МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ – МСХА имени К.А. ТИМИРЯЗЕВА»
(ФГБОУ ВО РГАУ - МСХА имени К.А. Тимирязева)

Институт экономики и управления АПК
Кафедра прикладной информатики

УТВЕРЖДАЮ:
Директор института
экономики и управления АПК
_____ Л.И. Хоружий
“__28__” ____08_____ 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.17 Информационная безопасность

для подготовки бакалавров

ФГОС ВО

Направление: 09.03.03 Прикладная информатика
Направленность: Системы искусственного интеллекта,
Программные решения для бизнеса

Курс 4
Семестр 7

Форма обучения: очная

Год начала подготовки: 2025

Москва, 2025

Разработчик (и): Худякова Е.В., д.э.н., профессор
(ФИО, ученая степень, ученое звание) (подпись)

(ФИО, ученая степень, ученое звание) (подпись)

« 28 » августа 2025 г.

Рецензент: Щедрина Е.А., к.пед.н., доцент
(ФИО, ученая степень, ученое звание) (подпись)

« 28 » августа 2025 г.

Программа составлена в соответствии с требованиями ФГОС ВО, профессионального стандарта и учебного плана по направлению подготовки 09.03.03 «Прикладная информатика»

Программа обсуждена на заседании кафедры прикладной информатики
протокол №1 от « 28 » августа 2025 г.

И.о. зав. кафедрой
прикладной информатики Худякова Е.В., д.э.н., профессор
(ФИО, ученая степень, ученое звание) (подпись)

« 28 » августа 2025 г.

Согласовано:

Председатель учебно-методической комиссии
института экономики и управления АПК
Гупалова Т.Н., к.э.н., доцент
(ФИО, ученая степень, ученое звание) (подпись)

« 28 » августа 2025 г.

И.о. заведующего выпускающей кафедрой
прикладной информатики Худякова Е.В., д.э.н., профессор
(ФИО, ученая степень, ученое звание) (подпись)

« 28 » августа 2025 г.

Заведующий отделом комплектования ЦНБ
(подпись)

СОДЕРЖАНИЕ

Аннотация
рабочей программы учебной дисциплины (индекс)
«Б1.О.17» Информационная безопасность
для подготовки бакалавра по направлению 09.03.03 «Прикладная информатика» направленности «Системы искусственного интеллекта», «Программные решения для бизнеса»

Цель освоения дисциплины: формирование у студентов компетенций в области информационной безопасности, а также развитие способности оценивать риски и разрабатывать меры защиты информации в различных информационных системах. Студенты должны овладеть методами защиты данных, средствами защиты сетевых и программных ресурсов, а также основами обеспечения конфиденциальности, целостности и доступности информации.

Место дисциплины в учебном плане: дисциплина включена в часть, формируемую участниками образовательных отношений учебного плана по направлению подготовки 09.03.03 «Прикладная информатика».

Требования к результатам освоения дисциплины: в результате освоения дисциплины формируются следующие компетенции (индикаторы): ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-4.3

Краткое содержание дисциплины:

Принципы построения компьютерных сетей. Типовая IP-сеть организации. Классификация сетевых уязвимостей и атак. Работа с базами атак и уязвимостей. Защитные механизмы и средства обеспечения безопасности. Базовые принципы сетевого взаимодействия. Стек сетевых протоколов операционных систем. Принципы функционирования сетевых протоколов, включающих криптографические алгоритмы. Риски, угрозы, уязвимости, атаки. Встроенные средства защиты в ОС. Идентификация и аутентификация. Разграничение доступа к ресурсам. Защита сетевого взаимодействия. Повышение уровня защищенности рабочей среды пользователей.

Общая трудоемкость дисциплины: 144/4 (часы/зач. ед.).

Промежуточный контроль: экзамен в 7 семестре.

1. Цель освоения дисциплины

Целью освоения дисциплины «Информационная безопасность» является формирование у студентов знаний и навыков в области информационной безопасности, необходимых для обеспечения защиты информации в современных информационных системах. Студенты изучат основные угрозы информационной безопасности, методы и средства защиты данных, а также принципы обеспечения конфиденциальности, целостности и доступности информации. Особое внимание будет уделено защите информации в сетевых и распределенных системах, а также управлению рисками безопасности. В рамках дисциплины студенты научатся анализировать возможные угрозы и разрабатывать эффективные меры защиты для предотвращения утечек и атак. Освоение дисциплины

также включает изучение актуальных стандартов и нормативных актов в области информационной безопасности.

2. Место дисциплины в учебном процессе

Дисциплина «Информационная безопасность» включена в часть, формируемую участниками образовательных отношений учебного плана направления 09.03.03 «Прикладная информатика», осваивается в 7 семестре. Дисциплина «Информационная безопасность» реализуется в соответствии с требованиями ФГОС ВО, ОПОП ВО и Учебного плана по направлению 09.03.03

«Прикладная информатика».

Предшествующими дисциплинами, на которых базируется дисциплина

«Информационная безопасность», являются: «Администрирование информационных систем», «Моделирование информационных систем», «Алгоритмизация и програмирование», «Операционные системы».

Рабочая программа дисциплины «Информационная безопасность» для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Образовательные результаты освоения дисциплины обучающимся, представлены в таблице 1.

Таблица 1

Требования к результатам освоения учебной дисциплины

№ п/п	Код компетенции	Содержание компетенции (или её части)	Индикаторы компетенций	В результате изучения учебной дисциплины обучающиеся должны:		
				знать	уметь	владеть
1	ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1 Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	основы информационной и библиографической культуры, типы информационных ресурсов, базовые положения информационной безопасности в ИКТ-среде	определять релевантные источники и каналы получения информации, учитывать требования к защите данных и правовой режим использования материалов	правилами корректного цитирования, ссылок и оформления заимствований с учетом норм информационной безопасности
			ОПК-3.2 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	методы структурирования и систематизации информации, принципы построения поисковых запросов и навигации по электронным ресурсам	формулировать информационные запросы, отбирать и интерпретировать полученные данные для решения прикладных задач	навыками применения офисных, сетевых и облачных сервисов для создания, совместного использования и хранения информации
			ОПК-3.3 Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научноисследовательской работе с учетом требований информационной безопасности	основные жанры научных текстов, требования к структуре обзора, аннотации, статьи и доклада, библиографические стандарты	анализировать и обобщать результаты исследований, формулировать выводы и оформлять их в виде обзоров, докладов и публикаций	инструментами управления библиографией, средствами набора и верстки научных текстов и презентаций с учетом ограничений по доступу и конфиденциальности

2	ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.3 Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы.	структуру технического задания, спецификаций, руководств пользователя и администратора, эксплуатационной документации	формализовать требования, описывать функции, ограничения и условия эксплуатации информационных систем понятным и однозначным языком	навыками подготовки документации, адаптированной к разным категориям пользователей и специалистов сопровождения

4. Структура и содержание дисциплины

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 4 зач. единицы (144 часов), их распределение по видам работ в 8 и 9 семестре представлено в табл. 2.

Таблица 2

Распределение трудоёмкости дисциплины по видам работ по семестрам

Вид учебной работы	Трудоёмкость		
	час.	в т.ч. в семестре	в т.ч. в семестре
		№ 7	
Общая трудоёмкость дисциплины по учебному плану	**144**	**144**	
1. Контактная работа:	**52,4**	**52,4**	
Аудиторная работа	**52,4**	**52,4**	
лекции (Л)	16	16	
практические занятия (ПЗ)	34	34	
контактная работа на промежуточном контроле (КРА)	0,4	0,4	
2. Самостоятельная работа (СРС)	**55,6**	**55,6**	
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к практическим занятиям и т.д.)	47,6	47,6	
Подготовка к экзамену (контроль)	8,6	8,6	
Вид промежуточного контроля:		экзамен	

4.2 Содержание дисциплины

Тематический план учебной дисциплины

Таблица 3

Наименование разделов и тем дисциплины	Всего часов на раздел	Аудиторная работа			Внеаудиторная работа
		Л	ПЗ	ПКР	СР
Тема 1. Принципы построения компьютерных сетей и базовые принципы сетевого взаимодействия	**36**	**2**	**4**	**-**	**5**
Тема 2. Сетевые уязвимости, атаки и методы их обнаружения	**19**	**2**	**6**	**-**	**10**

Наименование разделов и тем дисциплины	Всего часов на раздел	Аудиторная работа			Внеаудиторная работа
		Л	ПЗ	ПКР	СР
Тема 3. Безопасность физических и канальных уровней сети	**21**	**4**	**8**	**-**	**10**
Тема 4. Защита периметра и трафика сети	**19**	**2**	**8**	**-**	**10**
Тема 5. Анализ защищённости сети и превентивные механизмы защиты	**21**	**4**	**6**	**-**	**10**
Тема 6. Угрозы безопасности и встроенные средства защиты операционных систем	**27,6**	**2**	**4**	**-**	**10,6**
Контактная работа на промежуточном	**0,4**	**-**	**-**	**0,4**	**-**
Итого по дисциплине	**144**	**16**	**34**	**0,4**	**55,6**

Тема 1. Принципы построения компьютерных сетей и базовые принципы сетевого взаимодействия

Основные принципы построения компьютерных сетей, модели OSI и TCP/IP, компоненты типовой IP-сети организации, маршрутизация и управление трафиком, протоколы передачи данных, назначение и структура подсетей, базовые принципы сетевого взаимодействия, технологии коммутации и маршрутизации.

Тема 2. Сетевые уязвимости, атаки и методы их обнаружения

Классификация сетевых уязвимостей, типы атак (пассивные, активные, внутренние, внешние), работа с базами данных атак и уязвимостей (CVE), типичные уязвимости приложений (DNS, HTTP, FTP), системы обнаружения вторжений (IDS), методы анализа сетевого трафика, признаки сетевых атак, предотвращение распространённых атак (DDoS, атаки на пароли, SQL-инъекции).

Тема 3. Безопасность физических и канальных уровней сети

Проблемы физической безопасности сети, защита оборудования от несанкционированного доступа, уязвимости протокола ARP, защита на канальном уровне, применение стандарта 802.1x, механизмы контроля доступа на уровне порта, проблемы безопасности беспроводных сетей, физическое разделение сетей, защита каналов связи.

Тема 4. Защита периметра и трафика сети

Основы защиты периметра сети, межсетевые экраны и их конфигурация, системы предотвращения вторжений (IPS), защита трафика на сетевом уровне (VPN, IPsec), шифрование данных, безопасность транспортного уровня (TLS/SSL), фильтрация трафика, анализ маршрутов и управление политиками доступа, предотвращение утечек данных.

Тема 5. Анализ защищённости сети и превентивные механизмы защиты

Методы тестирования сети на наличие уязвимостей, инструменты анализа защищённости (Nmap, Wireshark), аудит безопасности сети, разработка превентивных мер, составление отчётов по защищённости, оценка рисков, мониторинг активности пользователей, анализ сетевых логов, применение рекомендаций по повышению уровня защищённости сети.

Тема 6. Угрозы безопасности и встроенные средства защиты операционных систем

Изучаются риски, угрозы и уязвимости операционных систем, а также способы их минимизации. Анализируются встроенные средства защиты операционных систем, включая антивирусы, межсетевые экраны, механизмы разграничения доступа и встроенные функции мониторинга безопасности.

4.3 Лекции/практические занятия

Таблица 4

Содержание лекций/практических занятий и контрольные мероприятия

№ п/п	Название раздела, темы	№ и название лекций/ лабораторных/ практических/ семинарских занятий	Формируемые компетенции	Вид контрольного мероприятия	Кол-во Часов/ из них практическая подготовка
1.	**Раздел 1.** Основы и теоретические аспекты цифровой трансформации				
	Тема 1. Принципы построения компьютерных сетей и базовые принципы сетевого взаимодействия	Лекция № 1. Принципы построения компьютерных сетей и основы сетевого взаимодействия	ОПК-3.1, ОПК-3.2	Устный опрос	2
	Тема 2. Сетевые уязвимости, атаки и методы их обнаружения	Лекция № 2. Сетевые уязвимости, атаки и методы их обнаружения	ОПК-3.2, ОПК-3.3	Устный опрос	2
	Тема 3. Безопасность физических и канальных уровней се-	Лекция № 3. Безопасность физических и канальных уровней сети	ОПК-3.1, ОПК-3.2	Устный опрос	2
		Практическое занятие № 1. Оценка уязвимостей и мето-	ОПК-3.2, ОПК-3.3	Защита практиче-	2

№ п/п	Название раздела, темы	№ и название лекций/ лабораторных/ практических/ семинарских занятий	Формируемые компетенции	Вид контрольного мероприятия	Кол-во Часов/ из них практическая подготовка
	ти	дов защиты физических и канальных уровней сети		ской работы № 1	
	Тема 4. Защита периметра и трафика сети	Практическое занятие № 2. Настройка и анализ средств защиты периметра и трафика сети	ОПК-4.3	Защита практической работы № 2	2
	Тема 5. Анализ защищённости сети и превентивные механизмы защиты	Практическое занятие № 3. Оценка защищённости сети и применение превентивных механизмов защиты	ОПК-4.3	Защита практической работы № 3	2
2.	**Раздел 2.** Оценка экономической эффективности ИТ и ИС				
	Тема 6. Угрозы безопасности и встроенные средства защиты операционных систем	Практическое занятие № 4. Анализ угроз безопасности и настройка встроенных средств защиты операционных систем	ОПК-3.2, ОПК-3.3	Защита практической работы № 4	2

Таблица 5

Перечень вопросов для самостоятельного изучения дисциплины

№ п/п	Название раздела, темы	Перечень рассматриваемых вопросов для самостоятельного изучения
1.	Тема 1. Принципы построения компьютерных сетей и базовые принципы сетевого взаимодействия	Основные принципы построения компьютерных сетей, модели OSI и TCP/IP, компоненты типовой IP-сети организации, маршрутизация и управление трафиком, протоколы передачи данных, назначение и структура подсетей, базовые принципы сетевого взаимодействия, технологии коммутации и маршрутизации (ОПК-3.1, ОПК-3.2).
2.	Тема 2. Сетевые уязвимости, атаки и методы их обнаружения	Классификация сетевых уязвимостей, типы атак (пассивные, активные, внутренние, внешние), работа с базами данных атак и уязвимостей (CVE), типичные уязвимости приложений (DNS, HTTP, FTP), системы обнаружения вторжений (IDS), методы анализа сетевого трафика, признаки сетевых

№ п/п	Название раздела, темы	Перечень рассматриваемых вопросов для самостоятельного изучения
		атак, предотвращение распространённых атак (DDoS, атаки на пароли, SQL-инъекции) (ОПК-3.2, ОПК-3.3).
3.	Тема 3. Безопасность физических и канальных уровней сети	Проблемы физической безопасности сети, защита оборудования от несанкционированного доступа, уязвимости протокола ARP, защита на канальном уровне, применение стандарта 802.1x, механизмы контроля доступа на уровне порта, проблемы безопасности беспроводных сетей, физическое разделение сетей, защита каналов связи (ОПК-3.1, ОПК-3.2, ОПК-3.3).
4.	Тема 4. Защита периметра и трафика сети	Основы защиты периметра сети, межсетевые экраны и их конфигурация, системы предотвращения вторжений (IPS), защита трафика на сетевом уровне (VPN, IPsec), шифрование данных, безопасность транспортного уровня (TLS/SSL), фильтрация трафика, анализ маршрутов и управление политиками доступа, предотвращение утечек данных (ОПК-3.2, ОПК-3.3)
5.	Тема 5. Анализ защищённости сети и превентивные механизмы защиты	Методы тестирования сети на наличие уязвимостей, инструменты анализа защищённости (Nmap, Wireshark), аудит безопасности сети, разработка превентивных мер, составление отчётов по защищённости, оценка рисков, мониторинг активности пользователей, анализ сетевых логов, применение рекомендаций по повышению уровня защищённости сети (ОПК-4.3).
6.	Тема 6. Угрозы безопасности и встроенные средства защиты операционных систем	Что включает в себя техническое задание на разработку информационной системы. Этапы разработки ТЗ. Методология и стандарты разработки ТЗ. Влияние требований заказчика на содержание ТЗ. Риски, связанные с недостаточной проработкой ТЗ (ОПК-4.3).

5. Образовательные технологии

При реализации программы дисциплины используются следующие современные методики и технологии обучения:

- гибкая архитектура программ – 25% содержания ежегодно обновляется с участием индустрии с учетом отраслевой направленности;
- адаптивные технологии взаимодействия с профессионалами из индустрии (наставничество, кейсы от индустриальных партнеров);
- проектно-соревновательный подход – хакатоны и командные решения отраслевых задач;
- проблемно-ориентированное обучение – работа над кейсами от индустриальных партнёров;
- решение практических задач на практических занятиях в лабораториях центра «Институт цифровой трансформации в АПК».

Таблица 6

Применение активных и интерактивных образовательных технологий

№ п/п	Тема и форма занятия		Наименование используемых активных и интерактивных образовательных технологий
1.	Принципы построения компьютерных сетей и базовые принципы сетевого взаимодействия	Л	Лекция-визуализация
2.	Сетевые уязвимости, атаки и методы их обнаружения	Л	Лекция-визуализация
3.	Безопасность физических и канальных уровней сети	Л	Лекция-визуализация
		ПЗ	Проблемно-поисковое занятие, творческие задания, групповое обсуждение
4.	Защита периметра и трафика сети	ПЗ	Проблемно-поисковое занятие, творческие задания, групповое обсуждение
5.	Анализ защищённости сети и превентивные механизмы защиты	ПЗ	Проблемно-поисковое занятие, творческие задания, групповое обсуждение
6.	Угрозы безопасности и встроенные средства защиты операционных систем	ПЗ	Проблемно-поисковое занятие, творческие задания, групповое обсуждение

6. Текущий контроль успеваемости и промежутзаочная аттестация по итогам освоения дисциплины

6.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности

6.1.1 Вопросы для устного опроса

Устный опрос проводится по первой, второй и третьей темам дисциплины «Информационная безопасность».

Тема 1. Принципы построения компьютерных сетей и базовые принципы сетевого взаимодействия

1. Что такое компьютерная сеть и какие основные типы сетей существуют?
2. Какие принципы лежат в основе построения локальных и глобальных компьютерных сетей?
3. Каковы основные компоненты компьютерной сети и их функции?

4. Что такое модель OSI и как она используется для организации сетевого взаимодействия?

5. Какие функции выполняют канальный и сетевой уровни модели OSI?

6. В чем заключается принцип адресации в компьютерных сетях?

7. Как происходит обмен данными между узлами сети и что такое протоколы связи?

8. Чем отличается коммутация пакетов от коммутации цепей в компьютерных сетях?

9. Какую роль в сетевом взаимодействии играет IP-адресация?

10. Что такое шлюз и как он используется для подключения различных сетей?

Тема 2. Сетевые уязвимости, атаки и методы их обнаружения

1. Что такое сетевые уязвимости и как они могут быть использованы злоумышленниками?

2. Какие виды атак на компьютерные сети существуют и как они классифицируются?

3. Что такое атака "отказ в обслуживании" (DoS) и как она влияет на функционирование сети?

4. Каковы особенности атак "человек посередине" (MITM) и методы их предотвращения?

5. Что такое SQL-инъекция и как она может быть использована для атак на сети?

6. Какие методы используются для обнаружения сетевых уязвимостей и их устранения?

7. Что такое сетевой сканер и как он используется для поиска уязвимостей в сети?

8. Какую роль в защите сети играют системы обнаружения вторжений (IDS)?

9. Какова разница между активными и пассивными методами обнаружения сетевых атак?

10. Что такое уязвимость нулевого дня (zero-day) и как она может повлиять на безопасность сети?

Тема 3. Безопасность физических и канальных уровней сети

1. Что такое физический уровень сети и какие угрозы безопасности могут возникать на этом уровне?

2. Каковы основные методы защиты канала связи на канальном уровне?

3. В чем заключается роль криптографических технологий в обеспечении безопасности на физическом уровне сети?

4. Какую роль в безопасности канала связи играет метод доступа к среде передачи данных (например, CSMA/CD)?

5. Какие уязвимости существуют в беспроводных сетях на физическом и канальном уровнях?

6. Как защита физических устройств (например, сетевых карт и маршрутизаторов) может повлиять на общую безопасность сети?

7. Что такое атака "перехват канала" и как она может быть предотвращена на физическом уровне?

8. Каковы основные способы защиты от атаки "подавление сигнала" в беспроводных сетях?

9. Какие методы аутентификации и контроля доступа используются для защиты канала связи?

10. Как принципы изоляции и сегментации на физическом и канальном уровнях помогают повышать безопасность сети?

6.1.2 Примеры заданий для практических работ

Перечень практических работ прикреплен к оценочным материалам дисциплине.

6.1.3 Перечень вопросов, выносимых на экзамен

1. Что такое компьютерная сеть и какие основные типы сетей существуют?

2. Охарактеризуйте основные принципы построения локальных и глобальных сетей.

3. В чем заключается принцип адресации в компьютерных сетях? Объясните, как работает IP-адресация.

4. Какие функции выполняет модель OSI и как она используется для организации сетевого взаимодействия?

5. Чем отличается коммутация пакетов от коммутации цепей?

6. Каковы основные протоколы канала передачи данных на канальном уровне?

7. Что такое маршрутизация и как она реализуется в компьютерных сетях?

8. В чем заключается роль сетевых устройств, таких как маршрутизаторы, коммутаторы и шлюзы, в обеспечении сетевого взаимодействия?

9. Что такое сетевые уязвимости и как их можно классифицировать?

10. Какие существуют основные виды атак на компьютерные сети и как они классифицируются?

11. Охарактеризуйте атаку "отказ в обслуживании" (DoS) и методы её предотвращения.

12. Что такое атака "человек посередине" (MITM)? Как её можно предотвратить?

13. Какие инструменты можно использовать для сканирования сети на уязвимости?

14. Как работает система обнаружения вторжений (IDS) и какие методы её работы?

15. Что такое уязвимость нулевого дня (zero-day) и чем она опасна для сети?

16. Чем отличаются активные и пассивные методы обнаружения атак в сети?

17. Какие угрозы существуют на физическом уровне сети?

18. Охарактеризуйте атаки на канальный уровень сети, такие как "перехват канала" или "подмена MAC-адресов".

19. Как можно обеспечить безопасность физической среды передачи данных, включая защиту от воздействия электромагнитных излучений?

20. Что такое техника "сканирования сети" и как её можно использовать для анализа уязвимостей канала связи?

21. Какие средства защиты существуют для обеспечения безопасности на канальном уровне (например, фильтрация MAC-адресов)?

22. В чем заключается роль криптографических технологий на канальном уровне для обеспечения безопасности данных?

23. Как защитить беспроводные сети на канальном уровне от перехвата и других атак?

24. Что такое защита периметра сети и какие основные методы защиты существуют?

25. Как работает межсетевой экран (firewall) и какие правила необходимо настроить для защиты сети?

26. Что такое NAT (Network Address Translation) и как он способствует безопасности сети?

27. Какую роль играют системы предотвращения вторжений (IPS) в защите периметра сети?

28. Какие методы используются для защиты трафика сети от атак, таких как eavesdropping или манипуляции с данными?

29. Что такое VPN и как он используется для защиты периметра сети?

30. Какие виды шифрования трафика применяются для защиты данных в процессе передачи?

31. Как настроить защиту от DDoS-атак на уровне периметра сети?

32. Какие методы оценки защищённости сети существуют?

33. Как проводится сканирование на уязвимости в сети с помощью инструментов, таких как Nessus или OpenVAS?

34. Что такое превентивная защита и какие её основные механизмы?

35. Как настроить системы защиты, чтобы предотвратить атаки на уровне сети (например, через фильтрацию и блокировку нежелательных пакетов)?

36. Как применяются технологии шифрования для защиты данных в сети?

37. Как работают системы управления уязвимостями и как они помогают предотвращать угрозы безопасности?

38. Какие принципы защиты важны при построении безопасной сети?

39. Как настроить системы мониторинга и анализа трафика для своевременного обнаружения угроз?

40. Какие угрозы безопасности характерны для операционных систем?

41. Какие встроенные средства защиты существуют в операционных системах (например, антивирусы, фаерволы, контроль доступа)?

42. Как настроить встроенные средства защиты операционной системы для защиты от вирусов и других вредоносных программ?

43. Что такое управление правами доступа и как оно влияет на безопасность операционной системы?

44. Как защитить операционную систему от атак через уязвимости в приложениях?

45. Как работает шифрование данных в операционных системах и какие методы защиты данных на уровне ОС существуют?

46. Что такое контроль целостности системы и как он помогает в обеспечении безопасности?

47. Как встроенные средства защиты операционной системы могут помочь в предотвращении атак, таких как SQL-инъекции или удалённое выполнение кода?

48. Что такое защита от вредоносных программ в операционных системах и как она работает?

Кейс-задача №1

«Архитектура комплексной системы мониторинга АПК»

Описание кейса. Россельхозбанк совместно с Проектным институтом цифровой трансформации АПК формирует систему мониторинга хозяйств. Она объединяет данные IoT сенсоров с полей и ферм, спутниковые снимки, данные о кредитах и субсидиях. Студент участвует в проектировании архитектуры: модули сбора и валидации данных, витрины BigData, модули ML прогнозирования урожайности и DSS дашборды. Сложность кейса — необходимость связать разнородные источники и обеспечить работу в реальном времени.

Задача: Разработать архитектуру интегрированной ИИ-системы мониторинга сельхозпредприятий.

Область применения: Цифровые платформы АПК, агроаналитика.

Кейс-задача №2

«Интеграция модуля компьютерного зрения в банковскую антифрод-систему»

Описание кейса. Антифрод-системы РСХБ анализируют транзакционные данные, но не учитывают биометрию. Для повышения защищённости Студент проектирует и внедряет модуль CV для распознавания и верификации лиц. Решение должно интегрироваться в существующую платформу банка, работать как на устройствах в офисах, так и в мобильных приложениях.

Важная часть — обеспечить точность и устойчивость моделей при работе на реальных потоках клиентов.

Задача: Реализовать модуль CV и встроить его в антифрод- систему банка.

Область применения: Финансовая безопасность, биометрия.

Кейс-задача №3

«Конвейер данных (DataOps) для скоринга и мониторинга хозяйств проектного института»

Описание кейса. Банковские и агроданные поступают из множества источников — госреестры, IoT-сенсоры, транзакции, климатические сервисы.

Студент разрабатывает сквозной пайплайн: автоматический сбор данных, валидация, очистка, построение витрин и мониторинг качества.

Задача: Спроектировать ETL/ELT- конвейер с контролем качества и версионностью данных.

Область применения: Big Data- платформы РСХБ.

Кейс-задача №4

«Платформа потоковой аналитики транзакций (real- time anti-fraud)»

Описание кейса. Финансовые операции клиентов должны контролироваться в реальном времени. Студент проектирует систему обработки потоков транзакций: event streaming, детекция аномалий и моментальная отправка алертов. Работа включает настройку Kafka/Spark Streaming, интеграцию с антифрод-сервисами и тестирование скорости реакции.

Задача: Реализовать потоковую архитектуру для выявления подозрительных транзакций.

Область применения: Финансовая безопасность, антифрод.

6.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Для оценки знаний, умений, навыков и формирования компетенций по дисциплине применяется традиционная система контроля и оценки успеваемости студентов.

При использовании традиционной системы контроля и оценки успеваемости студентов представлены критерии выставления оценок по четырехбалльной системе «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Промежуточный контроль знаний по дисциплине «Интеллектуальный анализ данных» проводится в форме экзамена. Критерии оценивания результатов обучения представлены в таблице 7.

Таблица 7

Критерии оценивания результатов обучения

Экзамен	Критерии оценивания
Высокий уровень «5» (отлично)	Оценку «**отлично**» заслуживает студент, освоивший знания, умения, компетенции и теоретический материал дисциплины без пробелов; практические навыки профессионального применения освоенных знаний сформированы. Студент самостоятельно и полностью раскрывает сущность теоретических вопросов, использует возможности программных средств для решения прикладных задач; подтверждает ответ конкретными примерами; правильно и обстоятельно отвечает на дополнительные вопросы.
Средний уровень «4» (хорошо)	Оценку **«хорошо»** заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал дисциплины; практические навыки студента в основном сформированы. Студент допускает незначительные ошибки в ответах, самостоятельно использует функции программных средств, подтверждает свои ответы конкретными примерами.

Пороговый уровень «3» (удовлетворительно)	Оценку **«удовлетворительно»** заслуживает студент, частично (с пробелами) освоивший знания, умения, компетенции и теоретический материал дисциплины; некоторые практические навыки студента не сформированы. Студент не может самостоятельно использовать значительную часть функций программных средств, затрудняется подтвердить свои ответы конкретными примерами; неполно отвечает на дополнительные вопросы.
Минимальный уровень «2» (неудовлетворительно)	Оценку «**неудовлетворительно»** заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал дисциплины; практические навыки студента не сформированы. Студент не может использовать программные средства при решении прикладных задач, подтвердить ответы конкретными примерами, не отвечает на дополнительные вопросы преподавателя.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1 Основная литература

1. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург : Лань, 2025. — 400 с. — ISBN 978-5-507-49250-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/414947 (дата обращения: 28.08.2025). — Режим доступа: для авториз. пользователей.

2. Информационная безопасность : учебное пособие / В. И. Лойко, В. Н. Лаптев, Г. А. Аршинов, С. Н. Лаптев. — Краснодар : КубГАУ, 2020. — 332 с. — ISBN 978-5-907346-50-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/254168 (дата обращения: 28.08.2025). — Режим доступа: для авториз. пользователей.

3. Басыня, Е. А. Сетевая информационная безопасность : учебник / Е. А. Басыня. — Москва : НИЯУ МИФИ, 2023. — 224 с. — ISBN 978-5-7262-2949-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/355511 (дата обращения: 28.08.2025). — Режим доступа: для авториз. пользователей.

7.2 Дополнительная литература

1. Раченко, Т. А. Информационная безопасность : учебно-методическое пособие / Т. А. Раченко. — Тольятти : ТГУ, 2025. — 135 с. — ISBN 978-5-8259-1612-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/427130 (дата обращения: 28.08.2025). — Режим доступа: для авториз. пользователей.

2. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург :

Лань, 2023. — 124 с. — ISBN 978-5-507-46010-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/293009 (дата обращения: 28.08.2025). — Режим доступа: для авториз. пользователей.

3. Волк, В. К. Базы данных. Проектирование, программирование, управление и администрирование : учебник для вузов / В. К. Волк. — 5-е изд., стер. — Санкт-Петербург : Лань, 2025. — 244 с. — ISBN 978-5-507-53648-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/493991 (дата обращения: 22.08.2025). — Режим доступа: для авториз. пользователей.

4. Баланов, А. Н. Создание цифровых экосистем : учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 480 с. — ISBN 978-5-507-49668-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/428036 (дата обращения: 22.08.2025). — Режим доступа: для авториз. пользователей.

5. Минаков, И. А. Экономика предприятий АПК / И. А. Минаков. — 3-е изд., перераб. и доп. — Санкт-Петербург : Лань, 2023. — 272 с. — ISBN 978-5-507-46081-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/327161 (дата обращения: 22.08.2025). — Режим доступа: для авториз. пользователей.

7.3 Журналы из «Белого списка» и Материалы конференций A/A

1. Anpeng Wu, Haoxuan Li, Chunyuan Zheng, Kun Kuang, and Kun Zhang. 2025. Classifying Treatment Responders: Bounds and Algorithms. In Proceedings of the 31st ACM SIGKDD Conference on Knowledge Discovery and Data Mining V.1 (KDD ’25), August 3–7, 2025, Toronto, ON, Canada. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3690624.3709191. – URL: https://dl.acm.org/doi/pdf/10.1145/3690624.3709191

2. Mina Dalirrooyfard, Konstantin Makarychev, Slobodan Mitrović Pruned Pivot: Correlation Clustering Algorithm for Dynamic, Parallel, and Local Computation Models // Proceedings of the 41 st International Conference on Machine Learning, Vienna, Austria. PMLR 235, 2024. – PP. – URL: https://openreview.net/pdf?id=saP7s0ZgYE

3. Jianhua Zhao, Changchun Shang, Shulan Li, Ling Xin, Philip L. H. Yu: Choosing the number of factors in factor analysis with incomplete data via a novel hierarchical Bayesian information criterion. Adv. Data Anal. Classif. 19(1): 209-235 (2025) – URL: https://link.springer.com/article/10.1007/s11634-024-00582-w

4. Подбор конференций уровня A/A*. – URL: https://portal.core.edu.au/conf-ranks/?search=A*+&by=all&source=CORE2023&sort=atitle&page=1

5. Материалы конференции International Conference on Machine Learning (ICML). – URL https://dblp.uni-trier.de/db/conf/icml/index.html

6. Материалы конференции ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD). – URL: https://dblp.uni-trier.de/db/conf/kdd/index.html

7. Материалы конференции Conference on Neural Information Processing Systems (NeurIPS). – URL: https://dblp.uni-trier.de/db/conf/nips/index.html

8. Материалы конференции Conference on Empirical Methods in Natural Language Processing (EMNLP). – URL: https://dblp.uni-trier.de/db/conf/emnlp/index.html

9. Материалы конференции European Conference on Computer Vision (ECCV). – URL: https://dblp.uni-trier.de/db/conf/emnlp/index.html

10. Материалы конференции IEEE International Conference on Data Mining (ICDM). – URL: https://dblp.uni-trier.de/db/conf/icdm/index.html и др.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Для освоения материала дисциплины рекомендуется использовать следующие Интернет-ресурсы:

1. . Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [Электронный ресурс]: принят Государственной Думой 8 июля 2006 г. — Режим доступа: [http://pravo.gov.ru]

2. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: принят Государственной Думой 12 июля 2017 г. — Режим доступа: [http://pravo.gov.ru].

3. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [Электронный ресурс]: принят Государственной Думой 25 марта 2011 г. — Режим доступа: [http://pravo.gov.ru].

4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]: принят Государственной Думой 8 июля 2006 г. — Режим доступа: [http://pravo.gov.ru].

5. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

6. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации в организациях банковской системы Российской Федерации. Общие положения».

7. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

8. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифро-

вальных (криптографических) средств защиты информации».

9. Перечень программного обеспечения

Для чтения лекций по дисциплине «Информационная безопасность» требуется аудитория, оснащенная мультимедийным оборудованием.

Для проведения практических занятий требуется сетевой компьютерный класс, оборудованный ПЭВМ с установленным клиентским программным обеспечением из расчета одна ПЭВМ на одного человека. Необходимое программное обеспечение в компьютерном классе перечислено в п. 8.

Таблица 8

Перечень программного обеспечения

№ п/п	Наименование темы учебной дисциплины	Наименование программы	Тип программы	Автор	Год разработки
1	Тема 1-8	Google Chrome	web-браузер	Google	2003 или выше
		Консультант Плюс, Гарант	справочно-правовая	Консультант-Плюс, Гарант	2003 или выше
		MS Office	пакет приложений	Microsoft Corp.	2003 или выше
		Deductor Studio Pro	аналитическая	BaseGroup Labs	2003 или выше

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Инфраструктурное обеспечение ОПОП ВО

в области искусственного интеллекта

Инфраструктура для реализации базового блока по глубокому и машинному обучению при подготовки бакалавров направления 09.03.03 Прикладная информатика по профилю «Системы искусственного интеллекта» включает аппаратное оборудования и специализированного программное обеспечение для выполнения высокопроизводительных вычислений, и позволяет выполнять для эффективное обучения глубоких нейронных сетей, использовать фреймворки для разработки и развёртывания моделей глубоких нейронных сетей, инструменты управления данными для обработки и хранения данных, облачные платформы, перифейрийные устройства и датчики для для создания систем искусственного интеллекта под задачи агропромышленного комплекса, что обеспечивает формирование практических навыков и компетенций у обучающихся, необходимых в профессиональной деятельности в сфере искусственного интеллекта и анализа данных.

Аппаратная части инфраструктуры позволяет решить задачи

- обеспечения высокопроизводительных вычислений для обработки больших объёмов данных и тренировки моделей машинного обучения;

- развёртывания специализированных серверов и облачных сервисов для GPU-вычислений и распределенных расчётов;

- организации хранилищ данных с высокой пропускной способностью и масштабируемостью;

- обеспечить возможность параллельной обработки больших объёмов данных за счет высокопроизводительных серверов и вычислительных кластеров позволяют масштабировать обучение моделей, .

Проведение учебных занятий (практических и лабораторных), курсовых работ и проектов работ, проектной деятельности, по блокам дисциплин глубокого обучения с использованием аппаратных средств поддержки высокопроизводительных вычислений компьютерных классов и лаборатории искусственного интеллекта классов, включающих:

- 17 профессиональных рабочих станций с процессорами Intel i9, графическими ускорителями NVIDIA GeForce RTX 4090, 128 ГБ оперативной памяти и 1 ТБ SSD;
- серверное оборудование: два модуля с суммарной производительностью 772 потока, 262 ГБ оперативной памяти и 87 ТБ SSD;
- высокопроизводительные процессоры Intel Xeon Gold/Platinum;
- GPU-кластер на базе NVIDIA H100 (7168 ГБ ОЗУ, 110 производительных ядер, 220 потоков, 400 ГБ видеопамяти, 84 480 CUDA-ядер, 72 ТБ хранилища, сеть 10 Гбит/с с резервированием);
- системы хранения Lenovo Storage V3700 V2 и «Гравитон» (до 600 накопителей, поддержка NVMe/SAS/SATA, интеграция с VMware, Hyper-V и Proxmox).

Программная часть инфраструктуры

Проведение учебных занятий (практических и лабораторных), курсовых работ и проектов работ, проектной деятельности, по блокам дисциплин глубокого обучения осуществляется с использованием программных средств поддержки высокопроизводительных вычислений компьютерных классов и лаборатории искусственного интеллекта классов, включающих:

1. Экосистему разработки и анализа данных

Инструменты для работы с данными, построения моделей, автоматизации и оптимизации процессов:

- Языки и окружения: Jupyter, Anaconda, Google Colaboratory, Visual Studio Code (VS Code), GitFlic.
- Библиотеки машинного обучения: Scikit-learn, Theano, Apache MXNet, Chainer, Fast.ai, Microsoft Cognitive Toolkit (CNTK), Deeplearning4j, ML.NET, XGBoost, Rasa, DeepSpeed.
- Фреймворки и системы глубокого обучения: TensorFlow, PyTorch, Keras, PaddlePaddle, Hugging Face Transformers.
- Инструменты для распределённых вычислений и управления процессами: Apache Hadoop, Apache Spark, Apache Airflow, Apache NiFi, Dask, Ray, Optuna, MLflow.
- Средства интеграции и потоковой обработки: Apache Kafka.
- Статистический и математический анализ: EViews, Stata/IC, Statistica 6 Ru, Mathcad Express, Wolfram Mathematica.
- Инструменты для моделирования и симуляций: Anilogic.

- Среды разработки интерфейсов: Qt Creator, Qt Designer.

2. Инструменты компьютерного зрения и анализа изображений

Используются для обработки фото-, видео- и сенсорных данных:

- Библиотеки и фреймворки: Open Source Computer Vision Library (OpenCV), Caffe, ONNX (Open Neural Network Exchange), Fast.ai, PaddlePaddle.
- Специализированные пакеты: Scanex image processor, Point Cloud Library (PCL).

3. BI-платформы и инструменты аналитики

Для визуализации, аналитики и принятия решений:

- BI-системы и дашборды: QGIS, PowerBI, Grafana.
- Отраслевые инструменты: ExactFarming, ExactScoring.

4. Системы управления данными и базами

Реляционные и нереляционные СУБД:

- PostgreSQL, MySQL, Microsoft SQL Server, MongoDB.

В учебном процессе используется инфраструктура учебно-научных лабораторий Центра «Проектный институт цифровой трансформации АПК», деятельность которого построена на принципах синергии между академическими знаниями и реальными потребностями агропромышленного комплекса. Стратегия направлена на создание устойчивой экосистемы, где студенты, преподаватели и бизнес-партнёры совместно разрабатывают решения для цифровизации отрасли, используя R&D-направления как основу для образовательных модулей и кейсов:

1. IoT-лаборатория (тестирование защищённых каналов управления сенсорами, IPv6/5G).
2. Лаборатория больших данных (контроль качества и предобработка датасетов).
3. Лаборатория цифровых двойников (моделирование агро-объектов).
4. Лаборатория ГИС и ДЗЗ (адаптация геоплатформ под точное земледелие).
5. Лаборатория информационной безопасности (аудит агро-ИТ-систем).
6. Лаборатория биоинформатики (геномные и фенотипические базы данных).
7. Лаборатория цифровых продуктов (прототипирование API и интерфейсов).
8. Лаборатория ИИ в АПК (верификация отраслевых моделей).

В учебном процессе особое место занимает IoT-полигон «Цифровое растениеводство и сельхозаналитика», создаваемый при поддержке индустриального партнёра – АО «Россельхозбанк». Его деятельность строится на принципах тесной интеграции образовательной среды и реального сектора экономики. Полигон обеспечивает студентам возможность работать с актуальными технологиями и оборудованием, применяемыми в агробизнесе, и формировать практические компетенции, напрямую востребованные отраслью.

Ключевая особенность полигона – использование отраслевых BI-платформ ExactFarming и ExactScoring, которые применяются в индустрии для анализа производственных данных и построения предиктивных моделей. Благодаря этому учебные модули

и практические кейсы строятся не на абстрактных примерах, а на реальных данных и инструментах, используемых агрохолдингами и фермерскими хозяйствами.

Стратегия функционирования полигона направлена на то, чтобы образовательные модули и проектная работа студентов опирались на реальные запросы индустриального партнёра. В учебные дисциплины интегрированы кейсы по анализу IoT-данных, разработке систем агроскоринга, предиктивному моделированию урожайности и созданию цифровых сервисов для сельского хозяйства. Для их реализации используются следующие оборудование и технологии:

- сенсорные столы NexTable с интерактивной ГИС-подложкой;
- зона проектной аналитики на 15–20 рабочих мест;
- VR-зона для иммерсивной работы с цифровыми двойниками хозяйств;
- витрины с IoT-датчиками (Metos, Sentek, MD514D) и симуляторами устройств;
- BI-дашборды ситуационного центра с аналитикой в реальном времени на базе ExactFarming и ExactScoring.

Такой формат позволяет студентам совместно с экспертами Россельхозбанка и индустриальными наставниками осваивать полный цикл работы с данными: от сбора информации с сенсоров и её предобработки – до визуализации, построения аналитических моделей и разработки готовых цифровых сервисов. В результате IoT-полигон становится связующим звеном между университетом и индустрией: он не только поддерживает научно-образовательную деятельность, но и формирует у студентов опыт взаимодействия с заказчиком, понимание требований бизнеса и готовность к внедрению решений в агропромышленный комплекс.

Робототехнические и сенсорные комплексы используются не как отдельные демонстрационные устройства, а как элементы сквозных образовательных сценариев.

- коллаборативные роботы AUBO-i5, xArm6 с системами машинного зрения интегрированы в занятия по компьютерному зрению и интеллектуальным системам управления: студенты программируют их действия, создают алгоритмы сортировки продукции и автоматизированного контроля качества, фактически имитируя задачи производственной роботизации в АПК;

- мобильные бионические платформы Unitree Go2 EDU позволяют моделировать работу автономных интеллектуальных систем: студенты разрабатывают алгоритмы навигации, анализа сенсорных данных и принятия решений в реальном времени. Такие кейсы приближают их к задачам роботизированного мониторинга хозяйств и сервисного применения ИИ в сельском хозяйстве.;

- почвенные датчики (pH, электропроводимость, влажность, солёность) дают возможность формировать собственные массивы данных для анализа. Студенты измеряют параметры почвы, готовят датасеты и используют их в дисциплинах по предиктивной аналитике и цифровому растениеводству. В результате лабораторные работы превращаются в полноценные исследования, где ИИ применяется для прогноза урожайности и оптимизации агротехнологий.;

- лидары DJI Zenmuse L1, NAVMOPO S1, спектральные камеры и 3D-сканеры применяются для построения цифровых карт и моделей полей. На этих данных студенты учатся выявлять болезни растений, определять биомассу и оценивать эффективность агротехнических мероприятий. Полученные результаты интегрируются в проекты по созданию цифровых двойников агроэкосистем.;

Характеристика материально-технического обеспечения учебного процесса при подготовке специалистов в области ИИ представлена в приложении Г.2 – «Сведения об обеспеченности образовательного процесса специализированными лабораториями».

Лекции по дисциплине проводятся в специализированной аудитории, оборудованной мультимедийным проектором для демонстрации компьютерных презентаций. Для проведения практических занятий требуется сетевой компьютерный класс, оборудованный ПЭВМ с установленным клиентским программным обеспечением из расчета, одна ПЭВМ на одного человека. Необходимое программное обеспечение в компьютерном классе перечислено в п. 9 настоящей рабочей программы.

Таблица 9

Сведения об обеспеченности специализированными аудиториями, кабинетами, лабораториями

Наименование специальных помещений и помещений для самостоятельной работы (№ учебного корпуса, № аудитории)	**Оснащенность специальных помещений и помещений для самостоятельной работы**
1	2
Аудитория для проведения занятий лекционного типа, *групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации* (№ 309, уч. корпус № 12)	Видеопроектор и экран для вывода изображения через проектор
Аудитория для проведения практических занятий, *групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации* (№310, уч. корпус №12)	Персональные компьютеры в количестве 24 штук
Аудитория для проведения практических занятий, *групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации* (№315, уч. корпус №12)	Персональные компьютеры в количестве 20 штук
Центральная научная библиотека имени Н.И. Железнова, читальный зал	
Общежитие, комнаты для самоподготовки	

11. Методические рекомендации студентам по освоению дисциплины

Освоение теоретических основ дисциплины предусматривает прослушивание и проработку материала лекций, работу с рекомендованными литературными источниками и Интернет-ресурсами. Лекции читаются в аудиториях, оснащенных мультимедийной техникой, на основе подготовленных презентаций.

Практические навыки по дисциплине приобретаются на практических занятиях. Практические занятия проводятся в компьютерных классах, оснащенных соответствующими техническими и программными средствами. В процессе выполнения заданий практических работ студенты могут обращаться к преподавателю за консультацией по конкретным вопросам.

Самостоятельная работа студентов организуется в соответствии с требованиями п. 4.3 настоящей рабочей программы. Студент обязан в полном объеме использовать предусмотренное время для изучения вопросов, вынесенных на самостоятельное изучение. Во время самостоятельной работы студент прорабатывает материал лекций и обязательной учебной литературы. В случае возникновения затруднений в освоении материала дисци-

плины студент обращается к преподавателю за разъяснениями во время, отведенное для индивидуальных консультаций.

Виды и формы отработки пропущенных занятий

Студент, пропустивший занятие лекционного типа, обязан отработать его в одной из следующих форм:

- самостоятельная проработка студентом лекционного материала с использованием рекомендуемой литературы, компьютерных презентаций и конспектов, выполненных другими студентами, с последующим устным опросом;
- реферат на тему, предложенную преподавателем.

При непосещении практического занятия студент обязан его отработать во внеаудиторное время и прийти подготовленным к следующему занятию. Студент самостоятельно прорабатывает материал пропущенного занятия с использованием основной и дополнительной литературы по дисциплине и компьютерных презентаций к лекциям.

12. Методические рекомендации преподавателям по организации обучения по дисциплине

Мультимедийные презентации по дисциплине используются на всех интерактивных лекционных занятиях. Иллюстрационный материал демонстрируется студентам с использованием спецоборудования (мультимедийного проектора) для компьютерных презентаций и программы Microsoft Power Point.

В лекциях рассматриваются только те вопросы, которые не выносятся на самостоятельное изучение. Определенная часть времени лекции выделяется на то, чтобы сориентировать студентов в использовании рекомендуемой литературы и других элементов учебно-методического комплекса дисциплины. Детально рассматриваются основные термины и категории понятийного уровня, что позволяет студентам освоить профессиональную терминологию и легко адаптироваться к реальным условиям производственной, научной и образовательной деятельности.

Практические занятия проводятся в сетевых компьютерных классах, оснащенных соответствующими техническими и программными средствами. Студенты должны быть проинструктированы по технике безопасности работы в компьютерных классах и обязаны выполнять требования инструкций, а также ставить в известность преподавателя и (или) сотрудников УИТ РГАУ-МСХА имени К.А. Тимирязева о фактах нарушения техники безопасности.

Если в процессе выполнения практических работ студент не находит решения стоящих перед ним задач, преподаватель индивидуально консультирует его по конкретным вопросам, связанным с применением изученной методики к конкретному объекту исследования (конкретным данным). Во время практических занятий для целей взаимного обучения разрешается коммуникация между студентами, не выходящая за рамки целей занятия.

При проведении практических занятий следует ориентироваться на современные активные и интерактивные образовательные технологии, основанные на принципах открытости, взаимодействия, активности обучаемых, равенства их аргументов, опоры на групповой опыт, обязательной обратной связи.

Программу разработали:

Музалев К.С. ассистент _____

Худякова Е.В., д.э.н., профессор _____

РЕЦЕНЗИЯ

рабочей программы учебной дисциплины (индекс) «Б1.О.17» Информационная безопасность
для подготовки бакалавра по направлению 09.03.03 «Прикладная информатика» направленности «Системы искусственного интеллекта», «Программные решения для бизнеса»

Ашмариной Татьяной Игоревной, доцентом кафедры экономики ФГБОУ ВО РГАУ-МСХА имени К.А. Тимирязева, кандидатом экономических наук (далее по тексту рецензент) проведена рецензия рабочей программы дисциплины «Информационная безопасность» ОПОП ВО по направлению 09.03.03 «Прикладная информатика», направленность «Системы искусственного интеллекта», «Программные решения для бизнеса» (бакалавриат), разработанной в ФГБОУ ВО «Российский государственный аграрный университет – МСХА имени К.А. Тимирязева» на кафедре прикладной информатики (разработчики – Степанцевич М.Н., доцент, к.э.н.; Худякова Е.В., профессор, д.э.н.).

Рассмотрев представленные на рецензию материалы, рецензент пришел к следующим выводам:

1. Предъявленная рабочая программа дисциплины «Информационная безопасность» (далее по тексту Программа) *соответствует* требованиям ФГОС ВО по направлению 09.03.03 «Прикладная информатика», компетентностно-ролевым моделям в сфере искусственного интеллекта. Программа *содержит* все основные разделы, *соответствует* требованиям к нормативно-методическим документам.

2. Представленная в Программе ***актуальность*** учебной дисциплины в рамках реализации ОПОП ВО *не подлежит сомнению* – дисциплина относится к обязательной части учебного цикла – Б1.О.17

3. Представленные в Программе ***цели*** дисциплины *соответствуют* требованиям ФГОС ВО направления 09.03.03 «Прикладная информатика» и компетентностно-ролевыми моделями в сфере искусственного интеллекта.

В соответствии с учебным планом и компетентностно-ролевыми моделями в сфере искусственного интеллекта, Программой за дисциплиной «Информационная безопасность» закреплены одна универсальная и две общепрофессиональных (УК-10.1; УК-10.2; УК-10.3; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-4.1; ОПК-4.2; ОПК-4.3.) ***компетенций***. Дисциплина «Информационная безопасность» и представленная Программа *способна реализовать* их в объявленных требованиях.

4. ***Результаты обучения***, представленные в Программе в категориях знать, уметь, владеть *соответствуют* специфике и содержанию дисциплины и *демонстрируют возможность* получения заявленных результатов.

5. Общая трудоёмкость дисциплины «Информационная безопасность» составляет 4 зачётные единицы (144 часов).

6. Информация о взаимосвязи изучаемых дисциплин и вопросам исключения дублирования в содержании дисциплин *соответствует* действительности. Дисциплина «Информационная безопасность» взаимосвязана с другими дисциплинами ОПОП ВО и Учебного плана по направлению 09.03.03 «Прикладная информатика» и возможность дублирования в содержании отсутствует.

7. Представленная Программа предполагает использование современных образовательных технологий, используемые при реализации различных видов учебной работы. Формы образовательных технологий *соответствуют* специфике дисциплины.

8. Программа дисциплины «Информационная безопасность» предполагает проведение занятий в интерактивной форме.

9. Виды, содержание и трудоёмкость самостоятельной работы студентов, представленные в Программе, *соответствуют* требованиям к подготовке выпускников, содержащимся во ФГОС ВО направления 09.03.03 «Прикладная информатика».

10. Представленные и описанные в Программе формы *текущей* оценки знаний (устный опрос, как в форме обсуждения отдельных вопросов, так и выступления, защита практических работ, защита проектной работы), *соответствуют* специфике дисциплины и требованиям к выпускникам.

Форма промежуточного контроля знаний студентов, предусмотренная Программой, осуществляется в форме экзамена, что *соответствует* статусу дисциплины, как дисциплины обязательной части учебного цикла – Б1.О.17 ФГОС ВО направления 09.03.03 «Прикладная информатика»**.**

11. Формы оценки знаний, представленные в Программе, *соответствуют* специфике дисциплины и требованиям к выпускникам.

12. Учебно-методическое обеспечение дисциплины представлено: основной литературой – 5 источника (базовый учебник), дополнительной литературой – 5 наименования, Интернет-ресурсы – 8 источников и *соответствует* требованиям ФГОС ВО направления 09.03.03 «Прикладная информатика» и компетентностно-ролевыми моделями в сфере искусственного интеллекта**.**

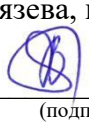
13. Материально-техническое обеспечение дисциплины соответствует специфике дисциплины «Информационная безопасность» и обеспечивает использование современных образовательных, в том числе интерактивных методов обучения.

14. Методические рекомендации студентам и методические рекомендации преподавателям по организации обучения по дисциплине дают представление о специфике обучения по дисциплине «Информационная безопасность».

ОБЩИЕ ВЫВОДЫ

На основании проведенной рецензии можно сделать заключение, что характер, структура и содержание рабочей программы дисциплины «Информационная безопасность» ОПОП ВО по направлению 09.03.03 «Прикладная информатика», направленность «Системы искусственного интеллекта», «Программные решения для бизнеса» (квалификация выпускника – специалитет), разработанной Степанцевич М.Н., доцентом кафедры прикладной информатики, к.э.н. и Худяковой Е.В., профессором кафедры прикладной информатики, д.э.н., соответствует требованиям ФГОС ВО, компетентностно-ролевым моделям в сфере искусственного интеллекта, современным требованиям экономики, рынка труда и позволит при её реализации успешно обеспечить формирование заявленных компетенций.

Рецензент: Щедрина Е.А., к.пед.н., доцент ФГБОУ ВО РГАУ-МСХА имени К.А. Тимирязева, кандидат экономических наук



«26» августа 2025 г.

(подпись)