Автономная некоммерческая образовательная организация высшего образования «Воронежский экономико-правовой институт» (АНОО ВО «ВЭПИ»)

АНОО ВО "ВОРОНЕЖСКИЙ ЭКОНОМИКО-ПРАВОВОЙ ИНСТИТУТ", АНОО ВО "ВЭПИ", ВЭПИ

Подписано цифровой подписью: АНОО ВО "ВОРОНЕЖСКИЙ ЭКОНОМИКО-ПРАВОВОЙ ИНСТИТУТ", АНОО ВО "ВЭПИ", ВЭПИ
Дата: 23.04.2024 8:58:21 +03'00'

УТВЕРЖДАЮ
Проректор
по учебно-методической работе
_____ А.Ю. Жильников
«23» апреля 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.22 Информационная безопасность
(наименование дисциплины (модуля)

38.05.01 Экономическая безопасность
(код и наименование направления подготовки)

Специализация Экономико-правовое обеспечение экономической безопасности в условиях цифровизации

Квалификация выпускника Специалист
(наименование квалификации)

Форма обучения Очная, заочная
(очная, заочная)

Рекомендована к использованию Филиалами АНОО ВО «ВЭПИ»

Воронеж 2024

Рабочая программа дисциплины (модуля) разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования, утвержденного приказом Минобрнауки России от 14.04.2021 № 293 (ред. От 27.02.2023), учебным планом образовательной программы высшего образования – программы специалитета 38.05.01 Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности в условиях цифровизации».

Рабочая программа рассмотрена и одобрена на заседании кафедры прикладной информатики.

Протокол от «15» апреля 2024 г. № 8

Заведующий кафедрой М.С. Агафонова

Разработчики:

Ст. преподаватель Д.В. Байбеков

1. Цель освоения дисциплины (модуля)

Целью освоения дисциплины (модуля) «Информационная безопасность» является формирование у обучающихся теоретических знаний и практических навыков в области информационной безопасности, изучение основных принципов, методов и средств защиты информации в информационных системах.

2. Место дисциплины (модуля) в структуре образовательной программы высшего образования – программы специалитета

Дисциплина «Информационная безопасность» относится к обязательной части Блока 1 «Дисциплины (модули)».

Для освоения данной дисциплины необходимы результаты обучения, полученные в предшествующих дисциплинах (модулях) и практиках: «Информатика и программирование», «Информационные технологии в экономике», «Информационный менеджмент.

Перечень последующих дисциплин (модулей) и практик, для которых необходимы результаты обучения, полученные в данной дисциплине: «Введение в системы искусственного интеллекта», «Бизнес-разведка», «Кадровая безопасность в цифровой экономике».

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с установленными в образовательной программе высшего образования – программе специалитета индикаторами достижения компетенций

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине (модулю)
ОПК-7. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	**ИОПК 7.1.** Знает и понимает принципы работы и возможности современных информационных технологий, предназначенных для решения задач обеспечения экономической безопасности	ЗНАТЬ – способы сбора, анализа, систематизации, оценки и интерпретации данных, необходимых для решения профессиональных задач – основные методы, способы и средства получения, хранения, переработки информации, навыки работы с компьютером как средством управления информацией, современные принципы работы с деловой информацией- – основные понятия, свойства, классификацию и этапы развития информационных технологий и систем, современные принципы работы с информационно-коммуникационными технологиями, методы и средства управления информацией и управление с помощью

		информации в целях обеспечения экономической безопасности; – основные принципы работы информационных технологий и систем для обеспечения экономической безопасности. УМЕТЬ – понимать принципы работы современных информационных технологий и использовать их для решения задач обеспечения информационной безопасности; ВЛАДЕТЬ – принципами работы современных информационных технологий с учетом обеспечения информационной безопасности – навыками работы с современными информационными технологиями для автоматизации процессов обеспечения экономической безопасности.
	ИОПК 7.2 Использует современные информационные технологии для решения задач профессиональной деятельности	ЗНАТЬ – особенности обеспечения информационной безопасности. УМЕТЬ – использовать информационно-коммуникационные технологии в экономической сфере деятельности предприятий или организаций; – использовать современные информационные технологии для решения задач профессиональной деятельности. ВЛАДЕТЬ – принципами работы современных информационных технологий с учетом обеспечения информационной безопасности – навыками работы с современными информационными технологиями для автоматизации процессов обеспечения экономической безопасности.

4. Структура и содержание дисциплины (модуля)

4.1. Структура дисциплины (модуля)

4.1.1. Объем дисциплины (модуля) и виды учебной работы по очной форме обучения:

Вид учебной работы		Всего часов	Семестр	
			№7	№ 8
			часов	часов
Контактная работа (всего):		128	68	60
В том числе: Лекции (Л)		64	34	30
Практические занятия (Пр)		64	34	30
Лабораторная работа (Лаб)				
Самостоятельная работа обучающихся (СР)		106	40	66
Промежуточная аттестация	Форма промежуточной аттестации		З	Э
	Количество часов	18		18
Общая трудоемкость дисциплины (модуля)	Часы	252	108	126
	Зачетные единицы	3		4

4.1.2. Объем дисциплины (модуля) и виды учебной работы по заочной форме обучения:

Вид учебной работы		Всего часов	Курс
			№ 5
			часов
Контактная работа (всего):		36	36
В том числе: Лекции (Л)		18	18
Практические занятия (Пр)		18	18
Лабораторная работа (Лаб)			
Самостоятельная работа обучающихся (СР)		203	203
Промежуточная аттестация	Форма промежуточной аттестации	З,Э	З,Э
	Количество часов	13	13
Общая трудоемкость дисциплины (модуля)	Часы	252	252
	Зачетные единицы	7	7

4.2. Содержание дисциплины (модуля)

4.2.1. Содержание дисциплины (модуля) по очной форме обучения

Наименование раздела, темы	Код компетенции, код индикатора достижения компетенции	Количество часов, выделяемых на контактную работу, по видам учебных занятий			Кол-во часов СР	Виды СР	Контроль
		Л	Пр	Лаб			
Тема 1. Проблема обеспечения ИБ. Основные понятия	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	4	3	-	10	Сбор, обработка и систематизация информации	сообщение
Тема 2. Угрозы ИБ	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	4	3	-	10	Анализ используемого материала. Разработка плана доклада	доклад
Тема 3. Основы теории ИБ	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	4	4	-	10	Анализ используемого материала. Разработка плана доклада	опрос
Тема 4. Оценка эффективности систем защиты информации	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	4	4	-	10	Сбор, обработка и систематизация информации	сообщение

Наименование раздела, темы	Код компетенции, код индикатора достижения компетенции	Количество часов, выделяемых на контактную работу, по видам учебных занятий			Кол-во часов СР	Виды СР	Контроль
		Л	Пр	Лаб			
Тема 5. Нормативные руководящие документы в сфере обеспечения ИБ	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	3	3	-	10	Анализ используемого материала. Разработка плана доклада	доклад
Тема 6. Программно-технические средства обеспечения ИБ	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	3	3	-	10	Анализ проведенного исследования	опрос
Тема 7. Межсетевые экраны	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	3	3	-	10	Сбор, обработка и систематизация информации	сообщение
Тема 8. Борьба с компьютерными вирусами	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	3	3	-	12	Сбор, обработка и систематизация информации	сообщение
Тема 9. Криптографические методы	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	3	3	-	12	Анализ используемого материала. Разработка плана доклада	доклад

Наименование раздела, темы	Код компетенции, код индикатора достижения компетенции	Количество часов, выделяемых на контактную работу, по видам учебных занятий			Кол-во часов СР	Виды СР	Контроль
		Л	Пр	Лаб			
Тема 10. Построение защищённых виртуальных сетей	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	3	3	-	12	Анализ используемого материала. Разработка плана доклада	опрос
Обобщающее занятие			2				зачет с оценкой
ВСЕГО ЧАСОВ:		34	34	-	106		

Тема 1. Проблема обеспечения ИБ. Основные понятия – 17 ч.

Лекции – 4 ч. Содержание: Основные понятия ИБ. Информация, защищаемая информация, ценность информации, уровень секретности. Объекты защиты информации. Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.

Практические занятия – 3 ч.

Вопросы:

1. Объекты защиты информации.
2. Информация, защищаемая информация, ценность информации, уровень секретности.

Темы докладов и научных сообщений:

1. Основные понятия ИБ.
2. Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.

Тема 2. Угрозы ИБ - 17 ч.

Лекции – 4 ч. Содержание: Классификация угроз безопасности: каналы утечки, воздействия. Прямые и косвенные каналы утечки данных.

Практические занятия – 3 ч.

Вопросы:

1. Каналы утечки
2. Косвенные каналы утечки данных.

Темы докладов и научных сообщений:
1. Классификация угроз безопасности.
2. Прямые и косвенные каналы утечки данных.

Тема 3. Основы теории ИБ - 18 ч.

Лекции – 4 ч. Содержание: Модель потенциального нарушителя. Способы мошенничества в информационных системах. Основные способы реализации угроз ИБ. Основные понятия теории ИБ.

Практические занятия – 4 ч.
Вопросы:
1. Модель потенциального нарушителя.
2. Способы мошенничества в информационных системах.

Тема 4. Оценка эффективности систем защиты информации - 18 ч.

Лекции – 4 ч. Содержание: Принципы организации систем обеспечения безопасности данных.

Требования, предъявляемые к системам обеспечения безопасности данных. Понятие мониторов безопасности. Физические средства защиты информации

Практические занятия – 4 ч.
Вопросы:
1. Понятие мониторов безопасности.
2. Физические средства защиты информации

Темы докладов и научных сообщений:
1. Принципы организации систем обеспечения безопасности данных.
2. Требования, предъявляемые к системам обеспечения безопасности данных.

Тема 5. Нормативные руководящие документы в сфере обеспечения ИБ - 16 ч.

Лекции – 3 ч. Содержание: Понятие политики безопасности. Дискреционные политики безопасности. Мандатные политики безопасности Модель безопасности информационных потоков. Показатели эффективности систем защиты информации. Способы оценки эффективности систем защиты информации. Руководящие документы Гостехкомиссии в сфере обеспечения

ИБ.

Практические занятия – 3 ч.
Вопросы:
1. Дискреционные политики безопасности.
2. Способы оценки эффективности систем защиты информации.

Темы докладов и научных сообщений:
1. Понятие политики безопасности.
2. Гостехкомиссии в сфере обеспечения ИБ.

Тема 6. Программно-технические средства обеспечения ИБ - 16 ч.

Лекции – 3 ч. Содержание: Основные понятия теории ИБ. Принципы организации систем обеспечения безопасности данных. Требования, предъявляемые к системам обеспечения безопасности данных. Понятие мониторов безопасности. Физические средства защиты информации

Практические занятия – 3 ч.
Вопросы:
1. Принципы организации систем обеспечения безопасности данных.
2. Понятие мониторов безопасности.

Тема 7. Межсетевые экраны - 16 ч.

Лекции – 3 ч. Содержание: Руководящие документы Гостехкомиссии в сфере обеспечения ИБ. «Общие критерии». Структура. Основные понятия. Программно-технические средства обеспечения ИБ. Межсетевые экраны.

Практические занятия – 3 ч.
Вопросы:
1. Гостехкомиссии в сфере обеспечения ИБ.
2. Программно-технические средства обеспечения ИБ.

Темы докладов и научных сообщений:
1. Руководящие документы Гостехкомиссии в сфере обеспечения ИБ.
2. Межсетевые экраны.

Тема 8. Борьба с компьютерными вирусами - 18 ч.

Лекции – 3 ч. Содержание: Типы компьютерных вирусов. Методы борьбы с компьютерными вирусами.

Практические занятия – 3 ч.
Вопросы:

1. Компьютерные вирусы
2. Борьба с вирусами

Темы докладов и научных сообщений:
1. Типы компьютерных вирусов.
2. Методы борьбы с компьютерными вирусами.

Тема 9. Криптографические методы - 18 ч.

Лекции – 3 ч. Содержание: Федеральный стандарт США на шифрование данных (стандарт DES). Отечественный стандарт на шифрование данных. Шифрование с открытым ключом, алгоритм RSA.

Практические занятия – 3 ч.
Вопросы:
1. Отечественный стандарт на шифрование данных.
2. Алгоритм RSA.

Темы докладов и научных сообщений:
1. Федеральный стандарт США на шифрование данных (стандарт DES).
2. Шифрование с открытым ключом, алгоритм RSA.

Тема 10. Построение защищённых виртуальных сетей - 18 ч.

Лекции – 3 ч. Содержание: Понятие, назначение и основные функции защищённой виртуальной сети. Средства построения защищённой виртуальной сети. Туннелирование в протоколах различных уровней.

Практические занятия – 3 ч.
Вопросы:
1. Средства построения защищённой виртуальной сети.
2. Туннелирование в протоколах различных уровней.

4.2.2. Содержание дисциплины (модуля) по заочной форме обучения

Наименование раздела, темы	Код компетенции, код индикатора достижения компетенции	Количество часов, выделяемых на контактную работу, по видам учебных занятий			Кол-во часов СР	Виды СР	Контроль
		Л	Пр	Лаб			
Тема 1. Проблема обеспечения ИБ. Основные понятия	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	2	2	-	25	Сбор, обработка и систематизация информации	сообщение
Тема 2. Угрозы ИБ	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	2	2	-	25	Анализ используемого материала. Разработка плана доклада	доклад
Тема 3. Основы теории ИБ	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	2	2	-	25	Анализ используемого материала. Разработка плана доклада	опрос
Тема 4. Оценка эффективности систем защиты информации	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	2	2	-	25	Сбор, обработка и систематизация информации	сообщение

Наименование раздела, темы	Код компетенции, код индикатора достижения компетенции	Количество часов, выделяемых на контактную работу, по видам учебных занятий			Кол-во часов СР	Виды СР	Контроль
		Л	Пр	Лаб			
Тема 5. Нормативные руководящие документы в сфере обеспечения ИБ	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	1	1	-	25	Анализ используемого материала. Разработка плана доклада	доклад
Тема 6. Программно-технические средства обеспечения ИБ	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	2	2	-	25	Анализ проведенного исследования	опрос
Тема 7. Межсетевые экраны	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	1	1	-	25	Сбор, обработка и систематизация информации	сообщение
Тема 8. Борьба с компьютерными вирусами	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	2	2	-	25	Сбор, обработка и систематизация информации	сообщение
Тема 9. Криптографические методы	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	2	2	-	27	Анализ используемого материала. Разработка плана доклада	доклад

Наименование раздела, темы	Код компетенции, код индикатора достижения компетенции	Количество часов, выделяемых на контактную работу, по видам учебных занятий			Кол-во часов СР	Виды СР	Контроль
		Л	Пр	Лаб			
Тема 10. Построение защищённых виртуальных сетей	ОПК-7 (ИОПК-7.1, ИОПК-7.2)	2	2	-	25	Анализ используемого материала. Разработка плана доклада	опрос
ВСЕГО ЧАСОВ:		18	18	-	252		

Тема 1. Проблема обеспечения ИБ. Основные понятия – 29 ч.

Лекции – 2 ч. Содержание: Основные понятия ИБ. Информация, защищаемая информация, ценность информации, уровень секретности. Объекты защиты информации. Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.

Темы докладов и научных сообщений:

1. Основные понятия ИБ.
2. Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.

Тема 2. Угрозы ИБ - 29 ч.

Лекции – 2 ч. Содержание: Классификация угроз безопасности: каналы утечки, воздействия. Прямые и косвенные каналы утечки данных.

Темы докладов и научных сообщений:

1. Классификация угроз безопасности.
2. Прямые и косвенные каналы утечки данных.

Тема 3. Основы теории ИБ - 29 ч.

Лекции – 2 ч. Содержание: Модель потенциального нарушителя. Способы мошенничества в информационных системах. Основные способы реализации угроз ИБ. Основные понятия теории ИБ.

Практические занятия – 2 ч.

Вопросы:

1. Модель потенциального нарушителя.
2. Способы мошенничества в информационных системах.

Тема 4. Оценка эффективности систем защиты информации - 29 ч.

Лекции – 2 ч. Содержание: Принципы организации систем обеспечения безопасности данных.

Требования, предъявляемые к системам обеспечения безопасности данных. Понятие мониторов безопасности. Физические средства защиты информации

Практические занятия – 2 ч.

Вопросы:

1. Понятие мониторов безопасности.
2. Физические средства защиты информации

Темы докладов и научных сообщений:

1. Принципы организации систем обеспечения безопасности данных.
2. Требования, предъявляемые к системам обеспечения безопасности данных.

Тема 5. Нормативные руководящие документы в сфере обеспечения ИБ - 27 ч.

Лекции – 1 ч. Содержание: Понятие политики безопасности. Дискреционные политики безопасности. Мандатные политики безопасности Модель безопасности информационных потоков. Показатели эффективности систем защиты информации. Способы оценки эффективности систем защиты информации. Руководящие документы Гостехкомиссии в сфере обеспечения ИБ.

Темы докладов и научных сообщений:

1. Понятие политики безопасности.
2. Гостехкомиссии в сфере обеспечения ИБ.

Тема 6. Программно-технические средства обеспечения ИБ - 29 ч.

Содержание: Основные понятия теории ИБ. Принципы организации систем обеспечения безопасности данных. Требования, предъявляемые к системам обеспечения безопасности данных. Понятие мониторов безопасности. Физические средства защиты информации

Практические занятия – 2 ч.
Вопросы:
1. Принципы организации систем обеспечения безопасности данных.
2. Понятие мониторов безопасности.

Тема 7. Межсетевые экраны - 27 ч.

Содержание: Руководящие документы Гостехкомиссии в сфере обеспечения ИБ. «Общие критерии». Структура. Основные понятия. Программно-технические средства обеспечения ИБ. Межсетевые экраны.

Практические занятия – 2 ч.
Вопросы:
1. Гостехкомиссии в сфере обеспечения ИБ.
2. Программно-технические средства обеспечения ИБ.

Темы докладов и научных сообщений:
1. Руководящие документы Гостехкомиссии в сфере обеспечения ИБ.
2. Межсетевые экраны.

Тема 8. Борьба с компьютерными вирусами - 29 ч.

Содержание: Типы компьютерных вирусов. Методы борьбы с компьютерными вирусами.

Практические занятия – 1 ч.
Вопросы:
1. Компьютерные вирусы
2. Борьба с вирусами

Темы докладов и научных сообщений:
1. Типы компьютерных вирусов.
2. Методы борьбы с компьютерными вирусами.

Тема 9. Криптографические методы - 31 ч.

Лекции – 1 ч. Содержание: Федеральный стандарт США на шифрование данных (стандарт DES). Отечественный стандарт на шифрование данных. Шифрование с открытым ключом, алгоритм RSA.

Темы докладов и научных сообщений:
1. Федеральный стандарт США на шифрование данных (стандарт DES).
2. Шифрование с открытым ключом, алгоритм RSA.

Тема 10. Построение защищённых виртуальных сетей - 29 ч.

Содержание: Понятие, назначение и основные функции защищённой виртуальной сети. Средства построения защищённой виртуальной сети. Туннелирование в протоколах различных уровней.

Практические занятия – 1 ч.
Вопросы:
1. Средства построения защищённой виртуальной сети.
2. Туннелирование в протоколах различных уровней.

5. Оценочные материалы дисциплины (модуля)

Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю) представлены в виде фонда оценочных средств по дисциплине (модулю).

6. Методические материалы для освоения дисциплины (модуля)

Методические материалы для освоения дисциплины (модуля) представлены в виде учебно-методического комплекса дисциплины (модуля).

7. Перечень учебных изданий, необходимых для освоения дисциплины (модуля)

№ п/п	Библиографическое описание учебного издания	Используется при изучении разделов (тем)	Режим доступа
1.	Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт].	Тема 1-10	https://urait.ru/bcode/491249
2.	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт,	Тема 1-10	https://urait.ru/bcode/498844

	2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт].		
3.	Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]	Тема 1-10	https://urait.ru/bcode/493262

8. Перечень электронных образовательных ресурсов, современных профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины (модуля)

8.1. Электронные образовательные ресурсы:

№ п/п	Наименование	Гиперссылка
1.	Министерства науки и высшего образования Российской Федерации:	https://minobrnauki.gov.ru
2.	Министерство просвещения Российской Федерации:	https://edu.gov.ru
3.	Федеральная служба по надзору в сфере образования и науки:	http://obrnadzor.gov.ru/ru/
4.	Федеральный портал «Российское образование»:	http://www.edu.ru/.
5.	Электронно-библиотечная система «Знаниум»:	https://znanium.ru/
6.	Электронная библиотечная система Юрайт:	https://urait.ru/

8.2. Современные профессиональные базы данных и информационные справочные системы:

№ п/п	Наименование	Гиперссылка (при наличии)
1	Информационная система	http://window.edu.ru/catalog/resources?p_rubr=2.2.74.12

	«Единое окно доступа к образовательным ресурсам». Раздел «Математика»:	
2	Общероссийский математический портал (информационная система)	http://www.mathnet.ru/
3	Справочно-правовая система «КонсультантПлюс»	https://www.consultant.ru/edu/
4	Справочно-правовая система «Гарант»	https://study.garant.ru/

9. Материально-техническое обеспечение дисциплины (модуля)

№ п/п	Наименование помещения	Перечень оборудования и технических средств обучения	Состав комплекта лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства
1	Компьютерный холл Аудитория для самостоятельной работы обучающихся	Мебель ученическая; доска ученическая; персональные компьютеры с подключением к сети Интернет	**Операционная система** Windows - Акт приемки-передачи неисключительного права № 9751 от 09.09.2018. Лицензия DreamSparkPremiumElectronicSoftwareDelivery (5 years) Renewal; MicrosoftOffice - Сублицензионный договор от 12.01.2017 № Вж_ПО_123015- 2017. Лицензия OfficeStd 2016 RUS OLP NL Acdmc **Антивирус:** Антивирус Dr.Web Desktop Security Suite - Сублицензионный договор от 27.07.2017 № ЮС-2017-00498; **Программное обеспечение:** 1С:Предприятие 8 - Сублицензионный договор от 02.07.2020 № ЮС-2020-00731; LibreOffice Свободно распространяемое программное обеспечение; 7-Zip Свободно распространяемое программное обеспечение отечественного производства **КонсультантПлюс"** - Договор от 17.05.2023 № 96-2023/RDD; **Справочно-правовая система "Гарант"** - Договор от 30.11.2023 № СК6030/01/24; MicrosoftOffice - Сублицензионный договор от 12.01.2017 № Вж_ПО_123015- 2017. Лицензия OfficeStd 2016 RUS OLP NL Acdmc; **Электронно-библиотечная система «Юрайт»:** Лицензионный договор № 5343 от 23.06.2022 (подписка 01.09.2022-31.08.2025) **Электронно-библиотечная система**

№ п/п	Наименование помещения	Перечень оборудования и технических средств обучения	Состав комплекта лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства
			«Знаниум»: Лицензионный договор № 697эбс от 17.07.2024 (Основная коллекция ЭБС) (подписка 01.09.2024-31.08.2027)
2	243 Учебная аудитория для проведения учебных занятий Лаборатория, оснащенная оборудованием, техническими средствами обучения и материалами Аудитория для проведения занятий семинарского типа Кабинет для курсового проектирования (выполнение курсовых работ) Аудитория для текущего контроля и промежуточной аттестации	Рабочее место преподавателя (стол, стул); мебель ученическая; доска ученическая; персональные компьютеры с подключением к сети Интернет	**Операционная система** Windows - Акт приемки-передачи неисключительного права № 9751 от 09.09.2018. Лицензия DreamSparkPremiumElectronicSoftwareDelivery (5 years) Renewal; MicrosoftOffice - Сублицензионный договор от 12.01.2017 № Вж_ПО_123015- 2017. Лицензия OfficeStd 2016 RUS OLP NL Acdmc **Антивирус:** Антивирус Dr.Web Desktop Security Suite - Сублицензионный договор от 27.07.2017 № ЮС-2017-00498; **Программное обеспечение:** 1С:Предприятие 8 - Сублицензионный договор от 02.07.2020 № ЮС-2020-00731; LibreOffice Свободно распространяемое программное обеспечение; 7-Zip Свободно распространяемое программное обеспечение отечественного производства **КонсультантПлюс"** - Договор от 17.05.2023 № 96-2023/RDD; **Справочно-правовая система "Гарант"** - Договор от 30.11.2023 № СК6030/01/24; MicrosoftOffice - Сублицензионный договор от 12.01.2017 № Вж_ПО_123015- 2017. Лицензия OfficeStd 2016 RUS OLP NL Acdmc; **Электронно-библиотечная система «Юрайт»:** Лицензионный договор № 5343 от 23.06.2022 (подписка 01.09.2022-31.08.2025) **Электронно-библиотечная система «Знаниум»:** Лицензионный договор № 697эбс от 17.07.2024 (Основная коллекция ЭБС) (подписка 01.09.2024-31.08.2027)
3	321 Учебная аудитория для проведения учебных занятий Аудитория для	Рабочее место преподавателя (стол, стул); мебель ученическая; доска	**Операционная система** Windows - Акт приемки-передачи неисключительного права № 9751 от 09.09.2018. Лицензия DreamSparkPremiumElectronicSoftwareDelivery (5 years) Renewal; MicrosoftOffice -

№ п/п	Наименование помещения	Перечень оборудования и технических средств обучения	Состав комплекта лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства
	проведения занятий лекционного типа Аудитория для проведения занятий семинарского типа Аудитория для текущего контроля и промежуточной аттестации	ученическая; баннеры; трибуна для выступлений; компьютер; мультимедийный проектор; колонки; веб-камера	Сублицензионный договор от 12.01.2017 № Вж_ПО_123015- 2017. Лицензия OfficeStd 2016 RUS OLP NL Acdmc **Антивирус:** Антивирус Dr.Web Desktop Security Suite - Сублицензионный договор от 27.07.2017 № ЮС-2017-00498; **Программное обеспечение:** 1С:Предприятие 8 - Сублицензионный договор от 02.07.2020 № ЮС-2020-00731; LibreOffice Свободно распространяемое программное обеспечение; 7-Zip Свободно распространяемое программное обеспечение отечественного производства **КонсультантПлюс"** - Договор от 17.05.2023 № 96-2023/RDD; **Справочно-правовая система "Гарант"** - Договор от 30.11.2023 № СК6030/01/24; MicrosoftOffice - Сублицензионный договор от 12.01.2017 № Вж_ПО_123015- 2017. Лицензия OfficeStd 2016 RUS OLP NL Acdmc; **Электронно-библиотечная система «Юрайт»:** Лицензионный договор № 5343 от 23.06.2022 (подписка 01.09.2022-31.08.2025) **Электронно-библиотечная система «Знаниум»:** Лицензионный договор № 697эбс от 17.07.2024 (Основная коллекция ЭБС) (подписка 01.09.2024-31.08.2027)

Лист регистрации изменений к рабочей программе дисциплины (модуля)

№ п/п	Дата внесения изменений	Номера измененных листов	Документ, на основании которого внесены изменения	Содержание изменений	Подпись разработчика рабочей программы
1					