федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИЧУРИНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

Кафедра математики, физики и информационных технологий

УТВЕРЖДЕНА
решением учебно-методического совета
университета
(протокол от 22 июня 2023 г. № 10)

УТВЕРЖДАЮ
Председатель учебно-методического
совета университета
___ __ С.В. Соловьев
«22» июня 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки 09.03.01 Информатика и вычислительная техника

Направленность (профиль) Системы автоматизированного проектирования

Квалификация бакалавр

Мичуринск – 2023

1. Цели освоения дисциплины (модуля)

Целями освоения дисциплины является формирование у обучающихся целостного представления о современных организационных, технических, алгоритмических и других методах и средствах защиты компьютерной информации, используемых в современных криптосистемах, знакомство с законодательством и стандартами в этой области.

При освоении данной дисциплины учитываются трудовые функции следующего профессионального стандарта: 06.026 «Системный администратор информационно-коммуникационных систем» Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 5 октября 2015 г. №686н.

2. Место дисциплины в структуре образовательной программы

Согласно учебному плану по направлению подготовки 09.03.01 Информатика и вычислительная техника дисциплина "Защита информации"является дисциплиной обязательной части Блока 1. Дисциплины (модули) (Б1.О.08)

Для освоения дисциплины «Защита информации» обучающиеся используют знания, умения, навыки, сформированные в ходе изучения дисциплин «Информатика», «Информационные технологии».

Материал дисциплины тесно взаимосвязан с такими дисциплинами, как «Администрирование вычислительных систем и сетей», «Сети и телекоммуникации», для прохождения производственных практик, написания выпускной квалификационной работы, подготовки к ГИА.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Управление доступом к программно-аппаратным средствам информационных служб инфокоммуникационной системы. С/02.6

Трудовые действия: Техническая поддержка пользователей в пределах выделенных зон ответственности по вопросам функционирования программного обеспечения на конечных устройствах пользователей.

Освоение дисциплины направлено на формирование следующих компетенций:

ОПК-2. Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности;

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальных компетенций	Критерии оценивания результатов обучения			
		низкий (допороговый, компетенция не сформирована)	пороговый	базовый	продвинутый
ОПК-2. Способен понимать принципы работы современных информационных	ИД-1$_{ОПК-2}$ – знает современные информационные технологии и методы их использования при решении задач профес-	Не знает современные информационные технологии и методы их использования при решении задач профессиональной деятельности.	Слабо знает современные информационные технологии и методы их использования при решении задач профессиональной деятельности.	Хорошо знает современные информационные технологии и методы их использования при решении задач профессиональной деятельности.	Знает и успешно использует существующие современные информационные технологии и методы их использования при решении задач профессиональной дея-

технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	сиональной деятельности.				тельности.
	ИД-2$_{ОПК-2}$- умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности	Не умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности	Слабо умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности	Хорошо умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности	Отлично умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности
	ИД-3$_{ОПК-2}$- владеет способами применения необходимых информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	Не владеет способами применения необходимых информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	Слабо владеет способами применения необходимых информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	Хорошо владеет способами применения необходимых информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	В совершенстве владеет способами применения необходимых информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований ин-	ИД-1$_{ОПК-3}$ Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной без-опасности.	Не знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной без-опасности.	Слабо знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной без-опасности.	Хорошо знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной без-опасности.	Отлично знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной без-опасности.
	ИД-2$_{ОПК-3}$ – Уметь: решать стандартные задачи профессиональной дея-	Не умеет решать стандартные задачи профессиональной деятельности на основе информационной	Слабо умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиогра-	Хорошо умеет решать стандартные задачи профессиональной деятельности на основе информа-	В совершенстве умеет решать стандартные задачи профессиональной деятельности на основе информаци-

формационной безопасности .	тельности на основе информационной и библиографической культуры с применением информационно коммуникационных технологий и с учетом основных требований информационной безопасности.	и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	фической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ционной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	онной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	ИД-З$_{ОПК-3}$ – Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно исследовательской работе с учетом требований информационной безопасности.	Не владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно исследовательской работе с учетом требований информационной безопасности.	Слабо владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно исследовательской работе с учетом требований информационной безопасности.	Хорошо владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно исследовательской работе с учетом требований информационной безопасности.	В совершенстве владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно исследовательской работе с учетом требований информационной безопасности.

В результате изучения дисциплины обучающийся должен:

знать правовые основы защиты компьютерной информации, математические основы криптографии, организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях, стандарты, модели и методы шифрования, методы идентификации пользователей, основы инфраструктуры систем, построенных с использованием публичных и секретных ключей, методы передачи конфиденциальной информации по каналам связи, методы установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных);

уметь применять известные методы и средства поддержки информационной безопасности в компьютерных системах, проводить сравнительный анализ, выбирать методы и средства, оценивать уровень защиты информационных ресурсов в прикладных системах, решать стандартные задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

владеть навыками построения программных систем, использующих сервисы и механизмы безопасности, протоколы аутентификации, навыками построения программных систем, содержащих криптографические алгоритмы шифрования передаваемой информации, алгоритмы простановки и проверки электронной цифровой подписи, алгоритмы хэш-функций, алгоритмы генерации псевдослучайных последовательностей чисел.

3.1 Матрица соотнесения тем/разделов учебной дисциплины и формируемых в них общекультурных и профессиональных компетенций

№	Темы, разделы дисциплины	Компетенции		Σ общее количество компетенций
		ОПК-2	ОПК-3	
1	Основные понятия и определения в области информационной безопасности. Традиционное шифрование: классические методы. Криптостойкость. Алгоритмы генерации псевдослучайных последовательностей чисел.	+	+	2
2	Хэш-функции и аутентификация сообщений. MD5, ГОСТ 3411. Электронная цифровая подпись (ЭЦП). Стандарты ЭЦП: DSS, ГОСТ 3410	+	+	2
3	Блочные и поточные алгоритмы симметричного шифрования. Стандарты и алгоритмы: американский DES, отечественный ГОСТ 28147, режимы их выполнения. Стандарт криптографической защиты 21 века (AES). Алгоритм Rijndael.	+	+	2
4	Асимметричные системы шифрования (системы с открытым ключом). RSA.	+	+	2
5	Криптография с использованием эллиптических кривых. Безопасность современных сетевых технологий. Протоколы аутентификации. Безопасность в открытых сетях. Инфраструктура цифровых сертификатов.	+	+	2

4. Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 5 зачетных единицы (180 ак.часов)

4.1. Объем дисциплины и виды учебной работы

Виды занятий	Количество ак. часов	
	по очной форме обучения 8 семестр	по заочной форме обучения 5 курс
Общая трудоемкость дисциплины	180	180
Контактная работа обучающихся с преподавателем, в т.ч.	72	24
аудиторные занятия, из них	72	24
лекции	24	8
лабораторные работы	48	16
Самостоятельная работа обучающихся	72	147
проработка учебного материала по дисциплине (конспектов лекций, учебников, материалов сетевых ресурсов)	30	90
выполнение индивидуальных заданий	30	30
подготовка к тестированию	12	27
Контроль	36	9
Вид итогового контроля	экзамен	

4.2. Лекции

№	Раздел дисциплины (модуля), темы лекций	Объем в ак. часах		Формируемые компетенции
		очная форма обучения	заочная форма обучения	
Раздел 1. Методы и средства защиты информации: информационная безопасность. Основные определения.				
1.1	Основные понятия и определения в области информационной безопасности. Традиционное шифрование: классические методы. Криптостойкость. Алгоритмы генерации псевдослучайных последовательностей чисел.	6	1	ОПК-3, ОПК-2
1.2	Хэш-функции и аутентификация сообщений. MD5, ГОСТ 3411. Электронная цифровая подпись (ЭЦП). Стандарты ЭЦП: DSS, ГОСТ 3410	4	1	ОПК-3, ОПК-2
Раздел 2. Методы и средства защиты информации.				
2.1	Блочные и поточные алгоритмы симметричного шифрования. Стандарты и алгоритмы: американский DES, отечественный ГОСТ 28147, режимы их выполнения. Стандарт криптографической защиты 21 века (AES). Алгоритм Rijndael.	4	2	ОПК-3, ОПК-2
2.2	Асимметричные системы шифрования (системы с открытым ключом). RSA.	4	2	ОПК-3, ОПК-2
Раздел 3. Криптографические методы защиты информации				
3.1	Криптография с использованием эллиптических кривых. Безопасность современных сетевых технологий. Протоколы аутентификации. Безопасность в открытых сетях. Инфраструктура цифровых сертификатов.	6	2	ОПК-3, ОПК-2
	Итого	24	8	

4.3. Лабораторные занятия

№	Наименование занятия	Объем в ак. часах		лабораторное оборудование и (или) программное обеспечение	Формируемые компетенции
		очная форма обучения	заочная форма обучения		
	Раздел 2. Методы и средства защиты информации.				
2.1	Шифрование информации методами традиционного шифрования. Генерация псевдослучайных	10	2	Microsoft Windows. DreamSpark Premium	

	последовательностей чисел в системах защиты информации.			Microsoft Windows. DreamSpark Premium	ОПК-3, ОПК-2
2.2	Хэш-функции и электронная цифровая подпись.	8	2		
2.3	Изучение американского стандарта шифрования данных DES. Изучение отечественного стандарта шифрования данных (ГОСТ 28147-89). Симметричный криптографический алгоритм с AES – подобной структурой Rijndael.	10	4		
Раздел 3. Криптографические методы защиты информации					
3.1	Асимметричные криптосистемы. Шифрование и электронная цифровая подпись на основе с помощью алгоритма RSA.	12	4	Microsoft Windows. DreamSpark Premium	
3.2	Выработка общего секретного ключа по алгоритму Диффи – Хэллмана.	8	4		
	Итого	48	16		

4.4. Практические занятия

Практические занятия не предусмотрены.

4.5. Самостоятельная работа обучающихся

Раздел дисциплины	Вид самостоятельной работы	Объем ак. часов	
		очная форма обучения	заочная форма обучения
Раздел 1. Методы и средства защиты информации: информационная безопасность. Основные определения.	Проработка учебного материала по дисциплине (конспектов лекций, учебников, материалов сетевых ресурсов)	10	30
	Выполнение индивидуальных заданий	10	10
	Подготовка к тестированию	4	9
Раздел 2. Методы и средства защиты информации.	Проработка учебного материала по дисциплине (конспектов лекций, учебников, материалов сетевых ресурсов)	10	30
	Выполнение индивидуальных заданий	10	10
	Подготовка к тестированию	4	9
Раздел 3. Криптографические методы защиты информации	Проработка учебного материала по дисциплине (конспектов лекций, учебников, материалов сетевых ресурсов)	10	30
	Выполнение индивидуальных заданий	10	10
	Подготовка к тестированию	4	9

Итого		72	147

Методическое пособие для проведения практических занятий по дисциплине «Защита информации» для направления подготовки 09.03.01 Информатика и вычислительная техника. – Мичуринск, 2020.

4.6. Выполнение контрольной работы обучающимися заочной формы

Приступать к выполнению контрольной работы необходимо после изучения материала по литературным источникам, убедившись путем ответов на вопросы для самопроверки, что материал темы усвоен.

Выполнение контрольного задания способствует закреплению знаний при самостоятельном изучении курса, а также вырабатывает навыки в работе при рассмотрении современных методов защиты информации.

Содержание контрольной работы. Структура работы включает в себя следующие основные элементы в порядке их расположения:

- титульный лист;
- содержание;
- введение;
- основная часть (ответы на вопросы задания согласно варианта);
- заключение;
- список использованных источников.

Титульный лист должен содержать сведения о образовательном учреждении, институте и кафедры, где выполнена контрольная работа и информация о обучающемся выполнившего контрольное задание. На титульном листе выпускник ставит свою подпись.

Во введении формулируется основные понятия дисциплины и изучаемого вопроса, место и значение в работе предприятий данной отрасли, а также в науке и практике.

В основной части излагается материал по теме контрольных заданий, выбранных по заданию согласно собственного варианта.

В заключении приводятся обобщенные итог, отражается результат выполненных контрольных заданий, предложения и рекомендации по использованию полученных знаний в изучении последующих дисциплин, а также их применение в производстве.

Текст контрольной работы можно отнести к текстовым документам. Согласно ГОСТ 2.105–95 "ЕСКД. Общие требования к текстовым документам" и ГОСТ 2.106–96 "ЕСКД. Текстовые документы" текстовые документы подразделяются на документы, содержащие в основном сплошной текст (технические описания, расчеты, пояснительные записки, инструкции и т.п.), и текст, разбитый на графы (спецификации, ведомости, таблицы и т.п.).

Если контрольная работа выполняется на компьютере, то текст излагают на одной стороне листа формата А4 с оставлением полей с левой стороны 30 мм, с правой 15 мм, сверху и снизу по 20 мм. Если выполняется от руки, то допускается написание работы в обычной тетради имеющую разбивку – клеточка.

Абзацы в тексте начинают отступом, равным 15-17 мм.

При оформлении контрольной работ с применением компьютерной техники набор текста можно осуществлять шрифтом "Times New Roman" размером 14 с интервалом 1,5.

Опечатки, описки и графические неточности, обнаруженные в процессе выполнения работы, допускается исправлять закрашиванием текстовым корректором и нанесением на том же месте исправленного текста (графики).

Повреждения листов, помарки и следы не полностью удаленного прежнего текста (рисунка) не допускается.

Нумерация страниц должна быть сквозной: первой страницей является титульный лист, второй – содержание, третьей – ответы на вопросы. Номер страницы проставляют в правом верхнем углу. На странице 1 (титульный лист) номер не ставят.

4.7. Содержание разделов дисциплины

Раздел 1. Методы и средства защиты информации: информационная безопасность. Основные определения.

Основные понятия и определения в области информационной безопасности. Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности; классификация атак; модели сетевой безопасности и безопасности информационной системы.

Традиционное шифрование: классические методы. Криптостойкость. Основные понятия и определения. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернама. Дисковые шифраторы. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернама.

Алгоритмы генерации псевдослучайных последовательностей чисел. Различные способы создания псевдослучайных чисел.

Хэш-функции и аутентификация сообщений. MD5, ГОСТ 3411. Основные понятия, относящиеся к обеспечению целостности сообщений с помощью MAC и хэш-функций; представлены простые хэш-функции и сильная хэш-функция MD5. Сильные хэш-функции SHA-1, SHA-2 и ГОСТ 3411. Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC.

Электронная цифровая подпись (ЭЦП). Стандарты ЭЦП: DSS, ГОСТ 3410. Основные требования к цифровым подписям, прямая и арбитражная цифровая подпись, стандарты цифровой подписи ГОСТ 3410 и DSS.

Раздел 2. Методы и средства защиты информации.

Блочные и поточные алгоритмы симметричного шифрования. Стандарты и алгоритмы: американский DES, отечественный ГОСТ 28147, режимы их выполнения. Основные понятия, относящиеся к алгоритмам симметричного шифрования: ключ шифрования, plaintext, ciphertext. Определение стойкости алгоритма, типы операций, используемые в алгоритмах симметричного шифрования. Сеть Фейштеля. Основные понятия криптоанализа, линейный и дифференциальный криптоанализ. Описание алгоритмов DES и тройного DES. Алгоритмы симметричного шифрования Blowfish, IDEA, ГОСТ 28147, а также режимы их выполнения.

Стандарт криптографической защиты 21 века (AES). Алгоритм Rijndael. Стандарт криптографической защиты 21 века(AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра.

Раздел 3. Криптографические методы защиты информации

Асимметричные системы шифрования (системы с открытым ключом). RSA. Понятия однонаправленной функции и однонаправленной функции с лазейкой. Функции дискретного логарифмирования и основанные на ней алгоритмы: схема Диффи-Хеллмана, схема Эль-Гамаля. Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости.

Криптография с использованием эллиптических кривых. Математические понятия, связанные с эллиптическими кривыми, в частности задача дискретного логарифмирования на эллиптической кривой. Аналог алгоритма Диффи-Хеллмана на эллиптических кривых, алгоритма цифровой подписи на эллиптических кривых и алгоритма шифрования с открытым ключом получателя на эллиптических кривых.

Безопасность современных сетевых технологий. Протоколы аутентификации. Способы несанкционированного доступа к информации в компьютерных сетях. Классификация способов несанкционированного доступа и жизненный цикл атак. Способы противодействия несанкционированному межсетевому доступу. Функции межсетевого экранирования. Построение защищенных виртуальных сетей. Способы создания защищенных виртуальных каналов. Обзор протоколов.

Безопасность в открытых сетях. Инфраструктура цифровых сертификатов. Инфраструктура на основе криптографии с открытыми ключами (ИОК). Цифровые сертификаты. Управление цифровыми сертификатами. Управление ключами.

5. Образовательные технологии

При изучении дисциплины используется инновационная образовательная технология на основе интеграции компетентностного и личностно-ориентированного подходов с элемента-

ми традиционного лекционно-семинарского и квазипрофессионального обучения с использованием интерактивных форм проведения занятий, исследовательской проектной деятельности и мультимедийных учебных материалов

Вид учебной работы	Образовательные технологии
Лекции	Электронные материалы (в т.ч. сетевые источники), использование мультимедийных средств, раздаточный материал.
Лабораторные занятия	Тестирование, выполнение групповых аудиторных заданий, индивидуальные доклады.
Самостоятельные работы	Выполнение реферативной работы; подготовка и защита сообщения с использованием слайдовых презентаций.

6. Оценочные средства дисциплины

6.1. Паспорт фонда оценочных средств по дисциплине

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Оценочное средство	
			наименование	кол-во
1	Основные понятия и определения в области информационной безопасности. Традиционное шифрование: классические методы. Криптостойкость. Алгоритмы генерации псевдослучайных последовательностей чисел.	ОПК-3, ОПК-2	Тестовые задания Вопросы для экзамена Индивидуальное задание	20 7 4
2	Хэш-функции и аутентификация сообщений. MD5, ГОСТ 3411. Электронная цифровая подпись (ЭЦП). Стандарты ЭЦП: DSS, ГОСТ 3410	ОПК-3, ОПК-2	Тестовые задания Вопросы для экзамена Индивидуальное задание	20 7 4
3	Блочные и поточные алгоритмы симметричного шифрования. Стандарты и алгоритмы: американский DES, отечественный ГОСТ 28147, режимы их выполнения. Стандарт криптографической защиты 21 века (AES). Алгоритм Rijndael.	ОПК-3, ОПК-2	Тестовые задания Вопросы для экзамена Индивидуальное задание	20 7 4
4	Асимметричные системы шифрования (системы с открытым ключом). RSA.	ОПК-3, ОПК-2	Тестовые задания Вопросы для экзамена Индивидуальное задание	20 7 4
5	Криптография с использованием эллиптических кривых. Безопасность современных сетевых технологий. Протоколы аутентификации. Безопасность в открытых сетях. Инфраструктура цифровых сертификатов.	ОПК-3, ОПК-2	Тестовые задания Вопросы для экзамена Индивидуальное задание	20 10 4

6.2. Перечень вопросов для экзамена

1. Роль информации в современном мире (ОПК-3, ОПК-2)

2. Значение защиты (ОПК-3, ОПК-2)
3. Аспекты защиты. Анализ схем защиты (ОПК-3, ОПК-2)
4. Современная система удостоверяющих документов и её недостатки (ОПК-3, ОПК-2)
5. Бесперспективность защиты носителей. Практика выявления поддельных документов (ОПК-3, ОПК-2)
6. Организация защиты информации в вычислительном центре (ВЦ) крупного предприятия. Внешнее окружение ВЦ (ОПК-3, ОПК-2)
7. Способы контроля доступа к информации. (ОПК-3, ОПК-2)
8. Применимость мер защиты. Надежность и восстановление ЭВМ (ОПК-3, ОПК-2)
9. Экономические проблемы ЗИ. (ОПК-3, ОПК-2)
10. Меры противодействия и затраты на их организацию (ОПК-3, ОПК-2)
11. Понятия, относящиеся к защите ВС. Целостность ресурсов, защита ресурсов, право владения, надежность. (ОПК-3, ОПК-2)
12. Защита вычислительной сети. Классификация вторжений. (ОПК-3, ОПК-2)
13. Концепция защищенной ВС. (ОПК-3, ОПК-2)
14. Защита объектов ВС на основе информационной культуры, с учетом основных требований информационной безопасности.. (ОПК-3, ОПК-2)
15. Защита линий связи. (ОПК-3, ОПК-2)
16. Защита баз данных. (ОПК-3, ОПК-2)
17. Защита подсистемы управления ВС. (ОПК-3, ОПК-2)
18. Классификация сбоев и нарушения прав доступа к информации. (ОПК-3, ОПК-2)
19. Физическая защита кабельной системы. (ОПК-3, ОПК-2)
20. Физическая защита систем электроснабжения. (ОПК-3, ОПК-2)
21. Системы архивирования и дублирования информации (ОПК-3, ОПК-2)
22. Защита информации в операционных системах. (ОПК-3, ОПК-2)
23. Защита информации в прикладном ПО. (ОПК-3, ОПК-2)
24. Способы идентификации пользователей. (ОПК-3, ОПК-2)
25. Основные механизмы проверки подлинности пароля. (ОПК-3, ОПК-2)
26. Механизм проверки подлинности "рукопожатие", с учетом основных требований информационной безопасности.(ОПК-3, ОПК-2)
27. Проблема защиты информации в распределенных сетях (ОПК-3, ОПК-2)
28. Брандмауеры. Основные понятия. (ОПК-3, ОПК-2)
29. Межсетевой экран. Классификация межсетевых экранов. (ОПК-3, ОПК-2)
30. Классификация компьютерных вирусов (ОПК-3, ОПК-2)
31. Структура файловых, резидентных вирусов и вирусов-червей (ОПК-3, ОПК-2)
32. Жизненный цикл компьютерных вирусов (ОПК-3, ОПК-2)
33. Способы и симптомы заражения вирусами (ОПК-3, ОПК-2)
34. Общая классификация средств защиты от вирусов (ОПК-3, ОПК-2)
35. Стандарт шифрования данных DES (ОПК-3, ОПК-2)
36. Асимметрические (открытые) криптосистемы (ОПК-3, ОПК-2)
37. Применение криптографии. (ОПК-3, ОПК-2)
38. Основные направления компьютерных преступлений. Использование основных правовых знаний в сфере защиты информации. (ОПК-3, ОПК-2)

6.3. Шкала оценочных средств

Уровни освоения компетенций	Критерии оценивания	Оценочные средства (кол-во баллов)
Продвинутый (75-100 баллов) «отлично»	- полное знание основ правовых знаний в различных сферах деятельности; - умение ясно, логично и грамотно излагать изученный материал, производить собственные раз-	тестовые задания (30-40 баллов) индивидуальное задание

	мышления, делать умозаключения и выводы с добавлением комментариев, пояснений, обоснований; На этом уровне обучающийся способен творчески применять полученные знания путем самостоятельного конструирования способа деятельности.	(8-10 баллов); вопросы к экзамену (37-50 баллов)
Базовый (50-74 балла) «хорошо»	- знание основных теоретических и методических положений по изученному материалу и методов обработки различных материалов; - знание классификаций ОС, функций и свойств ОС, основных понятий ОС. На этом уровне обучающимся используется комбинирование известных приемов деятельности, эвристического мышления.	тестовые задания (20-30 баллов) индивидуальное задание (5-7 баллов); вопросы к экзамену (25-37 баллов)
Пороговый (35-49 баллов) «удовлетворительно»	- поверхностное знание основных типов ОС; - поверхностное знание назначения и функций ОС; На этом уровне обучающийся способен по памяти воспроизводить ранее усвоенную методику.	тестовые задания (15-20 баллов) индивидуальное задание (2-4 балла); вопросы к экзамену (18-25 баллов)
Низкий (допороговый) (компетенция не сформирована) (менее 35 баллов) «не удовлетворительно»	- незнание терминологии дисциплины, приблизительное представление о предмете и методах дисциплины, отрывочное, без логической последовательности изложение информации, косвенным образом затрагивающей некоторые аспекты программного материала.	тестовые задания (0-13 баллов); индивидуальное задание (0-3 балла); вопросы к экзамену (0-18 баллов)

Все комплекты оценочных средств (контрольно-измерительных материалов), необходимых для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения дисциплины (модуля) подробно представлены в документе «Фонд оценочных средств дисциплины (модуля)».

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1Основная учебная литература:

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268 (дата обращения: 28.06.2023).

3. *Внуков, А. А.* Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01678-9. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/444046

4. *Щеглов, А. Ю.* Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2019. — 309 с.

— (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/433715
5. *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, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/437163
6. Леонтьев, А. С. Защита информации : учебное пособие / А. С. Леонтьев. — Москва : РТУ МИРЭА, 2021. — 79 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182491
7. *Нестеров, С. А.* Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/434171

7.2 Дополнительная учебная литература:

1. Современные методы обеспечения защиты информации [Электронный ресурс] : учебное пособие. — Электрон. дан. — Уфа : БГПУ имени М. Акмуллы, 2016. — 112 с. — Режим доступа: https://e.lanbook.com/book/90965. — Загл. с экрана.
2. Введение в защиту информации от внутренних ИТ-угроз [Электронный ресурс] : учебное пособие. — Электрон. дан. — Москва : , 2016. — 39 с. — Режим доступа: https://e.lanbook.com/book/100720. — Загл. с экрана.
3. Современные методы обеспечения защиты информации [Электронный ресурс] : учебное пособие. — Электрон. дан. — Уфа : БГПУ имени М. Акмуллы, 2016. — 112 с. — Режим доступа: https://e.lanbook.com/book/90965. — Загл. с экрана.
4. Аникин, Д.В. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / Д.В. Аникин. — Электрон. дан. — Санкт-Петербург : ИЭО СПбУТУиЭ, 2011. — 269 с. — Режим доступа: https://e.lanbook.com/book/63950. — Загл. с экрана.
5. Бахаров, Л.Е. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / Л.Е. Бахаров. — Электрон. дан. — Москва : МИСИС, 2015. — 43 с. — Режим доступа: https://e.lanbook.com/book/116711. — Загл. с экрана.
6. Гультяева, Т.А. Основы защиты информации [Электронный ресурс] : учебное пособие / Т.А. Гультяева. — Электрон. дан. — Новосибирск : НГТУ, 2018. — 83 с. — Режим доступа: https://e.lanbook.com/book/118234. — Загл. с экрана.
7. Краковский, Ю.М. Защита информации [Электронный ресурс] : учебное пособие / Ю.М. Краковский. — Электрон. дан. — Ростов-на-Дону : Феникс, 2016. — 347 с. — Режим доступа: https://e.lanbook.com/book/102279. — Загл. с экрана.
8. Малюк, А.А. Теория защиты информации [Электронный ресурс] / А.А. Малюк. — Электрон. дан. — Москва : Горячая линия-Телеком, 2015. — 184 с. — Режим доступа: https://e.lanbook.com/book/111077. — Загл. с экрана.

7.3 Методические указания по освоению дисциплины

Методическое пособие для проведения практических занятий по дисциплине «Защита информации» для направления подготовки 09.03.01 Информатика и вычислительная техника. – Мичуринск, 2023.

7.4 Информационные и цифровые технологии (программное обеспечение, современные профессиональные базы данных и информационные справочные системы)

Учебная дисциплина (модуль) предусматривает освоение информационных и цифровых технологий. Реализация цифровых технологий в образовательном пространстве является одной из важнейших целей образования, дающей возможность развивать конкурентоспособные качества обучающихся как будущих высококвалифицированных специалистов.

Цифровые технологии предусматривают развитие навыков эффективного решения задач профессионального, социального, личностного характера с использованием различных видов коммуникационных технологий. Освоение цифровых технологий в рамках данной дисциплины (модуля) ориентировано на способность безопасно и надлежащим образом получать доступ, управлять, интегрировать, обмениваться, оценивать и создавать информацию с помощью цифровых устройств и сетевых технологий. Формирование цифровой компетентности предполагает работу с данными, владение инструментами для коммуникации.

7.4.1 Электронно-библиотечная системы и базы данных

1. ООО «ЭБС ЛАНЬ» (https://e.lanbook.ru/) (договор на оказание услуг от 10.03.2020 № ЭБ СУ 437/20/25 (Сетевая электронная библиотека)

2. Электронно-библиотечная система издательства «Лань» (https://e.lanbook.ru/) (договор на оказание услуг по предоставлению доступа к электронным изданиям ООО «Издательство Лань» от 03.04.2023 № 1)

3. Электронно-библиотечная система издательства «Лань» (https://e.lanbook.ru/) (договор на оказание услуг по предоставлению доступа к электронным изданиям ООО «Издательство Лань» от 06.04.2023 № 2)

4. База данных электронных информационных ресурсов ФГБНУ ЦНСХБ (договор по обеспечению доступа к электронным информационным ресурсам ФГБНУ ЦНСХБ через терминал удаленного доступа (ТУД ФГБНУ ЦНСХБ) от 07.04.2023 № б/н)

5. Электронно-библиотечная система «AgriLib» ФГБОУ ВО РГАЗУ (http://ebs.rgazu.ru/) (дополнительное соглашение на предоставление доступа от 13.04.2023 № б/н к Лицензионному договору от 04.07.2013 № 27)

6. Электронная библиотечная система «Национальный цифровой ресурс «Руконт»: Коллекции «Базовый массив» и «Колос-с. Сельское хозяйство» (https://rucont.ru/) (договор на оказание услуг по предоставлению доступа от 04.04.2023 № 2702/бп22)

7. ООО «Электронное издательство ЮРАЙТ» (https://urait.ru/) (договор на оказание услуг по предоставлению доступа к образовательной платформе ООО «Электронное издательство ЮРАЙТ» от 06.04.2023 № 6)

8. Электронно-библиотечная система «Вернадский» (https://vernadsky-lib.ru) (договор на безвозмездное использование произведений от 26.03.2020 № 14/20/25)

9. База данных НЭБ «Национальная электронная библиотека» (https://rusneb.ru/) (договор о подключении к НЭБ и предоставлении доступа к объектам НЭБ от 01.08.2018 № 101/НЭБ/4712)

10. Соглашение о сотрудничестве по оказанию библиотечно-информационных и социокультурных услуг пользователям университета из числа инвалидов по зрению, слабовидящих, инвалидов других категорий с ограниченным доступом к информации, лиц, имеющих трудности с чтением плоскопечатного текста ТОГБУК «Тамбовская областная универсальная научная библиотека им. А.С. Пушкина» (https://www.tambovlib.ru) (соглашение о сотрудничестве от 16.09.2021 № б/н)

7.4.2. Информационные справочные системы

1. Справочная правовая система КонсультантПлюс (договор поставки и сопровождения экземпляров систем КонсультантПлюс от 03.02.2023 № 11481 /13900/ЭС)

2. Электронный периодический справочник «Система ГАРАНТ» (договор на услуги по сопровождению от 22.12.2022 № 194-01/2023)

7.4.3. Современные профессиональные базы данных

1. База данных нормативно-правовых актов информационно-образовательной программы «Росметод» (договор от 11.07.2022 № 530/2022)
2. База данных Научной электронной библиотеки eLIBRARY.RU – российский информационно-аналитический портал в области науки, технологии, медицины и образования - https://elibrary.ru/
3. Портал открытых данных Российской Федерации - https://data.gov.ru/
4. Открытые данные Федеральной службы государственной статистики - https://rosstat.gov.ru/opendata
5. Профессиональные базы данных. Защита информации http://www.iso27000.ru/
6. Профессиональные базы данных. им. Е.И. Овсянкина. Информационная безопасность. Защита информацииhttp://all-ib.ru/
7. Профессиональные базы данных. Основы безопасности веб-приложенийhttps://martinfowler.com/articles/web-security-basics.html

7.4.4. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

№	Наименование	Разработчик ПО (правообладатель)	Доступность (лицензионное, свободно распространяемое)	Ссылка на Единый реестр российских программ для ЭВМ и БД (при наличии)	Реквизиты подтверждающего документа (при наличии)
1	Microsoft Windows, Office Professional	Microsoft Corporation	Лицензионное	-	Лицензия от 04.06.2015 № 65291651 срок действия: бессрочно
2	Антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса	АО «Лаборатория Касперского» (Россия)	Лицензионное	https://reestr.digital.gov.ru/reestr/366574/?sphrase_id=415165	Сублицензионный договор с ООО «Софтекс» от 06.07.2022 № б/н, срок действия: с 22.11.2022 по 22.11.2023
3	МойОфис Стандартный - Офисный пакет для работы с документами и почтой (myoffice.ru)	ООО «Новые облачные технологии» (Россия)	Лицензионное	https://reestr.digital.gov.ru/reestr/301631/?sphrase_id=2698444	Контракт с ООО «Рубикон» от 24.04.2019 № 036410000081900001 2 срок действия: бессрочно
4	Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат ВУЗ» (https://docs.antiplagiaus.ru)	АО «Антиплагиат» (Россия)	Лицензионное	https://reestr.digital.gov.ru/reestr/303350/?sphrase_id=2698186	Лицензионный договор с АО «Антиплагиат» от 17.04.2023 № 6627, срок действия: с 17.04.2023 по 16.04.2024
5	Acrobat Reader - просмотр документов PDF, DjVU	Adobe Systems	Свободно распространяемое	-	-
6	Foxit Reader	Foxit Corporation	Свободно рас-	-	-

	- просмотр документов PDF, DjVU		пространяемое		

7.4.5. Ресурсы информационно-телекоммуникационной сети «Интернет»

1. CDTOwiki: база знаний по цифровой трансформации https://cdto.wiki/
2. CIT Forum. URL: http://www.citforum.ru (дата обращения 12.06.2011).
3. Журнал «Защита информации. Инсайд». URL: https://www.inside-zi.ru/ (дата обращения 12.06.2011).
4. InformationSecurity: Информационная безопасность. URL: http://www.itsec.ru/main.php (дата обращения 12.06.2011).
5. Информационная безопасность. URL: https://securityvulns.ru/ (дата обращения 12.06.2011).

7.4.6. Цифровые инструменты, применяемые в образовательном процессе

1. LMS-платформа Moodle
2. Виртуальная доска Миро: miro.com
3. Виртуальная доска SBoard https://sboard.online
4. Виртуальная доска Padlet: https://ru.padlet.com
5. Облачные сервисы: Яндекс.Диск, Облако Mail.ru
6. Сервисы опросов: Яндекс Формы, MyQuiz
7. Сервисы видеосвязи: Яндекс телемост, Webinar.ru
8. Сервис совместной работы над проектами для небольших групп Trello http://www.trello.com

7.4.7. Цифровые технологии, применяемые при изучении дисциплины

№	Цифровые технологии	Виды учебной работы, выполняемые с применением цифровой технологии	Формируемые компетенции
	Облачные технологии	Лекции Лабораторные работы	ОПК-2
	Большие данные	Лекции Лабораторные работы	ОПК-2
	Технологии беспроводной связи	Лекции Лабораторные работы	ОПК-2
	Новые производственные технологии	Лекции Лабораторные работы	ОПК-2

8. Материально-техническое обеспечение дисциплины (модуля)

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Учебная аудитория для проведения занятий лекционного типа (г. Мичуринск, ул.	1. Проектор Acer X1261P (nV 3D) DLP 2700LUMENS (инв. № 2101045353); 2. Экран Draper Luma NTSC (3:4) 305/120" ручной, настенно-	1. Microsoft Windows 7 (лицензия от 31.12.2013 № 49413124, бессрочно). 2. Microsoft Office 2010 (лицензия от 04.06.2015 № 65291658, бессрочно).

Интернациональная, дом № 101, 1/103)	потолочный (инв. № 2101065491) 3. Ноутбук Lenovo IdeaPad V580c (инв.№21013400405) 4. Наборы демонстрационного оборудования и учебно-наглядных пособий.	
Кабинет информатики (компьютерный класс) (г. Мичуринск, ул. Интернациональная, д. 101 - 1/211)	1. Доска медиум (инв. №2101041642); 2. Плоттер (инв. №1101044028); 3. Принтер LV-1100 (инв. №2101042316); 4. Сканер (инв. №2101060636); 5. Компьютер Intel Core 2 Quad Q9400 Монитор Asus TFT 21,5 "(инв. № 2101045131); 6. Компьютер Intel Core 2 Quad Q9400 Монитор Asus TFT 21,5 "(инв. № 2101045130); 7. Компьютер Intel Core 2 Quad Q9400 Монитор Asus TFT 21,5 "(инв. № 2101045129); 8. Компьютер Intel Core 2 Quad Q9400 Монитор Asus TFT 21,5 "(инв. № 2101045128); 9. Компьютер Intel Core 2 Quad Q9400 Монитор Asus TFT 21,5 "(инв. № 2101045127); Компьютерная техника подключена к сети «Интернет» и обеспечена доступом к ЭИОС университета. Кабинет оснащен макетами, наглядными учебными пособиями, тренажерами и другими техническими средствами.	1. Microsoft Windows 7 (лицензия от 31.12.2013 № 49413124, бессрочно). 2. Microsoft Office 2010 (лицензия от 04.06.2015 № 65291658, бессрочно). 3. AutoCAD Design Suite Ultimate 2016 (3ds Max 2016, Alias Design 2016, AutoCAD 2016, AutoCAD Raster Design 2016, ReCap 2016, Showcase 2016) (договор от 17.04.2015 № 110000940282); 4. nanoCAD (версия 5.1 локальная, образовательная лицензия, серийный номер NC50B-270716 лицензия действительна бессрочно, бесплатная). 5. Программный комплекс «АСТ-ТестPlus» (лицензионный договор от 18.10.2016 № Л-21/16)
Учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (компьютерный класс) (г. Мичуринск, ул. Интернациональная, д. 101 - 1/114)	1. Компьютер С-600 (инв. № 1101044333, 1101044334, 1101044335, 1101044336, 1101044337, 1101044338, 1101044339, 1101044340) 2. Компьютер С-700 (инв. № 1101045328) 3. Концентратор сетевой (инв. № 2101061671) 4. Компьютер Р-233 (инв. № 2101041453, 2101041454, 2101041455, 2101041456, 2101041457, 2101041458, 2101041459, 2101041460, 2101041461) 5. Системный комплект: Процессор Intel Original LGA 1155 Celeron G 1610 OEM (2.6/2 Mb), монитор 20” Asus As MS202D , материнская плата Asus, вентилятор, память, жесткий диск, корпус, клавиатура, мышь (инв. № 21013400425, 21013400446, 21013400453, 21013400454, 21013400481, 21013400480, 21013400455, 21013400482, 21013400505) Компьютерная техника подключена к сети «Интернет» и обеспечена доступом к ЭИОС университета.	1. Microsoft Windows XP (лицензия от 31.12.2013 № 49413124, бессрочно). 2. Microsoft Office 2003 (лицензия от 04.06.2015 № 65291658, бессрочно). 3. Project Expert 7 (договор от 18.12.2012 № 0354/1П-06). 4. Audit Expert 4 Professional (договор от 18.12.2012 № 0354/1П-06). 5. Statistica Base 6 (договор от 12.01.2012 № 6/12/А) 6. Statistica Ultimate, контракт от 25.04.2016 №0364100000816000014, бессрочно; Statistica Ultimate, контракт от 05.05.2017 №0364100000817000006; Statistica Ultimate, контракт от 07.05.2018 №0364100000818000014). 7. Система Консультант Плюс, договор от 10.03.2017 № 7844/13900/ЭС; Система Консультант Плюс, договор от 20.02.2018 № 9012 /13900/ЭС; Система Консультант Плюс, договор от 01.11.2018 № 9447/13900/ЭС; Система Консультант Плюс, договор от 26.02.2019 № 9662/13900/ЭС. 8. Электронный периодический справочник «Система ГАРАНТ», договор от 27.12.2016 № 154-01/17; Электронный периодический справочник «Система ГАРАНТ», договор от 09.01.2018 № 194- 01/2018СД; Электронный периодический справочник «Система ГАРАНТ», договор от 02.07.2018 № 194-02/2018СД.

		9. Программы для ЭВМ и базы данных 1С: Библиотека ПРОФ (сублицензионный договор от 19.05.2017 № ПРКТ-14698) 10. Программы для ЭВМ и базы данных 1С: Музей (сублицензионный договор от 19.05.2017 № ПРКТ-14699)
Помещение для самостоятельной работы (г. Мичуринск, ул. Интернациональная, д. 101 - 1/115)	1. Компьютер Celeron E3500 (инв. №2101045275) 2. Компьютер Celeron E3500 (инв. №2101045276) 3. Компьютер Celeron E3500 (инв. №2101045277) 4. Компьютер Celeron E3500 (инв. №2101045278) 5. Компьютер Celeron E3500 (инв. №2101045279) 6. Компьютер Celeron E3500 (инв. №2101045280) 7. Компьютер Celeron E3500 (инв. №2101045281) 8. Компьютер Celeron E3500 (инв. №2101045274) Компьютерная техника подключена к сети «Интернет» и обеспечена доступом к ЭИОС университета.	1. Microsoft Windows XP (лицензия от 31.12.2013 № 49413124, бессрочно). 2. Microsoft Office 2003 (лицензия от 04.06.2015 № 65291658, бессрочно). 3. Project Expert 7 (договор от 18.12.2012 № 0354/1П-06). 4. Audit Expert 4 Professional (договор от 18.12.2012 № 0354/1П-06). 5. Statistica Base 6 (договор от 12.01.2012 № 6/12/А) 6. Statistica Ultimate, контракт от 25.04.2016 №0364100000816000014, бессрочно; Statistica Ultimate, контракт от 05.05.2017 №0364100000817000006; Statistica Ultimate, контракт от 07.05.2018 №0364100000818000014). 7. Программное обеспечение «Антиплагиат. ВУЗ» (лицензионный договор от 21.03.2018 №193; лицензионный договор от 10.05.2018 №193-1; лицензионный договор от 19.03.2019 № 1043). 8. Информационно-образовательная программа «Росметод» (договор от 17.07.2018 № 2135; договор от 02.07.2019 № 405).

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО – бакалавриат по направлению подготовки 09.03.01 Информатика и вычислительная техника, утвержденного приказом Минобрнауки РФ от 19.09.2017г., №929.

Автор:

Доцент кафедры математики, физики и ИТ, к.с/х.н. Макова Н.Е. _____

Доцент кафедры математики, физики и ИТ, к.т.н. Трейгер В.В.

Старший преподаватель кафедры математики, физики и ИТ Пчелинцева Н.В.

Рецензент:

заведующий кафедрой стандартизации, метрологии и технического сервиса, к.т.н., доцент Хатунцев В.В. _____

Рабочая программа разработана в соответствии с требованиями ФГОС ВО.

Программа рассмотрена на заседании кафедры математики, физики и информационных технологий. Протокол № 7 от «26» марта 2019 г.

Программа рассмотрена на заседании учебно-методической комиссии инженерного института ФГБОУ ВО Мичуринский ГАУ, протокол № 9 от 22 апреля 2019 г.

Программа утверждена Решением учебно-методического совета университета протокол №8 от 25 апреля 2019 года.

Рабочая программа переработана в соответствии с требованиями ФГОС ВО.

Программа рассмотрена на заседании кафедры математики, физики и информационных технологий. протокол № 8 от «08» апреля 2020 г.

Программа рассмотрена на заседании учебно-методической комиссии инженерного института ФГБОУ ВО Мичуринский ГАУ, протокол № 9 от 13 апреля 2020 г.

Программа утверждена Решением учебно-методического совета университета протокол №8 от 23 апреля 2020 года.

Программа переработана и дополнена в соответствии с требованиями ФГОС ВО.

Программа рассмотрена на заседании кафедры математики, физики и информационных технологий. Протокол № 10 от «09» марта 2021 г.

Программа рассмотрена на заседании учебно-методической комиссии инженерного института ФГБОУ ВО Мичуринский ГАУ, протокол № 9 от 05 апреля 2021 г.

Программа утверждена Решением учебно-методического совета университета протокол №8 от 22 апреля 2021 года.

Программа переработана и дополнена в соответствии с требованиями ФГОС ВО.

Программа рассмотрена на заседании кафедры математики, физики и информационных технологий. Протокол № 10 от «10» июня 2021 г.

Программа рассмотрена на заседании учебно-методической комиссии инженерного института ФГБОУ ВО Мичуринский ГАУ, протокол № 11 от 15 июня 2021 г.

Программа утверждена Решением учебно-методического совета университета протокол №12 от 30 июня 2021 года.

Программа переработана и дополнена в соответствии с требованиями ФГОС ВО.

Программа рассмотрена на заседании кафедры математики, физики и информационных технологий. Протокол № 8 от «12» апреля 2022 г.

Программа рассмотрена на заседании учебно-методической комиссии инженерного института ФГБОУ ВО Мичуринский ГАУ, протокол № 7 от 14 апреля 2022 г.

Программа утверждена Решением учебно-методического совета университета протокол №8 от 21 апреля 2022 года.

Программа переработана и дополнена в соответствии с требованиями ФГОС ВО.

Программа рассмотрена на заседании кафедры математики, физики и информационных технологий. Протокол № 9 от «01» июня 2023 г.

Программа рассмотрена на заседании учебно-методической комиссии инженерного института ФГБОУ ВО Мичуринский ГАУ, протокол № 10 от 19 июня 2023 г.

Программа утверждена Решением учебно-методического совета университета протокол №10 от 22 июня 2023 года.