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)
КОДИРОВАНИЕ И ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки 09.04.02 Информационные системы и технологии

Направленность (профиль) Информационные системы и технологии в АПК

Квалификация магистр

Мичуринск - 2023

1. Цели освоения дисциплины (модуля)

Целями освоения дисциплины (модуля) 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 (модуля) учитываются трудовые функции следующих профессиональных стандартов:

Профессиональный стандарт - 06.016 Руководитель проектов в области информационных технологий, утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014 г. N 893н.

Профессиональный стандарт - 06.026 Системный администратор информационно-коммуникационных систем, утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 29 сентября 2020 г. N 680н.

2. Место дисциплины (модуля) в структуре образовательной программы

Согласно учебному плану по направлению подготовки 09.04.02 Информационные системы и технологии дисциплина (модуль) «Кодирование и защита информации» относится к Блоку 1. Дисциплины (модуля) (Б1.В.ДВ.01.02)

Для освоения дисциплины (модуля) «Кодирование и защита информации» обучающиеся используют знания, умения, навыки, сформированные в ходе изучения дисциплин «Современные сетевые технологии в системах хранения данных», «Компьютерные нейросетевые технологии».

Материал дисциплины (модуля) тесно взаимосвязан с такими дисциплинами (модулями), как «Поддержка и предоставление IT сервисов в АПК». Знания, умения и навыки, сформированные в ходе изучения данной дисциплины (модуля) необходимы в дальнейшем для прохождения производственной технологической (проектно-технологической) практики, подготовки к ГИА.

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

В результате изучения дисциплины (модуля) обучающийся должен освоить трудовые функции и трудовые действия:

Трудовые функции - планирование конфигурационного управления в проектах малого и среднего уровня сложности в области ИТ. B/01.7

Трудовые действия: разработка плана конфигурационного управления, разработка правил именования и версионирования базовых элементов конфигурации, разработка правил использования репозитория проекта.

Трудовые функции - разработка планов модернизации или замены компонентов информационно-коммуникационной системы. E/02.7

Трудовые действия: Сбор данных о потребностях пользователей информационно-коммуникационной системы, анализ потребностей пользователей информационно-коммуникационной системы, прогнозирование сроков модернизации сетевых устройств, разработка краткосрочных и долгосрочных планов модернизации информационно-коммуникационной системы, планирование работ по развертыванию, конфигурированию и эксплуатации сетевых устройств, составление анкет для выявления требований и пожеланий с целью обнаружения системных проблем обработки информации, анализ выявленных требований и пожеланий с целью обнаружения системных проблем обработки информации.

Освоение дисциплины (модуля) направлено на формирование следующих компетенций:

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

ПК-1 Способен управлять проектами в области информационных технологий малого и среднего уровня сложности в условиях неопределенностей, порождаемых запросами на изменения, с применением формальных инструментов управления рисками и проблемами проекта;

ПК-2 Способен разрабатывать проекты модернизации информационно-коммуникационной системы.

Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальных компетенций	Критерии оценивания результатов обучения			
		низкий (допороговый, компетенция не сформирована)	пороговый	базовый	продвинутый
Категория универсальных компетенций - Системное и критическое мышление					
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода,вырабатывать стратегию действий	ИД-1$_{УК-1}$ – Знает принципы сбора, отбора и обобщения информации.	Не знает принципы сбора, отбора и обобщения информации.	Слабо знает принципы сбора, отбора и обобщения информации.	Хорошо знает принципы сбора, отбора и обобщения информации.	Отлично знает принципы сбора, отбора и обобщения информации.
	ИД-2$_{УК-1}$ – Умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности.	Не может соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности.	Не достаточно четко соотносит разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности.	Достаточно быстро соотносит разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности..	Успешно соотносит разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности..
	ИД-3$_{УК-1}$ – Имеет практический опыт работы с информационными источниками, опыт научного поиска, создания научных текстов.	Не имеет практического опыта работы с информационными источниками, опыт научного поиска, создания научных текстов.	Имеет маленький практического опыта работы с информационными источниками, опыт научного поиска, создания научных текстов.	Имеет достаточный практического опыта работы с информационными источниками, опыт научного поиска, создания научных текстов.	Имеет большой практического опыта работы с информационными источниками, опыт научного поиска, создания научных текстов.

Тип деятельности: проектный

ПК-1. Способен управлять проектами в области информационных технологий малого и среднего уровня сложности в условиях неопределенностей, порождаемых запросами на изменения, с применением формальных инструментов управления рисками и проблемами проекта	ИД-1$_{ПК-1}$ – Знает основы системного администрирования, возможности ИС, основы финансового планирования в проектах, типы договоров и формы договорных отношений	Не знает основы системного администрирования, возможности ИС, основы финансового планирования в проектах, типы договоров и формы договорных отношений	Слабо знает основы системного администрирования, возможности ИС, основы финансового планирования в проектах, типы договоров и формы договорных отношений	Хорошо знает основы системного администрирования, возможности ИС, основы финансового планирования в проектах, типы договоров и формы договорных отношений	Отлично знает основы системного администрирования, возможности ИС, основы финансового планирования в проектах, типы договоров и формы договорных отношений
	ИД-2$_{ПК-1}$ – Умеет проводить переговоры, анализировать исходные данные	Не умеет проводить переговоры, анализировать исходные данные	Слабо умеет проводить переговоры, анализировать исходные данные	Хорошо умеет проводить переговоры, анализировать исходные данные программирования	В совершенстве умеет проводить переговоры, анализировать исходные данные
	ИД-3$_{ПК-1}$ – Владеет управлением изменений в проекте, управлением рисками в проектах	Не владеет управлением изменений в проекте, управлением рисками в проектах	Слабо владеет управлением изменений в проекте, управлением рисками в проектах	Хорошо владеет управлением изменений в проекте, управлением рисками в проектах	В совершенстве владеет управлением изменений в проекте, управлением рисками в проектах
Тип деятельности: научно - исследовательский					
ПК-2. Способен разрабатывать проекты модернизации информационно-коммуникационной системы	ИД-1$_{ПК-2}$ – знает методы прогнозирования и оценки текущих требований к информационно-коммуникационной системе	Не знает методы прогнозирования и оценки текущих требований к информационно-коммуникационной системе	Слабо знает методы прогнозирования и оценки текущих требований к информационно-коммуникационной системе	Хорошо знает методы прогнозирования и оценки текущих требований к информационно-коммуникационной системе	Отлично знает методы прогнозирования и оценки текущих требований к информационно-коммуникационной системе
	ИД-2$_{ПК-2}$ – умеет обосновы-	Не умеет обосновывать выбор техниче-	Слабо умеет обосновывать выбор техниче-	Хорошо умеет обосновывать выбор техниче-	В совершенстве умеет обосновы-

	вать выбор технических требований к оборудованию для выполнения модернизации информационно-коммуникационной системы	ских требований к оборудованию для выполнения модернизации информационно-коммуникационной системы	ских требований к оборудованию для выполнения модернизации информационно-коммуникационной системы	ских требований к оборудованию для выполнения модернизации информационно-коммуникационной системы	вать выбор технических требований к оборудованию для выполнения модернизации информационно-коммуникационной системы
	ИД-З$_{ПК-2}$ – владеет навыками разработки планов модернизации или замены компонентов информационно-коммуникационной системы и разработки рекомендаций по обновлению информационно-коммуникационной системы.	Не владеет навыками разработки планов модернизации или замены компонентов информационно-коммуникационной системы и разработки рекомендаций по обновлению информационно-коммуникационной системы.	Слабо владеет навыками разработки планов модернизации или замены компонентов информационно-коммуникационной системы и разработки рекомендаций по обновлению информационно-коммуникационной системы.	Хорошо владеет навыками разработки планов модернизации или замены компонентов информационно-коммуникационной системы и разработки рекомендаций по обновлению информационно-коммуникационной системы.	В совершенстве владеет навыками разработки планов модернизации или замены компонентов информационно-коммуникационной системы и разработки рекомендаций по обновлению информационно-коммуникационной системы.

В результате изучения дисциплины (модуля) 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), приоритеты собственной деятельности и способы ее совершенствования на основе самооценки;

уметь разрабатывать проекты модернизации информационно-коммуникационной системы, управлять проектами в области информационных технологий малого и среднего уровня сложности в условиях неопределенностей, порождаемых запросами на изменения, с применением формальных инструментов управления рисками и проблемами проекта, при-

менять 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, осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий, определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки, осуществлять критический анализ проблемных ситуаций на основе системного подхода,вырабатывать стратегию действий.

владеть навыками управления проектами в области информационных технологий малого и среднего уровня сложности в условиях неопределенностей, порождаемых запросами на изменения, с применением формальных инструментов управления рисками и проблемами проекта, способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий, способами разработки проектов модернизации информационно-коммуникационной системы.

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

Темы, разделы дисциплины (модуля)	Компетенции			Общее количество компетенций
	УК-1	ПК-1	ПК-2	
1. Основные понятия и определения в области информационной безопасности автоматизированных систем	+	+	+	3
2. Основные виды уязвимостейавтоматизированных систем	+	+	+	3
3. Основные виды информационных атак	+	+	+	3
4. Модели защиты автоматизированных системот информационных атак	+	+	+	3
5. Анализ существующихмоделей процесса обнаружения информационных атак	+	+	+	3
6. Аудит информационнойбезопасности и оценка рисков	+	+	+	3
7. Обзор существующих средств защиты информации	+	+	+	3

4. Структура и содержание дисциплины (модуля)

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

4.1. Объем дисциплины (модуля) и виды учебной работы

Виды занятий	Количество ак. часов	
	по очной форме обучения 3 семестр	по заочной форме обучения 2 курс
Общая трудоемкость дисциплины (модуля)	180	180
Контактная работа обучающихся с преподавателем, в т.ч.	48	28
аудиторные занятия, из них	48	28
лекции	16	12
практические работы	32	16
Самостоятельная работа обучающихся	132	148
проработка учебного материала по дисциплине (конспектов лекций, учебников, материалов сетевых ресурсов)	105	105
выполнение индивидуальных заданий	17	33
подготовка к тестированию	10	10
Контроль	-	4
Вид итогового контроля	зачет	

4.2. Лекции

№	Раздел дисциплины (модуля), темы лекций и их содержание	Объем в ак. часах		Формирующие компетенции
		очная форма обучения	заочная форма обучения	
1.	Основные понятия и определения в области информационной безопасности автоматизированных систем	2	2	УК-1, ПК-1, ПК-2
2.	Основные виды уязвимостейавтоматизированных систем	2	2	УК-1, ПК-1, ПК-2
	Основные виды информационных атак	2	2	УК-1, ПК-1, ПК-2
4.	Модели защиты автоматизированных системот информационных атак	2	2	УК-1, ПК-1, ПК-2
5.	Анализ существующихмоделей процесса обнаружения информационных атак	2	2	УК-1, ПК-1, ПК-2
6.	Аудит информационнойбезопасности и оценка рисков	3	1	УК-1, ПК-1, ПК-2
7.	Обзор существующих средств защиты информации	3	1	УК-1, ПК-1, ПК-2
Всего		16	12	

4.3. Практические занятия

№	Раздел дисциплины (модуля) (модуля),темы лекций и их содержание	Объем в ак.часах		Формирующие компетенции
		очная форма обучения	заочная форма обучения	
1.	Основные понятия и определения в области информационной безопасности автоматизированных систем	4	2	УК-1, ПК-1, ПК-2
2.	Основные виды уязвимостейавтоматизированных систем	4	2	УК-1, ПК-1, ПК-2
3.	Основные виды информационных атак	4	2	УК-1, ПК-1, ПК-2
4.	Модели защиты автоматизированных системот информационных атак	4	2	УК-1, ПК-1, ПК-2
5.	Анализ существующихмоделей процесса обнаружения информационных атак	4	2	УК-1, ПК-1, ПК-2
6.	Аудит информационнойбезопасности и оценка рисков	6	2	УК-1, ПК-1, ПК-2
7.	Обзор существующих средств защиты информации	6	4	УК-1, ПК-1, ПК-2
Всего		32	16	

4.4. Лабораторные работы

Лабораторные работы не предусмотрены.

4.5. Самостоятельная работа обучающихся

Раздел дисциплины (модуля)	Вид самостоятельной работы	Объем ак. часов	
		очная форма обучения	заочная форма обучения
1. Основные понятия и определения в областиинформационной безопасности автоматизированных систем	Проработка учебного материала по дисциплине (конспектов лекций, учебников, материалов сетевых ресурсов)	15	15
	Выполнение индивидуальных заданий	2	6
	Подготовка к тестированию	2	2
2. Основные виды уязвимостей автоматизированных систем	Проработка учебного материала по дисциплине (конспектов лекций, учебников, материалов сетевых ресурсов)	15	15
	Выполнение индивидуальных заданий	2	6
	Подготовка к тестированию	2	2
3. Основные виды информационных атак	Проработка учебного материала по дисциплине (конспектов лекций, учебников, материалов сетевых ресурсов)	15	15
	Выполнение индивидуальных заданий	2	6
	Подготовка к тестированию	2	2

4. Модели защиты автоматизированных систем от информационных атак	Проработка учебного материала по дисциплине (конспектов лекций, учебников, материалов сетевых ресурсов)	15	15
	Выполнение индивидуальных заданий	3	6
	Подготовка к тестированию	2	2
5. Анализ существующих моделей процесса обнаружения информационных атак	Проработка учебного материала по дисциплине (конспектов лекций, учебников, материалов сетевых ресурсов)	15	15
	Выполнение индивидуальных заданий	4	6
	Подготовка к тестированию	1	1
6. Аудит информационной безопасности и оценка рисков	Проработка учебного материала по дисциплине (конспектов лекций, учебников, материалов сетевых ресурсов)	15	15
	Выполнение индивидуальных заданий	4	3
	Подготовка к тестированию	1	1
7. Обзор существующих средств защиты информации	Проработка учебного материала по дисциплине (конспектов лекций, учебников, материалов сетевых ресурсов)	15	15
Итого:		132	148

Методические указания для проведения практических занятий по дисциплине «Кодирование и защита информации» для направления подготовки 09.04.02 Информационные системы и технологии . – Мичуринск, 2021.

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.

Целью контрольной работы по дисциплине является рассмотрение теоретических аспектов и применение основного инструментария управления научным исследованием.

Требования к оформлению.

Контрольная работа может быть выполнена в ученической (школьной) тетради или на листах формата А4 печатным или рукописным (четким, читаемым) способом. Выполненные задания располагаются по представленному порядку. Список используемой литературы приводится в конце работы.

На титульном листе располагается следующая информация: название дисциплины, Ф.И.О. обучающийся, курс, группа, номер зачѐтной книжки, номер выбранного варианта и номера выполненных заданий по порядку в следующем виде:

Сроки выполнения**.** Выполненная контрольная работа подписывается обучающимся и сдается на проверку преподавателю на кафедру «Математики, физики и информационных технологий» в установленные сроки, как правило, за 10 дней до начала сессии. Проверка контрольной работы преподавателем осуществляется в течение недели после ее сдачи. Контрольная работа должна быть зачтена к началу экзаменационной сессии.

4.7. Содержание разделов дисциплины (модуля)

1. Основные понятия и определения в области информационной безопасности автоматизированных систем Информация как основной объект защиты. Автоматизированная система как среда для обработки, хранения и передачи информации

2. Основные виды уязвимостей автоматизированных систем

Уязвимости «buffer overflow». Уязвимости «SQL injection». Уязвимости «format string». Уязвимости «Directory traversal» . Уязвимости «Cross Site Scripting» . Уязвимости программных реализаций стека TCP/IP.Уязвимости протоколов стека TCP/IP.

3. Основные виды информационных атак Стадия рекогносцировки. Стадия

вторжения и атакующего воздействия. Стадия дальнейшего развития атаки. Возможные последствия информационных атак

3. Модели защиты автоматизированных систем от информационных атак.
Анализ существующих моделей информационных атак. Табличные и диаграммные модели информационных атак. Формализованные модели информационных атак. Математическая модель информационных атак, построенная на основе теоретико- множественного аппарата.

5. Анализ существующих моделей процесса обнаружения информационных атак. Сигнатурные модели процесса обнаружения атак. Поведенческие модели процесса выявления атак. Поведенческая модель выявления аномалий в сетевом трафике.

6. Аудит информационной безопасности и оценка рисков Основные понятия аудита безопасности. Модели оценки рисков информационной безопасности. Модель оценки рисков, базирующаяся на основе графовой модели атак. Особенности использования графовой модели оценки рисков безопасности.

7. Обзор существующих средств защиты информации. Средства криптографической защиты информации. Средства разграничения доступа пользователей к информационным ресурсам АС. Средства межсетевого экранирования.

5. Образовательные технологии

При изучении дисциплины (модуля) используются инновационные образовательные технологии на основе интеграции компетентностного и личностно-ориентированного подходов с элементами 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.
Практические 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 (модуля)

Основными видами дисциплинарных оценочных средств при функционировании модульно-рейтинговой системы обучения являются: на стадии рубежного рейтинга, формируемого по результатам модульного компьютерного тестирования – тестовые задания; на стадии поощрительного рейтинга, формируемого по результатам написания и защиты рефератов по актуальной проблематике, на стадии промежуточного рейтинга, определяемого по результатам сдачи зачета – теоретические вопросы, контролирующие теоретическое содержание учебного материала, и компетентностно-ориентированные задания, контролирующие практические навыки из различных видов профессиональной деятельности обучающегося по ОПОП данного направления, формируемые при изучении дисциплины (модуля) «Кодирование и защита информации»

6.1. Паспорт фонда оценочных средств по дисциплине

№ п/п	Контролируемые разделы (темы) дисциплины (модуля)	Код контролируемой компетенции	Оценочное средство	
			Наименование	Количество

1.	Основные понятия и определения в областиинформационной безопасности автоматизированных систем	УК-1, ПК-1, ПК-2	Тестовые задания Темы рефератов Вопросы для зачета	15 3 5
2.	Основные виды уязвимостейавтоматизированных систем	УК-1, ПК-1, ПК-2	Тестовые задания Темы рефератов Вопросы для зачета	18 3 5
3.	Основные виды информационных атак	УК-1, ПК-1, ПК-2	Тестовые задания Темы рефератов Вопросы для зачета	17 3 4
4.	Модели защиты автоматизированных системот информационных атак	УК-1, ПК-1, ПК-2	Тестовые задания Темы рефератов Вопросы для зачета	18 3 4
5.	Анализ существующих моделей процесса обнаружения информационных атак	УК-1, ПК-1, ПК-2	Тестовые задания Темы рефератов Вопросы для зачета	10 3 4
6.	Аудит информационной безопасности и оценка рисков	УК-1, ПК-1, ПК-2	Тестовые задания Темы рефератов Вопросы для зачета	10 3 4
7.	Обзор существующих средств защиты информации	УК-1, ПК-1, ПК-2	Тестовые задания Темы рефератов Вопросы для зачета	12 2 4

6.2. **Перечень вопросов для зачета** (УК-1, ПК-1, ПК-2)

1. Информация как основной объект защиты.
2. Автоматизированная система как среда для обработки, хранения и передачи информации.
3. Уязвимости «buffer overflow».
4. Уязвимости «SQL injection».
5. Уязвимости «format string».
6. Уязвимости «Directory traversal» .
7. Уязвимости «Cross Site Scripting» .
8. Уязвимости программных реализаций стека TCP/IP.
9. Уязвимости протоколов стека TCP/IP.
10. Стадия рекогносцировки.
11. Стадия вторжения и атакующего воздействия.
12. Стадия дальнейшего развития атаки.
13. Возможные последствия информационных атак.
14. Анализ существующих моделей информационных атак.
15. Табличные и диаграммные модели информационных атак.
16. Формализованные модели информационных атак.
17. Математическая модель информационных атак, построенная на основе теоретико-множественного аппарата.
18. Сигнатурные модели процесса обнаружения атак.
19. Поведенческие модели процесса выявления атак.
20. Поведенческая модель выявления аномалий в сетевом трафике.
21. Основные понятия аудита безопасности.
22. Модели оценки рисков информационной безопасности.
23. Модель оценки рисков, базирующаяся на основе графовой модели атак.

24. Особенности использования графовой модели оценки рисков безопасности.
25. Средства криптографической защиты информации.
26. Средства разграничения доступа пользователей к информационным ресурсам АС.
27. Средства межсетевого экранирования.
28. Аутентификация пользователей на основе сетевых адресов.
29. Аутентификация пользователей на основе паролей.
30. Биометрическая аутентификация пользователей.

6.3. Шкала оценочных средств

Уровни освоения компетенций	Критерии оценивания	Оценочные средства (кол-во баллов)
Продвинутый (75-100 баллов) «зачтено»	Отлично знает принципы сбора, отбора и обобщения информации. Имеет большой практический опыт работы с информационными источниками, опыт научного поиска. В совершенстве владеет управлением изменений в проекте, управлением рисками в проектах. В совершенстве умеет обосновывать выбор технических требований к оборудованию для выполнения модернизации информационно-коммуникационной системы. На этом уровне обучающийся способен творчески применять полученные знания путем самостоятельного конструирования способа деятельности.	тестовые задания (30-40 баллов) индивидуальное задание (8-10 баллов); вопросы к зачету (37-50 баллов)
Базовый (50-74 балла) «зачтено»	Хорошо знает принципы сбора, отбора и обобщения информации. Имеет достаточный практического опыта работы с информационными источниками, опыт научного поиска, создания научных текстов. Хорошо владеет управлением изменений в проекте, управлением рисками в проектах. Хорошо умеет обосновывать выбор технических требований к оборудованию для выполнения модернизации информационно-коммуникационной системы. На этом уровне обучающимся используется комбинирование известных приемов деятельности, эвристического мышления.	тестовые задания (20-30 баллов) индивидуальное задание (5-7 баллов); вопросы к зачету (25-37 баллов)
Пороговый (35-49 баллов) «зачтено»	Слабо знает принципы сбора, отбора и обобщения информации. Имеет маленький практического опыта работы с информационными источниками, опыт научного поиска, создания научных текстов. Слабо владеет управлением изменений в проекте, управлением рисками в проектах. Слабо умеет обосновывать выбор технических требований к оборудованию для выполнения модернизации информационно-коммуникационной системы. На этом уровне обучающийся способен по памяти воспроизводить ранее усвоенную методику.	тестовые задания (15-20 баллов) индивидуальное задание (2-4 балла); вопросы к зачету (18-25 баллов)
Низкий (допороговый)	Не знает принципы сбора, отбора и обобщения информации. Не имеет практического опыта работы с	тестовые задания (0-13 баллов);

(компетенция не сформирована) (менее 35 баллов) «не зачтено»	информационными источниками, опыт научного поиска, создания научных текстов. Не владеет управлением изменений в проекте, управлением рисками в проектах. Не умеет обосновывать выбор технических требований к оборудованию для выполнения модернизации информационно-коммуникационной системы	индивидуальное задание (0-3 балла); вопросы к зачету (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. *Акмаров*, П. Б. Кодирование и защита информации: учебное пособие / П. Б. Акмаров. — Ижевск : Ижевская ГСХА, 2016. — 136 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/133975 (дата обращения: 29.09.2021). — Режим доступа: для авториз. пользователей.

2. *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

3. *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

4. *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

5. *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

6. УМКД «Кодирование и защита информации» для направления подготовки 09.04.02 Информационные системы и технологии, Мичуринск -2021

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 (модуля)

Методические указания для проведения практических занятий по дисциплине «Кодирование и защита информации» для направления подготовки 09.04.02 Информационные системы и технологии

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. Основы безопасности веб-приложенийhttps://martinfowler.com/articles/web-security-basics.html

7. Профессиональные базы данных. им. Е.И. Овсянкина. Информационная безопасность. Защита информацииhttp://all-ib.ru/

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	АО «Лаборатория Касперского»	Лицензионное	https://reestr.digital.gov.ru/reestr/366574/?sphrase_id=415165	Сублицензионный договор с ООО «Софтекс» от

	Endpoint Security для бизнеса	(Россия)			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 - просмотр документов PDF, DjVU	Foxit Corporation	Свободно распространяемое	-	-

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).
6. Сайт Федеральной службы государственной статистики (Росстат). Электронный ресурс. Режим доступа: http://www.gks.ru/
7. Сайт Территориального органа Федеральной службы государственной статистики по Тамбовской области (Тамбовстат). Электронный ресурс. Режим доступа: http://tmb.gks.ru/
8. Режим доступа: http://www.rbc.ru/ - РосБизнесКонсалтинг
9. Режим доступа: http://www.devbusiness.ru/development/staff.htm
10. Сайт высшей аттестационной комиссии // http://vak.ed.gov.ru

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

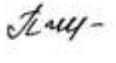
№	Цифровые технологии	Виды учебной работы, выполняемые с применением цифровой технологии	Формируемые компетенции
1.	Облачные технологии	Лекции Практические работы (Лабораторные работы)	ПК-1, ПК-2
2.	Технологии беспроводной связи	Лекции Практические работы (Лабораторные работы)	ПК-1, ПК-2
3.	Новые производственные технологии	Лекции Практические работы (Лабораторные работы)	ПК-1, ПК-2

8. Материально-техническое обеспечение дисциплины (модуля) (модуля)

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
393760, Россия, Тамбовская область, г. Мичуринск, ул. Интернациональная, дом № 101, 2/32	Учебная аудитория для проведения учебных занятий лекционного типа: Интерактивная доска – 1 шт.; Системный комплект – 1 шт.; Проектор Viewsonic – 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий.
393760, Россия, Тамбовская область, г. Мичуринск, ул. Интернациональная, дом № 101, 1/114	Учебная аудитория для проведения учебных занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (компьютерный класс): Системный комплект (Процессор Intel Original LGA 1155 Celeron) – 9 шт.; Кабинет оснащен макетами, наглядными учебными пособиями, тренажерами и другими техническими средствами. Компьютерная техника подключена к сети «Интернет» и обеспечена доступом в ЭИОС университета.
393760, Тамбовская область, г. Мичуринск, ул. Интернациональная, дом № 101, 1/210	Помещение для самостоятельной работы: принтер – 3 шт., МФУ Canon i-Sensys MF 4410, ноутбук Hewlett Packard Pavilion, компьютер – 3 шт, компьютер Celeron E 3300, компьютер Dual Core, компьютер OLDI 310 КД, копировальный аппарат Kyocera. Компьютерная техника подключена к сети «Интернет» и обеспечен доступ в электронную информационно-образовательную среду университета.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО – магистратура по направлению подготовки 09.04.02 Информационные системы и технологии, утвержденного приказом Минобрнауки РФ № 917 от 19.09.2017

Автор:
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. 

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 №10 от 24 июня 2021 года.

Программа переработана и дополнена в соответствии с требованиями ФГОС ВО.

Программа рассмотрена на заседании кафедры математики, физики и информационных технологий. Протокол № 7 от «14» марта 2022 г.

Программа рассмотрена на заседании учебно-методической комиссии инженерного института ФГБОУ ВО Мичуринский ГАУ, протокол № 8 от 17 марта 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.