	+		+						+									
ПК-4	Умеет: разрабатывать подходы, согласно действующих норм, для создания безопасных информационных систем	+				+					+		+							+
ПК-4	Имеет практический опыт: применения стандартов в области информационной безопасности	+																+	+	+

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. Вестник УрФО : Безопасность в информационной сфере Юж.-Урал. гос. ун-т; ЮУрГУ журнал. - Челябинск: Издательство ЮУрГУ, 2011-

г) методические указания для студентов по освоению дисциплины:

1. Методические рекомендации

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Методические рекомендации

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Дополнительная литература	Электронно-библиотечная система издательства Лань	Чио, К. Машинное обучение и безопасность : руководство / К. Чио, Д. Фримэн ; перевод с английского А. В. Снастина. — Москва : ДМК Пресс, 2020. — 388 с. — ISBN 978-5-97060-713-8. — Текст : электронный // Лань : электронно-библиотечная система. Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/131707
2	Основная литература	Электронно-библиотечная система издательства Лань	Леонтьев, А. С. Защита информации : учебное пособие / А. С. Леонтьев. — Москва : РТУ МИРЭА, 2021. — 79 с. — Текст : электронный // Лань : электронно-библиотечная система. Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/182491
3	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. Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/156401
4	Основная литература	Электронно-библиотечная система издательства Лань	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. Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/130184 (дата обращения: 07.12.2021)

Перечень используемого программного обеспечения:

Нет

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
Экзамен	112 (3г)	Персональный компьютер
Лекции	112 (3г)	Персональный компьютер у преподавателя, проектор
Практические занятия и семинары	112 (3г)	Персональный компьютер