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: 2023.09.26 10:30:51 +03'00'

УТВЕРЖДАЮ
Проректор
по учебно-методической работе
А.Ю. Жильников
«__» _____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.17 Информационная безопасность
(наименование дисциплины (модуля))

09.03.03 Прикладная информатика
(код и наименование направления подготовки)

Направленность (профиль) Прикладная информатика в экономике
(наименование направленности (профиля))

Квалификация выпускника Бакалавр
(наименование квалификации)

Форма обучения Очная, заочная
(очная, заочная)

Рекомендована к использованию Филиалами АНОО ВО «ВЭПИ»

Воронеж 2023

Рабочая программа дисциплины (модуля) разработана в соответствии с требованиями ФГОС ВО, утвержденного приказом Минобрнауки России от 19.09.2017 № 922 (ред. от 08.02.2021), учебным планом по направлению подготовки 09.03.03 Прикладная информатика, направленность (профиль) «Прикладная информатика в экономике».

Рабочая программа рассмотрена и одобрена на заседании кафедры прикладной информатики.

Протокол от «01» сентября 2023 г. № 1

Заведующий кафедрой М.С. Агафонова

Разработчики:

Ст. преподаватель К.А. Андреева

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 бакалавриата

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: «Вычислительные системы, сети и телекоммуникации», «Базы данных», «Операционные системы», «Информационные системы и технологии».

Перечень последующих дисциплин (модулей) и практик, для которых необходимы результаты обучения, полученные в данной дисциплине: «Проектный практикум».

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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине (модулю)
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	ИУК-1.1. Выполняет поиск, критический анализ и синтез информации для решения поставленных задач.	знать: -основные законы, стандарты в области защиты информации; уметь: -осуществлять поиск и анализ информации, а также определять уровень ее безопасности; владеть: -навыком технической обработки информации .
	ИУК-1.2. Использует системный подход для решения поставленных задач.	знать: -методы обеспечения защиты информации; уметь: -систематизировано использовать аппаратно – программные средства при осуществлении защиты информации; владеть: -средствами защиты информации.
ОПК-2. Способен понимать принципы работы современных информационных технологий и программных средств, в том числе	ИОПК-2.1. Использует принципы работы современных информационных технологий и программных	знать: − современные информационные технологии и программные средства, в том числе

отечественного производства, и использовать их при решении задач профессиональной деятельности	средств, в том числе отечественного производства при решении задач профессиональной деятельности.	отечественного производства при решении задач информационной безопасности; уметь: − правильно выбирать и применять современные информационные технологии и программные средства, в том числе отечественного производства для обеспечения информационной безопасности при решении задач профессиональной деятельности; Владеть: − навыками выбора и применения современных информационных технологий и программных средств, в том числе отечественного производства для обеспечения информационной безопасности при решении задач профессиональной деятельности.

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 № 8 часов
Контактная работа (всего):		68	68
В том числе: Лекции (Л)		34	34
Практические занятия (Пр)		34	34
Лабораторная работа (Лаб)			
Самостоятельная работа обучающихся (СР)		76	76
Промежуточная аттестация	Форма промежуточной аттестации	ЗО	ЗО
	Количество часов		
Общая трудоемкость дисциплины (модуля)	Часы	144	144
	Зачетные единицы	4	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):		20	20
В том числе: Лекции (Л)		10	10
Практические занятия (Пр)		10	10
Лабораторная работа (Лаб)			
Самостоятельная работа обучающихся (СР)		120	120
Промежуточная аттестация	Форма промежуточной аттестации	ЗО	ЗО
	Количество часов	4	4
Общая трудоемкость дисциплины (модуля)	Часы	144	144
	Зачетные единицы	4	4

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	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	4	3	-	8	Сбор, обработка и систематизация информации	сообщение
Тема 2. Угрозы ИБ	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	4	3	-	8	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 3. Основы теории ИБ	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	4	4	-	8	Анализ используемого материала. Разработка плана доклада	опрос
Тема 4. Оценка эффективности систем защиты информации	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	4	4	-	8	Сбор, обработка и систематизация информации	сообщение
Тема 5. Нормативные руководящие документы в сфере обеспечения ИБ	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	3	3	-	8	Анализ используемого материала. Разработка плана доклада	доклад
Тема 6. Программно-технические средства обеспечения ИБ	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	3	3	-	8	Анализ проведенного исследования	опрос
Тема 7. Межсетевые экраны	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	3	3	-	7	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 8. Борьба с компьютерными вирусами	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	3	3	-	7	Сбор, обработка и систематизация информации	сообщение
Тема 9. Криптографические методы	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	3	3	-	7	Анализ используемого материала. Разработка плана доклада	доклад
Тема 10. Построение защищённых виртуальных сетей	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	3	3	-	7	Анализ используемого материала. Разработка плана доклада	опрос
Обобщающее занятие			2				зачет с оценкой
ВСЕГО ЧАСОВ:		34	34	-	76		

Тема 1. Проблема обеспечения ИБ. Основные понятия – 15 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 - 15 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 - 16 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 - 16 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 - 14 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 - 14 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 - 13 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 - 13 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 - 13 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 - 13 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	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	2	-	-	13	Сбор, обработка и систематизация информации	сообщение
Тема 2. Угрозы ИБ	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	2	-	-	13	Анализ используемого материала. Разработка плана доклада	доклад
Тема 3. Основы теории ИБ	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	2	2	-	13	Анализ используемого материала. Разработка плана доклада	опрос
Тема 4. Оценка эффективности систем защиты информации	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	2	2	-	13	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	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	1	-	-	13	Анализ используемого материала. Разработка плана доклада	доклад
Тема 6. Программно-технические средства обеспечения ИБ	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	-	2	-	13	Анализ проведенного исследования	опрос
Тема 7. Межсетевые экраны	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	-	2	-	13	Сбор, обработка и систематизация информации	сообщение
Тема 8. Борьба с компьютерными вирусами	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	-	1	-	13	Сбор, обработка и систематизация информации	сообщение
Тема 9. Криптографические методы	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	1	-	-	8	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	УК-1 (ИУК-1.1, ИУК-1.2) ОПК-2 (ИОПК-2.1)	-	1	-	8	Анализ используемого материала. Разработка плана доклада	опрос
ВСЕГО ЧАСОВ:		10	10	-	120		

Тема 1. Проблема обеспечения ИБ. Основные понятия – 15 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 - 15 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 - 17 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 - 17 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 - 14 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 - 15 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 - 15 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 - 14 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 - 9 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 - 9 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.	Информационная система «Единое окно доступа к образовательным ресурсам»:	http://window.edu.ru/
6.	Единая коллекция цифровых образовательных ресурсов:	http://school-collection.edu.ru/
7.	Федеральный центр информационно-образовательных ресурсов:	http://fcior.edu.ru/
8.	Электронно-библиотечная система «IPRbooks»:	http://www.IPRbooks.ru/
9.	Электронная библиотечная система Юрайт:	https://biblio-online.ru/
10.	База данных электронных журналов:	http://www.iprbookshop.ru/6951.html

8.2. Современные профессиональные базы данных и информационные справочные системы:

№ п/п	Наименование	Гиперссылка (при наличии)
1	Информационная система «Единое окно доступа к образовательным ресурсам». Раздел «Математика»:	http://window.edu.ru/catalog/resources?p_rubr=2.2.74.12
2	Общероссийский математический портал (информационная система)	http://www.mathnet.ru/
3	Справочно-правовая система «КонсультантПлюс»	www.consultant.ru
4	Справочно-правовая система «Гарант»	www.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.	Персональные компьютеры с подключением к сети Интернет	1С:Предприятие 8. Сублицензионный договор от 27.07.2017 № ЮС-2017-00498.Операционная система Windows. Акт приемки-передачи неисключительного права № 9751 от 09.09.2016. Лицензия Dream Spark Premium Electronic Software Delivery (5 years) Renewal. Справочно-правовая система «КонсультантПлюс». Договор от 01.09.2020 № 75-2020/RDD. Справочно-правовая система «Гарант». Договор от 05.11.2014 № СК6030/11/14. Microsoft Office 2007. Сублицензионный договор от 12.01.2016 № Вж_ПО_123015-2016. Лицензия Office Std 2016 RUS OLP NL Acdmc.

№ п/п	Наименование помещения	Перечень оборудования и технических средств обучения	Состав комплекта лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства
			Антивирус ESET NOD32. Сублицензионный договор от 27.07.2017 № ЮС-2017-00498. LibreOffice. Свободно распространяемое программное обеспечение. 7-Zip. Свободно распространяемое программное обеспечение отечественного производства.

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					