

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю

Зам. директора по УР

Н.А. Андреева

«28»

09

2026 г.

Рабочая программа практики

Б2.В.01(П) Производственная практика

**(первичные профессиональные умения и навыки в области
прикладных систем искусственного интеллекта)**

Кафедра: **Информационная безопасность**
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем (по отрасли или в
сфере профессиональной деятельности)**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО))

Вид учебной работы	ОФО	
	ЗЕ	Часов/семестр
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	3	108/5
Контактная работа, в том числе (по семестрам, курсам):		
Лекции		
Лабораторных работ		
Практических занятий		
Семинаров		
Иная контактная работа		2/5
Самостоятельная работа		106/5
Контроль		
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с оценкой с разбивкой по семестрам (курсам)		1/5
Число экзаменов с разбивкой по семестрам (курсам)		

Программу составил:

И.о. зав. кафедрой ИБ, д.пол.н, к.т.н., доцент Жуковский А.Г.

Рабочая программа дисциплины

«Производственная практика (первичные профессиональные умения и навыки в области прикладных систем искусственного интеллекта)»

Разработана в соответствии с ФГОС ВО:

направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. N 1427

Составлена на основании учебного плана

направления 10.03.01 Информационная безопасность, профиля «Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)», одобренного Учёным советом СКФ МТУСИ, протокол № 8 от 31.03. 2026 г., и утвержденного директором СКФ МТУСИ 31.03. 2026 г.

Рассмотрена и одобрена на заседании кафедры

Информационная безопасность

Протокол от «28» 04 2026 г. № 9

И.о. зав. кафедрой



А.Г. Жуковский.

1. Цели изучения дисциплины

Целями изучения дисциплины **"Производственная практика (первичные профессиональные умения и навыки в области прикладных систем искусственного интеллекта)"** является закрепление и углубление теоретической подготовки по направлению подготовки 10.03.01 Информационная безопасность, получение обучающимися практических навыков и компетенций по видам профессиональной деятельности, приобретение практических навыков и компетенций в сфере профессиональной деятельности и их применение при решении производственных задач в области прикладных систем искусственного интеллекта).

Задачи производственной практики:

- изучение теоретических и экспериментальных методов получения, обработки и хранения научной информации с привлечением современных информационных технологий; - изучение опыта проведения конкретных научных исследований в организации и лабораториях кафедры университета,
- развитие навыков сбора, обработки, анализ и систематизации научно-технической информации по теме исследования;
- выбор методик и средств решения поставленных задач;
- изучение форм и порядка составления отчетной научно-технической документации и внедрения результатов научных исследований;
- формирование навыков ведения научных исследований в области прикладных систем искусственного интеллекта, как целостного процесса, в том числе навыков анализа конкретной проблемной ситуации, формулировки проблемы и выдвижения гипотезы, разработки плана эксперимента, проведения эксперимента, обработки результатов, формулировки выводов и представления итогов проделанной работы в виде научных отчетов, рефератов или статей;
- разработка плана и программы проведения научных исследований и технических разработок по выбранной теме исследования.

Вид практики: производственная

Тип практики: первичные профессиональные умения и навыки в области прикладных систем искусственного интеллекта

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у обучающегося способности решать профессиональные задачи в соответствии с **эксплуатационной деятельностью**.

Результатом освоения дисциплины являются сформированные у обучающегося следующие компетенции:

ПК-3: Администрирование средств защиты информации прикладного и системного программного обеспечения
Знать:
Архитектуру подсистем защиты информации в прикладных системах искусственного интеллекта
Принципы построения систем управления базами знаний прикладных систем искусственного интеллекта
Основные средства и методы анализа программных реализаций
Принципы построения антивирусного программного обеспечения
Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению
Источники угроз информационной безопасности программного обеспечения и меры по их предотвращению
Уязвимости используемого программного обеспечения и методы их устранения

Виды и формы функционирования вредоносного программного обеспечения
 Характерные признаки наличия вредоносного программного обеспечения
 Средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения
 Принципы функционирования программных средств криптографической защиты информации
 Порядок обеспечения безопасности информации при эксплуатации программного обеспечения
 Нормативные правовые акты в области защиты информации
 Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры
 Организационные меры по защите информации.

Уметь:

Анализировать угрозы безопасности информации в прикладных системах искусственного интеллекта
 Формулировать правила безопасной эксплуатации программного обеспечения прикладных систем искусственного интеллекта
 Обосновывать правила безопасной эксплуатации программного обеспечения
 Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия
 Производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации
 Осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения
 Определять порядок функционирования программного обеспечения с целью обеспечения защиты информации
 Анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения.

Владеть:

- определением порядка установки программного обеспечения прикладных систем искусственного интеллекта с целью соблюдения требований по защите информации;
- контролем за соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение;
- навыками формулирования требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения;
- выполнением работ по обнаружению вредоносного программного обеспечения;
- навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования;
- навыками формулирования требований к встроенным средствам защиты информации программного обеспечения.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):

1	Б1.О.24 Искусственный интеллект и машинное обучение в кибербезопасности
2	Б1.О.29 Методы и средства криптографической защиты информации
3	Б1.О.32 Основы управления информационной безопасностью
4	Б1.О.33 Программно-аппаратные средства защиты информации
5	Б1.В.03 Защита информации от вредоносного программного обеспечения
6	Б1.В.04 Разработка безопасного программного обеспечения (Проектирование защищенных информационных систем)

Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:

1	Б1.О.36.01 Безопасность операционных систем
2	Б1.О.36.03 Безопасность компьютерных сетей
3	Б1.О.36.04 Безопасность систем баз данных
4	Б1.О.36.05 Методы оценки безопасности компьютерных систем (Аудит компьютерных систем)

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 108 часов, 2 часа контактной работы, 106 часов самостоятельной работы)

Код зан.	Тема и краткое содержание работы	Кол. часов	Компетенции	УМИО
Модуль 1				
1.1	Инструктаж по ПМБ. Получение задания на исследовательскую практику и разработка индивидуальной учебной программы прохождения практики (совместно с руководителем), определение направления исследований, формирование целей и задач исследования.	12	ПК-3	Л1.1 Л1.2
1.2	Анализ научной литературы и проведение теоретических и экспериментальных исследований в области прикладных систем искусственного интеллекта и процессов по заданной теме исследовательской практики, в том числе с использованием современных информационно коммуникационных технологий.	12	ПК-3	Л2.1-Л2.10
1.3	Определение необходимой материально-технической базы, определение проблемы, объекта и предмета исследования, формулирование цели и задач исследования, теоретический анализ литературы и исследований по проблеме, проведение обзора и выбор современных информационных технологий по исследуемой проблематике.	16	ПК-3	Л1.1 Л1.2
1.4	Проведение технологического обследования объекта информационной защиты, сбор экспериментального и экспертного материала и его теоретическое обобщение, проведение исследований и экспериментов	16	ПК-3	Л1.1 Л1.2
1.5	Ознакомление с принципами формирования политики информационной безопасности в информационной системе, оценка информационных рисков в информационной системе, знакомство с применяемыми принципами технического, программного и информационного обеспечения защищенных информационных систем, методами и средствами обеспечения сетевой безопасности, безопасности операционных систем, безопасности в СУБД. Использование в СУБД систем поддержки принятия решений и нейронных сетей.	16	ПК-3	Л1.1 Л1.2
1.6	Определение проектной задачи для разработки технологических решений в проектной форме, проведение самостоятельного решения задачи, исследований и экспериментов, разработка технических предложений, написание программного кода	16	ПК-3	Л1.1 Л1.2
1.7	Разработка предложений по использованию на практике	12	ПК-3	Л1.1

	интегрированных знаний для осуществления инновационной реализации исследовательской деятельности в области информационных систем и процессов с применением систем искусственного интеллекта			Л1.2
1.8	Подведение итогов производственной практике с перечислением приобретенных профессиональные умения и навыки в области прикладных систем искусственного интеллекта Написание отчёта по производственной практике (первичные профессиональные умения и навыки в области прикладных систем искусственного интеллекта) и получение отзыва о проделанной работе.	8	ПК-3	Л1.1 Л1.2
	Зачёт с оценкой	2	ПК-3	Л1.1- Л1.4 Л2.1-Л2.10 Л3.1
Итого – 108 ч				

5. Формы отчетности по практике

Формами отчетности обучающихся по практике являются:

1) *Заполненный дневник с отзывом руководителя практики.*

Содержание дневника должно соответствовать индивидуальному заданию и плану производственной практики. Подписи представителя организации о прибытии на практику и убытии с неё, а также подпись руководителя практики от предприятия под его отзывом должны быть заверены печатью организации, в которой проводилась практика.

2) *Отчет по практике.*

Отчет по практике оформляется отдельным документом в печатном виде на бумаге формата А4. Он должен содержать:

- титульный лист (образец приведен на сайте филиала);
- содержание практики (в соответствии с Программой производственной практики);
- краткие теоретические сведения и свидетельства выполнения Плана и Программы практики (скриншоты, фотографии оборудования, должностные инструкции.)
- перечень и обзор использованных обучающимся информационных источников и нормативных документов;
- выводы и предложения обучающегося по практике.

Отчет по практике подписывается обучающимся, проверяется и визируется руководителем практики от организации и руководителем практики от института. Защита отчетов производится в соответствии с установленным графиком защиты отчетов. Нарушение сроков прохождения практики и сроков защиты считается невыполнением учебного плана. По результатам защиты отчетов по практике в институте обучающемуся выставляется оценка.

3) *Ответы на контрольные вопросы и выполнение задач.*

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Рекомендуемая литература

6.1.1. Основная литература

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л1.1	П.С. Ложников, А.Е. Сомотуга, С.С. Жумажанова, А.Е.	Безопасность систем искусственного интеллекта. Ч.2. Доверенный искусственный интеллект: учебное пособие	Омск : Омский государственный технический университет,	Э1

	Сулавко		2023	
Л1.2	Никифоров С.Н.	Методы защиты информации. Пароли, скрытие, шифрование — 5-е изд., стер.	Санкт-Петербург : Лань, 2023. — 124 с.	Э2
6.1.2. Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1		Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 14.07.2022) "О персональных данных"		Э3
Л2.2		Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 14.07.2022) "Об электронной подписи"		Э4
Л2.3		Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 30.12.2021) "О связи" (с изм. и доп., вступ. в силу с 01.05.2022)		Э5
Л2.4		Федеральный закон от 17.07.1999 N 176-ФЗ (ред. от 27.12.2019) "О почтовой связи"		Э6
Л2.5		Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 14.07.2022) "Об информации, информационных технологиях и о защите информации"		Э7
Л2.6		Закон РФ от 21.07.1993 N 5485-1 (ред. от 04.08.2022) "О государственной тайне"		Э8
Л2.7		Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена"		Э9
Л2.8		Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"		Э10
Л2.9		ГОСТ 34.936-91 Информационная технология. Локальные вычислительные сети. Определение услуг уровня управления доступом к среде		Э11
Л2.10		ГОСТ Р 53724-2009 Качество услуг связи. Общие положения		Э12
6.1.3. Учебно-методическое обеспечение				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Дейвенпорт Т.,	Внедрение искусственного интеллекта	Москва : Альпина	Э13

	Мамедьяров З.	в бизнес-практику: преимущества и сложности : практическое руководство	Паблшшр, 2021. - 316 с.	
6.2. Электронные образовательные ресурсы				
Э1	https://www.iprbookshop.ru/140828.html			
Э2	https://e.lanbook.com/book/338018			
Э3	https://www.consultant.ru/document/cons_doc_LAW_61801/			
Э4	https://www.consultant.ru/document/cons_doc_LAW_112701/			
Э5	https://www.consultant.ru/document/cons_doc_LAW_43224/			
Э6	https://www.consultant.ru/document/cons_doc_LAW_6719/			
Э7	https://www.consultant.ru/document/cons_doc_LAW_61798/			
Э8	https://www.consultant.ru/document/cons_doc_LAW_2481/			
Э9	https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=180102&dst=			
Э10	https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17			
Э11	https://www.infosait.ru/Pages_gost/19099.htm			
Э12	https://docs.cntd.ru/document/1200082201			
Э13	https://znanium.ru/catalog/product/1841898			
6.3 Информационно-справочные системы и профессиональные базы данных				
5.3.1	Консультант Плюс - https://www.consultant.ru/			
5.3.2	Гарант - https://www.garant.ru/			
5.3.2	Консорциум Кодекс – https://docs.cntd.ru/			
5.3.3	Научная электронная библиотека – https://www.elibrary.ru/			
5.3.4	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)			
5.3.5	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)			
5.3.6	Научно информационная сеть https://www.researchgate.net/			
5.3.7	Национальный открытый университет «ИНТУИТ» - https://intuit.ru/			
5.3.8	Электронный ресурс http://www.securitylab.ru/			
6.4. Программное обеспечение				
СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:				
П.1	Linux (свободное ПО)			
П.2	LibreOffice (свободное ПО)			
П.3	Kaspersky Endpoint Security (лицензия)			

7. Материально-техническое обеспечение практической подготовки	
Прохождение практики обеспечивается материально-техническими средствами организации, осуществляющей деятельность по профилю образовательной программы (в том числе в структурном подразделении профильной организации, предназначенном для проведения практической подготовки) и/или структурных подразделений СКФ МТУСИ, предназначенных для проведения практической подготовки, а также учебными аудиториями для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенных оборудованием и техническими средствами обучения, а так же помещениями для самостоятельной работы обучающихся, оснащенными специализированной мебелью и компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ. Проведение практики обеспечено материально-технической базой, соответствующей действующим противопожарным правилам и нормам.	

8. Оценочные материалы

Оценочные материалы и перечень видов оценочных средств текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе практики.

9. Методические рекомендации для обучающихся по проведению практической подготовки

9.1 Методические рекомендации преподавателю

Перед началом практики кафедра ответственная за ее организацию должна ознакомить обучающихся с рабочей программой и оценочными материалами по дисциплине, с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, с формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

Кафедра, ответственная за организацию практики утверждает общий план её проведения, обеспечивает контроль проведения, организует и проводит инструктивное совещание с руководителями практики, обобщает информацию по аттестации обучающихся, готовит отчет по итогам практики.

Практика осуществляется на основе договоров между образовательным учреждением и предприятиями, в соответствии с которыми последние предоставляют места для прохождения практики. В договоре оговариваются все вопросы, касающиеся проведения практики. Консультирование по выполнению заданий, контроль посещения мест производственной практики, проверка отчетов по итогам практики и выставление оценок осуществляется руководителем практики от СКФ МТУСИ.

Перед началом практики проводится организационное собрание. Посещение организационного собрания и консультаций по практике – обязательное условие её прохождения.

Организационное собрание проводится с целью ознакомления обучающихся с приказом, сроками практики, порядком организации работы во время практики в организации, оформлением необходимой документации, правилами техники безопасности, распорядком дня, видами и сроками отчетности и т.п.

С момента зачисления практикантов на рабочие места на них распространяются правила охраны труда и внутреннего распорядка, действующие на предприятии.

Контроль за реализацией практической подготовки практикой зам. директора СКФ МТУСИ по УР.

9.1.1 Обязанности руководителя практики от СКФ МТУСИ:

- провести организационное собрание обучающихся перед началом практики;
- обеспечить контроль своевременного начала практики, прибытия и нормативов работы обучающихся на предприятии;
- обеспечить контроль соблюдения сроков практики и ее содержания;
- оказывать методическую помощь обучающимся при сборе материалов и выполнении отчетов;
- провести итоговый контроль отчета по практике в форме зачета, которая выставляется руководителем практики на основании оценок со стороны куратора практики от предприятия, собеседования со обучающимся с учетом его личных наблюдений;
- вносить предложения по улучшению и совершенствованию проведения практики перед руководством СКФ МТУСИ.

9.1.2 Обязанности куратора практики от предприятия

Ответственность за организацию и проведение практики возлагается на руководителя подразделения, в котором обучающиеся проходят практику.

Куратор практики:

- знакомится с содержанием заданий на практику и способствует их выполнению на рабочем месте;
- знакомит практиканта с правилами внутреннего распорядка;
- предоставляет максимально возможную информацию, необходимую для выполнения заданий практики;
- в случае необходимости вносит коррективы в содержание и процесс организации практики обучающихся;
- по окончании практики дает характеристику о работе обучающегося – практиканта;
- оценивает работу практиканта во время практики.

9.2 Методические рекомендации обучающимся

Перед прохождением практики обучающийся должен изучить программу, представленную учебно-методическую документацию по практике и обратиться к соответствующим нормативным материалам, литературе с тем, чтобы быть подготовленным к выполнению поручений, данных руководителем практики, к решению задач практики, конкретных практических вопросов.

При прохождении практики на предприятиях обучающиеся при необходимости должны подготовить необходимые документы (получить медицинскую справку по форме, требуемой предприятием-базой практики, подготовить фотографии и паспортные данные (ксерокопии разворотов с фотографиями и регистрацией места жительства для оформления пропусков на предприятия и т.д.).

В рамках самостоятельной работы обучающимся рекомендуется просмотреть конспекты лекций, учебники и другие учебные издания.

При прохождении практики обучающиеся обязаны: своевременно прибыть на место прохождения практики, иметь при себе все необходимые документы: индивидуальное задание, план (график) практики; подчиняться действующим правилам внутреннего трудового распорядка организации - места прохождения практики; изучить и строго соблюдать правила охраны труда, техники безопасности, пожарной безопасности; выполнять задания, предусмотренные программой практики; быть вежливым, внимательным в общении с работниками; вести записи о проделанной работе, чтобы в дальнейшем в отчете описать содержание проделанной работы; в установленный срок отчитаться о прохождении практики руководителю практики от университета, подготовить и сдать отчет и другие документы по практике на кафедру.

При подготовке к практике и во время прохождения практики рекомендуется по возникшим вопросам обращаться к учебной литературе, методическим материалам. При возникновении затруднений в процессе практики обучающийся может обратиться к руководителю практики от университета либо от организации-базы практики и получить необходимые разъяснения.

В результате практики бакалавра готовит краткий отчет (рекомендуемый объем – 15-25 страниц). В отчет следует помещать информацию об использованной литературе по теме дисциплины исследования, результаты исследований.

По окончании практики в дневнике делаются отметки, заверенные печатью, о сроках пребывания бакалавра на практике и дается отзыв научного руководителя.

Контроль качества самостоятельной работы обучающихся производится при защите отчета по практике.

10. Особенности прохождения практики для инвалидов и лиц с ограниченными возможностями здоровья

Выбор мест прохождения практики для обучающихся с ограниченными возможностями здоровья осуществляется с учетом рекомендаций медико-социальной экспертизы, отраженных в индивидуальной программе реабилитации, доступности рекомендованных условий труда для данной категории обучающихся (сюда относятся профильные доступные организации, готовые принять обучающихся, кафедры Филиала).

Обучающимся с ограниченными возможностями здоровья и инвалидам необходимо не позже чем за 2 месяца до начала практики написать заявление с приложением документов, подтверждающих необходимость подбора места практики с учетом их индивидуальных особенностей.

Содержание индивидуального задания для практики обсуждается обучающимся совместно с руководителем практики от организации, учитывая специфику организации и возможности в предоставлении материалов по отдельным аспектам организационной работы.

Обучающиеся должны проходить практику в соответствии с планом, выполняя все задания и по возникающим вопросам обращаться к руководителю практики от кафедры, сообщая о результатах проведенной работы не реже, чем два раза в неделю, при личном посещении или по электронной почте.

11. Дополнения и изменения в Рабочей программе

**Лист актуализации рабочей программы практики
«Производственная практика (первичные профессиональные умения и навыки в области
прикладных систем искусственного интеллекта) Б2.В.01(П)»
для использования в 20__/20__ учебном году**

Утверждаю

Зам. директора по УР _____
«__» _____ 20__ г.

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения: очная

(Возможны следующие варианты):

- а) Рабочая программа действует без изменений.
- б) В рабочую программу вносятся следующие изменения:
 - 1)
 - 2)
 - 3)

Разработчик (и): _____
(ФИО, ученая степень, ученое звание)
«__» _____ 20__ г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБ
Протокол № _____ от «__» _____ 20__ г.

Заведующий кафедрой _____

Оценочные материалы для проведения текущего контроля и промежуточной аттестации по дисциплине

1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

1.1 Шкала оценивания компетенций

Шкала оценивания компетенций		
Оценка	Уровень освоения компетенции	Критерии оценивания
«Отлично»	Высокий уровень	Обучающийся показывает всестороннее, систематическое и глубокое знание основного и дополнительного материала в рамках практической подготовки, умеет свободно выполнять задания, предусмотренные программой; усвоил основную и знаком с дополнительной рекомендованной литературой; может объяснить взаимосвязь основных понятий дисциплины в их значении для последующей профессиональной деятельности; проявляет творческие способности в понимании, изложении и использовании учебного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знаний в пределах основного материала в рамках практической подготовки, без существенных ошибок выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; способен объяснить взаимосвязь основных понятий дисциплины при дополнительных вопросах преподавателя. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся показывает знания основного материала в рамках практической подготовки в минимальном объеме, необходимом для дальнейшей учебы; справляется с выполнением заданий, предусмотренных программой, допуская при этом большое количество не принципиальных ошибок; знаком с основной литературой, рекомендованной программой. Допускает существенные погрешности в ответах, но обладает необходимыми знаниями для их устранения под руководством преподавателя.
«Неудовлетворительно»	Минимальный уровень не достигнут	Обучающийся обнаруживает пробелы в знаниях основного материала в рамках практической подготовки, допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не знаком с рекомендованной литературой, не может исправить допущенные ошибки. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение

		или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.
--	--	--

1.2 Показатели, критерии и шкалы оценивания компетенций

ПК-3: Администрирование средств защиты информации прикладного и системного программного обеспечения		
Знать:		
Архитектура подсистем защиты информации в прикладных системах искусственного интеллекта Принципы построения систем управления базами знаний прикладных систем искусственного интеллекта Основные средства и методы анализа программных реализаций Принципы построения антивирусного программного обеспечения Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению Источники угроз информационной безопасности программного обеспечения и меры по их предотвращению Уязвимости используемого программного обеспечения и методы их устранения Виды и формы функционирования вредоносного программного обеспечения Характерные признаки наличия вредоносного программного обеспечения Средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения Принципы функционирования программных средств криптографической защиты информации Порядок обеспечения безопасности информации при эксплуатации программного обеспечения Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры Организационные меры по защите информации.	Индивидуальное задание	Модуль 1 0-20 «Неудовлетворительно» - 0-7 «Удовлетворительно» – 8-12 «Хорошо» – 12-16 «Отлично» –16-20
Уметь:		
Анализировать угрозы безопасности информации в прикладных системах искусственного интеллекта Формулировать правила безопасной эксплуа-	Индивидуальное задание	Модуль 1 0-15 «Неудовлетворительно» - 0-5 «Удовлетворительно» – 6-9

тации программного обеспечения прикладных систем искусственного интеллекта Обосновывать правила безопасной эксплуатации программного обеспечения Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия Производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации Осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения Определять порядок функционирования программного обеспечения с целью обеспечения защиты информации Анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения.		«Хорошо» – 9-12 «Отлично» –12-15
Владеть:		
определением порядка установки программного обеспечения прикладных систем искусственного интеллекта с целью соблюдения требований по защите информации; контролем за соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение; навыками формулирования требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения; выполнением работ по обнаружению вредоносного программного обеспечения; навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования; навыками формулирования требований к встроенным средствам защиты информации программного обеспечения	Индивидуальное задание	Модуль 1 0-15 «Неудовлетворительно» - 0-5 «Удовлетворительно» – 6-9 «Хорошо» – 9-12 «Отлично» –12-15
Зачет с оценкой	Защита отчета о прохождении практики	0-100 «Неудовлетворительно» - 0-40 «Удовлетворительно» - 41-60 «Хорошо» - 61-80 «Отлично» - 81-100

1.3. Оценочные материалы: типовые контрольные задания, иные материалы

1.3.1 Оценочные материалы текущего контроля для очной формы обучения

Модуль 1 (100 баллов):

Модуль содержит 214 часов самостоятельной работы в форме практической подготовки в организации, выбранной в качестве места практики, по итогам которой проводится зачет с оценкой – 2 часа. Максимальное количество баллов за модуль 1 составляет 100.

Типовой план проведения практики должен содержать следующие пункты:

- 1 Прохождение инструктажа по правилам и мерам безопасности.
- 2 Изучение требований безопасности на рабочем месте.
- 3 Проведение поиска и изучение нормативной и правовой документации в области систем искусственного интеллекта в соответствии со списком рекомендованных источников.
- 5 Выполнение индивидуального задания.
- 6 Оформление дневника и отчета по практике.
7. Предоставление дневника и отчета о прохождении практики руководителю, защита отчета.

Все пункты плана практики устанавливаются руководителем практики. Данные пункты являются базовыми, но они могут быть дополнены или изменены исходя из индивидуальных особенностей обучающегося или в целях научно-исследовательской работы в филиале.

В индивидуальное задание выносятся вопросы, которые должны быть отражены в отчете по практике.

Типовой вариант индивидуального задания для прохождения практики:

- 1 Пройти инструктажа по правилам и мерам безопасности.
- 2 Изучить требования безопасности на рабочем месте.
4. Изучить правила организации рабочего места.
5. Выполнять обязанности должностного лица. Получить умения и навыки выполнения обязанностей, соответствующих должности, на которой проходит практика.
6. Типовые вопросы, раскрываемые обучающимся в отчете о прохождении практики:
 - 6.1 Искусственные нейронные сети. Структуры, виды и особенности (ПК-3).
 - 6.2 Достоинства и недостатки искусственных нейронных сетей по сравнению с регрессией и решающими деревьями (ПК-3).
 - 6.3 Сверточные нейронные сети. Цель. Структура и особенности (ПК-3).
 - 6.4 Применение нейронных сетей для задач генерации признаков (ПК-3).
 - 6.5 Глубокое обучение (Deep learning) (ПК-3).
 - 6.6 Метод обратного распространения ошибок. Основная идея. Основные недостатки и способы их устранения (ПК-3).
 - 6.7 Какие основные признаки или характеристики используют для определения фишинговых сайтов? (ПК-3)
 - 6.8 Какие методы машинного обучения наиболее подходят для задачи прогнозирования фишинговых сайтов? (ПК-3)
 - 6.9 В чем разница между обучением с учителем и без учителя в контексте обнаружения фишинга? (ПК-3)
 - 6.10 Какие источники данных используют для обучения моделей по прогнозированию фишинговых сайтов? (ПК-3)
 - 6.11 Какие метрики используют для оценки эффективности моделей по обнаружению фишинговых сайтов? (ПК-3)
 - 6.12 Как можно использовать результаты модели для автоматической блокировки или предупреждения пользователя о потенциальных фишинговых сайтах? (ПК-3)
7. Оформить дневник и отчёт по практике.
8. Отчитаться о прохождении практики перед руководителем от предприятия и получить от него отзыв о работе.

1.3.2 Оценочные материалы промежуточной аттестации для очной формы обучения

По результатам освоения программы практики обучающиеся представляют письменный отчет с промежуточной аттестацией в форме зачета с оценкой.

Отчет о прохождении практики должен содержать текстовую часть и приложения. В нём излагаются результаты прохождения практической подготовки в соответствии с индивидуальным заданием.

Примерный перечень вопросов при защите отчета о практике:

- 6 Искусственные нейронные сети. Структуры, виды и особенности.
- 7 Достоинства и недостатки искусственных нейронных сетей по сравнению с регрессией и решающими деревьями.
- 8 Сверточные нейронные сети. Цель. Структура и особенности.
- 9 Применение нейронных сетей для задач генерации признаков.
- 10 Глубокое обучение (Deep learning).
- 11 Метод обратного распространения ошибок. Основная идея. Основные недостатки и способы их устранения.
- 12 Какие основные признаки или характеристики используют для определения фишинговых сайтов?
- 13 Какие методы машинного обучения наиболее подходят для задачи прогнозирования фишинговых сайтов?
- 14 В чем разница между обучением с учителем и без учителя в контексте обнаружения фишинга?
- 15 Какие источники данных используют для обучения моделей по прогнозированию фишинговых сайтов?
- 16 Какие метрики используют для оценки эффективности моделей по обнаружению фишинговых сайтов?
- 17 Как можно использовать результаты модели для автоматической блокировки или предупреждения пользователя о потенциальных фишинговых сайтах?

2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Порядок и методика проведения текущего контроля и промежуточной аттестации

Предусмотрены следующие виды контроля:

- текущий контроль – проводится в форме контроля на каждом этапе практической подготовки в соответствии с планом практики в процессе работы обучающегося в рамках его индивидуального задания.

- промежуточная аттестация – проводится в форме зачета с оценкой.

С целью повышения качества обучения за счет побуждения обучающихся к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса, снижения роли случайных и субъективных факторов при оценивании учебной деятельности обучающихся в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимися в рамках текущего контроля баллы могут быть переведены в оценку:

- «неудовлетворительно» - от 0 до 40 от максимального количества баллов;
- «удовлетворительно» - от 41 до 60 максимального количества баллов;
- «хорошо» - от 61 до 80 максимального количества баллов;
- «отлично» - от 81 до 100 максимального количества баллов.

Соотношения максимального количества баллов, полученных обучающимся по блокам модулей,

показаны в Таблице1.

Таблица 1 - Распределение баллов по блокам модулей Производственная практика (первичные профессиональные умения и навыки в области прикладных систем искусственного интеллекта)

Модуль	Всего баллов (Максимальное значение)	Теоретический блок	Практический блок (контрольные вопросы)
Модуль 1	100	0	100
Зачет с оценкой	100	100	

3 Промежуточная аттестация

Промежуточная аттестация проводится в форме зачета с оценкой. Аттестацию обучающихся по итогам практики проводит руководитель практики от СКФ МТУСИ на основании оформленного отчета. Защита отчета проводится в форме индивидуального собеседования.

Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

4 Тестовые задания по дисциплине Б2.В.01(П) Производственная практика (первичные профессиональные умения и навыки в области прикладных систем искусственного интеллекта)

Тестовые задания позволяют оценить уровень сформированности компетенции:

ПК-3 - Администрирование средств защиты информации прикладного и системного программного обеспечения

Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень (Блок А) содержит примерно 50 % заданий.

Он формируется из заданий с выбором одного или нескольких верных ответов из предложенных или воспроизведения фактического материала (терминология, факты, классификация, параметры и др.);

Повышенный уровень (Блок Б) в среднем составляет 35 % заданий.

В нем используются задания на сопоставление, сравнение, установление последовательности;

Высокий уровень (Блок В) в среднем составляют – 15 % заданий.

В задании используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Количество заданий по компетенции ПК-3 равно 20.

Комплект тестовых вопросов с указанием правильных ответов хранится у заведующего кафедрой.

ПК-3 - Администрирование средств защиты информации прикладного и системного программного обеспечения

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Тексты заданий
1	"Обучение системы искусственного интеллекта без учителя" характеризуется отсутствием: 1. эксперта, корректирующего процесс обучения 2. желаемого выхода сети 3. обучающего множества
2	"Обучение системы искусственного интеллекта без учителя" это - 1. подстройка входных данных для получения нужных выходов

№ задания	Тексты заданий
	2. использование знаний эксперта 3. использование сравнения с идеальными ответами 4. подстройка матрицы весов для получения нужных ответов
3	К методам анализа программных реализаций прикладных систем искусственного интеллекта относятся 1. Тестирование. 2. Проверка кода. 3. Анализ требований. 4. Методы обнаружения уязвимостей. 5. Резервирование 6. Испытание на прочность
4	Адаптация информационной системы это... 1. подстройка параметров и структуры системы с целью достижения требуемого качества управления в условиях непрерывных изменений внешних условий 2. процесс непрерывного совершенствования системы для достижения полного превосходства при реализации бизнес - процессов 3. процесс обучения системы, при котором дополнительная информация о верности реакции системе не сообщается 4. процесс их настройки на меняющиеся условия эксплуатации и потребности пользователей и бизнес-процессов 5. процесс, в результате которого система постепенно приобретает способность отвечать нужными реакциями на определенные совокупности внешних воздействий
5	К методам устранения уязвимостей относятся: 1. Установка патча или новой версии. 2. Отключение сетевой службы, если есть возможность её заменить или отказаться вовсе. 3. Ограничение доступа к уязвимому сервису или активу (например, ограничение по IP). 4. Разграничение прав доступа 5. Соблюдение политики безопасности 6. Использование средств защиты, блокирующих эксплуатацию уязвимости.
6	Аномалии, связанные с системами искусственного интеллекта, включают: 1. Дрейф данных. 2. Дубликаты в данных. 3. Дрейф концепций. 4. Шпионское ПО 5. Утечку данных 6. Заражение данных
7	Алгоритмы разобучения применяются для: 1. "забывания" некорректных весовых изменений 2. "забывания" ложных образов 3. "забывания" повторяющихся обучающих пар
8	Для подтверждения соответствия требованиям стандарта ГОСТ Р 56939-2016 «Разработка безопасного программного обеспечения» документация разработчика ПО должна содержать: 1. План тестирования, описание выполняемых тестов инструментальных средств, используемых для функционального тестирования программы; 2. Фактические результаты тестирования; 3. Отчеты, содержащие список выявленных несоответствий требованиям безопасности, описание действий, направленных на их устранение, либо обоснование невозможности или отсутствия необходимости в устранении несоответствия требованиям; 4. Планы на будущие разработки ПО.
9	К интеллектуальным задачам можно отнести: 1. доказательство теорем 2. решение алгебраических уравнений 3. поиск кратчайшего пути на графе 4. распознавание образов 5. численное интегрирование дифференциальных уравнений
10	Метод «Дельфы» относится к 1. эвристическим методам 2. количественным методам 3. формализованным методам

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия

Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Сопоставьте причины важности обеспечения безопасности систем искусственного интеллекта и их обоснование: 1. Обеспечение целостности системы; 2. Защита конфиденциальных данных; 3. Обеспечение доступности служб ИИ. Расставьте в соответствии тем последствиям, которые характеризуют данные категории А. Системы ИИ обрабатывают огромные объёмы конфиденциальных данных, в том числе финансовые, медицинские, личные сведения; Б. Незащищённые уязвимости могут создать возможность для взлома моделей, которые в результате начнут выдавать неточные или опасные результаты; В. Нарушения безопасности часто приводят к перебоям в работе, что может нарушить работу жизненно важных служб.
12	Сопоставьте угрозы безопасности систем искусственного интеллекта и их последствия: 1. Состязательные атаки. 2. Порча данных. 3. Атаки методом инверсии модели. А. Злоумышленники внедряют вредоносные или вводящие в заблуждение данные в набор обучения системы ИИ. Это может привести к выдаче неточных или опасных результатов. Б. Злоумышленники используют прогнозы модели ИИ для восстановления конфиденциальной информации, на которой обучалась модель. Это может привести к раскрытию конфиденциальных данных, таких как личные сведения, не предназначенные для публичного использования. В. Происходят на этапе использования уже обученной модели ИИ, незначительные изменения входных данных могут приводить к ошибочным выводам модели.
13	Сопоставьте меры по обеспечению безопасности систем ИИ и их содержание: 1. Безопасное проектирование 2. Управление рисками 3. Человеческий контроль 4. Защита активов 5. Надёжная инфраструктур. А. Обеспечение безопасности платформ, на которых работает ИИ Б. Закрепление ответственности людей за функционирование ИИ. В. Регулярная оценка потенциальных уязвимостей Г. Интеграция защитных механизмов на этапе разработки. Д. Безопасное хранение и обработка данных, моделей и промпта.
14	Сопоставьте принципы построения антивирусного программного обеспечения и их содержание: 1. Сигнатурный анализ 2. Эвристический анализ 3. Поведенческий мониторинг 4. Машинное обучение и ИИ 5. Регулярные обновления. А. Обеспечивает антивирусу доступ к последним сведениям о новых угрозах Б. Создаёт «песочницу» — изолированную среду, где запускает подозрительную программу. Ведет наблюдение за действиями программы. В. Анализирует структуру и код программы на предмет подозрительных элементов. Он ищет признаки, характерные для вредоносного ПО Г. Использует базу данных сигнатур — уникальных идентификаторов вредоносных программ. Д. Алгоритмы обучаются на больших наборах данных для выявления паттернов, характерных для вредоносного ПО. Позволяет прогнозировать новые типы атак.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Определить правильный порядок действий по аудиту безопасности систем ИИ: 1. Сбор и систематизация данных. 2. Оценка технического и программного обеспечения 3. Обследование информационных процессов. 4. Подготовка отчёта для руководства (заказчика) . 5. Сравнение текущей картины с техническим заданием. 6. Определение границ и глубины оценки.
16	Установить правильный порядок действий по категорированию объектов критической информационной инфраструктуры (КИИ) 1. Направление сведений о результатах категорирования в ФСТЭК России; 2. Подготовка акта категорирования объекта КИИ; 3. Категорирование объектов КИИ; 4. Определение перечня объектов КИИ, подлежащих категорированию; 5. Формирование исходных данных для категорирования; 6. Создание комиссии по категорированию.
17	Расставьте в правильном порядке этапы категорирования объектов КИИ согласно Федеральному закону №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и Постановлением Правительства РФ №127: 1. Утверждение и регистрация — результаты категорирования утверждаются в установленном порядке, данные о категорированных объектах заносятся в реестр значимых объектов КИИ РФ. 2. Идентификация объектов — определение информационных систем, сетей и систем управления, которые могут быть отнесены к критическим; 3. Присвоение категории — комиссия присваивает категорию на основе оценки; 4. Оценка значимости — анализ возможных последствий утраты конфиденциальности, целостности или доступности информации;

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	_____ искусственный интеллект (ИИ) — это концепция разработки и эксплуатации систем ИИ, которые гарантированно обладают свойствами надёжности, безопасности, эффективности, продуктивности, прозрачности, конфиденциальности, справедливости и этичности получаемых результатов.
19	Объяснимость — алгоритмы работы ИИ должны быть доступны для изучения и подконтрольны человеку. Подотчётность — возможность использования систем ИИ с обеспечением человеческого надзора и контроля над поведением и результатами. Конфиденциальность — использование механизмов защиты и контроля доступа к собираемым и генерируемым данным. Справедливость — внедрение методов проверки предвзятости и учёта интересов всех, на кого распространяются системы ИИ. Здесь перечислены принципы концепции _____ ИИ
20	Энергетика; Транспорт. Здравоохранение. Финансы. Связь. Наука. Государственная регистрация прав на недвижимое имущество и сделок с ним. Ракетно-космическая промышленность. Промышленность. Оборона и государственное управление Это сферы, в которых используются _____

Система оценивания выполнения тестовых заданий по компетенции ПК-3, формируемой дисциплиной Б2.В.01(П) Производственная практика (первичные профессиональные умения и навыки в области прикладных систем искусственного интеллекта)

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует- 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.