федеральное государственное бюджетное образовательное учреждение высшего образования

«МИЧУРИНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

кафедра экономической безопасности и права

УТВЕРЖДЕНА
решением учебно-методического совета университета
(протокол №8 от 23 апреля 2025 г.)

УТВЕРЖДАЮ
Председатель учебно-методического совета университета
Р.А. Чмир
«23» апреля 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Специальность 38.05.01 Экономическая безопасность

Специализация Экономико–правовое обеспечение экономической безопасности

Квалификация: экономист

Мичуринск– 2025

1. Цели освоения дисциплины (модуля)

Целями освоения дисциплины (модуля) «Информационная безопасность» являются:

формирование у обучающихся знаний в области теоретических основ информационной безопасности (ИБ) и защиты информации (ЗИ) в компьютерных комплексах, умений и навыков их практического применения, эффективного использования программных средств и систем защиты информации (СЗИ) в вычислительных системах и сетях (ВСС) и изучение современных технических и программных средств в области защиты информации; обучение навыкам работы с программными средствами при решении задач обеспечения информационной безопасности; обучение правилам постановки задачи и ее решения средствами компьютерной техники при защите информации; формирование умений использовать основные законодательные акты и программные продукты при обеспечении защиты информации.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина (модуль) «Информационная безопасность» относится к дисциплинам (модулям) Базовой части Блока1 «Дисциплины (модули)» (Б1.В.ДВ.02.01).

Дисциплина (модуль) основывается на знаниях, умениях и навыках следующих дисциплин (модулей): «Математика», «Экономическая теория».

Освоение данной дисциплины необходимо для изучения таких дисциплин (модулей), как: «Информационные системы в аграрной экономике», «Теория и механизмы современного государственного управления», «Экономическая безопасность», «Документационное обеспечение управления».

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

Процесс изучения дисциплины (модуля) направлен на формирование следующих универсальных и профессиональных компетенций:

УК–1 – Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;

ПК – 2 – Способен собирать и анализировать информацию, необходимую для принятия решений по обеспечению экономической безопасности хозяйствующих субъектов, осуществлять стратегическое управление ключевыми экономическими показателями и бизнес–процессами

Планируемые результаты обучения* (показатели освоения компетенции)	Критерии оценивания результатов обучения			
	Низкий (допороговый) компетенция не сформирована	Пороговый	Базовый	Продвинутый
УК–1				
Знать: систему различных информационных ресурсов и	Фрагментарные знания системы различных информационны	Общие, но не структурированные знания системы	Сформированные, но содержащие отдельные	Успешное и систематическое применение знаний о системе

технологий, основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	х ресурсов и технологий, основных методов, способов и средств получения, хранения, поиска, систематизации, обработки и передачи информации	различных информационных ресурсов и технологий, основных методов, способов и средств получения, хранения, поиска, систематизации, обработки и передачи информации	пробелы знания системы различных информационны х ресурсов и технологий, основных методов, способов и средств получения, хранения, поиска, систематизации, обработки и передачи информации	различных информационны х ресурсов и технологий, основных методов, способов и средств получения, хранения, поиска, систематизации, обработки и передачи информации
Уметь: работать с различными информационны ми ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	Частично освоенное умение работать с различными информационны ми ресурсами и технологиями	В целом успешная, но не систематически осуществляемая работа с различными информационны ми ресурсами и технологиями	В целом успешное, но содержащее отдельные пробелы в применении основных методов, способов и средств получения, хранения, поиска, систематизации, обработки и передачи информации	Сформированное умение работать с различными информационны ми ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации
Владеть: навыками сбора, обработки, систематизации и анализа информации	Фрагментарное применение навыков сбора, обработки, систематизации и анализа информации	В целом успешное, но не систематическое применение навыков сбора, обработки, систематизации и анализа информации	В целом успешные, но содержащие отдельные пробелы навыки сбора, обработки, систематизации и анализа информации	Успешные и систематические навыки сбора, обработки, систематизации и анализа информации
ПК–2				
Знать:	Фрагментарные	Общие, но не	Сформированны	Успешное и

содержание и структуру инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации и способы обоснования их выбора	знания содержания и структуры инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации и способов обоснования своего выбора	структурированные знания содержания и структуры инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации и способов обоснования своего выбора	е, но содержащие отдельные пробелы знания содержания и структуры инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации и способов обоснования своего выбора	систематическое применение знаний содержания и структуры инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации и способов обоснования своего выбора
Уметь: применять систему инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации	Частично применять систему инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации	В целом успешное, но не систематическое применение системы инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации	В целом успешное, но содержащее отдельные пробелы применение системы инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации	Сформированное умение применения системы инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации
Владеть: навыками выбора инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации	Фрагментарное владение навыками выбора инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации	В целом успешное, но не систематическое владение навыками выбора инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации	В целом успешное, но содержащее отдельные пробелы владение навыками выбора инструментальных средств для обработки финансовой, бухгалтерской и иной	Успешное и систематическое владение навыками выбора инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации

			экономической информации	

В результате освоения дисциплины (модуля)обучающийся должен:

Знать:

− основы информационной безопасности (ИБ) и защиты информации (ЗИ);

− основные методы и средства поиска, систематизации, обработки, передачи и защиты информации;

− способы и мероприятия по обеспечению ИБ в профессиональной деятельности, принципы криптографических преобразований;

− типовые программно–аппаратные средства и системы зашиты информации от несанкционированного доступа (НСД) в компьютерную среду.

Уметь:

− реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности по ЗИ, обеспечивающие его должную экономическую безопасность;

− проводить анализ защищенности конфиденциальной информации, обеспечивать повышение уровня ее зашиты с учетом развития математического и программного обеспечения СЗИ для вычислительных систем и сетей;

− использовать методы и средства обеспечения ИБ с целью предотвращения несанкционированного доступа, злоумышленной модернизации или утраты информации, составляющей государственную тайну, и иной служебной информации;

− модифицировать средства и системы защиты информации (СЗИ).

Владеть:

− навыками работы с типовыми средствами ЗИ в вычислительных системах и сетях.

− навыками обеспечения ЗИ, составляющей государственную тайну, и иной служебной информации.

3.1 Матрица соотнесения тем/разделов учебной дисциплины (модуля) и формируемых в них универсальных, профессиональных компетенций

№	Темы, разделы дисциплины (модуля)	Компетенции		
		УК–1	ПК–2	общее количество компетенций
РАЗДЕЛ 1 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭКОНОМИЧЕСКИХ СИСТЕМ				
1	Основные понятия курса информационная безопасность (ИБ). Виды атак на информацию. Современное состояние информационной безопасности в России. Экономическая информация как товар и объект безопасности	+	+	2
2	Природа возникновения угроз. Классификация угроз. Защита от несанкционированного доступа	+	+	2
РАЗДЕЛ 2 ЗАКОНОДАТЕЛЬНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ				
1	Значение законодательного уровня ИБ. Обзор российского законодательства в области ИБ.	+	+	2

	Правовые акты общего назначения, затрагивающие вопросы ИБ			
2	Стандарты и спецификации в области ИБ	+	+	2
РАЗДЕЛ 3. АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ				
1	Особенности административного уровня информационной безопасности. Политика безопасности. Управление рисками.	+	+	2
2	Процедурный уровень ИБ**.** Основные классы мер процедурного уровня. Управление персоналом. Реагирования на нарушения	+	+	2
РАЗДЕЛ 4. ПРОГРАММНО–ТЕХНИЧЕСКИЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ ЗАЩИТЫ				
1	Основные понятия программно–технического уровня ИБ. Архитектурная безопасность. Идентификация, аутентификация, управление доступом	+	+	2
2	Обзор биометрических технологий. Аппаратно–программные средства контроля доступа. Биометрические устройства вода. Комбинированные устройства ввода. Электронные замки	+	+	2
РАЗДЕЛ 5. ОСНОВЫ КРИПТОГРАФИИ				
1	Основные понятия криптографии. Классификация шифров	+		1

4. Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) 4 зачетные единицы, 144 академических часов.

4.1. Объем дисциплины (модуля) и виды учебной работы

Виды занятий	Всего ак.часов	
	По очной форме обучения 4 семестр	По заочной форме обучения 2 курс
Общая трудоемкость дисциплины (модуля)	144	144
Контактная работа обучающихся с преподавателем	54	10
аудиторные занятия	36	10
лекции	18	4
практические занятия	18	6
Самостоятельная работа обучающихся	72	125
проработка учебного материала по дисциплине (модулю) (конспектов лекций, учебников, материалов сетевых	26	40

ресурсов)		
подготовка к практическим занятиям, коллоквиумам, защите реферата	12	40
выполнение индивидуальных заданий	20	45
подготовка к сдаче модуля (выполнение тренировочных тестов)	14	–
Контроль	36	9
Вид итогового контроля	экзамен	

4.2. Лекции

№	Раздел дисциплины (модуля), темы лекций и их содержание	Объем в ак. часах		Формируемые компетенции
		Очная форма обучения	Заочная форма обучения	
РАЗДЕЛ 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭКОНОМИЧЕСКИХ СИСТЕМ				
1	Тема 1. Основные понятия курса информационная безопасность (ИБ). Виды атак на информацию. Современное состояние информационной безопасности в России. Экономическая информация как товар и объект безопасности	2	2	УК–1
	Тема 2. Природа возникновения угроз. Классификация угроз. Защита от несанкционированного доступа	2		УК–1
РАЗДЕЛ 2. ЗАКОНОДАТЕЛЬНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ				
2	Тема 3. Значение законодательного уровня ИБ. Обзор российского законодательства в области ИБ. Правовые акты общего назначения, затрагивающие вопросы ИБ	2		УК–1
	Тема 4. Стандарты и спецификации в области ИБ	2		УК–1, ПК–2
РАЗДЕЛ 3. АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ				
3	Тема 5. Особенности административного уровня информационной безопасности. Политика безопасности. Управление рисками.	2		УК–1, ПК–2
	Тема 6. Процедурный уровень ИБ**.** Основные классы мер процедурного уровня. Управление персоналом. Реагирования на нарушения	2		УК–1, ПК–2
4	Программно–технический уровень информационной защиты Тема 7. Основные понятия программно–технического уровня ИБ. Архитектурная безопасность. Идентификация, аутентификация,	2	2	УК–1, ПК–2

	управление доступом			
	Тема 8. Обзор биометрических технологий. Аппаратно–программные средства контроля доступа. Биометрические устройства вода. Комбинированные устройства ввода. Электронные замки	2		УК–1, ПК–2
РАЗДЕЛ 4. ОСНОВЫ КРИПТОГРАФИИ				
	Тема 9. Основные понятия криптографии. Классификация шифров	2		УК–1
	Итого	18	4	

4.3. Лабораторные работы не предусмотрены

4.4. Практические занятия

№	Раздел дисциплины (модуля), темы практических занятий и их содержание	Объем в ак.часах		Формируемые компетенции
		Очная форма обучения	Заочная форма обучения	
1	Встроенные системы и сервисы защиты информации ЭВМ Тема 1. Встроенная система защиты современных операционных систем	1	2	УК–1, ПК–2
	Тема 2. Изучение средств управления встроенной системы защиты Windows	1		УК–1, ПК–2
	Тема 3. Установление доступа к файлам и папкам. Оценка защищенности компьютера	2		УК–1, ПК–2
2	Нормативно–правовое обеспечение информационной безопасности Тема 4. Применение российского законодательства в области ИБ для решения задач обеспечения защиты информации на разных уровнях. Правовые акты общего назначения, затрагивающие вопросы ИБ. Работа в «Консультант плюс».	1		УК–1, ПК–2
	Тема 5. Применение стандартов и спецификаций в области ИБ. Работа в «Консультант плюс»	2		УК–1, ПК–2
3	Организация защиты информации в экономических системах Тема 6. Анализ рисков информационной безопасности	2	2	УК–1, ПК–2
	Тема 7. Анализ обеспечения информационной безопасности в ведущих зарубежных странах	2		УК–1, ПК–2
	Тема 8. Построение концепции информационной безопасности предприятия	1		УК–1, ПК–2
4	Основы обеспечения защиты информации в сети Internet	1		УК–1, ПК–2

	Тема 9. Программно–аппаратные методы защиты от удаленных атак в сети Internet. Программные методы защиты, применяемые в сети Internet.			
	Тема 10. Работа с антивирусными средствами защиты информации. Классификация антивирусных программ. Сканеры	1	2	УК–1, ПК–2
	Тема 11. Электронная цифровая подпись и особенности ее применения. Защита информации в Интернете	1		УК–1, ПК–2
	Тема 12. Поиск, использование и сохранение программных продуктов. Обзор современных антивирусных программ.	1		УК–1, ПК–2
5	Криптография и шифрование Тема 13. Алгоритмы и ключи	1		УК–1, ПК–2
	Тема 14. Работа с шифрами	1		ПК–2
	Итого	18	6	

4.5. Самостоятельная работа обучающихся

Раздел дисциплины (модуля)	Вид самостоятельной работы	Объем ак.часов	
		Очная форма обучения	Заочная форма обучения
Раздел 1. Основы информационной безопасности	проработка учебного материала по дисциплине (модулю) (конспектов лекций, учебников, материалов сетевых ресурсов)	5	10
	подготовка к практическим занятиям, коллоквиумам, защите реферата	5	10
	выполнение индивидуальных заданий	5	12
	подготовка к сдаче модуля (выполнение тренировочных тестов)	5	–
Раздел 2. Государственное политика в области информационной безопасности	проработка учебного материала по дисциплине (модулю) (конспектов лекций, учебников, материалов сетевых ресурсов)	5	10
	подготовка к практическим занятиям, коллоквиумам, защите реферата	5	10
	выполнение индивидуальных заданий	3	11
	подготовка к сдаче модуля (выполнение тренировочных тестов)	4	–
Раздел 3. Административный уровень информационной безопасности	проработка учебного материала по дисциплине (модулю) (конспектов лекций, учебников, материалов сетевых ресурсов)	5	10
	подготовка к практическим занятиям, коллоквиумам, защите реферата	2	10
	выполнение индивидуальных заданий	2	11

	подготовка к сдаче модуля (выполнение тренировочных тестов)	3	–
Раздел 4. Обеспечение защиты информации в сети Internet	проработка учебного материала по дисциплине (модулю) (конспектов лекций, учебников, материалов сетевых ресурсов)	5	10
	подготовка к практическим занятиям, коллоквиумам, защите реферата	3	10
	выполнение индивидуальных заданий	2	11
	подготовка к сдаче модуля (выполнение тренировочных тестов)	3	–
	Итого	72	125

Перечень учебно–методического обеспечения для самостоятельной работы по дисциплине (модулю):

1. Грязнев А. Н. Учебно–методический комплекс по дисциплине (модулю) «Информационная безопасность». Мичуринск: Изд–во Мичуринского ГАУ, 2022 г.

4.6. Выполнение контрольной работы обучающимися заочной формы

Обучающиеся заочной формы обучения выполняют контрольную работу, которая должна: выполняться на стандартных листах формата А 4; иметь титульный лист, план работы с нумерацией страниц в соответствии с его пунктами, введение, текст самой работы, заключение, список литературы, использованной при написании, приложения, если таковые имеются; быть сдана на кафедру не менее чем за 14 дней до начала сессии.

Обучающиеся, сдавшие письменные работы позже установленного срока, до сдачи зачета не допускаются.

Титульный лист должен быть оформлен по форме и в обязательном порядке должен содержать название кафедры, на которой выполняется работа, название предмета и тему, по которой выполняется работа, Ф.И.О. и регалии преподавателя, проверяющего работу; Ф.И.О. и курс обучающегося, выполнившего работу.

Страницы работы должны быть пронумерованы.

Пункты плана должны отражать структуру работы, название глав и параграфов дублироваться в тексте работы без изменений. Изложение плана, введения, глав, заключения, списка литературы и приложений должно начинаться с новой страницы.

Текст работы пишется только с одной стороны листа.

Список литературы должен содержать не менее 3 источников, на которые в тексте работы в обязательном порядке должны содержаться ссылки. Текст без ссылок и списка литературы не проверяется и не рецензируется.

Источники в списке литературы должны быть оформлены следующим образом: Ф.И.О. автора. Название монографии без кавычек. Место издания, год издания. Ф.И.О. автора. Название статьи без кавычек // Название журнала или газеты без кавычек. Год издания. Номер.

Ф.И.О. автора. Название статьи без кавычек // Название сборника без кавычек / под ред. Ф.И.О. Место издания, год издания.

Список литературы должен быть составлен в алфавитном порядке по фамилиям авторов.

Объем письменной работы должен быть не менее 12 машинописных листов. Текст печатается шрифтом размера 14 и с интервалом 1.5, при отступах от левого края 3 см, правого и верхнего – 1.5 см, нижнего – 2 см.

Выбор варианта контрольной работы осуществляется по первой букве фамилии обучающегося:

Контрольная работа № 1: А, Д, И

Контрольная работа № 2: Б, Е, К, Ч

Контрольная работа № 3: В, Ж, Л, Э

Контрольная работа № 4: М, Р, Ш

Контрольная работа № 5:З, Н, Т, Х

Контрольная работа № 6: О, С, Ц, Я.

Контрольная работа № 7: П, У, Ф

Контрольная работа № 8: Г, Щ, Ю

Перечень тем контрольных работ:

1. Основная идея теория информации по К. Шеннону, её отличие от семантической теории информации по Ю.А. Шрейдеру.

2. Виды информации, её свойства и особенности их взаимодействия.

3. Соотношение между материей и информацией.

4. Понятие информации по К. Шеннону и Н. Винеру.

5.Семантический, лингвистический, прагматический и технический аспекты информации.

6. Основные признаки информации.

7. Информация, данные и знание, их взаимосвязь и различие.

8. Основные документы, определяющие концептуальные основы информационной безопасности РФ.

9.Концепция национальной безопасности РФ. Важнейшие задачи обеспечения национальной безопасности в информационной сфере.

10. Доктрина информационной безопасности.

11. Понятие национальных интересов.

12. Национальные интересы страны в информационной сфере, угрозы национальным интересам.

13. Причины и источники угроз национальным интересам страны.

14. Виды безопасности.

15. Национальная безопасность и её составляющие.

16. Субъекты системы и уровни обеспечения национальной безопасности РФ.

17. Основные задачи по обеспечению национальной безопасности.

18. Возможные сценарии подрыва безопасности России без применения военных средств.

19. Понятие «Информационной безопасности».

20. Место информационной безопасности в системе национальной безопасности России.

21. Важнейшие федеральные нормативные правовые акты, касающиеся информационной безопасности.

22. Законы, непосредственно касающиеся защиты компьютерной информации.

23. Информация и право. Информация как объект правового регулирования.

24. Информационные отношения.

25. Законы, действующие в области производства, распространения и потребления информации.

26. Информационная война, методы и средства её ведения.

27. Информационное оружие, его классификация и возможности.

28. Методы нарушения конфиденциальности, целостности и доступности информации.

29. Причины, виды, каналы утечки и искажения информации.

30. Основные направления обеспечения информационной безопасности объектов информационной сферы.

31. Методы и средства обеспечения ИБ объектов информационной сферы.

32. Стандарты и нормативы в сфере обеспечения информационной безопасности.

33. Определение безопасности компьютерной системы и категории требований безопасности.

34. Базовые требования безопасности компьютерной системы.

35. Классы безопасности компьютерных систем, понятие риска.

36. Сущность понятий: «Вычислительная база защиты», «Монитор обращений», «Ядро безопасности».

37. Режимы функционирования компьютерной системы.

38. Сущность понятий: идентификация, аутентификация; авторизация.

39. Адекватность средств защиты.

40. Понятие продукта ИТ и системы обработки информации.

39. Классы средств защиты информации.

40. Федеральная целевая программа "Электронная Россия"

4.7. Содержание разделов дисциплины (модуля)

Раздел 1. Теоретические аспекты информационной безопасности экономических систем

Тема 1. Основные понятия курса информационная безопасность (ИБ). Виды атак на информацию. Современное состояние информационной безопасности в России. Экономическая информация как товар и объект безопасности.

Тема 2. Угрозы информационной безопасности. Природа возникновения угроз. Классификация угроз. Защита от несанкционированного доступа

Раздел 2. Законодательный уровень информационной безопасности

Тема 3. Значение законодательного уровня ИБ. Обзор российского законодательства в области ИБ. Правовые акты общего назначения, затрагивающие вопросы ИБ

Тема 4. Стандарты и спецификации в области ИБ. Основные понятия. Классы безопасности. Информационная безопасность распределенных систем. Рекомендации X.800

Сетевые сервисы безопасности. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий». Требования доверия информации. Гармонизированные критерии Европейских стран. Интерпретация «Оранжевой книги» для сетевых конфигураций. Руководящие документы Гостехкомиссии России. Расследование компьютерных преступлений

Раздел 3. Административный уровень информационной безопасности

Тема 5. Особенности административного уровня информационной безопасности. Особенности политики безопасности на административном уровне. Программа безопасности на предприятиях различных уровней. Синхронизация программы безопасности с жизненным циклом систем.

Тема 6. Процедурный уровень ИБ. Основные классы мер процедурного уровня. Управление персоналом для обеспечения защиты информации на предприятиях различных сфер. Реагирования на нарушения.

Раздел 4.Программно–технический уровень информационной защиты

Тема 7. Основные понятия программно–технического уровня ИБ. Особенности архитектурной безопасности. Идентификация, аутентификация, управление доступом

Тема 8. Обзор биометрических технологий. Аппаратно–программные средства контроля доступа к информации на различных уровнях Биометрические устройства вода. Комбинированные устройства ввода. Электронные замки

Раздел 5. Основы криптографии

Тема 9. Основные понятия криптографии. Классификация шифров

.

5. Образовательные технологии

Вид учебной работы	Образовательные технологии
Лекции	Электронные материалы, использование мультимедийных средств, раздаточный материал
Практические занятия	Деловые и ролевые игры, разбор конкретных ситуаций, тестирование, кейсы, выполнение групповых аудиторных заданий, индивидуальные доклады
Самостоятельная работа	Защита и презентация результатов самостоятельного исследования на занятиях

6. Оценочные средства дисциплины (модуля)

6.1. Паспорт фонда оценочных средств по дисциплине (модулю) «Информационная безопасность»

№	Контролируемые разделы (темы) дисциплины (модуля)	Код контролируемой компетенции	Оценочное средство	
			наименование	кол–во
1	Встроенные системы и сервисы защиты информации ЭВМ Тема 1. Встроенная система защиты современных операционных систем	УК–1, ПК–2	Тестовые задания Темы рефератов Вопросы для экзамена	8 2 2
	Тема 2. Изучение средств управления встроенной системы защиты Windows	УК–1, ПК–2	Тестовые задания Темы рефератов Вопросы для экзамена	8 2 2
	Тема 3. Установление доступа к файлам и папкам. Оценка защищенности компьютера	УК–1, ПК–2	Тестовые задания Темы рефератов Вопросы для экзамена	8 1 2
2	Нормативно–правовое обеспечение	УК–1, ПК–2	Тестовые задания	8

	информационной безопасности Тема 4. Применение российского законодательства в области ИБ для решения задач обеспечения защиты информации на разных уровнях. Правовые акты общего назначения, затрагивающие вопросы ИБ. Работа в «Консультант плюс».		Темы рефератов Вопросы для экзамена	2 2
	Тема 5. Применение стандартов и спецификаций в области ИБ. Работа в «Консультант плюс»	УК–1, ПК–2	Тестовые задания Темы рефератов Вопросы для экзамена	8 2 2
3	Организация защиты информации в экономических системах Тема 6. Анализ рисков информационной безопасности	УК–1, ПК–2	Тестовые задания Темы рефератов Вопросы для экзамена	8 1 2
	Тема 7. Анализ обеспечения информационной безопасности в ведущих зарубежных странах	УК–1, ПК–2	Тестовые задания Темы рефератов Вопросы для экзамена	8 1 2
	Тема 8. Построение концепции информационной безопасности предприятия	УК–1, ПК–2	Тестовые задания Темы рефератов Вопросы для экзамена	8 2 2
4	Основы обеспечения защиты информации в сети Internet Тема 9. Программно–аппаратные методы защиты от удаленных атак в сети Internet. Программные методы защиты, применяемые в сети Internet.	УК–1, ПК–2	Тестовые задания Темы рефератов Вопросы для экзамена	8 2 2

	Тема 10. Работа с антивирусными средствами защиты информации. Классификация антивирусных программ. Сканеры	УК–1, ПК–2	Тестовые задания Темы рефератов Вопросы для экзамена	8 1 2
	Тема 11. Электронная цифровая подпись и особенности ее применения. Защита информации в Интернете	УК–1, ПК–2	Тестовые задания Темы рефератов Вопросы для экзамена	8 1 2
	Тема 12. Поиск, использование и сохранение программных продуктов. Обзор современных антивирусных программ.	УК–1, ПК–2	Тестовые задания Темы рефератов Вопросы для экзамена	4 1 2
5	Криптография и шифрование Тема 13. Алгоритмы и ключи	УК–1, ПК–2	Тестовые задания Темы рефератов Вопросы для экзамена	4 2 2
	Тема 14. Работа с шифрами	УК–1, ПК–2	Тестовые задания Вопросы для экзамена	4 2

6.2 Перечень вопросов для экзамена

1. Понятие информационной безопасности (ИБ) и защиты информации. Современное состояние информационной безопасности в России. Экономическая информация как товар и объект безопасности (УК–1, ПК–2).

2. Атаки на информационные ресурсы. Виды атак на информацию. Классификация. Способы борьбы (УК–1, ПК–2).

3. Понятие угроза ИБ. Угрозы информационной безопасности. Природа возникновения угроз. Классификация угроз. Защита от несанкционированного доступа (УК–1, ПК–2).

4. Уровни защиты информации. Основные характеристики каждого уровня ИБ (УК–1, ПК–2).

5. Значение законодательного уровня ИБ. Обзор российского законодательства в области ИБ. Правовые акты общего назначения, затрагивающие вопросы ИБ (УК–1, ПК–2).

6. Применение российского законодательства в области ИБ для решения задач обеспечения защиты информации на разных уровнях (УК–1, ПК–2).

7. Правовые акты общего назначения, затрагивающие вопросы ИБ. Работа в «Консультант плюс» (УК–1, ПК–2).

8. Стандарты и спецификации в области ИБ. Основные понятия. Классы безопасности.

9. Информационная безопасность распределенных систем. Рекомендации X.800 (УК–1, ПК–2).

10. Сетевые сервисы безопасности. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий». Требования доверия информации (УК–1, ПК–2).

11. Гармонизированные критерии Европейских стран. Интерпретация «Оранжевой книги» для сетевых конфигураций (УК–1, ПК–2).

12. Руководящие документы Гостехкомиссии России. Расследование компьютерных преступлений (УК–1, ПК–2).

13. Административный уровень информационной безопасности. Особенности политики безопасности на административном уровне (УК–1, ПК–2).

14. Программа безопасности на предприятиях различных уровней. Синхронизация программы безопасности с жизненным циклом систем (УК–1, ПК–2).

15. Процедурный уровень ИБ. Основные классы мер процедурного уровня. Управление персоналом для обеспечения защиты информации на предприятиях различных сфер. Реагирования на нарушения (УК–1, ПК–2).

16. Построение концепции информационной безопасности предприятия. Уровни, механизмы, особенности (УК–1, ПК–2).

17. Программно–аппаратные методы защиты от удаленных атак в сети Internet. Программные методы защиты, применяемые в сети Internet (УК–1, ПК–2).

18. Основные понятия программно–технического уровня ИБ. Особенности архитектурной безопасности. Идентификация, аутентификация, управление доступом (УК–1, ПК–2).

19. Определение безопасности компьютерной системы и категории требований безопасности (УК–1, ПК–2).

20. Базовые требования безопасности компьютерной системы. Классы безопасности компьютерных систем, понятие риска (УК–1, ПК–2).

21. Обзор биометрических технологий. Аппаратно–программные средства контроля доступа к информации на различных уровнях Биометрические устройства вода. Комбинированные устройства ввода. Электронные замки (УК–1, ПК–2).

22. Работа с антивирусными средствами защиты информации. Классификация антивирусных программ. Сканеры (УК–1, ПК–2).

23. Электронная цифровая подпись и особенности ее применения. Защита информации в Интернете (УК–1, ПК–2).

24. Защита информационных ресурсов в банковских системах (УК–1, ПК–2).

25. Защита информационных ресурсов в налоговых органах (УК–1, ПК–2).

26. Защита информационных ресурсов в пенсионном фонде (УК–1, ПК–2).

27. Криптологические методы защиты информации. История возникновения. Обзор современных методов кодирования (УК–1, ПК–2).

28. Шифрование текста в информационных системах. Обзор шифров и программного обеспечения (УК–1, ПК–2).

29. Цифровые методы современного шифрования информации (УК–1, ПК–2).

6.3.Шкала оценочных средств

Уровни освоения компетенций	Критерии оценивания	Оценочные средства (кол–во баллов)
Продвинутый (75 –100 баллов) «отлично»	знает – демонстрирует прекрасное знание предмета, соединяя при ответе знания из разных разделов, добавляя комментарии, пояснения, обоснования; умеет – отвечая на вопрос, может быстро и безошибочно проиллюстрировать ответ собственными примерами; свободно владеет терминологией из различных разделов курса	тестовые задания (30–40 баллов); реферат (7–10 баллов); вопросы к экзамену (38–50 баллов);
Базовый (50 –74 балла) – «хорошо»	знает – хорошо владеет всем содержанием, видит взаимосвязи, может провести анализ и т.д., но не всегда делает это самостоятельно без помощи экзаменатора умеет – может подобрать соответствующие примеры, чаще из имеющихся в учебных материалах; владеет терминологией, делая ошибки; при неверном употреблении сам может их исправить	тестовые задания (20–29 баллов); реферат (5–6 баллов); вопросы к экзамену (25–36 балл)
Пороговый (35 – 49 баллов) – «удовлетворительно»	знает – отвечает только на конкретный вопрос, соединяет знания из разных разделов курса только при наводящих вопросах экзаменатора; умеет – с трудом может соотнести теорию и практические примеры из учебных материалов; примеры не всегда правильные; владеет – редко использует при ответе термины, подменяет одни понятия другими, не всегда понимая разницы	тестовые задания (14–19 баллов); реферат (3–4 балла); вопросы к экзамену (18–26 баллов)
Низкий (допороговый) (компетенция не сформирована) (менее 35 баллов) – «не удовлетворительно»	не знает значительной части программного материала, допускает существенные ошибки; умеет – неуверенно, с большими затруднениями выполняет практические работы; не владеет терминологией	тестовые задания (0–13 баллов); реферат (0–2 балла); вопросы к экзамену (0–20 баллов)

Весь комплект 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)

7.1 Основная учебная литература:

1.Чернова, Е. В. Информационная безопасность человека: учебное пособие для вузов / Е. В. Чернова. – 3–е изд., перераб. и доп.– Москва: Издательство Юрайт, 2024. – 327 с. – (Высшее образование). – ISBN 978–5–534–16772–6. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/542739.

2. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. – 2–е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 107 с. – (Высшее образование). – ISBN 978–5–534–16388–9. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/544290.

3. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. – 2–е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 277 с. – (Высшее образование). – ISBN 978–5–534–16450–3. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/544029.

4. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. – Москва : Издательство Юрайт, 2024. – 325 с. – (Высшее образование). – ISBN 978–5–534–03600–8. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/536225.

5. Козырь, Н. С. Экономические аспекты информационной безопасности : учебник и практикум для вузов / Н. С. Козырь, Л. Л. Оганесян. – Москва : Издательство Юрайт, 2024. – 131 с. – (Высшее образование). – ISBN 978–5–534–17863–0. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/545066 .

7.2. Дополнительная учебная литература

1. Корабельников, С. М. Преступления в сфере информационной безопасности: учебное пособие для вузов / С. М. Корабельников.– Москва: Издательство Юрайт, 2024.– 111 с.– (Высшее образование).– ISBN 978–5–534–12769–0. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/543351 .

7.4. Методические указания по освоению дисциплины (модуля)

1. Грязнев А. Н. Учебно–методический комплекс по дисциплине (модулю) «Информационная безопасность». Мичуринск: Изд–во Мичуринского ГАУ, 2022 г.

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.

7.5.1 Электронно-библиотечные системы и базы данных

1. ООО «ЭБС ЛАНЬ» (https://e.lanbook.ru/) (договор на оказание услуг от 03.04.2024 № б/н (Сетевая электронная библиотека)

2. 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 09.04.2024 № 04-УТ/2024)

3.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 26.04.2024 № 1901/БП22)

4. ООО «Электронное издательство ЮРАЙТ» (https://urait.ru/) (договор на оказание услуг по предоставлению доступа к образовательной платформе ООО «Электронное издательство ЮРАЙТ» от 07.05.2024 № 6555)

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

6. База данных НЭБ «Национальная электронная библиотека» (https://rusneb.ru/) (договор о подключении к НЭБ и предоставлении доступа к объектам НЭБ от 02.02.2024 № 101/НЭБ/4712-п)

7. 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)

7.5.2. Информационные справочные системы

1. Справочная правовая система КонсультантПлюс (договор поставки, адаптации и сопровождения экземпляров систем КонсультантПлюс от 28.02.2025 № 12413 /13900/ЭС).

2. Электронный периодический справочник «Система ГАРАНТ» (договор на услуги по сопровождению от 28.02.2025 № 194-01/2025).

7.5.3. Современные профессиональные базы данных

1. База данных нормативно-правовых актов информационно-образовательной программы «Росметод» (договор от 05.09.2024 № 512/2024)

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

7.5.4. 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	MicrosoftWindows, OfficeProfessional	MicrosoftCorporation	Лицензионное	-	Лицензия от 04.06.2015 № 65291651 срок действия: бессрочно
2	Антивирусное программное обеспечение KasperskyEndpointSecurity для бизнеса	АО «Лаборатория Касперского» (Россия)	Лицензионное	https://reestr.digital.gov.ru/reestr/366574/?sphrase_id=415165	Сублицензионный договор с ООО «Софтекс» от 09.12.2024 № б/н, срок действия: с 09.12.2024 по 09.12.2025
3	МойОфисСтандартный - 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 № 0364100000819000012 срок действия: бессрочно
4	Офисный пакет «Р7-Офис» (десктопная версия)	АО «Р7»	Лицензионное	https://reestr.digital.gov.ru/reestr/306668/?sphrase_id=4435041	Контракт с ООО «Софтекс» от 24.10.2023 № 0364100000823000007 срок действия: бессрочно
5	Операционная система «Альт Образование»	ООО "Базальт свободное программное обеспечение"	Лицензионное	https://reestr.digital.gov.ru/reestr/303262/?sphrase_id=4435015	Контракт с ООО «Софтекс» от 24.10.2023 № 0364100000823000007 срок действия: бессрочно
6	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 23.05.2024 № 8151, срок действия: с 23.05.2024 по 22.05.2025
7	AcrobatReader - просмотр документов PDF, DjVU	AdobeSystems	Свободно распространяемое	-	-
8	FoxitReader - просмотр документов PDF, DjVU	FoxitCorporation	Свободно распространяемое	-	-

7.5.5. Ресурсы информационно-телекоммуникационной сети «Интернет»

1. CDTOwiki: база знаний по цифровой трансформации https://cdto.wiki/
2. Справочная правовая система ГАРАНТ. Режим доступа http://www.garant.ru
3. Справочно-правовая система «КонсультантПлюс». Режим доступа http://www.consultant.ru
4. Журнал «Аудитор». Режим доступа www. http://auditor-mag.ru

7.5.6. Цифровые инструменты, применяемые в образовательном процессе

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

7.5.7. Цифровые технологии, применяемые при изучении дисциплины

№	Цифровые технологии	Виды учебной работы, выполняемые с применением цифровой технологии	Формируемые компетенции
1.	Облачные технологии	Лекции Практические занятия	УК–1 – Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
2.	Большие данные	Лекции Практические занятия	ПК–2 – Способен собирать и анализировать информацию, необходимую для принятия решений по обеспечению экономической безопасности хозяйствующих субъектов, осуществлять стратегическое управление ключевыми экономическими показателями и бизнес–процессами

7.5. Информационные технологии (программное обеспечение и информационные справочные материалы) , в том числе современные профессиональные базы данных и информационные справочные системы

1. ООО «ЭБС ЛАНЬ» (https://e.lanbook.ru/) (договор на оказание услуг от 03.04.2024 № б/н (Сетевая электронная библиотека)

2. 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 09.04.2024 № 05–УТ/2024)

3.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 26.04.2024 № 1901/БП22)

4. ООО «Электронное издательство ЮРАЙТ» (https://urait.ru/) (договор на оказание услуг по предоставлению доступа к образовательной платформе ООО «Электронное издательство ЮРАЙТ» от 07.05.2024 № 6555)

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

6. 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)

7. 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)

8. Материально–техническое обеспечение дисциплины (модуля)

Кабинет информатики (компьютерный класс) (ул. Интернациональная, д. 101 – 1/211)	1. Доска медиум (инв. №2101041642); 2. Плоттер (инв. №1101044028); 3. Принтер LV–1100 (инв. №213/2001042316); 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.	1. Лицензия от 31.12.2006 № 18495261: Microsoft Windows XP Professional Russian, Windows Office Professional 2003 Win 32 Russian; 2. 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); 3. nanoCAD (версия 5.1 локальная, образовательная лицензия, серийный номер NC50B–270716 лицензия действительна бессрочно, бесплатная). 4. Программный комплекс «АСТ–Plus» версии 4.x.x с аппаратным ключом защиты (сервер, плейер, администратор, статистика) (лицензионный договор от 18.10.2016 № Л21/16)
Учебная аудитория для проведения занятий семинарского типа, групповых и	1. Ноутбук (инв.№1101047129). 2. Проектор Acer X113H (инв. №21013400641). 3. Экран на штативе Lumien Eco	1.Лицензия от 31.12.2013 № 49413124: Microsoft Windows XP, 7, Microsoft Office 2003, 2010. 2. Справочная

индивидуальных консультаций, текущего контроля и промежуточной аттестации (ул. Интернациональная, д. 101 – 2/50)	View с возможностью настенного крепления инв. №21013400642). 4. Макеты. 5. Наглядные учебные пособия. 6. Комплект криминалиста (ин. №.....). 7. Интерактивный лазерный тир (ин. №.....). 8. Наборы демонстрационного оборудования и учебно–наглядных пособий. Компьютерная техника подключена к сети «Интернет» и обеспечена доступом к ЭИОС университета.	правовая система Консультант Плюс (договор поставки, адаптации и сопровождения экземпляров систем Консультант Плюс от 11.03.2024 № 11921 /13900/ЭС) 3.Электронный периодический справочник «Система ГАРАНТ» (договор на услуги по сопровождению от 15.01.2024 № 194–01/2024) 4. Программная система для обнаружения текстовых заимствований в учебных и научных работах Лицензионный договор с АО «Антиплагиат» от 23.05.2024 № 8151, срок действия: с 23.05.2024 по 22.05.2025 5. База данных нормативно–правовых актов информационно–образовательной программы «Росметод» (договор от 11.07.2022 № 530/2022).
Помещение для хранения и профилактического обслуживания учебного оборудования (ул. Интернациональная, д. 101 – 2/49)	1. Компьютер Celeron (инв. № 2101041315). 2.Ксерокс Canon (инв. 2101041316). 3. Холодильник Саратов (инв.№ 2101041313). 4.Телевизор LG (инв. № 2101041317). 5. Принтер (ксерокс) Канон MF 3228 (инв. № 2101041321). 6. Компьютер OLDI 310 KD (инв. № 2101041322). 7. Компьютер С–1000 (инв. № 2101041326). 8. Компьютер С–1000 (инв. № 2101041326). 9.Сканер HP– 2200 (инв. № 2101063543). 10.Компьютер С–1100 (инв. № 1101042852).	Лицензия от 31.12.2006 № 18495261: Microsoft Windows XP Professional Russian, Windows Office Professional 2003 Win 32 Russian

	11. Компьютер 486 ДХ (инв. № 1101042853). 12. Коммутатор (инв. № 1101042854). 13. Компьютер Celeron (инв. № 210134004876). 14. Регулируемая тестовая нагрузка. 15. Портативный мультимер. 16. Набор прецизионных микроотверток для ремонта планшетогв, ноутбуков, компьютеров. 17. Набор инструментов для обслуживания ПК и ноутбуков. 18. Стеллажи, столы, ремонтные комплекты. Компьютерная техника подключена к сети «Интернет» и обеспечена доступом в ЭИОС университета.	
Помещение для самостоятельной работы (ул. Интернациональная, д. 101 – 1/210)	1.Шкаф канцелярский (инв. № 2101062853). 2.Шкаф канцелярский (инв. № 2101062852). 3.Холодильник Стинол (инв. № 2101040880). 4. Принтер HP–1100 (инв. №2101041634). 5. Принтер HP Laser Jet 1200 (инв. №1101047381). 6. Принтер Canon (инв. №2101045032). 7. МФУ Canon i–Sensys (инв. №41013400760). 8. Системный комплект (инв. №21013400429):Процессор Intel Original LGA 1155 CeleronG 1610 OEM (2.6/2 Mb), монитор 20 Asus As MS202D , материнская плата Asus, вентилятор, память, жесткий диск, корпус, клавиатура, мышь (инв. № 21013400429). 9. Ноутбук Hewlett Packard (инв.№21013400617). 10. Доска классная+маркер (инв.№	1.Лицензия от 31.12.2013 № 49413124: Microsoft Windows XP, 7, Microsoft Office 2003, 2010. 2. Справочная правовая система Консультант Плюс (договор поставки, адаптации и сопровождения экземпляров систем Консультант Плюс от 11.03.2024 № 11921 /13900/ЭС) 3.Электронный периодический справочник «Система ГАРАНТ» (договор на услуги по сопровождению от 15.01.2024 № 194–01/2024) 4. Программная система для обнаружения текстовых заимствований в учебных и научных работах Лицензионный договор с АО «Антиплагиат» от 23.05.2024 № 8151, срок действия: с 23.05.2024 по 22.05.2025 5. База данных

	1101063872). 11. Компьютер (инв.№41013401070). 12. Компьютер (инв.№41013401082). 13. Компьютер Celeron E 3300 (инв.№2101045217). 14. Компьютер Celeron E 3300 (инв.№1101047398). 15. Компьютер Dual Core (инв.№2101045268). 16. Компьютер OLDI 310 КД (инв.№2101045044). 17. Копировальный аппарат Kyocera Mita TASKalfa 180 (инв.№ 21013400369). Компьютерная техника подключена к сети «Интернет» и обеспечена доступом к ЭИОС университета.	нормативно–правовых актов информационно–образовательной программы «Росметод» (договор от 15.08.2023 № 542/2023) 6. Профессиональная база данных: Ассоциация российских банков. – Режим доступа: http://www.arb.ru 7. Профессиональная база данных: Ассоциация региональных банков России. – Режим доступа: http://www.asros.ru 8. Профессиональная база данных: Профессиональный союз негосударственной сферы безопасности. – Режим доступа: http://profnsb.ru

Рабочая программа дисциплины (модуля) «Информационная безопасность» составлена в соответствии с требованиями ФГОС ВО по специальности 38.05.01 Экономическая безопасность, утвержденного приказом Министерства образования и науки Российской Федерации № 20 от «16» января 2017 г.

Автор старший преподаватель кафедры экономической безопасности и права Грязнев А. Н.

Рецензент: доцент кафедры математики, физики и информационных технологий, к.т.н., Брижанский Л.В.

Рабочая программа рассмотрена на заседании кафедры экономической безопасности и права, протокол № 9 от «18» апреля 2022 г.

Рабочая программа рассмотрена на заседании учебно-методической комиссии Института экономики и управления Мичуринского ГАУ, протокол № 8 от «19» апреля 2022 г.

Рабочая программа утверждена Решением Учебно-методического совета университета, протокол № 8 от «21» апреля 2022 г.

Рабочая программа рассмотрена на заседании кафедры экономической безопасности и права, протокол № 11 от «9» июня 2023 г.

Рабочая программа рассмотрена на заседании учебно-методической комиссии Института экономики и управления Мичуринского ГАУ, протокол № 10 от «20» июня 2023 г.

Рабочая программа утверждена Решением Учебно-методического совета университета, протокол № 10 от «22» июня 2023 г.

Рабочая программа рассмотрена на заседании кафедры экономической безопасности и права, протокол № 11 от «06» мая 2024 г.

Рабочая программа рассмотрена на заседании учебно-методической комиссии Института экономики и управления Мичуринского ГАУ, протокол № 9 от «21» мая 2024 г.

Рабочая программа утверждена Решением Учебно-методического совета университета, протокол № 09 от 23 мая 2024 года

Рабочая программа рассмотрена на заседании кафедры экономической безопасности и права, протокол № 10 от «14» апреля 2025 г.

Программа рассмотрена на заседании учебно-методической комиссии Института экономики и управления Мичуринского ГАУ, протокол № 8 от «15» апреля 2025 г.

Программа утверждена Решением Учебно-методического совета университета, протокол № 8 от 23 апреля 2025 года

Оригинал программы хранится на кафедре экономической безопасности и права