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.В.ДВ.02.02 «Технологии искусственного интеллекта в кибербезопасности АПК»

для подготовки магистров

ФГОС ВО

Направление: 09.04.03 «Прикладная информатика»
Направленность: «Архитектура систем искусственного интеллекта», «ИТ-инновации и цифровые решения для бизнеса»

Курс 2
Семестр 4

Форма обучения: очная

Год начала подготовки: 2025

Москва, 2025

Разработчик: _Греченева А.В._____
(ФИО, ученая степень, ученое звание)

«28» августа 2025г.

Рецензент: ___Ашмарина Т.И._____
(ФИО, ученая степень, ученое звание)

(подпись)

«28» августа 2025г.

Программа составлена в соответствии с требованиями ФГОС ВО, профессионального стандарта и учебного плана по направлению подготовки 09.04.03 «Прикладная информатика»

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

И.о. зав. кафедрой прикладной информатики
д.э.н., профессор Худякова Е.В._____
(подпись)

«28» августа 202_г.

Согласовано:

Председатель учебно-методической
комиссии института экономики и управления АПК
к.э.н., доцент Гупалова Т.Н. _____
(подпись)

«28» августа 2025г.

И.о. заведующий выпускающей кафедрой
прикладной информатики
д.э.н., профессор Худякова Е.В._____
(подпись)

«28» августа 2025г.

Заведующий отделом комплектования ЦНБ _____
(подпись)

СОДЕРЖАНИЕ

АННОТАЦИЯ

рабочей программы учебной дисциплины Б1.В.ДВ.02.02 «Технологии искусственного интеллекта в кибербезопасности АПК» для подготовки магистра по направлению 09.04.03 «Прикладная информатика», направленности «Архитектура систем искусственного интеллекта», «ИТ- инновации и цифровые решения для бизнеса»

Цель освоения дисциплины: формирование у обучающихся теоретических и практико-ориентированных компетенций по применению методов и технологий искусственного интеллекта для выявления, предотвращения и реагирования на киберугрозы в информационных системах и цифровых платформах АПК, включая задачи мониторинга, анализа событий безопасности и обеспечения устойчивости критически важных бизнес-процессов.

Задачи дисциплины:

1. Формирование понятийного аппарата в области кибербезопасности АПК и применения технологий искусственного интеллекта в задачах защиты информации.
2. Освоение моделей угроз и нарушителя для цифровых платформ и информационных систем АПК, включая сценарии атак на данные, сервисы и ИИ-компоненты.
3. Изучение методов интеллектуального анализа данных безопасности (журналы, сетевой трафик, телеметрия, события SIEM/SOC) и подходов к подготовке и нормализации данных.
4. Овладение алгоритмами ИИ для детектирования аномалий и атак (машинное обучение, методы без учителя, графовые и вероятностные модели, модели последовательностей), включая настройку и оценку качества.
5. Формирование навыков построения и оценки моделей классификации инцидентов и приоритизации реагирования с учетом бизнес-критичности активов и процессов АПК.
6. Изучение принципов устойчивости и безопасности ИИ-систем (угрозы к данным и моделям, атаки на ML, смещение данных, контроль качества и доверия к результатам).
7. Освоение инструментальных средств и практик MLOps/SecOps для внедрения ИИ-компонентов в контур безопасности (версионирование, воспроизводимость, мониторинг, аудит, контроль изменений).
8. Развитие компетенций проектирования архитектуры решений AI-for-Security в составе ИТ-ландшафта предприятия АПК (интеграция с SIEM/SOAR, источниками данных и ИС предприятия).
9. Формирование навыков подготовки аналитических материалов и отчетности по инцидентам и результатам интеллектуального мониторинга в соответствии с регламентами и нормативными требованиями организации.

Место дисциплины в учебном плане: Дисциплина Б1.В.ДВ.02.02 «Технологии искусственного интеллекта в кибербезопасности АПК» относится к дисциплинам по выбору (Б1.В.ДВ.02) части, формируемой участниками образовательных отношений, учебного плана подготовки магистров по направлению 09.04.03 «Прикладная информатика» (направленности «Архитектура систем искусственного интеллекта» и «ИТ-инновации и цифровые решения для бизнеса»). Предшествующая подготовка, на которую опирается дисциплина, включает (в зависимости от выбранной траектории и освоенных модулей): «Архитектурное моделирование в проектировании интеллектуальных систем в АПК», «Современные технологии разработки программного обеспечения», «Технологии баз данных и знаний», «Методы управления знаниями и принятием решений», а также дисциплины, формирующие навыки работы с данными и инженерии программных систем.

Требования к результатам освоения дисциплины: в результате освоения дисциплины формируются следующие компетенции (индикаторы) их достижения: ПКос-1 (индикаторы: ПКос-1.1, ПКос-1.2, ПКос-1.3), ПКос-2 (индикаторы: ПКос-2.1, ПКос-2.2, ПКос-2.3), ПКос-4 (индикаторы: ПКос-4.1, ПКос-4.2, ПКос-4.3).

Краткое содержание дисциплины: основы кибербезопасности цифровых систем АПК. Модели угроз, активов и нарушителя для ИИ-ориентированных информационных систем. Архитектуры SOC/SIEM/SOAR и сбор телеметрии безопасности. Журналы событий, сетевой трафик, данные хостов и облачных платформ. Предобработка, нормализация и корреляция данных безопасности. Методы машинного обучения для выявления аномалий и атак. Сигнатурные, поведенческие и статистические подходы к детектированию. Классификация инцидентов и приоритизация реагирования по бизнес-критичности. Метрики качества детектирования и оценка ложных срабатываний. Объяснимость моделей и интерпретация решений в задачах безопасности. Атаки на модели и данные, угрозы надежности ИИ, дрейф и деградация. Защита ML-контуров, контроль целостности данных и моделей. MLOps/SecOps, воспроизводимость экспериментов, аудит и мониторинг. Проектирование безопасной архитектуры ИИ-сервисов, политики доступа и управление ключами. Инцидент-респонс, форензика и регламентированная отчетность. Практические кейсы киберугроз в АПК и критически важных цифровых процессах.

Общая трудоемкость дисциплины: 108/3 (часы/зач. ед.).

Промежуточный контроль: зачет.

1. Цель освоения дисциплины

Сформировать у обучающихся системных знаний и практических навыков проектирования и применения технологий искусственного интеллекта для обеспечения кибербезопасности цифровых решений АПК, включая интеллектуальный мониторинг, выявление аномалий и атак, оценку рисков и принятие управленческих решений в условиях неопределенности, а также интеграцию ИИ-компонентов в архитектуру корпоративных контуров

безопасности (SIEM/SOC/SOAR) с учетом требований надежности, объяснимости и доверия к результатам.

2. Место дисциплины в учебном процессе

Дисциплина Б1.В.ДВ.02.02 «Технологии искусственного интеллекта в кибербезопасности АПК» относится к дисциплинам по выбору (Б1.В.ДВ.02) части, формируемой участниками образовательных отношений, учебного плана подготовки магистров по направлению 09.04.03 «Прикладная информатика» (направленности «Архитектура систем искусственного интеллекта» и «ИТ-инновации и цифровые решения для бизнеса»).

Дисциплина реализуется в соответствии с требованиями ФГОС ВО, ОПОП и учебного плана, и изучается в 4 семестре, когда у обучающихся уже сформирован базовый фундамент в области проектирования и эксплуатации информационных систем и ИИ-компонентов. Размещение в 4 семестре обеспечивает практико-ориентированную интеграцию ранее освоенных знаний (архитектура ИС, методы анализа данных, проектирование ИИ-систем, управление ИТ-проектами) с задачами обеспечения безопасности цифровых платформ АПК.

Предшествующая подготовка, на которую опирается дисциплина, включает (в зависимости от выбранной траектории и освоенных модулей): «Архитектурное моделирование в проектировании интеллектуальных систем в АПК», «Современные технологии разработки программного обеспечения», «Технологии баз данных и знаний», «Методы управления знаниями и принятием решений», а также дисциплины, формирующие навыки работы с данными и инженерии программных систем.

Дисциплина носит обобщающий и прикладной характер и ориентирована на подготовку обучающихся к решению задач, связанных с безопасной разработкой и эксплуатацией ИИ-компонентов и сервисов, а также к выполнению научно-исследовательской работы и выпускной квалификационной работы (ВКР) в тематике кибербезопасности, доверенного ИИ и устойчивости цифровых решений в АПК.

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

Образовательные результаты освоения дисциплины обучающимся, представлены в таблице 1.

4. Структура и содержание дисциплины

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 3 зач. единиц (108 часов), их распределение по видам работ представлено в табл. 2.

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	ПКос-1	Способность применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС	ПКос-1.1 Знать методы прикладной информатики	методы прикладной информатики	-	-
			ПКос-1.2 Уметь применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС	-	применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС	-
			ПКос-1.3 Владеть инструментальными средствами прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС	-	-	инструментальными средствами прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС
2	ПКос-2	Способность проектировать архитектуру ИС предприятий и организаций в прикладной области	ПКос-2.1 Знает способы проектирования архитектуры ИС	Способы проектирования архитектуры ИС	-	-
			ПКос-2.2	-	проектировать архитектуру ИС	-

			Умеет проектировать архитектуру ИС предприятий и организаций АПК		предприятий и организаций АПК	
			ПКос-2.3 Владеет методикой проектирования архитектуры ИС предприятий	-	-	методикой проектирования архитектуры ИС предприятий
3	ПКос-4	Способность принимать эффективные проектные решения в условиях неопределенности и риска	ПКос-4.1 Знает методы принятия управленческих решений	методы принятия управленческих решений	-	-
			ПКос-4.2 Умеет принимать эффективные проектные решения в условиях неопределенности и риска	-	принимать эффективные проектные решения в условиях неопределенности и риска	-
			ПКос-4.3 Владеет инструментами обоснования эффективных проектных решений в условиях неопределенности и риска	-	-	инструментами обоснования эффективных проектных решений в условиях неопределенности и риска

Таблица 2

Распределение трудоёмкости дисциплины по видам работ по семестрам

Вид учебной работы	Трудоёмкость	
	час. всего /*	В т.ч. по семестрам
		№4
Общая трудоёмкость дисциплины по учебному плану	**108/4**	**108/4**
1. Контактная работа:	34,25/4	34,25/4
Аудиторная работа	34,25/4	34,25/4
лекции (Л)	8	8
практические занятия (ПЗ)	26/4	26/4
курсовая работа (проект) (КР/КП) (консультация, защита)	-	-
консультации перед экзаменом		
контактная работа на промежуточном контроле (КРА)	0,25	0,25
2. Самостоятельная работа (СРС)	**73,75**	**73,75**
курсовая работа (подготовка)	-	-
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам и т.д.)	64,75	64,75
Подготовка к зачету (контроль)	9	9
Вид промежуточного контроля:	зачет	

* в том числе практическая подготовка

4.2 Содержание дисциплины

Таблица 3

Тематический план учебной дисциплины

Наименование разделов и тем дисциплин (укрупнённо)	**Всего**	**Аудиторная работа**			**Внеаудиторная работа СР**
		Л	**ПЗ/С всего/***	**ПКР**	
Тема 1. Киберугрозы и специфика кибербезопасности цифровых систем АПК	28,00	2	6	-	20,00
Тема 2. Данные безопасности и подготовка датасетов для ИИ-аналитики	28,00	2	6/2	-	20,00
Тема 3. Методы ИИ для детектирования атак и аномалий	28,00	2	6/2	-	20,00

Наименование разделов и тем дисциплин (укрупнённо)	**Всего**	**Аудиторная работа**			**Внеаудиторная работа СР**
		Л	**ПЗ/С** **всего/***	**ПКР**	
Тема 4. Архитектура AI-for-Security и эксплуатация (SOC/SIEM/SOAR, надежность и доверие)	23,75	2	8	-	13,75
Контактная работа на промежуточном контроле (КРА)	0,25	-	-	0,25	
Всего за 1 семестр	108/4	8	26/4	0,25	73,75
Итого по дисциплине	**108/4**	**8**	**26/4**	**0,25**	73,75

* в том числе практическая подготовка

Тема 1 Киберугрозы и специфика кибербезопасности цифровых систем АПК

Активы и критические процессы АПК в цифровом контуре. Модель нарушителя и типовые векторы атак на ИТ/ОТ/IoT-среды. Поверхности атак для платформ данных и ИИ-сервисов. Таксономии угроз и инцидентов, типовые сценарии компрометации. Риск-ориентированная постановка требований безопасности и приоритизация мер защиты.

Тема 2 Данные безопасности и подготовка датасетов для ИИ-аналитики

Источники телеметрии безопасности: журналы, сетевые события, данные хостов и облака. Форматы событий и нормализация, временные шкалы и корреляция. Инженерия признаков для задач детектирования, агрегирование и построение профилей “нормального” поведения. Метрики качества данных безопасности и правила валидации датасета. Практики документирования датасетов и контроль целостности.

Тема 3 Методы ИИ для детектирования атак и аномалий

Задачи классификации инцидентов и выявления аномалий в кибербезопасности. Методы обучения с учителем и без учителя, модели последовательностей и поведенческие подходы. Оценка качества детектирования, баланс ошибок и управление ложными срабатываниями. Интерпретация решений моделей и анализ ошибок. Критерии применимости моделей в эксплуатационных условиях.

Тема 4. Архитектура AI-for-Security и эксплуатация (SOC/SIEM/SOAR, надежность и доверие)

Архитектурные схемы AI-for-Security и интеграция с SOC/SIEM/SOAR. Pipeline данных безопасности, контуры хранения, потоковой обработки и сервисов детектирования. Метрики эксплуатации и качества: SLA, TPR/FPR, precision@k, задержки и устойчивость. Мониторинг дрейфа, деградации и качества данных. Угрозы надежности ML и контроль рисков моделей в продуктивной среде, аудит и регламентирование реагирования.

4.3 Лекции/ практические занятия

Таблица 4

Содержание лекций/ практических занятий и контрольные мероприятия

№ п/п	Название раздела, темы	№ и название лекций/практических занятий	Формируемые компетенции (индикаторы)	Вид контрольного мероприятия	Кол-во часов / из них практическая подготовка
1	**Тема 1. Киберугрозы и специфика кибербезопасности цифровых систем АПК**	**Лекция №1.** Киберугрозы АПК и модель нарушителя: активы, поверхности атак, сценарии воздействия на цифровые контуры и ИИ-сервисы.	ПКос-1, ПКос-2, ПКос-4	–	2
		Практическая работа №1. Инвентаризация активов и построение модели угроз для кейса АПК (asset inventory, attack surface).	ПКос-1, ПКос-4	Защита работы	2
		Практическая работа №2. STRIDE/LINDDUN-анализ сервиса АПК. Требования безопасности и трассировка на угрозы.	ПКос-2, ПКос-4	Защита работы	2
		Практическая работа №3. Матрица рисков (вероятность/ущерб). Приоритизация мер защиты по бизнес-критичности.	ПКос-4	Защита работы	2
2	**Тема 2. Данные безопасности и подготовка датасетов для ИИ-аналитики**	**Лекция №2.** Телеметрия безопасности: логи, сетевые события, данные хостов/облака. Нормализация, корреляция, признаки.	ПКос-1, ПКос-2	–	2
		Практическая работа №4. Подготовка датасета из событий безопасности: парсинг, нормализация, временная шкала, атрибуты.	ПКос-1	Защита работы	2/2
		Практическая работа №5. Инженерия признаков для детектирования: частотные/временные/поведенческие признаки, профили “нормы”.	ПКос-1, ПКос-2	Защита работы	2

		Практическая работа №6. Метрики качества данных и валидация: полнота, пропуски, дубликаты, согласованность; правила контроля качества.	ПКос-1	Защита работы	2
3	**Тема 3. Методы ИИ для детектирования атак и аномалий**	**Лекция №3.** ML-подходы в кибербезопасности: классификация, аномалия-детекция, модели последовательностей. Оценка качества.	ПКос-1, ПКос-2	–	2
		Практическая работа №7. Базовая модель классификации инцидентов и оценка качества (Precision/Recall/F1, ROC-AUC).	ПКос-1, ПКос-4	Защита работы	2/2
		Практическая работа №8. Аномалия-детекция без учителя (Isolation Forest/One-Class SVM/Autoencoder). Анализ ложных срабатываний.	ПКос-1	Защита работы	2
		Практическая работа №9. Интерпретация решений (SHAP/LIME/feature importance). Анализ ошибок детектирования.	ПКос-1, ПКос-4	Защита работы	2
4	**Тема 4. Архитектура AI-for-Security и эксплуатация (SOC/SIEM/SOAR, надежность и доверие)**	**Лекция №4.** Архитектура AI-for-Security: интеграция с SOC/SIEM/SOAR. Pipeline данных. Требования надежности, аудита и доверия.	ПКос-2, ПКос-4	–	2
		Практическая работа №10. Проектирование архитектуры AI-for-Security (контекст/компоненты/потоки данных) для кейса АПК.	ПКос-2	Защита работы	2
		Практическая работа №11. Сценарии реагирования (SOAR-playbooks). Приоритизация инцидентов (severity, бизнес-влияние).	ПКос-4	Защита работы	2
		Практическая работа №12. Метрики эксплуатации	ПКос-1, ПКос-4	Защита работы	2

		детектирования: TPR/FPR, precision@k, MTTA/MTTR. Пороговая настройка и контроль качества.			
		Практическая работа №13. Угрозы надежности ML и меры защиты (poisoning/evasion/model extraction). Чек-лист контроля и требования к контуру.	ПКос-2, ПКос-4	Защита работы	2

Таблица 5

Перечень вопросов для самостоятельного изучения дисциплины

№ п/п	Название раздела, темы	Перечень рассматриваемых вопросов для самостоятельного изучения
1	Тема 1. Киберугрозы и специфика кибербезопасности цифровых систем АПК	Регуляторные и отраслевые контексты защиты информации для цифровых платформ АПК. Классы активов и критичность данных в цепочках агропроизводства и логистики. Угрозы для ИИ-ориентированных контуров: data exfiltration, model inversion, membership inference, model stealing. Киберустойчивость бизнес-процессов и модели непрерывности (BCP/DRP) в агросекторе. Точки доверия и цепочки поставок (software supply chain), SBOM, угрозы компрометации зависимостей. Концепции Zero Trust и сегментация для гибридных ИТ/OT/IoT-ландшафтов. Модель доверия к данным и источникам телеметрии. Компетенции: ПКос-2, ПКос-4.
2	Тема 2. Данные безопасности и подготовка датасетов для ИИ-аналитики	Стандарты представления и обмена данными кибербезопасности: STIX/TAXII, OpenC2, Sigma rules. Схемы событий и нормализация: ECS (Elastic Common Schema), CEF/LEEF, сопоставление полей и единая таксономия. Методы снижения смещения данных: sampling, reweighting, data augmentation для редких классов атак. Генерация синтетической телеметрии (simulated attacks, log synthesis) и оценка пригодности. Управление качеством датасетов: datasheets for datasets, data lineage, контроль целостности и версионирование. Анонимизация/псевдонимизация журналов и оценка влияния на детектирование. Компетенции: ПКос-1, ПКос-2.
3	Тема 3. Методы ИИ для детектирования атак и аномалий	Современные направления AI-for-Security: self-supervised представления, contrastive learning, foundation models для киберданных. Детектирование по графам: графы потоков, графы зависимостей, техники GNN, link prediction для выявления lateral movement. Методы калибровки вероятностей и доверительных оценок (reliability, calibration curves) для принятия решений в SOC. Редкие события и дисбаланс классов: anomaly scoring, cost-sensitive learning, evaluation under imbalance.

		Комплексные метрики: PR-AUC, MCC, balanced accuracy, expected cost, time-to-detect. Анализ устойчивости моделей к шуму и пропускам в телеметрии. Компетенции: ПКос-1, ПКос-4.
4	Тема 4. Архитектура AI-for-Security и эксплуатация (SOC/SIEM/SOAR, надежность и доверие)	Архитектура потоковой обработки данных безопасности: streaming/near-real-time, окна агрегации, требования к задержкам и консистентности. Метрики эксплуатации и инженерии надежности: SLO/SLI, error budget, устойчивость сервиса детектирования. Мониторинг моделей в продакшене: data drift/concept drift, стабильность признаков, контроль деградации качества и авто-триггеры переобучения. Управление жизненным циклом моделей: model registry, approvals, аудит, воспроизводимость экспериментов, контроль изменений. Безопасность ML-контура: защита артефактов модели, контроль доступа, секреты, защита пайплайнов, hardening контейнеров. Подходы Purple Teaming/Red Teaming для AI-for-Security и проверка эффективности playbooks. Компетенции: ПКос-2, ПКос-4.

5. Образовательные технологии

Таблица 6

Применение активных и интерактивных образовательных технологий

№ п/п	Тема и форма занятия		Наименование используемых активных и интерактивных образовательных технологий
1	Тема 1. Киберугрозы и специфика кибербезопасности цифровых систем АПК	**Л**	Лекция-визуализация, разбор отраслевых кейсов и сценариев атак, обсуждение моделей угроз и рисков.
		ПЗ	Решение задач профессиональной направленности, проблемно-поисковое занятие, групповое обсуждение (модель угроз, риск-матрица, требования безопасности).
2	Тема 2. Данные безопасности и подготовка датасетов для ИИ-аналитики	**Л**	Лекция-визуализация, демонстрация источников телеметрии и схем данных, разбор примеров нормализации и корреляции событий.
		ПЗ	Решение задач профессиональной направленности, практикум по подготовке данных, проблемно-поисковое занятие, групповое обсуждение (признаки, качество данных).
3	Тема 3. Методы ИИ для детектирования атак и аномалий	**Л**	Лекция-визуализация, разбор архитектур ML-детекторов, обсуждение метрик качества и ошибок детектирования.
		ПЗ	Решение задач профессиональной направленности, практикум по построению и оценке моделей, проблемно-поисковое

			занятие, групповое обсуждение (ложные срабатывания, интерпретация).
4	Тема 4. Архитектура AI-for-Security и эксплуатация (SOC/SIEM/SOAR, надежность и доверие)	**Л**	Лекция-визуализация, анализ архитектурных схем SOC/SIEM/SOAR и AI-контура, обсуждение эксплуатационных метрик и требований аудита.
		ПЗ	Решение задач профессиональной направленности, проектно-ориентированное занятие, проблемно-поисковое занятие, групповое обсуждение (архитектура, playbooks, мониторинг дрейфа/качества).

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

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

1) Примеры заданий практических работ

Практическая работа №2. STRIDE/LINDDUN-анализ сервиса АПК. Требования безопасности и трассировка на угрозы

Цель работы. Формирование навыков выявления и структурирования угроз для цифрового сервиса АПК с применением методик STRIDE/LINDDUN и обоснования требований безопасности.
Рекомендуемые источники и ресурсы. Материалы по STRIDE и LINDDUN; шаблоны threat modeling; OWASP ASVS и OWASP Top 10; MITRE ATT&CK (обзор тактик и техник); примеры требований безопасности для ИС.
Задание. На основе описания цифрового сервиса АПК (выдается преподавателем либо выбирается обучающимся) выполнить анализ угроз и сформировать требования безопасности:

1. Определить границы системы и состав компонентов (клиент, сервер/микросервисы, БД, интеграции, внешние API, контур ИИ).
2. Сформировать DFD/контекстную схему потоков данных (минимум 1 уровень детализации).
3. Выполнить STRIDE-анализ для ключевых компонентов и потоков данных; зафиксировать не менее 12 угроз.
4. При необходимости дополнить анализ по LINDDUN для сценариев, связанных с персональными/коммерчески значимыми данными (минимум 6 рисков приватности).
5. Сформировать таблицу трассировки «угроза → требование → мера контроля», указав приоритет (High/Medium/Low) и тип меры (организационная/техническая).
6. Выбрать 3 наиболее критичные угрозы и предложить архитектурные решения по снижению риска (аутентификация/авторизация, сегментация, шифрование, контроль целостности, журналирование, rate limiting и др.).

Отчетность (форма сдачи). Отчет (7–10 стр.) с: схемой DFD/контекста, таблицей STRIDE/LINDDUN, трассировкой требований, перечнем мер и обоснованием критичности; приложение — исходные предпосылки и допущения.
Критерии оценивания. Полнота идентификации угроз и корректность методики; качество схемы потоков данных; обоснованность критичности и приоритизации; логичность

требований и мер контроля; связность трассировки «угроза–требование–мера»; качество оформления отчета.

Практическая работа №5. Инженерия признаков для детектирования: частотные/временные/поведенческие признаки, профили “нормы”

Цель работы. Формирование навыков разработки признакового описания и профилей нормального поведения для задач интеллектуального мониторинга безопасности.
Рекомендуемые источники и ресурсы. Примеры логов и событий безопасности (учебный набор преподавателя); документация ECS/CEF (для семантики полей); материалы по feature engineering для временных рядов и событий; справочные материалы по базовым статистическим признакам.
Задание. На основе предоставленного набора событий (логов) сформировать признаки и базовый профиль “нормы”:

1. Провести семантическую нормализацию ключевых полей (время, источник, субъект, действие, результат, ресурс).
2. Выполнить агрегацию по временным окнам (например, 1 мин, 10 мин, 1 час) и сформировать частотные признаки: количество событий, количество уникальных субъектов/адресов, доли неуспешных действий.
3. Сформировать временные признаки: межсобытийные интервалы, сезонность по времени суток/дню недели, всплески активности.
4. Сформировать поведенческие признаки: последовательности действий пользователя/узла, отношение “успех/ошибка”, “новый ресурс/типовой ресурс”, редкость событий.
5. Сформировать baseline-профиль нормального поведения (например, медиана/квантили по окнам; допустимые диапазоны; список типовых действий) и описать правила отклонений.
6. Подготовить датасет для последующего обучения/оценки детектора (таблица признаков; описание признаков и их смысла).

Отчетность (форма сдачи). Jupyter Notebook или отчет с приложением таблицы признаков: описание данных, перечень признаков (не менее 20), выбранные окна агрегации, baseline-профиль и краткие выводы.
Критерии оценивания. Корректность нормализации и агрегации; содержательность и разнообразие признаков; пригодность baseline-профиля для выявления отклонений; воспроизводимость (структурированный notebook/скрипт); качество интерпретации результатов.

Практическая работа №8. Аномалия-детекция без учителя (Isolation Forest/One-Class SVM/Autoencoder). Анализ ложных срабатываний

Цель работы. Освоение методов выявления аномалий в данных безопасности без разметки и навыков анализа ложных срабатываний в эксплуатационном контексте.
Рекомендуемые источники и ресурсы. Учебный датасет событий безопасности/трафика; документация scikit-learn (Isolation Forest, One-Class SVM); материалы по оценке аномалий и выбору порогов; справочные материалы по PR-AUC и cost-sensitive оценке.
Задание. Построить и оценить детектор аномалий для телеметрии безопасности:

1. Подготовить матрицу признаков (использовать результат предыдущей подготовки данных либо готовый набор).
2. Обучить минимум 2 модели: Isolation Forest и One-Class SVM (либо Autoencoder при наличии подготовленной среды).
3. Получить anomaly score и выполнить выбор порога детектирования с учетом заданного ограничения на ложные срабатывания (например, не более 5% событий).

4. Рассчитать показатели качества на контрольной выборке (если есть частичная разметка) либо через экспертную проверку top-k аномалий: precision@k, доля FPR, число алертов в сутки.
5. Выполнить разбор ложных срабатываний: выделить типовые причины, предложить корректировки (признаки, порог, фильтры, исключения).
6. Сформировать рекомендации по внедрению в SOC-контур (частота запуска, окно агрегации, формат алерта).

Отчетность (форма сдачи). Notebook/отчет: параметры моделей, график распределения score, выбранный порог, результаты top-k, анализ ложных срабатываний, рекомендации по эксплуатации.

Критерии оценивания. Корректность постановки задачи и выбора модели; обоснование порога; наличие эксплуатационных метрик (число алертов/сутки, precision@k); качество анализа ложных срабатываний; воспроизводимость и ясность оформления.

Практическая работа №12. Метрики эксплуатации детектирования: TPR/FPR, precision@k, MTTA/MTTR. Пороговая настройка и контроль качества

Цель работы. Формирование навыков выбора и интерпретации метрик эксплуатации AI-for-Security, настройки порогов и построения контроля качества детектирования в контуре SOC.

Рекомендуемые источники и ресурсы. Материалы по KPI SOC (MTTA, MTTR); справочные материалы по confusion matrix и ROC/PR; примеры отчетности SOC/SIEM; методические материалы по SLI/SLO для сервисов.

Задание. Для заданного детектора (результаты модели или предоставленные преподавателем оценки) разработать метрики эксплуатации и регламент контроля:

1. Сформировать матрицу ошибок (TP, FP, TN, FN) и рассчитать TPR, FPR, Precision, Recall, F1; дополнительно precision@k для приоритизированного списка алертов.
2. Выполнить сравнение 2 вариантов порога (или 2 моделей) с учетом стоимости ошибок: цена пропуска инцидента и цена ложного алерта.
3. Рассчитать эксплуатационные показатели: прогнозируемое число алертов/сутки, нагрузка на аналитиков (оценка), MTTA и MTTR по предложенному сценарию реагирования.
4. Сформировать целевые значения SLI/SLO для детектора (качество, задержка, стабильность), определить “границы допустимости” и триггеры пересмотра порога.
5. Подготовить шаблон мини-отчета для руководителя SOC/ИТ-службы: текущие KPI, динамика, риски, рекомендации.

Отчетность (форма сдачи). Отчет (5–7 стр.) или notebook: расчеты метрик, сравнение вариантов порога/модели, предложенные SLI/SLO, шаблон отчета и выводы.

Критерии оценивания. Корректность метрик и расчетов; обоснованность выбора порогов с учетом стоимости ошибок; наличие эксплуатационных KPI (алерты/сутки, MTTA/MTTR); качество предложенных SLI/SLO; применимость выводов для управленческого решения.

2) Примерный перечень вопросов, выносимых на промежуточную аттестацию (зачет)

1. Понятие кибербезопасности цифровых систем АПК: объекты защиты, типовые активы, критерии критичности.
2. Модель нарушителя для ИТ/ОТ/IoT-контуров АПК: роли, мотивация, возможности, ограничения.
3. Поверхность атак и основные классы векторов атак на цифровые платформы и сервисы АПК.

4. Подходы к формированию требований безопасности на основе сценариев угроз и рисков.
5. Методология threat modeling: назначение, этапы, результаты, типовые артефакты.
6. Методика STRIDE: категории угроз, применение к компонентам и потокам данных.
7. Методика LINDDUN: риски приватности и их связь с архитектурными решениями.
8. Матрица рисков: параметры оценки (вероятность/ущерб), способы приоритизации мер защиты.
9. Источники телеметрии безопасности: логи приложений, системные журналы, сетевые события, события конечных точек.
10. Нормализация и корреляция событий безопасности: назначение, типовые подходы, ограничения.
11. Понятие признаков (features) в задачах AI-for-Security: группы признаков, интерпретируемость, устойчивость.
12. Методы формирования признаков для событийных и временных данных (частотные, временные, поведенческие).
13. Проблема дисбаланса классов в данных кибербезопасности и её последствия для обучения моделей.
14. Задачи классификации инцидентов и задачи аномалия-детекции: различия постановок и применимость.
15. Базовые метрики качества детектирования: Precision, Recall, F1, ROC-AUC, PR-AUC; области корректного применения.
16. Понятие ложных срабатываний и пропусков инцидентов: причины, способы снижения, компромиссы.
17. Подходы к выбору порога срабатывания детектора и влияние порога на нагрузку SOC.
18. Интерпретация решений моделей в кибербезопасности: назначение explainability и типовые методы (feature importance/SHAP/LIME).
19. Архитектура AI-for-Security в составе SOC/SIEM/SOAR: основные компоненты и потоки данных.
20. Эксплуатационные показатели и метрики SOC: MTTA, MTTR, объем алертов, приоритизация инцидентов.
21. Мониторинг качества моделей в эксплуатации: деградация, drift данных/концепции, контроль стабильности признаков.
22. Угрозы надежности и безопасности ML-моделей: отравление данных, уклонение (evasion), извлечение модели (model extraction), инверсия (model inversion).
23. Подходы к защите ML-контура: контроль доступа, аудит, изоляция, защита данных и артефактов модели, регламенты обновлений.
24. Роль документирования и воспроизводимости в проектах AI-for-Security: основные артефакты и требования к ним.

6.2. Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Оценочные средства текущего контроля успеваемости и сформированности компетенций основана на подсчете баллов, «заработанных» студентом в течение семестра.

Успеваемость студента по дисциплине оценивается в баллах от 0 до 100.

Оценка знаний проводится по следующим критериям:

- посещение занятий – 30 баллов;
- выполнение практических заданий – 30 баллов;

− промежуточный контроль (зачет) – 40 баллов;

Соответствие балльной оценки общепринятой 4-х балльной шкале оценок приведено в таблице 7.

Таблица 7

Соответствие балльных оценок по 4-х балльной шкале

Балльная оценка	Оценка по 4хбалльной шкале	Оценка по шкале «Зачтено» / «Не зачтено»
0-59	Неудовлетворительно - 2	Не зачтено
60-69	Удовлетворительно - 3	Зачтено
70-89	Хорошо – 4	Зачтено
90-100	Отлично - 5	Зачтено

Критерии оценивания результатов обучения показаны в таблицах 8,9.

Таблица 8

Критерии оценивания по шкале «Зачтено» / «Не зачтено»

Оценка «Зачтено/Не зачтено»	Критерии оценивания
Зачтено	Оценка «**зачтено**» ставится, если студент показал глубокие систематизированные знания в объеме, необходимом для дальнейшей учебы и в предстоящей работе по профессии, владеет приемами рассуждения и сопоставления материала из разных источников: теорию связывает с практикой, другими темами данного курса, других изучаемых предметов; выполнил все практические задания, предоставив правильные и аргументированные выводы в соответствии с предъявленными требованиями.
Незачтено	Оценка «**не зачтено**» ставится, если студент в ответах не раскрыл основное содержание вопросов, носящих несистематизированный, отрывочный, поверхностный характер; студент не понимает существа излагаемых им вопросов, что свидетельствует о том, что студент не может дальше продолжать обучение или приступать к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине; не выполнил практические задания в соответствии с предъявленными требованиями.

Таблица 9

Критерии оценивания результатов обучения (зачет с оценкой)

Оценка	**Критерии оценивания**
Высокий уровень «5» (отлично)	оценку **«отлично»** заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки

	профессионального применения освоенных знаний сформированы. **Компетенции**, закреплённые за дисциплиной, **сформированы на уровне – высокий**.
Средний уровень «4» (хорошо)	оценку **«хорошо»** заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки. **Компетенции**, закреплённые за дисциплиной, **сформированы на уровне – хороший (средний)**.
Пороговый уровень «3» (удовлетворительно)	оценку **«удовлетворительно»** заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы. **Компетенции**, закреплённые за дисциплиной, **сформированы на уровне – достаточный**.
Минимальный уровень «2» (неудовлетворительно)	оценку «**неудовлетворительно»** заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы. **Компетенции**, закреплённые за дисциплиной, **не сформированы**.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Внуков А. А. Защита информации: учебное пособие для вузов. – 3-е изд., пер. и доп. – Электрон. дан. – Москва: Юрайт, 2022. – 161 с. – (Высшее образование). – URL: https://urait.ru/bcode/490277. – ISBN 978-5-534-07248-8.

2. Часовских В. П., Акчурина Г. А., Лабунец В. Г., Стариков Е. Н., Кох Е. В. Администрирование и кибербезопасность информационных систем: учебное пособие. – Екатеринбург: УрГЭУ, 2022. – 173 с. – URL: https://e.lanbook.com/book/417746.

7.2. Дополнительная литература

1. Кочин В. П., Воротницкий Ю. И. Проектирование и обеспечение безопасности интегрированных образовательных информационно-коммуникационных систем: монография. – Минск: БГУ, 2022. – 167 с. – URL: https://e.lanbook.com/book/386312. – ISBN 978-985-881-355-0.

2. Казарин О. В., Шубинский И. Б. Надежность и безопасность программного обеспечения: учебное пособие для вузов. – Электрон. дан. –

Москва: Юрайт, 2022. – 342 с. – (Высшее образование). – URL: https://urait.ru/bcode/493262. – ISBN 978-5-534-05142-1.

3. Шелухин О. И., Осин А. В., Раковский Д. И. Искусственный интеллект и машинное обучение в кибербезопасности: учебно-методическое пособие для выполнения лабораторных работ. направление подготовки: 10.03.01 информационная безопасность. профили: «безопасность компьютерных систем», «безопасность автоматизированных систем». – Москва: МТУСИ, 2022. – 52 с. – URL: https://e.lanbook.com/book/333755.

7.3. Нормативные правовые акты

1. Гост 19.001-77. Единая система программной документации: Общие положения. – М.: Изд.-во стандартов, 1994.

2. Гост 19.101-77. Единая система программной документации: Виды программ и программных документов. – М.: Изд.-во стандартов, 1994.

3. Гост 19.102-77. Единая система программной документации: Стадии разработки. – М.: Изд.-во стандартов, 1994.

4. Гост 19.105-78. Единая система программной документации: Общие требования к программным документам. – М.: Изд.-во стандартов, 1994.

5. Гост 19.201-78. Единая система программной документации: Техническое задание. Требования к содержанию и оформлению. – М.: Изд.-во стандартов, 1994.

6. Гост 19.202-78. Единая система программной документации: Спецификация. Требования к содержанию и оформлению. – М.: Изд.-во стандартов, 1994.

7. Гост 19.502-78. Единая система программной документации: Описание применения. Требования к содержанию и оформлению. – М.: Изд.-во стандартов, 1994.

8. Гост 19.404-79. Единая система программной документации: Пояснительная записка. Требования к содержанию и оформлению. – М.: Изд.-во стандартов, 1994.

9. Гост 3.11.09-82. Система технологической документации: Термины и определения основных понятий. – М.: Изд.-во стандартов, 1994.

10. Гост 34.201-89. Виды, комплектность и обозначение документов при создании автоматизированных систем. – М.: Изд.-во стандартов, 1991.

11. ГОСТ 34.601-90. Автоматизированные Системы Стадии создания. Комплекс стандартов на автоматизированные системы. - М.: Изд-во стандартов, 1997

12. ISO/IEC 12207:1995

13. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

14. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

15. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

16. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

17. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

18. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».
19. Указ Президента РФ от 05.12.2016 № 646 «Доктрина информационной безопасности Российской Федерации».
20. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы».
21. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (национальная стратегия развития ИИ).
22. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации».
23. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
24. Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации».
25. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных…».
26. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
27. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

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

1. MITRE ATT&CK (база тактик и техник атак) [Электронный ресурс]. – Режим доступа: https://attack.mitre.org/ – открытый доступ.
2. MITRE ATLAS (Adversarial Threat Landscape for AI Systems) [Электронный ресурс]. – Режим доступа: https://atlas.mitre.org / – открытый доступ.
3. OWASP Top 10 (актуальные риски веб-приложений) [Электронный ресурс]. – Режим доступа: https://owasp.org/www-project-top-ten/ – открытый доступ.
4. OWASP ASVS (стандарт требований безопасности приложений) [Электронный ресурс]. – Режим доступа: https://owasp.org/www-project-application-security-verification-standard / – открытый доступ.
5. NIST Cybersecurity Framework (CSF) [Электронный ресурс]. – Режим доступа: https://www.nist.gov/cyberframework – открытый доступ.
6. NIST AI Risk Management Framework (AI RMF) [Электронный ресурс]. – Режим доступа: https://www.nist.gov/itl/ai-risk-management-framework – открытый доступ.

7. NIST SP 800-61 (Computer Security Incident Handling Guide) [Электронный ресурс]. – Режим доступа: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final – открытый доступ.
8. CISA Known Exploited Vulnerabilities Catalog (KEV) [Электронный ресурс]. – Режим доступа: https://www.cisa.gov/known-exploited-vulnerabilities-catalog – открытый доступ.
9. NVD (National Vulnerability Database) [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/ – открытый доступ.
10. CVE (реестр уязвимостей) [Электронный ресурс]. – Режим доступа: https://www.cve.org/ – открытый доступ.
11. FIRST CVSS (методика оценивания критичности уязвимостей) [Электронный ресурс]. – Режим доступа: https://www.first.org/cvss/ – открытый доступ.
12. CIS Controls (базовые меры киберзащиты) [Электронный ресурс]. – Режим доступа: https://www.cisecurity.org/controls – открытый доступ.
13. ENISA Threat Landscape (обзор ландшафта угроз) [Электронный ресурс]. – Режим доступа: https://www.enisa.europa.eu/publications/enisa-threat-landscape – открытый доступ.
14. SigmaHQ (репозиторий Sigma-правил для детектирования) [Электронный ресурс]. – Режим доступа: https://github.com/SigmaHQ/sigma – открытый доступ.
15. OASIS STIX/TAXII (стандарты описания и обмена киберугрозами) [Электронный ресурс]. – Режим доступа: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti – открытый доступ.
16. FSTEC России (нормативные документы и сведения по ИБ) [Электронный ресурс]. – Режим доступа: https://fstec.ru/ – открытый доступ.
17. Роскомнадзор (разъяснения по персональным данным и защите информации) [Электронный ресурс]. – Режим доступа: https://rkn.gov.ru/ – открытый доступ.

9. Перечень программного обеспечения и информационных справочных систем

1. Базы данных Министерства сельского хозяйства Российской Федерации: www.mcx.ru.
2. Базы данных Федеральной службы государственной статистики: www.gks.ru.
3. Справочная правовая система «КонсультантПлюс». www.consultant.ru
4. Справочная правовая система «Гарант». www.garant.ru
5. http://www.osp.ru – электронный журнал «Открытые системы».
6. http://www.clin.ru/marketing/ - Корпоративный менеджмент.
7. http://www.bytemag.ru/ - журнал ИТ-профессионалов.

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

Таблица 10

Перечень программного обеспечения

№ п/п	Наименование раздела учебной дисциплины	Наименование программы	Тип программы	Автор (разработчик)	Год разработки
1	Темы 1–4	Microsoft Office (Word, PowerPoint, Excel)	Офисный пакет (подготовка текста, таблиц, презентаций)	Microsoft	1989
2	Темы 1–4	Visual Studio Code	Редактор исходного кода	Microsoft	2015
3	Темы 1–4	Git	Система контроля версий	Linus Torvalds / сообщество	2005
4	Темы 2–4	Python	Язык программирования / среда вычислений	Python Software Foundation	1991
5	Темы 2–4	Anaconda (Miniconda)	Дистрибутив Python / управление окружениями	Anaconda Inc.	2012
6	Темы 2–4	Jupyter Notebook / JupyterLab	Интерактивная среда (ноутбуки)	Project Jupyter	2014
7	Темы 1–4	Docker	Контейнеризация и изоляция сервисов	Docker, Inc.	2013
8	Темы 2–4	Wireshark	Анализатор сетевого трафика (PCAP)	Wireshark Foundation / сообщество	1998
9	Темы 2–4	Zeek (Network Security Monitor)	Мониторинг сети, генерация телеметрии безопасности	Zeek Project / сообщество	1998
10	Темы 2–4	Suricata	IDS/IPS, сетевой детект (правила/сигнатуры)	Open Information Security Foundation	2010
11	Темы 2–4	Elastic Stack (Elasticsearch, Logstash, Kibana)	Аналитика логов, поиск, визуализация (SIEM-уровень)	Elastic N.V. / сообщество	2010
12	Темы 2–4	Wazuh	HIDS/SIEM (агенты, корреляция, алерты)	Wazuh Inc. / сообщество	2015
13	Темы 3–4	scikit-learn	Библиотека ML (классификация/аномалии)	Сообщество Python	2010
14	Тема 4	MLflow	Трекинг экспериментов, реестр моделей	Databricks / сообщество	2018

15	Тема 3	SHAP	Интерпретация моделей (explainability)	Сообщество (S. Lundberg и др.)	2017

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
Корпус 1, Аудитория 201 Количество рабочих мест: 24	Встроенные сетевые адаптеры (Intel I219-V или Realtek RTL8111H), интерфейс RJ-45, скорость 10/100/1000 Мбит/с. Точки доступа: Ubiquiti UniFi AP AC Pro, стандарты IEEE 802.11a/b/g/n/ac, частоты 2.4 ГГц (450 Мбит/с) и 5 ГГц (1300 Мбит/с), поддержка MU-MIMO, питание PoE.
Корпус 1, Аудитория 203 Количество рабочих мест: 18	Встроенные сетевые адаптеры (Intel I219-V или Realtek RTL8111H), интерфейс RJ-45, скорость 10/100/1000 Мбит/с. Точки доступа: Ubiquiti UniFi AP AC Pro, стандарты IEEE 802.11a/b/g/n/ac, частоты 2.4 ГГц (450 Мбит/с) и 5 ГГц (1300 Мбит/с), поддержка MU-MIMO, питание PoE.Структурное подразделение: Кафедра Цифровая кафедра
Корпус 1, Аудитория 206 Количество рабочих мест: 24	Встроенные сетевые адаптеры (Intel I219-V или Realtek RTL8111H), интерфейс RJ-45, скорость 10/100/1000 Мбит/с. Точки доступа: Ubiquiti UniFi AP AC Pro, стандарты IEEE 802.11a/b/g/n/ac, частоты 2.4 ГГц (450 Мбит/с) и 5 ГГц (1300 Мбит/с), поддержка MU-MIMO, питание PoE.
Центральная научная библиотека имени Н.И. Железнова	Читальные залы библиотеки
Студенческое общежитие	Комната для самоподготовки

11. Методические рекомендации обучающимся по освоению дисциплины

Образовательный процесс по дисциплине организован в форме учеб-ных занятий (контактная работа (аудиторной и внеаудиторной) обучающихся с преподавателем и самостоятельная работа обучающихся). Учебные занятия(в том числе по реализации практической подготовки) представлены следу-ющими видами, включая учебные занятия, направленные на практическую подготовку обучающихся и проведение текущего контроля успеваемости:

лекции (занятия лекционного типа);

семинары, практические занятия, лабораторные работы (занятия семинар-ского типа);

индивидуальные консультации и иные учебные занятия, предусматрива-ющие индивидуальную работу преподавателя с обучающимся;

самостоятельная работа обучающихся;

занятия иных видов.

На учебных занятиях обучающиеся выполняют запланированные настоящей программой отдельные виды учебных работ, в том числе отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Виды и формы отработки пропущенных занятий

Студент, пропустивший занятия обязан отработать:

Пропущенные лекции – предоставив преподавателю конспект лекции, ответив на вопросы устно, пройдя собеседование по пропущенной теме, пройти тестирование.

Пропущенные практические занятия – в форме выполненных заданий, устного опроса, посещения дополнительных занятий.

Защита индивидуальных заданий проводятся в часы в дни и часы, устанавливаемые преподавателем.

Пропуск занятия по документально подтвержденной дирекцией уважительной причине не является основанием для снижения оценки выполненной практической работы.

Методические рекомендации преподавателям по организации обучения по дисциплине

Преподавание курса должно носить контекстный характер. В процессе обучения должна четко прослеживаться целевая установка на развитие личности; интеграционное единство форм, методов и средств обучения; взаимодействие обучаемых и педагогов; индивидуальный стиль педагогической деятельности.

Реализация технологий контекстного обучения в профессионально-образовательном процессе обеспечивается соблюдением следующих условий:

– мотивационное обеспечение субъектов педагогической деятельности и учение, основанное на реализации их личностных функций в этом процессе;

– наличие четкой и диагностически заданной цели образования, т.е. измеримого представления об ожидаемом результате;

– представление учебного материала в виде системы познавательных и практических задач, ситуаций, заданий, проектов, упражнений и др.;

– указание способов взаимодействия субъектов профессионально-образовательного процесса;

– обозначение границ правилосообразной (алгоритмической) и творческой деятельности педагогов, допустимого отклонения от правил;

– обеспечение открытости обучения профессиональному будущему, направленность на его предвосхищение.

В результате изучения дисциплины студенты получают знания о распространении программного обеспечения, а также методологии и стандартах на основе лицензии и договоров, а также применять достижения отечественной и зарубежной науки и практики.

Методика преподавания дисциплины строится на сочетании лекций с практическими занятиями; групповыми и индивидуальными консультациями по отдельным разделам программы; внеаудиторной самостоятельной работой студентов (работа с учебниками, учебными пособиями, методическими указаниями, заданиями, специальной литературой, поиск необходимой информации в сети Интернет).

Лекционный курс, как одна из составляющей дисциплины, должен быть логическим и последовательным. Каждая лекция должна, согласно правилам дидактики, начинаться с актуализации знаний. Чтение лекций должно происходить на основе проблемного метода обучения, что будет стимулировать деятельность студентов к самостоятельному поиску знаний. Интерес к изучению материала преподаватель должен стимулировать, используя наглядные методы обучения (мультимедийные презентации, иллюстрации, стенды и т.д.). Помимо традиционной лекции необходимо использовать проблемные лекции, лекции-визуализации, бинарные лекции, дискуссии и т.д.

В начале каждой лекции следует четко формулировать цель, которую необходимо достигнуть посредством решения ряда задач. При этом сами задачи должны быть четко оговорены. Важная роль на лекции должна быть отведена дискуссии. Преподаватель заранее должен продумать траекторию изучения материала с вовлечением студентов в дискуссии. Это позволит на смену авторитарному методу обучению, укоренившемуся в современной системе образования, быть студентам собеседниками преподавателя. Эта особенность лекции важна для более глубокого понимания изучаемого материала.

Как и любое занятие, лекция должна заканчиваться подведением итогов и формулировкой выводов.

Что касается практических занятий, то для них должны соблюдаться такая же структура, как и для лекционных занятий: актуализация знаний, постановка цели и задач и т.д. Практическая работа также должна соответствовать принципам контекстного подхода, с использованием решения исследовательских задач профессиональной направленности. На практических занятиях должны быть использованы технологии дифференцированного обучения студентов, уделяя большее внимание «слабым» студентам.

Практические занятия проводятся под руководством преподавателя. В рамках этих занятий производится анализ типовых ошибок, допущенных при выполнении заданий, рассматриваются наиболее удачные варианты. Студенты привлекаются к разбору и сравнительному анализу предлагаемых вариантов решений. Происходит коллективное обсуждение, в результате которого приобретаются навыки ведения дискуссии по обсуждаемым вопросам.

Успех закрепления знаний и умений определяется стройной системой подобранных вопросов для текущего контроля.

В процессе самостоятельной работы студенты отрабатывают теоретические положения, изложенные на лекциях, и изучают примеры, рассмотренные на практических занятиях.

Конкретная тема обсуждается с каждым студентом и учитывает направление научных интересов студента или тему выпускной квалификационной работы.

Большое значение в ходе самостоятельной работы студентов имеет работа над литературой и другими источниками информации (периодические издания, Интернет и т.д.).

Особенности методики преподавания данной дисциплины состоят в интенсификации теоретической, практической и самостоятельной работы

студентов и широком применении активных и интерактивных форм и методов обучения.

Программу разработал:

Греченева А.В. к.т.н.,доцент 

РЕЦЕНЗИЯ

на рабочую программу дисциплины Б1.В.ДВ.02.02 «Технологии искусственного интеллекта в кибербезопасности АПК» ОПОП ВО по направлению подготовки 09.04.03 «Прикладная информатика», направленности «Архитектура систем искусственного интеллекта», «ИТ- инновации и цифровые решения для бизнеса» (квалификация выпускника – магистр)

Ашмариной Татьяной Игоревной, кандидатом экономических наук, доцентом кафедры экономики и организации производства ФГБОУ ВО «Российский государственный аграрный университет – МСХА им. К.А. Тимирязева» (далее по тексту рецензент), проведено рецензирование рабочей программы дисциплины Б1.В.ДВ.02.02 «Технологии искусственного интеллекта в кибербезопасности АПК» ОПОП ВО по направлению подготовки 09.04.03 «Прикладная информатика», направленности «Архитектура систем искусственного интеллекта», «ИТ- инновации и цифровые решения для бизнеса» (магистратура) разработанной в ФГБОУ ВО «Российский государственный аграрный университет – МСХА имени К.А. Тимирязева», на кафедре прикладной информатики (разработчик – Греченева Анастасия Владимировна, доцент кафедры прикладной информатики, кандидат технических наук).

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

1. Предъявленная рабочая программа дисциплины «Технологии искусственного интеллекта в кибербезопасности АПК» (далее по тексту Программа) *соответствует* требованиям ФГОС ВО по направлению *подготовки* 09.04.03 «Прикладная информатика». 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 дисциплинам по выбору части формируемой участниками образовательного процесса учебного цикла – Б1.О.

3. Представленные в Программе *цели* дисциплины *соответствуют* требованиям ФГОС ВО направления подготовки 09.04.03 «Прикладная информатика».

4. В соответствии с Программой за дисциплиной «Технологии искусственного интеллекта в кибербезопасности АПК» закреплено 3 компетенции (9 индикаторов). Дисциплина «Технологии искусственного интеллекта в кибербезопасности АПК» и представленная Программа *способна реализовать* ее в объявленных требованиях. 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 «Технологии искусственного интеллекта в кибербезопасности АПК» составляет 3 зачётных единицы (108 часов).

6. Информация о взаимосвязи изучаемых дисциплин и вопросам исключения дублирования в содержании дисциплин *соответствует* действительности. Дисциплина «Технологии искусственного интеллекта в кибербезопасности АПК» взаимосвязана с другими дисциплинами ОПОП ВО и Учебного плана по направлению 09.04.03 «Прикладная информатика».

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

8. Программа дисциплины «Технологии искусственного интеллекта в кибербезопасности АПК» 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 09.04.03 «Прикладная информатика».

10. Представленные и описанные в Программе формы *текущей* оценки знаний (защита практических работ, групповое обсуждение) *соответствуют* специфике дисциплины и требованиям к выпускникам. Форма промежуточного контроля знаний студентов, предусмотренная Программой, осуществляется в форме зачета в 4 семестре, что *соответствует* статусу дисциплины, как дисциплины, включенной в дисциплины по выбору части формируемой участниками образовательного процесса учебного цикла – Б1.В.ФТД. ФГОС ВО направления 09.04.03 «Прикладная информатика».

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

12. Учебно-методическое обеспечение дисциплины представлено: основной литературой – 2 источника, дополнительной литературой – 3 наименования, Интернет-ресурсы – 6 источников и *соответствует* требованиям ФГОС ВО направления 09.04.03 «Прикладная информатика».

13. Материально-техническое обеспечение дисциплины соответствует специфике дисциплины «Технологии искусственного интеллекта в кибербезопасности АПК» 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 «Технологии искусственного интеллекта в кибербезопасности АПК».

ОБЩИЕ ВЫВОДЫ

На основании проведенного рецензирования можно сделать заключение, что характер, структура и содержание рабочей программы дисциплины «Технологии искусственного интеллекта в кибербезопасности АПК» ОПОП ВО по направлению 09.04.03 «Прикладная информатика», направленности «Архитектура систем искусственного интеллекта», «ИТ-инновации и цифровые решения для бизнеса» (квалификация выпускника – магистр), разработанная Греченевой А.В., соответствует требованиям ФГОС ВО, современным требованиям экономики, рынка труда и позволит при её реализации успешно обеспечить формирование заявленных компетенций.

Рецензент:
Ашмарина Т.И., кандидат экономических наук, доцент, доцент кафедры экономики и организации производства ФГБОУ ВО РГАУ-МСХА имени К.А. Тимирязева

«28» августа 2025 г.