Автономная некоммерческая организация
высшего образования
«Российский новый университет»
(АНО ВО «Российский новый университет»)

УТВЕРЖДАЮ
Проректор по качеству
образования и аккредитации
_____ И.В. Дарда
«30» 09 2024 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Искусственный интеллект:

применение в информационной безопасности»

Объем программы: 72 часа

Москва

1. Общая характеристика программы

1.1. Дополнительная профессиональная программа – программа повышения квалификации направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации необходимой для профессиональной деятельности слушателей, в сфере информационной безопасности (ИБ) направленной на использование технологий искусственного интеллекту при разработке алгоритмов и программно-технических средств, решающих задачи информационной безопасности в различных предметных областях.

1.2. Нормативно-правовые акты, регламентирующие разработку программы повышения квалификации:

– Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

– Порядок организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденный приказом Минобрнауки России от 1 июля 2013 г. № 499;

– Устав Автономной некоммерческой организации высшего образования «Российский новый университет»;

– Локально - нормативные акты, регламентирующие образовательную деятельность по дополнительным образовательным программам.

– Программа повышения квалификации разработана с учетом требований:

– Профессионального стандарта «Системный аналитик» (Зарегистрировано в Минюсте России 25.05.2023 N 73453), утвержденный приказом Минтруда России от 27.04.2023 N 367н;

– Федерального государственного образовательного стандарта высшего образования - по направлению подготовки 09.04.03 Прикладная информатика, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 N 916.

1.3. Категория обучающихся: лица, имеющие или получающие высшее, или среднее профессиональное образование.

Срок освоения программы: 72 часа (3 недели).

Режим обучения - 2 дня в неделю, 4 часа в день.

Форма обучения – заочная с применением дистанционных образовательных технологий.

Формы аттестации обучающихся: промежуточная и итоговая аттестация в форме зачетов.

Документ о квалификации: лицам, успешно освоившим программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации, образца, установленного АНО ВО «Российский новый университет».

1.5. Цель программы: совершенствование компетенций слушателей, необходимых для их профессиональной деятельности в сфере информационной безопасности (ИБ) направленной на использование технологий искусственного интеллекта при разработке алгоритмов и программно-технических средств, решающих задачи информационной безопасности в различных предметных областях.

Слушатель, освоивший программу повышения квалификации, в соответствии с целью на которую ориентирована программа, должен быть готов решать следующие **профессиональные задачи:**

1. Уметь формулировать корректные и актуальные математические постановки задач в области безопасности систем искусственного интеллекта, а также применять методы искусственного интеллекта в задачах обеспечения информационной безопасности;
2. Уметь разрабатывать алгоритмы анализа защищенности систем, построенных с использованием методов искусственного интеллекта и машинного обучения;
3. Уметь разрабатывать и реализовывать методы анализа безопасности и защищенности программ и их поведения с использованием методов искусственного интеллекта и машинного обучения, в том числе интерпретируемого машинного обучения;
4. Уметь анализировать устойчивость моделей машинного обучения к атакам, обеспечивать робастность моделей машинного обучения.

2. Планируемые результаты обучения:

Программа повышения квалификации направлена на формирование (совершенствование) следующих профессиональных компетенций

КОД	Формулировка компетенции
ПК 1	Способен осуществлять выработку научных решений по применению интеллектуальных систем для решения задач информационной безопасности
ПК 2	Способен эксплуатировать интеллектуальные системы
ПК-3	Способен руководить проектами по созданию комплексных систем искусственного интеллекта
ПК-4	Выбирает комплексы методов и инструментальных средств искусственного интеллекта для решения задач в информационной безопасности

ПК-5	Способен руководить проектами по созданию, внедрению и использованию одной или не скольких сквозных цифровых технологий искусственного интеллекта в прикладных областях

В результате освоения дополнительной профессиональной программы – программы повышения квалификации, слушатель должен **знать:**

1. Современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач.

2. Новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях.

3. Основные методы и принципы исследований и разработки новых решений при проектировании интеллектуальных средств информационной безопасности.

4. Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; методы защиты информации от несанкционированного доступа и утечки по техническим каналам; нормативные правовые акты в области защиты информации.

5. Основные виды и процедуры обработки информации, модели и методы решения задач обработки информации.

В результате освоения дополнительной профессиональной программы повышения квалификации, слушатель должен **уметь:**

1. Искать и анализировать существующие решения в области разработки средств антивирусной защиты компьютерных систем, адаптировать их для решения задач в новых предметных областях.

2. Определять подлежащие защите информационные ресурсы автоматизированных систем; оценивать информационные риски в автоматизированных системах; классифицировать и оценивать угрозы безопасности информации.

3. Осуществлять постановку задач и использовать различные алгоритмы обработки информации.

4. Формулировать правила безопасной эксплуатации программного обеспечения; обосновывать правила безопасной эксплуатации программного обеспечения; определять порядок функционирования программного обеспечения с целью обеспечения защиты информации; анализировать эффективность сформулированных требований к встроенным

средствам защиты информации программного обеспечения.

5. Разрабатывать и тестировать программные компоненты информационных систем.

В результате освоения дополнительной профессиональной программы повышения квалификации слушатель должен **иметь практический опыт (владеть):**

1. Навыками анализа методов решения новых задач в области информационной безопасности, а также приемами разрешения проблемных ситуаций с помощью адаптации существующих или разработки новых интеллектуальных систем.

2. Методикой оценки последствий выявленных инцидентов и обнаружения нарушения правил разграничения доступа.

3. Навыками работы с программными средствами, осуществляющими обработку информации.

4. Методикой формулирования требований к встроенным средствам защиты информации программного обеспечения.

5. Приемами отладки приложений, поиска ошибок и обработки исключений.

3. Формы аттестации

Формами аттестации слушателей по программе повышения квалификации являются: промежуточная и итоговая аттестация.

Промежуточная аттестация проводится в форме зачетов и предназначена для объективного подтверждения и оценивания достигнутых результатов обучения после завершения изучения дисциплины. Оценивание результатов формирования компетенций в рамках дисциплины у слушателей осуществляется по промежуточной аттестации.

Итоговая аттестация слушателей по программе повышения квалификации включает итоговый зачет, который проходит в форме тестового задания.

4. Документ об обучении (образовании)

Лицам, успешно освоившим дополнительную профессиональную программу и прошедшим итоговую аттестацию, выдаётся удостоверение о повышении квалификации.

При освоении дополнительной профессиональной программы параллельно с получением среднего профессионального образования и (или) высшего образования удостоверение о повышении квалификации выдается одновременно с получением соответствующего документа об образовании и о квалификации.

Лицам, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также лица освоившим часть дополнительной

профессиональной программы и (или) отчисленным из организации, выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому организацией.

5. Учебный план

УЧЕБНЫЙ ПЛАН

программы повышения квалификации

«Искусственный интеллект:

применение в информационной безопасности»

№п/п	Наименование учебных курсов, дисциплин (модулей) практик	Всего час.	В том числе			Сам. раб	Форма контроля	Формируемые компетенции
			аудит. занят.	лекции	практич. зан.			
1	Компьютерная безопасность	24	8	4	4	16	зачет	ПК-1 ПК-2
2	Применение машинного обучения для задач информационной безопасности	24	8	4	4	16	зачет	ПК-3 ПК-4
3	Проекты искусственного интеллекта в области информационной безопасности	24	8	4	4	16	зачет	ПК-4 ПК-5
4	Итоговая аттестация	зачет						
	ВСЕГО:	72	24	12	12	48		

Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

Промежуточный контроль проходит на последнем занятии контактной работы с преподавателем.

6. Календарный учебный график

Календарный учебный график – локальный документ, регламентирующий организацию образовательного процесса при реализации программы дополнительного профессионального образования – программы повышения квалификации.

Календарный учебный график разрабатывается и утверждается на каждую учебную группу.

Образовательный период в данной группе начинается по мере ее комплектования.

Первым днем, первой недели обучения, считать день зачисления слушателей на обучение по данной образовательной программе. Количество учебных дней в неделю не

может превышать 5 дней. Количество учебных часов в день не может превышать 4 часов. Завершение учебного процесса согласно календарному учебному графику.

Календарный учебный график
Дополнительная профессиональная программа повышения квалификации
«Искусственный интеллект: применение в информационной безопасности»

Учебные недели/ Наименование учебных курсов, дисциплин (модулей) практик	1	2	3
Компьютерная безопасность	А	А	
Применение машинного обучения для задач информационной безопасности	А	А	
Проекты искусственного интеллекта в области информационной безопасности		А	А
Итоговая аттестация			ИА

Условные обозначения:
А – Аудиторное занятие (лекция, практическое занятие, самостоятельная работа)
ИА - Итоговая аттестация

7. Содержание программ дисциплин (рабочие программы учебных курсов, дисциплин (модулей) практик)

Рабочие программы учебных курсов, дисциплин (модулей) практик представлены по каждому учебному курсу, дисциплине (модулю) практике в форме учебно – тематического плана, в котором обозначено содержание данной учебной дисциплины.

Учебно - тематический план по дисциплине: **«Компьютерная безопасность»**

№п/п	Наименование раздела (темы) по учебной дисциплине	Всего час.	В том числе			Сам. раб	Текущая аттестация (опрос +/-)
			аудит. занят.	лекции	практич. зан.		
1	Тема 1. Типы атак в информационной безопасности.	6	2	1	1	4	+
2	Тема 2. Безопасность компьютерных сетей и сетевых протоколов.	6	2	1	1	4	+
3	Тема 3. Криптография.	6	2	1	1	4	+
4	Тема 4. Безопасность в ОС Linux. Инъекции.	6	2	1	1	4	+
5	Промежуточный контроль:	зачет					
6	ВСЕГО:	24	8	4	4	16	

Содержание программы:

Эволюция архитектур информационных систем. Политика информационной безопасности объекта защиты. Описание объекта защиты. Определение основных приоритетов информационной безопасности. Анализ рисков. Формирование перечня критичных ресурсов. Модели нарушителя и угроз. Информационная система как объект защиты. Общие требования построения защищенной информационной системы.

Требования к подсистеме обеспечения безопасности сетевого взаимодействия. Требования к подсистеме аутентификации и управления доступом. Требования к подсистемам резервирования/ восстановления информации, контроля эталонного состояния информации и рабочей среды. Требования к средствам построения защищенных сетей и управления безопасностью. Многоуровневая модель защиты в информационной системе на архитектуре «клиент-сервер»: методы защиты информации на физическом, канальном, сетевом, транспортном, сеансовом и прикладном уровнях модели. Протокол формирования защищенного туннеля на канальном уровне.

Учебно - тематический план по дисциплине: **«Применение машинного обучения для задач информационной безопасности»**

№п/п	Наименование раздела (темы) по учебной дисциплине	Всего час.	В том числе			Сам. раб	Текущая аттестация (опрос +/-)
			аудит. занят.	лекции	практич. зан.		
1	Тема 1. Определение спама. Классификация сетевых атак.	6	2	1	1	4	+
2	Тема 2. Определение злонамеренных (malicious) сайтов. Определение инъекций.	6	2	1	1	4	+
3	Тема 3. Поиск злонамеренного программного обеспечения (malware).	6	2	1	1	4	+
4	Тема 4. Анализ аномалий в активности пользователей.	6	2	1	1	4	+
5	Промежуточный контроль:	зачет					
6	ВСЕГО:	24	8	4	4	16	

Содержание программы:

Стратегии с применением теория игр. Человеческий фактор как один из базовых рисков. Организационные меры защиты информации. Политики информационной безопасности. Практическая игра с распределение ролей и функций. Понимания ландшафта угроз. Технологии защиты сетевой инфраструктуры. Жизненный цикл атаки. Стандартизация в области информационной безопасности. Виртуализация. Понятие privacy. Законодательные акты и стандарты в области защиты информации. Основные принципы и особенности применения на практике. Управление рисками информационной безопасности: методы и инструменты. Способы обнаружения и предотвращения информационных атак Кейс-стади.

Применение модели Cyber Kill Chain на практике. Как анализ данных и машинное обучение помогают в решении практических задач в области информационной безопасности. Криптографические и стенографические методы защиты информации. Криптопротоколы и методы доказательства их корректности. Применение ML в криптоанализе. Уязвимости информационных систем. Методы выявления и устранения с применением методов ML. Спам-рассылки: технологии, организация и методы защиты Кейс-стади. Системы и методы защиты от спама. Спам-фильтры. Культурные особенности применения ИБ. Пользовательский интерфейс как фактор безопасности. Принципы и методы анализа безопасности программного обеспечения методами МЛ Кейс-стади. Практический пример статического анализа кода на уязвимости.

Учебно - тематический план по дисциплине: **«Проекты искусственного интеллекта в области информационной безопасности»**

№п/п	Наименование раздела (темы) по учебной дисциплине	Всего час.	В том числе			Сам. раб	Текущая аттестация (опрос +/-)
			аудит. занят.	лекции	практич. зан.		
1	Тема 1. Жизненный цикл проекта создания приложений искусственного интеллекта для информационной безопасности.	6	2	1	1	4	+
2	Тема 2. Подготовка набора данных в информационной безопасности. Выбор модели и ее обучение.	6	2	1	1	4	+
3	Тема 3. Оценка качества модели. Разработка приложения, использующего модель.	6	2	1	1	4	+
4	Тема 4. Внедрение приложения в практическое использование.	6	2	1	1	4	+
5	Промежуточный контроль:	зачет					
6	ВСЕГО:	24	8	4	4	16	

Содержание программы:

Антивирусное программное обеспечение; Программы для защиты от несанкционированного доступа и сетевых хакерских атак; Фильтры нежелательной корреспонденции; Проверка в режиме реального времени; Проверка по требованию; Поддержание актуальности антивирусных баз; Фильтрация нежелательных электронных сообщений; Персональная антиспамовая программа; Применение методов искусственного интеллекта в рассмотренных программах; - Применение перспективных методов при разработке антивирусных

программ; Проектирование антивирусного ПО для защиты домашнего компьютера на базе методов искусственного интеллекта; Основы построения локальной компьютерной сети; Рабочие станции и сетевые серверы, почтовые серверы и шлюзы; Уровни антивирусной защиты: уровень защиты рабочих станций и сетевых серверов, уровень защиты почтовых серверов, уровень защиты шлюзов; Централизованное управление антивирусной защитой; Компоненты системы удаленного централизованного управления: клиентская антивирусная программа, сервер администрирования, агент администрирования, консоль администрирования; Организация сбора статистики в системе антивирусной защиты и использование этой информации в интеллектуальных системах информационной безопасности; Червь Caribe - вредоносная программа для мобильных телефонов; Антивирусы для мобильных устройств; Политики обеспечения информационной безопасности при работе с мобильными устройствами. Политика «нулевого доверия»; Разработка организационных методов реализации политики безопасности предприятия при проектировании системы антивирусной защиты для удаленных рабочих мест; Организация и управление коллективной разработкой системы антивирусной защиты корпоративной сети предприятия, включающей удаленные рабочие места; Применение методов искусственного интеллекта.

8. Организационно – педагогические условия программы

8.1. Материально – технические условия реализации программы.

Реализация программы повышения квалификации осуществляется на материально-технической базе АНО ВО «Российский новый университет», обеспечивающей проведение всех видов учебных занятий, предусмотренных учебным планом.

Учебный процесс обеспечен учебной аудиторией, соответствующей санитарно-гигиеническим требованиям для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы, хранения и профилактического обслуживания учебного оборудования. Помещение укомплектовано мебелью и техническими средствами обучения, служащими для представления учебной информации. Аудитория соответствует нормам освещенности, оснащена системой кондиционирования воздуха.

В учебном помещении имеется необходимая для процесса обучения компьютерная техника, учебно-наглядные пособия, обеспечивающие тематические иллюстрации, соответствующие содержанию программы, освоению дисциплин (модулей).

Помещение подключено к сети "Интернет", также в нем обеспечен доступ в электронную информационно-образовательную среду организации. Рабочее место

преподавателя оснащено web-камерой с микрофоном и гарнитурой, необходимой для работы в MS Skype.

8.2.Учебно – методическое и информационное обеспечение программы

Слушателям предоставляется бесплатный доступ к ресурсам электронной информационно-образовательной среды на сайте Университета. Каждый слушатель во время самостоятельной подготовки обеспечивается рабочим местом в компьютерном классе или через выход в Интернет получает доступ к использованию электронных изданий, в соответствии с объемом изучаемых дисциплин.

Каждый слушатель на время занятий обеспечивается комплектом учебно-методических материалов, содержащим электронные и печатные информационные разработки, учебные видеофильмы.

8.3.Кадровое обеспечение образовательного процесса.

К реализации программы привлечены представители образовательных организаций высшего образования, научных организаций и представители компаний со стажем работы в профильной организации. Представители образовательной организации высшего образования и научной организации имеют высшее образование, ученую степень кандидата наук, стаж научно-педагогической работы более трех лет. Члены преподавательского состава имеет за последние 3 года научные публикации, соответствующие направлению данной программы.

№ п/ п	Фамилия, имя, отчество (при наличии)	Место основной работы и должность, ученая степень и ученое звание (при наличии)	Стаж работы по специальности
1	Клименко Игорь Семенович	АНО ВО «Российский новый университет»	60 лет
2	Лабунец Леонид Витальевич	АНО ВО «Российский новый университет»	50 лет
3	Золотарев Олег Васильевич	АНО ВО «Российский новый университет»	39 лет

9. Контроль и оценка результатов освоения программы

9.1.Формы аттестации

Реализация программы повышения квалификации включает в себя промежуточную и итоговую аттестацию.

Текущий контроль проводится по итогам самостоятельной - внеаудиторной работы слушателя.

Промежуточная аттестация проводится по итогам освоения дисциплины (модуля) в форме зачета.

Завершается освоение программы повышения квалификации итоговой аттестацией обучающихся в форме итогового зачета.

9.2.Оценочные средства

9.2.1. Примерный перечень вопрос для проведения промежуточной и текущей аттестации:

1. Особенности поиска, отбора, хранения, передачи, кодирования, обработки и защита и анализа данных методами машинного обучения применительно к задачам информационной безопасности.

2. Классификация угроз и уязвимостей.

3. Классификация методов защиты.

4. Основные библиотеки, применяемые для анализа данных в информационной безопасности.

5. Особенности и сферы применения моделей машинного обучения в информационной безопасности.

6. Модели машинного обучения для анализа угроз и атак.

7. Модели анализа и управления рисками в информационной безопасности.

8. Жизненный цикл внедрения методов машинного обучения в системы информационной безопасности.

9. Лучшие практики и анализ на основе алгоритмов машинного обучения.

10. Юридические, экономические и социальные проблемы внедрения алгоритмов машинного обучения в бизнес-процессы.

11. Применение методов машинного обучения для анализа поведения людей и систем.

12. Особенности подготовки данных для обучения систем машинного обучения.

13. Особенности настройки параметров систем машинного обучения.

14. Методы оценки эффективности алгоритмов и систем машинного обучения в информационной безопасности.

15. Особенности дата-центрированного подхода для информационной безопасности и

его отличие от других подходов.

16. Уязвимости систем машинного обучения.

17. Применение алгоритмов машинного обучения в криптоанализе.

18. Будущее систем машинного обучения. Возможности и ограничения.

19. Перспективы применения машинного обучения для обнаружения вредоносных программ.

20. Интеллектуальные методы защиты от атак на беспроводные сети.

21. Антивирусная защита ОС семейства Эльбрус с использованием методов искусственного интеллекта.

22. Методы защиты конфиденциальной информации при проведении переговоров в неспециализированных помещениях.

23. Настройка антивирусного программного обеспечения для защиты вебсайта с использованием методов искусственного интеллекта.

24. Методы защиты новостных порталов от вирусных атак с использованием методов искусственного интеллекта.

25. Методы защиты от атак, связанных с системными структурами жёстких дисков, с использованием методов искусственного интеллекта.

26. Антивирусная защита ИСПДн на основе отечественной аппаратно-программной платформы с использованием методов искусственного интеллекта.

27. Методы защиты технологии SDN

28. Обеспечение антивирусной защиты цифровых систем управления запасами в логистике терминально-складских комплексов с использованием методов искусственного интеллекта.

29. Обеспечение антивирусной защиты Департамента Логистики и Планирования компании Z с использованием методов искусственного интеллекта.

30. Обеспечение антивирусной защиты мультимодальных транспортно-логистических центров с использованием методов искусственного интеллекта.

31. Обеспечение антивирусной защиты персонального компьютера при разработке платформы имитационной модели складского процесса с использованием методов искусственного интеллекта.

32. Обеспечение антивирусной защиты цифровой платформы «Личные диаметры» с использованием методов искусственного интеллекта.

33. Обеспечение антивирусной защиты в бизнес-процессах закупочной логистики с использованием методов искусственного интеллекта.

34. Обеспечение антивирусной защиты при работе оператора, использующего технологию «Физический интернет».

35. Обеспечение антивирусной защиты при работе оператора, использующего цифровую платформу ЭТП ГП.

36. Обеспечение антивирусной защиты контейнерного терминала компании «UNIVERSAL LOGISTICS SERVICES» (ULS) с использованием методов искусственного интеллекта.

37. Обеспечение антивирусной защиты Департамента управления персоналом компании ПГК с использованием методов искусственного интеллекта.

38. Организация антивирусной защиты от автоматизированных методов сбора информации из открытых интернет-ресурсов с использованием методов искусственного интеллект.

39. Основные направления исследований в области искусственного интеллекта.

40. Классификация интеллектуальных информационных систем.

41. Системы с интеллектуальным интерфейсом.

42. Экспертные системы.

43. Самообучающиеся системы.

44. Нейронные сети.

45. Информационные хранилища.

46. Адаптивные информационные системы.

47. Основные этапы разработки интеллектуальной системы

48. Классифицирующие ЭС.

49. Доопределяющие ЭС.

50. Трансформирующие ЭС.

9.2.2. Примерный перечень тестовых заданий для проведения итоговой аттестации:

1. Экспертные системы:

а) интерпретация данных

б) диалог с человеком

в) анализ изображений

2. В каком нормативно-правовом документе прописаны цели, стратегия искусственного интеллекта:

а) Распоряжение Правительства №2129-р от 19.08.2020 об утверждении «Концепции регулирования искусственного интеллекта и робототехники до 2024 года»

б) Федеральный закон от 24 апреля 2020 г. N 123-ФЗ

в) Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации»

3. Цифровая трансформация включает все, исключая:

а) ревизию имеющихся данных

б) ревизию и анализ метрик процесса

в) сбор данных

4. Базовые принципы развития искусственного интеллекта в России характеризуются следующими тезисами:

а) искусственные интеллект-продукты должны быть понятными с точки зрения принятия решений

б) искусственные интеллект-продукты должны быть безопасными

в) оба варианта верны

г) нет верного ответа

5. Технологии искусственного интеллекта включают:

а) температуру

б) симптомы

в) компьютерное зрение

6. «Посильные» задачи для успеха искусственного интеллекта:

а) замена обработки большого объема данных человеком

б) решение многопараметрической или сложно-алгоритмизируемой задачи

в) оба варианта верны

г) нет верного ответа

7. Суть машинного обучения заключается в:

а) повышении квалификации

б) обучении специалистов

в) программировании

8. Когда возникла задача создания искусственного подобия человеческого разума:

а) в XX веке

б) в XVIII веке

в) в XIX веке

9. Слабый Искусственный интеллект:

а) решение сложных задач с участием человека

б) решение простых задач на основе данных без участия человека

в) решение простых задач с участием человека

10. К какому направлению развития искусственного интеллекта относится модель лабиринтного поиска:

а) Кибернетика «черного ящика»

б) Нейрокибернетика

в) Кибернетика «серого ящика»

11. Сильный искусственный интеллект:

а) замена человека при решении разных, в том числе новых или творческих задач

б) результат работы ученых

в) гипотеза в философии

12. Какие инструментальные средства не требуют от разработчика интеллектуальной системы знания программирования:

а) декларативные языки программирования

б) оболочки экспертных систем

в) традиционные языки программирования

13. Разработка продукта включает:

а) прототип (MVP)

б) проверку в реальной клинической практике

в) проверку продукта экспертами

14. Направление «нейрокибернетика» базируется на:

а) моделировании входных воздействий и выходных сигналов, аналогичных выдаваемым человеческим мозгом

б) моделировании структур человеческого мозга

в) моделировании структур, решающих задачи интеллектуального типа

15. Разработка продукта включает:

а) проверку в реальной клинической практике

б) проверку продукта экспертами

в) техническую документацию

16. Что означает проверка способности классификатора к обобщению:

а) подача на построенный классификатор экзаменационной последовательности образов

б) подача на классификатор последовательности образов, с которыми классификатор не встречался при обучении, для коррекции решающей функции

в) подача на построенный классификатор последовательности образов

17. Обработка естественного языка включает:

а) извлечение контента из текста

б) классификацию

в) генерацию изображений

18. Персептрон имеет структуру:

а) четырехслойную

б) трехслойную

в) двухслойную

19. Независимые клинические испытания включают:

а) публикации в рецензируемой литературе

б) получение разрешения на вывод на рынок

в) проверку продукта экспертами

20. Главным направлением исследований в области искусственного интеллекта является:

а) объектно-ориентированные СУБД

б) машинный интеллект

в) автоматизированные информационные системы

21. Не стоит поручать искусственному интеллекту:

а) интеллектуальные задачи, требующие знаний и трудно решаемые самим человеком

б) решение многопараметрической или сложно-алгоритмизируемой задачи

в) замену обработки большого объема данных человеком

22. Главным направлением исследований в области искусственного интеллекта является:

а) автоматизированные информационные системы

б) искусственный разум

в) объектно-ориентированные СУБД

23. Не стоит поручать искусственному интеллекту:

а) замену обработки большого объема данных человеком

б) решение многопараметрической или сложно-алгоритмизируемой задачи

в) задачи, по которым данные представлены не релевантной выборкой

24. Всякий символ переменной или константной буквы является:

а) булевой константой

б) термом

в) квантором

25. Наиболее перспективными направлениями для искусственного интеллекта являются:

а) фармацевтика

б) превентивная медицина

в) диагностика и анализы

26. Формирование на основе некоторых высказываний новых суждений называется:

а) выводом

б) рассуждением

в) предикатом

27. Мониторинг безопасности включает:

а) тиражирование

б) проверку продукта экспертами

в) отчет опытной эксплуатации

28. Искусственный интеллект:

а) комплекс технологических решений, позволяющий имитировать когнитивные функции человека

б) отрасль кибернетики

в) отрасль генетики

29. Мониторинг безопасности включает:

а) рекламу, продвижение

б) проверку продукта экспертами

в) отчет опытной эксплуатации

30. Компьютерное зрение:

а) интерпретация данных

б) анализ изображений

в) машинный перевод

31. Что такое компьютерное зрение?

а) Область искусственного интеллекта, связанная с анализом изображений и видео.

б) Модель машинного обучения, построенная на основе устройства глаза человека.

в) Область искусственного интеллекта, связанная с анализом и синтезом текстов.

г) Технология управления автомобилями без водителя.

32. Что такое обработка естественного языка?

а) Область искусственного интеллекта, связанная с анализом изображений и видео.

б) Область искусственного интеллекта, связанная с анализом и синтезом текстов.

в) Область искусственного интеллекта, связанная с анализом формальных языков.

г) Область искусственного интеллекта, связанная с распознаванием и синтезом речи.

33. Что такое распознавание речи?

а) Область искусственного интеллекта, связанная с анализом изображений и видео.

б) Технология автоматического перевода специального назначения.

в) Область искусственного интеллекта, связанная с преобразованием речевого сигнала в цифровую информацию.

г) Область искусственного интеллекта, связанная с формированием речевого сигнала по тексту.

34. Что такое синтез речи?

а) Область искусственного интеллекта, связанная с поддержкой принятия решений.

б) Модель машинного обучения, построенная по аналогии с органами артикуляции человека.

в) Область искусственного интеллекта, связанная с преобразованием речевого сигнала в цифровую информацию.

г) Область искусственного интеллекта, связанная с формированием речевого сигнала по тексту.

35. Как искусственный интеллекта применяется для дефектоскопии?

а) Система обработки естественного языка автоматически находит дефекты в сочинениях учеников.

б) Система компьютерного зрения автоматически находит дефекты материала.

в) Система распознавания речи автоматически определяет дефекты речи человека.

г) Система генерации речи в автоматическом режиме генерирует речь на основе текста с исправлением дефектов.

36. Что описывает экспериментальный правовой режим эксплуатации самоуправляемых автомобилей (высокоавтоматизированных транспортных средств) в России?

а) Требования к обучению самоуправляемых автомобилей.

б) Экономические особенности разработки и внедрения самоуправляемых автомобилей.

в) Правила эксплуатации самоуправляемых автомобилей на дорогах общего пользования.

г) Экспериментальный правовой режим эксплуатации самоуправляемых автомобилей в России не действует.

37. На какой дороге общего пользования в настоящее время проводится испытания самоуправляемых грузовых автомобилей «Камаз»?

а) Платная трасса М11 «Нева», Москва – Санкт-Петербург.

б) Трасса М4 «Дон», Москва – Новороссийск.

в) Самоуправляемые грузовые автомобили «Камаз» могут передвигаться по любым дорогам общего пользования в России.

г) Самоуправляемым грузовым автомобилям запрещено передвигаться по дорогам общего пользования в России.

38. Может ли искусственный интеллект поставить диагноз на основе анализа медицинского изображения?

а) Да, может.

б) Нет, диагноз ставит только врач-человек.

в) Может, если будет предоставлена дополнительная информация о пациенте.

г) Диагноз может поставить только консилиум, состоящий минимум из трех независимых систем искусственного интеллекта.

39. Каким образом искусственный интеллект может применяться для обнаружения мошенничества в банках?

а) Система фрод-мониторинга обнаруживает мошеннические операции по банковским картам.

б) Система искусственного интеллекта по чекам определяет предпочтения мошенника.

в) Система искусственного интеллекта может определить проблему, возникшую у мошенника, до того, как мошенник обратился в техническую поддержку банка.

г) Система распознавания лиц может обнаруживать мошенников, которые пытаются получить кредиты по чужим документам.

40. Для каких целей искусственный интеллект применяется в телекоммуникационных компаниях?

а) Анализ соблюдения клиентами требований промышленной безопасности.

б) Предсказание оттока абонентов.

в) Дефектоскопия абонентского оборудования.

г) Планирование расположения оборудования сетей связи.

9.3.Критерии оценивания

Отметка *«зачтено»* выставляется обучающемуся, знающему программный материал, грамотно и по существу, излагающему его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач.

Отметка *«не зачтено»* выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.