МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

Кафедра информационных систем

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ

# ПО ПРОВЕДЕНИЮ ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

(для магистров по направлению подготовки 09.04.03
«Прикладная информатика»,
магистерская программа
«Искусственный интеллект в кибербезопасности»)

Ставрополь, 2026

Содержание

## 1 Общие положения

Порядок сдачи государственного экзамена регламентируется приказом Министерства образования и науки Российской Федерации от 29 июня 2015 года № 636 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам высшего образования — программам бакалавриата, программам специалитета и программам магистратуры» и Положением о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования — программам бакалавриата, программам специалитета и программам магистратуры в ФГБОУ ВО Ставропольский ГАУ.

К государственному экзамену допускается обучающийся, не имеющий академической задолженности и в полном объеме выполнивший учебный план или индивидуальный учебный план по осваиваемой образовательной программе высшего образования.

Обучающимся и лицам, привлекаемым к процедуре приема государственного экзамена, во время ее проведения запрещается иметь при себе и использовать средства связи.

Государственный экзамен не может быть заменен оценкой, полученной выпускником в ходе освоения образовательной программы в рамках промежуточной аттестации.

Государственный экзамен носит комплексный междисциплинарный характер.

## 2 Цель проведения государственного экзамена

Государственный экзамен проводится в целях определения соответствия результатов освоения обучающимися основной образовательной программы планируемым результатам освоения, сформулированным в общей

характеристике образовательной программы, и требованиям федерального государственного образовательного стандарта высшего образования — магистратура по направлению подготовки 09.04.03 «Прикладная информатика», утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 916.

Целью государственного экзамена является комплексная оценка уровня теоретической и практической подготовки выпускников по направлению подготовки 09.04.03 «Прикладная информатика», магистерская программа «Искусственный интеллект в кибербезопасности», а также определение готовности выпускников к решению профессиональных задач в области прикладной информатики, искусственного интеллекта, машинного обучения, разработки и сопровождения защищенных информационных систем, анализа защищенности, управления рисками и расследования компьютерных инцидентов.

## 3 Задачи, решаемые в ходе государственного экзамена

На государственном экзамене проверяется сформированность следующих компетенций:

| Код и наименование индикатора компетенций | Результаты освоения ОП ВО |
|---|---|
| ОПК-1.1<br>Осуществляет поиск и критический анализ научно-технической информации, в том числе на иностранных языках | Знания: источников научно-технической информации, методов поиска, отбора и критического анализа данных в области прикладной информатики, искусственного интеллекта и кибербезопасности;<br>Умения: осуществлять поиск, анализировать и оценивать научно-техническую информацию, в том числе на иностранных языках;<br>Навыки: критического анализа и систематизации научно-технической информации для решения профессиональных задач. |
| ОПК-1.2 | Знания: математических и информационных методов формализации прикладных задач, включая задачи анализа данных, обнаружения аномалий и сетевых угроз; |

| | |
|---|---|
| Формализует прикладную задачу на языке математики и информатики | Умения: формализовать прикладные задачи с использованием математического аппарата и методов информатики;<br>Навыки: построения формальных моделей прикладных задач в области информационных систем и кибербезопасности. |
| ОПК-1.3<br>Выбирает и адаптирует методы из смежных областей для решения новой проблемы | Знания: методов теории вероятностей, машинного обучения, криптографии и смежных областей, применяемых для решения нестандартных профессиональных задач;<br>Умения: выбирать и адаптировать методы из смежных областей для решения новых задач;<br>Навыки: применения междисциплинарных подходов при решении задач прикладной информатики и кибербезопасности. |
| ОПК-2.1<br>Разрабатывает алгоритмы обработки данных и принятия решений с элементами искусственного интеллекта | Знания: методов обработки данных, алгоритмов машинного обучения и интеллектуального анализа данных;<br>Умения: разрабатывать алгоритмы обработки данных и принятия решений с применением элементов искусственного интеллекта;<br>Навыки: проектирования алгоритмов на основе нейронных сетей, деревьев решений, кластеризации и иных методов ИИ. |
| ОПК-2.2<br>Реализует алгоритмы в виде программного кода на выбранных языках программирования | Знания: языков программирования и принципов реализации алгоритмов в программном коде;<br>Умения: реализовывать алгоритмы на языках программирования Python, Java, C++ и других языках;<br>Навыки: программной реализации, тестирования и отладки алгоритмов для решения профессиональных задач. |
| ОПК-2.3<br>Использует библиотеки машинного обучения и фреймворки для кибербезопасности | Знания: библиотек машинного обучения и программных фреймворков, применяемых в задачах кибербезопасности;<br>Умения: использовать scikit-learn, TensorFlow, PyTorch, Suricata, Snort и другие инструменты для решения профессиональных задач;<br>Навыки: применения библиотек машинного обучения и средств кибербезопасности при разработке интеллектуальных систем защиты информации. |
| ОПК-3.1<br>Проводит сбор и систематизацию данных об угрозах, уязвимостях и инцидентах из открытых и закрытых источников | Знания: источников информации об угрозах, уязвимостях и инцидентах информационной безопасности;<br>Умения: собирать и систематизировать сведения из CVE, MITRE ATT&CK, бюллетеней ФСТЭК и иных источников;<br>Навыки: аналитической обработки данных об угрозах и уязвимостях компьютерных систем. |
| ОПК-3.2<br>Составляет аналитические отчеты с графиками, таблицами и выводами | Знания: требований к структуре и оформлению аналитических отчетов;<br>Умения: представлять результаты анализа в виде отчетов, таблиц, графиков и обоснованных выводов; |

| | |
|---|---|
| | Навыки: подготовки аналитических материалов по результатам исследования профессиональной информации. |
| ОПК-3.3<br>Формулирует практические рекомендации по повышению уровня защищенности | Знания: методов повышения уровня защищенности информационных систем;<br>Умения: формулировать рекомендации по устранению уязвимостей и снижению рисков информационной безопасности;<br>Навыки: разработки практических предложений по обеспечению защищенности компьютерных систем и сетей. |
| ОПК-4.1<br>Воспроизводит эксперименты из актуальных научных статей по применению ИИ в кибербезопасности | Знания: современных научных подходов к применению искусственного интеллекта в кибербезопасности;<br>Умения: воспроизводить эксперименты, описанные в научных публикациях;<br>Навыки: проведения экспериментальных исследований с использованием методов искусственного интеллекта. |
| ОПК-4.2<br>Модифицирует существующие методы для повышения их эффективности | Знания: существующих методов обнаружения вторжений, анализа данных и защиты информации;<br>Умения: модифицировать алгоритмы и методы для повышения их эффективности;<br>Навыки: адаптации и улучшения методов искусственного интеллекта и кибербезопасности под конкретные задачи. |
| ОПК-4.3<br>Оценивает точность, полноту и вычислительную сложность разработанных методов | Знания: показателей качества и эффективности алгоритмов, включая точность, полноту и вычислительную сложность;<br>Умения: оценивать результативность разработанных методов;<br>Навыки: сравнительного анализа эффективности алгоритмов и программных решений. |
| ОПК-5.1<br>Проектирует архитектуру программных средств защиты информации с учетом требований производительности и масштабируемости | Знания: принципов проектирования архитектуры программных средств защиты информации;<br>Умения: проектировать программные решения с учетом требований производительности, надежности и масштабируемости;<br>Навыки: разработки архитектурных решений для защищенных информационных систем. |
| ОПК-5.2<br>Интегрирует программные модули в единую систему | Знания: принципов интеграции программных модулей и средств защиты информации;<br>Умения: объединять антивирусные средства, DLP, SIEM и другие модули в единую систему;<br>Навыки: интеграции программных компонентов в составе информационных и автоматизированных систем. |
| ОПК-5.3<br>Выполняет настройку аппаратных средств защиты и их взаимодействие с программным обеспечением | Знания: аппаратных средств защиты информации и принципов их взаимодействия с программным обеспечением;<br>Умения: выполнять настройку межсетевых экранов, криптошлюзов и иных аппаратных средств защиты;<br>Навыки: настройки и сопровождения программно-аппаратных средств защиты информации. |

| | |
|---|---|
| ОПК-6.1<br>Анализирует тенденции развития ИИ, больших данных и квантовых вычислений применительно к задачам кибербезопасности | Знания: современных тенденций развития искусственного интеллекта, больших данных и квантовых вычислений;<br>Умения: анализировать влияние новых технологий на задачи кибербезопасности;<br>Навыки: оценки перспектив применения современных информационных технологий в профессиональной деятельности. |
| ОПК-6.2<br>Оценивает социальные, правовые и этические аспекты применения автоматизированных систем защиты | Знания: социальных, правовых и этических аспектов применения автоматизированных систем защиты информации;<br>Умения: оценивать последствия внедрения автоматизированных решений в области информационной безопасности;<br>Навыки: учета правовых и этических требований при применении систем защиты информации. |
| ОПК-6.3<br>Участвует в дискуссиях и научных семинарах по проблемам цифровой безопасности | Знания: актуальных проблем цифровой безопасности и научной коммуникации;<br>Умения: аргументированно представлять профессиональную позицию по вопросам цифровой безопасности;<br>Навыки: участия в научных дискуссиях, семинарах и профессиональном обсуждении проблем информационной безопасности. |
| ОПК-7.1<br>Строит математические модели угроз | Знания: математических подходов к моделированию угроз информационной безопасности;<br>Умения: строить графовые, вероятностные и игровые модели угроз;<br>Навыки: разработки математических моделей угроз для анализа защищенности информационных систем. |
| ОПК-7.2<br>Проводит имитационное моделирование поведения нарушителя и эффективности защиты | Знания: методов имитационного моделирования процессов нарушения и защиты информационных систем;<br>Умения: моделировать поведение нарушителя и оценивать эффективность защитных мер;<br>Навыки: проведения имитационных экспериментов для анализа защищенности компьютерных систем. |
| ОПК-7.3<br>Интерпретирует результаты моделирования и использует их для оптимизации конфигурации информационных систем | Знания: методов интерпретации результатов математического и имитационного моделирования;<br>Умения: использовать результаты моделирования для оптимизации конфигурации информационных систем;<br>Навыки: анализа результатов моделирования и выработки решений по повышению защищенности ИС. |
| ОПК-8.1<br>Применяет метрики и инструменты контроля качества кода | Знания: метрик качества программного кода и инструментов статического анализа;<br>Умения: применять SonarQube, статические анализаторы и другие инструменты контроля качества;<br>Навыки: оценки качества программного кода при разработке защищенного программного обеспечения. |
| ОПК-8.2<br>Организует процессы CI/CD и управления версиями | Знания: принципов непрерывной интеграции, непрерывной доставки и управления версиями; |

| | |
|---|---|
| | Умения: организовывать процессы CI/CD с использованием Git, Jenkins, GitLab и иных инструментов;<br>Навыки: настройки процессов автоматизированной сборки, тестирования и управления версиями программных продуктов. |
| ОПК-8.3<br>Проводит технико-экономическое обоснование выбора методологии разработки для проектов информационной безопасности | Знания: методологий разработки программного обеспечения и основ технико-экономического обоснования ИТ-проектов;<br>Умения: обосновывать выбор методологии разработки для проектов информационной безопасности;<br>Навыки: оценки экономической и организационной целесообразности выбора Waterfall, Agile и иных подходов. |
| ПК-1.1<br>Выявляет уязвимости и слабые места в компьютерных системах с использованием сканеров безопасности и методов ИИ | Знания: методов выявления уязвимостей, сканеров безопасности и подходов искусственного интеллекта к анализу защищенности;<br>Умения: использовать Nessus, OpenVAS, nmap и методы ИИ для выявления слабых мест компьютерных систем;<br>Навыки: проведения инструментального анализа защищенности компьютерных систем. |
| ПК-1.2<br>Разрабатывает и тестирует модели машинного обучения для обнаружения сетевых атак | Знания: методов машинного обучения, применяемых для обнаружения сетевых атак;<br>Умения: разрабатывать и тестировать модели для выявления DDoS-атак, ботнетов, APT и иных угроз;<br>Навыки: построения и оценки моделей машинного обучения для задач кибербезопасности. |
| ПК-1.3<br>Интерпретирует результаты инструментального мониторинга защищенности и формирует научно обоснованные заключения | Знания: методов инструментального мониторинга защищенности и анализа его результатов;<br>Умения: интерпретировать данные сканирования, мониторинга и анализа событий безопасности;<br>Навыки: подготовки научно обоснованных заключений по результатам оценки защищенности. |
| ПК-2.1<br>Собирает и сохраняет цифровые доказательства с соблюдением процессуальных норм | Знания: принципов сбора, фиксации и хранения цифровых доказательств;<br>Умения: собирать образы дисков, журналы событий, сетевые дампы и иные цифровые следы;<br>Навыки: сохранения цифровых доказательств с соблюдением требований целостности и процессуальных норм. |
| ПК-2.2<br>Применяет методы машинного обучения для выявления признаков вредоносной активности и установления цепочки атаки | Знания: методов машинного обучения, используемых для анализа вредоносной активности и реконструкции атак;<br>Умения: выявлять признаки вредоносной активности и устанавливать цепочку атаки;<br>Навыки: применения интеллектуальных методов анализа данных при расследовании компьютерных инцидентов. |
| ПК-2.3<br>Составляет экспертные заключения о причинах и последствиях инцидента, предлагает меры по предотвращению повторения | Знания: структуры экспертного заключения и методов анализа причин компьютерных инцидентов;<br>Умения: определять причины и последствия инцидента, формулировать меры профилактики;<br>Навыки: подготовки экспертных заключений по результатам расследования компьютерных инцидентов. |

| | |
|---|---|
| ПК-3.1<br>Пишет программный код на выбранных языках с применением принципов защитного программирования | Знания: языков программирования и принципов защитного программирования;<br>Умения: писать программный код на Python, C++, Go и других языках с учетом требований безопасности;<br>Навыки: разработки защищенного программного кода для информационных систем. |
| ПК-3.2<br>Интегрирует готовые модули ИИ в разрабатываемое программное обеспечение | Знания: готовых модулей и библиотек искусственного интеллекта, применяемых в программных системах;<br>Умения: интегрировать модули распознавания образов, обработки естественного языка, прогнозирования и анализа данных;<br>Навыки: внедрения интеллектуальных компонентов в разрабатываемое программное обеспечение. |
| ПК-3.3<br>Проводит отладку и рефакторинг кода, документирует программные интерфейсы | Знания: методов отладки, рефакторинга и документирования программных интерфейсов;<br>Умения: выявлять и устранять ошибки в коде, улучшать структуру программного продукта, оформлять API-документацию;<br>Навыки: сопровождения, оптимизации и документирования программного обеспечения. |
| ПК-4.1<br>Разрабатывает планы управления конфигурациями и выпусками версий программного продукта | Знания: принципов управления конфигурациями, версиями и релизами программных продуктов;<br>Умения: разрабатывать планы управления конфигурациями и выпусками версий;<br>Навыки: планирования релизной политики и сопровождения жизненного цикла программного продукта. |
| ПК-4.2<br>Координирует работу распределенной команды разработчиков и тестировщиков с использованием систем отслеживания задач | Знания: методов координации работы ИТ-команд и инструментов управления задачами;<br>Умения: организовывать работу распределенной команды с применением Jira, Redmine и аналогичных систем;<br>Навыки: управления командным взаимодействием при реализации проектов в области информационной безопасности. |
| ПК-4.3<br>Оценивает риски проекта и принимает решения по их минимизации | Знания: видов проектных рисков и методов их оценки;<br>Умения: оценивать технические, ресурсные и временные риски проекта;<br>Навыки: разработки решений по минимизации рисков при управлении жизненным циклом программных продуктов. |
| ПК-5.1<br>Устанавливает, настраивает и сопровождает средства криптографической защиты, межсетевые экраны и антивирусное программное обеспечение | Знания: средств криптографической защиты информации, межсетевых экранов, антивирусного программного обеспечения и принципов их функционирования;<br>Умения: устанавливать, настраивать и сопровождать средства защиты информации;<br>Навыки: администрирования программно-аппаратных средств защиты информационных систем. |
| ПК-5.2<br>Реализует политики управления доступом и | Знания: принципов управления доступом, мониторинга событий безопасности и настройки политик безопасности; |

| | |
|---|---|
| мониторинга событий безопасности на уровне ОС и прикладного ПО | Умения: реализовывать политики доступа и мониторинга на уровне операционных систем и прикладного программного обеспечения;<br>Навыки: настройки и сопровождения механизмов контроля доступа и мониторинга событий безопасности. |
| ПК-5.3<br>Проводит анализ корректности функционирования средств защиты и оперативно устраняет неисправности | Знания: методов диагностики и анализа корректности функционирования средств защиты информации;<br>Умения: выявлять сбои, ошибки настройки и неисправности средств защиты;<br>Навыки: оперативного устранения неисправностей и обеспечения устойчивой работы средств защиты информации. |

## 4 Перечень и содержание тем, вынесенных на государственный экзамен

| № п/п | Наименование тем (разделов) | Содержание тем (разделов) | Код и наименование индикатора компетенции |
|---|---|---|---|
| 1 | Управление проектами жизненного цикла информационных систем | Понятие жизненного цикла информационной системы. Этапы проектирования, разработки, внедрения и сопровождения ИС. Методологии управления ИТ-проектами. Планирование сроков, ресурсов и результатов проекта. Управление требованиями, рисками, конфигурациями и версиями программного продукта. | УК-2.1;<br>УК-2.2;<br>УК-2.3;<br>ОПК-8.3;<br>ПК-4.1;<br>ПК-4.3 |
| 2 | Научные основы аналитических исследований в прикладной информатике | Методы поиска, отбора и критического анализа научно-технической информации. Подготовка аналитических обзоров, отчетов и научных публикаций. Формулирование цели, задач, гипотезы и критериев оценки результатов исследования в области ИТ, искусственного интеллекта и кибербезопасности. | ОПК-1.1;<br>ОПК-3.1;<br>ОПК-3.2;<br>ОПК-4.1 |
| 3 | Методы моделирования и анализа сложных систем | Понятие сложной системы. Математическое, имитационное и вероятностное моделирование. Модели угроз информационной безопасности. Анализ поведения нарушителя и эффективности механизмов защиты. Интерпретация результатов моделирования для оптимизации информационных систем. | ОПК-1.2;<br>ОПК-7.1;<br>ОПК-7.2;<br>ОПК-7.3 |

| | | | |
|---|---|---|---|
| 4 | Современные интеллектуальные системы и технологии | Понятие интеллектуальной системы. Основные направления развития искусственного интеллекта. Машинное обучение, нейронные сети, экспертные системы, интеллектуальные агенты. Применение интеллектуальных технологий в анализе данных, прогнозировании, автоматизации принятия решений и обеспечении кибербезопасности. | ОПК-2.1; ОПК-2.3; ОПК-6.1; ПК-3.2 |
| 5 | Проектирование инфраструктуры и архитектуры информационных систем | Архитектура информационных систем. Корпоративные, распределенные, облачные и критически важные информационные системы. Проектирование инфраструктуры с учетом требований надежности, масштабируемости, производительности и информационной безопасности. | ОПК-5.1; ОПК-5.2; ОПК-7.3; ПК-5.2 |
| 6 | Программирование высокопроизводительных систем | Принципы разработки высокопроизводительных программных систем. Параллельные и распределенные вычисления. Оптимизация алгоритмов и программного кода. Оценка вычислительной сложности и производительности программных решений. | ОПК-2.2; ОПК-4.3; ОПК-8.1; ПК-3.1; ПК-3.3 |
| 7 | Проектирование автономных ИИ-агентов | Понятие автономного интеллектуального агента. Архитектура ИИ-агентов. Методы восприятия, планирования, принятия решений и взаимодействия с внешней средой. Применение автономных ИИ-агентов в мониторинге, анализе событий и автоматизации реагирования на инциденты. | ОПК-2.1; ОПК-2.3; ОПК-6.1; ПК-3.2 |
| 8 | Прикладная статистика и анализ данных | Основные методы прикладной статистики. Предобработка, визуализация и анализ данных. Статистические показатели, корреляционный анализ, классификация, кластеризация и прогнозирование. Применение анализа данных при выявлении аномалий и угроз информационной безопасности. | ОПК-1.2; ОПК-2.1; ОПК-3.2; ПК-1.2 |
| 9 | Технологии разработки защищенного программного обеспечения | Принципы безопасной разработки программного обеспечения. Защитное программирование. Типовые уязвимости программного кода. Методы тестирования, отладки, рефакторинга и документирования | ОПК-5.1; ОПК-8.1; ПК-3.1; ПК-3.3 |

| | | | |
|---|---|---|---|
| | | программных интерфейсов. Контроль качества и безопасности программного кода. | |
| 10 | Атаки на системы искусственного интеллекта | Понятие атак на системы искусственного интеллекта. Угрозы машинному обучению и интеллектуальным системам. Атаки на обучающие данные, модели и результаты классификации. Методы защиты ИИ-систем от adversarial attacks, poisoning attacks и model extraction. | ОПК-3.1; ОПК-4.2; ОПК-6.1; ПК-1.2 |
| 11 | Машинное обучение в кибербезопасности | Применение методов машинного обучения для обнаружения сетевых атак, вредоносной активности и аномалий. Классификация, кластеризация, деревья решений, нейронные сети. Оценка качества моделей машинного обучения: точность, полнота, F-мера, вычислительная сложность. | ОПК-2.1; ОПК-2.3; ОПК-4.3; ПК-1.2; ПК-2.2 |
| 12 | Инструментальный анализ защищенности и тестирование на проникновение | Методы инструментального анализа защищенности компьютерных систем и сетей. Сканеры уязвимостей, анализ сетевой инфраструктуры, выявление слабых мест. Основные этапы тестирования на проникновение. Интерпретация результатов проверки защищенности и подготовка заключений. | ОПК-3.1; ОПК-3.3; ПК-1.1; ПК-1.3 |
| 13 | Технологии непрерывной разработки и безопасности | Понятие CI/CD. Непрерывная интеграция, доставка и развертывание программных продуктов. DevOps и DevSecOps. Автоматизация тестирования и контроля качества кода. Управление версиями, репозиториями и артефактами программного продукта. | ОПК-8.1; ОПК-8.2; ПК-4.1; ПК-4.2 |
| 14 | Прикладные системы искусственного интеллекта | Классификация прикладных систем искусственного интеллекта. Интеллектуальный анализ данных, распознавание образов, обработка естественного языка, прогнозирование и поддержка принятия решений. Интеграция готовых модулей ИИ в прикладное программное обеспечение. | ОПК-2.1; ОПК-2.2; ОПК-2.3; ПК-3.2 |
| 15 | Современные системы управления базами данных | Понятие базы данных и системы управления базами данных. Реляционные и нереляционные СУБД. Проектирование структуры данных, обеспечение целостности, надежности и безопасности хранения информации. | ОПК-5.2; ОПК-6.1; ПК-5.2 |

| | | | |
|---|---|---|---|
| | | Администрирование, резервное копирование и восстановление данных. | |
| 16 | Управление информационной безопасностью | Понятие информационной безопасности. Политики безопасности, управление доступом, управление рисками и инцидентами. Организация мониторинга событий безопасности. Нормативно-правовые, организационные и технические основы защиты информации. | ОПК-3.3; ОПК-6.2; ПК-5.2; ПК-5.3 |
| 17 | Инженерия серверных веб-систем | Архитектура серверных веб-систем. Клиент-серверное взаимодействие, API, обработка запросов, масштабирование и отказоустойчивость. Основы безопасной разработки серверных приложений. Защита веб-систем от типовых угроз и уязвимостей. | ОПК-5.1; ОПК-5.2; ПК-3.1; ПК-3.3 |
| 18 | Инженерия требований к безопасным системам | Понятие требований к информационной системе. Функциональные и нефункциональные требования. Требования к безопасности, надежности, производительности и сопровождаемости. Анализ, документирование, согласование и управление изменениями требований к безопасным системам. | УК-2.1; ОПК-8.3; ПК-4.1; ПК-4.3 |
| 19 | Администрирование безопасных информационных систем | Задачи администрирования защищенных информационных систем. Управление учетными записями, правами доступа, журналированием и политиками безопасности. Настройка операционных систем и прикладного программного обеспечения с учетом требований защиты информации. | ОПК-5.3; ПК-5.1; ПК-5.2; ПК-5.3 |
| 20 | Администрирование защищенных сетей | Основы построения и администрирования защищенных компьютерных сетей. Межсетевые экраны, маршрутизаторы, коммутаторы, VPN, IDS/IPS. Мониторинг сетевого трафика, настройка правил фильтрации и обеспечение устойчивой работы сетевой инфраструктуры. | ОПК-5.3; ПК-1.1; ПК-5.1; ПК-5.3 |
| 21 | Обнаружение и анализ вредоносного программного обеспечения | Понятие вредоносного программного обеспечения. Классификация вредоносных программ. Методы статического и динамического анализа. Признаки вредоносной активности. Использование инструментов анализа | ОПК-3.1; ПК-2.2; ПК-2.3 |

| | | | |
|---|---|---|---|
| | | и методов машинного обучения для выявления вредоносного поведения. | |
| 22 | Поведенческий анализ и мониторинг защищенности с использованием ИИ | Понятие поведенческого анализа. Сбор и обработка журналов событий, сетевых пакетов и цифровых следов. Обнаружение аномалий и подозрительных действий с применением методов искусственного интеллекта. Использование SIEM-систем и моделей машинного обучения для мониторинга защищенности. | ОПК-2.1; ОПК-3.1; ПК-1.1; ПК-1.3; ПК-2.2 |
| 23 | Безопасность облачных технологий | Понятие облачных вычислений и облачной инфраструктуры. Модели IaaS, PaaS, SaaS. Основные угрозы безопасности облачных сервисов. Управление доступом, защита данных, мониторинг, резервирование и обеспечение соответствия требованиям информационной безопасности в облачной среде. | ОПК-5.1; ОПК-6.1; ПК-5.2; ПК-5.3 |
| 24 | Технологии расследования компьютерных преступлений и инцидентов | Понятие компьютерного инцидента и компьютерного преступления. Этапы расследования инцидентов информационной безопасности. Сбор, фиксация и сохранение цифровых доказательств. Анализ журналов, сетевых дампов, образов дисков и артефактов вредоносного ПО. Подготовка экспертного заключения. | ОПК-3.2; ПК-2.1; ПК-2.2; ПК-2.3 |
| 25 | Программно-аппаратные средства защиты информации | Назначение и классификация программно-аппаратных средств защиты информации. Межсетевые экраны, криптографические средства, антивирусные комплексы, DLP, IDS/IPS. Установка, настройка, сопровождение и анализ корректности функционирования средств защиты. | ОПК-5.2; ОПК-5.3; ПК-5.1; ПК-5.3 |

## 5 Перечень документов и материалов, которыми разрешается пользоваться выпускнику на государственном экзамене

При подготовке ответа на государственном экзамене выпускник может пользоваться только материалами, предусмотренными программой государственного экзамена и выданными государственной экзаменационной комиссией.

Использование средств связи, электронных справочных материалов, устройств с доступом к информационно-телекоммуникационной сети «Интернет», а также иных неразрешенных материалов во время проведения государственного экзамена не допускается.

## 6 Перечень материалов для проведения государственного экзамена

Для проведения государственного экзамена используются:

- программа государственного экзамена;
- перечень теоретических вопросов, выносимых на государственный экзамен;
- практико-ориентированные задания;
- экзаменационные билеты;
- критерии оценивания результатов сдачи государственного экзамена;
- перечень рекомендованной литературы для подготовки к государственному экзамену;
- протокол заседания государственной экзаменационной комиссии.

### 6.1 Перечень теоретических вопросов для проведения государственного экзамена

1. Понятие информационной системы, ее структура и основные компоненты.
2. Жизненный цикл информационной системы: основные этапы и модели.
3. Методологии управления жизненным циклом информационных систем.

4. Управление требованиями при разработке информационных систем.

5. Управление конфигурациями и версиями программного продукта.

6. Управление рисками в проектах разработки информационных систем.

7. Agile, Scrum и Kanban в управлении ИТ-проектами.

8. DevOps и DevSecOps как подходы к организации разработки и сопровождения программных систем.

9. Показатели качества программного продукта и методы их оценки.

10. Технико-экономическое обоснование выбора методологии разработки программного обеспечения.

11. Понятие научно-технической информации и методы ее поиска.

12. Критический анализ научно-технической информации в области прикладной информатики.

13. Структура аналитического обзора по проблемам искусственного интеллекта и кибербезопасности.

14. Основные этапы проведения научного исследования в прикладной информатике.

15. Формулирование цели, задач, объекта и предмета исследования.

16. Методы подготовки научных отчетов, публикаций и аналитических материалов.

17. Источники информации об угрозах, уязвимостях и инцидентах информационной безопасности.

18. Использование баз CVE, CWE, CAPEC и MITRE ATT&CK при анализе угроз.

19. Методы систематизации данных об угрозах и уязвимостях.

20. Формирование практических рекомендаций по повышению защищенности информационных систем.

21. Понятие сложной системы и особенности ее анализа.

22. Математическое моделирование сложных информационных систем.

23. Имитационное моделирование процессов функционирования информационных систем.

24. Вероятностные модели в задачах анализа киберугроз.

25. Графовые модели угроз информационной безопасности.

26. Игровые модели поведения нарушителя и защиты информационных систем.

27. Моделирование поведения нарушителя в компьютерной системе.

28. Оценка эффективности защитных механизмов на основе моделирования.

29. Интерпретация результатов моделирования защищенности информационной системы.

30. Использование результатов моделирования для оптимизации конфигурации информационной системы.

31. Понятие искусственного интеллекта и основные направления его развития.

32. Интеллектуальные системы: назначение, структура и классификация.

33. Экспертные системы и системы поддержки принятия решений.

34. Машинное обучение как направление искусственного интеллекта.

35. Нейронные сети и их применение в прикладной информатике.

36. Методы классификации и кластеризации данных.

37. Интеллектуальный анализ данных: задачи, методы и инструменты.

38. Применение искусственного интеллекта в задачах кибербезопасности.

39. Интеллектуальные агенты: понятие, свойства и архитектура.

40. Автономные ИИ-агенты в мониторинге и реагировании на инциденты безопасности.

41. Понятие архитектуры информационной системы.

42. Корпоративные, распределенные и облачные информационные системы.

43. Проектирование инфраструктуры информационных систем.

44. Требования к надежности, масштабируемости и производительности информационных систем.

45. Требования к безопасности при проектировании информационных систем.

46. Программно-аппаратные средства защиты информации.

47. Межсетевые экраны: назначение, виды и принципы работы.

48. Системы обнаружения и предотвращения вторжений IDS/IPS.

49. Антивирусные комплексы и средства защиты от вредоносного программного обеспечения.

50. Криптографические средства защиты информации и особенности их применения.

51. Основы высокопроизводительного программирования.

52. Параллельные и распределенные вычисления.

53. Оценка вычислительной сложности алгоритмов.

54. Методы оптимизации программного кода.

55. Принципы защитного программирования.

56. Типовые уязвимости программного обеспечения.

57. Безопасная разработка программного обеспечения.

58. Отладка, тестирование и рефакторинг программного кода.

59. Документирование программных интерфейсов API.

60. Метрики качества кода и инструменты статического анализа.

61. Понятие машинного обучения и его основные задачи.

62. Обучение с учителем, без учителя и с подкреплением.

63. Подготовка данных для построения моделей машинного обучения.

64. Метрики оценки качества моделей машинного обучения.

65. Применение машинного обучения для обнаружения сетевых атак.

66. Обнаружение аномалий в сетевом трафике.

67. Использование нейронных сетей в задачах кибербезопасности.

68. Модели машинного обучения для выявления вредоносной активности.

69. Проблема переобучения моделей машинного обучения и методы ее решения.

70. Интерпретируемость моделей машинного обучения в задачах информационной безопасности.

71. Понятие атак на системы искусственного интеллекта.

72. Атаки на обучающие данные в системах машинного обучения.

73. Атаки на модели искусственного интеллекта.

74. Adversarial attacks: сущность и методы противодействия.

75. Poisoning attacks: сущность и методы защиты.

76. Model extraction и model inversion attacks.

77. Угрозы безопасности интеллектуальных систем.

78. Методы повышения устойчивости моделей искусственного интеллекта.

79. Защита данных, используемых для обучения моделей искусственного интеллекта.

80. Оценка рисков применения искусственного интеллекта в системах кибербезопасности.

81. Инструментальный анализ защищенности компьютерных систем.

82. Сканеры уязвимостей: назначение и принципы применения.

83. Использование nmap, Nessus и OpenVAS для анализа защищенности.

84. Основные этапы тестирования на проникновение.

85. Подготовка отчета по результатам тестирования на проникновение.

86. Интерпретация результатов инструментального мониторинга защищенности.

87. SIEM-системы: назначение, структура и основные функции.

88. Сбор и анализ журналов событий безопасности.

89. Поведенческий анализ в задачах мониторинга защищенности.

90. Использование искусственного интеллекта для выявления подозрительной активности.

91. Понятие вредоносного программного обеспечения и его классификация.

92. Методы статического анализа вредоносного программного обеспечения.

93. Методы динамического анализа вредоносного программного обеспечения.

94. Признаки вредоносной активности в компьютерной системе.

95. Использование методов машинного обучения для анализа вредоносного программного обеспечения.

96. Понятие компьютерного инцидента и этапы его расследования.

97. Сбор и сохранение цифровых доказательств.

98. Анализ журналов событий, сетевых дампов и образов дисков при расследовании инцидентов.

99. Установление цепочки атаки с использованием MITRE ATT&CK.

100. Подготовка экспертного заключения по результатам расследования компьютерного инцидента.

101. Понятие базы данных и системы управления базами данных.

102. Реляционные и нереляционные базы данных.

103. Проектирование структуры базы данных.

104. Обеспечение целостности, доступности и конфиденциальности данных.

105. Администрирование современных систем управления базами данных.

106. Резервное копирование и восстановление данных.

107. Безопасность серверных веб-систем.

108. Архитектура клиент-серверных приложений.

109. Защита веб-приложений от типовых угроз и уязвимостей.

110. Управление доступом в информационных системах.

111. Понятие облачных вычислений и облачной инфраструктуры.

112. Модели облачных сервисов IaaS, PaaS, SaaS.

113. Основные угрозы безопасности облачных технологий.

114. Управление доступом и защита данных в облачной среде.

115. Мониторинг безопасности облачной инфраструктуры.

116. Резервирование и обеспечение отказоустойчивости облачных сервисов.

117. Инженерия требований к безопасным информационным системам.

118. Функциональные и нефункциональные требования к информационной системе.

119. Требования к безопасности, надежности и сопровождаемости программных систем.

120. Управление изменениями требований при разработке защищенных информационных систем.

## 6.2. Перечень практико-ориентированных задач для государственного экзамена

Перечень практико-ориентированных задач для государственного экзамена по направлению подготовки 09.04.03 «Прикладная информатика», магистерская программа «Искусственный интеллект в кибербезопасности»

### Задача 1

Исходные данные:

В корпоративной сети организации используются сервер приложений, сервер базы данных, рабочие станции пользователей, межсетевой экран и VPN-шлюз.

Требуется:

1 Определить основные угрозы безопасности для данной информационной системы.
2 Предложить меры защиты для наиболее критичных компонентов системы.

Задача 2

Исходные данные:

По результатам сканирования сети выявлены открытые порты 22, 80, 443, 3306 и 3389. Сервер базы данных доступен из внешней сети.

Требуется:

1 Составить текстовое описание модели угроз для данной инфраструктуры.
2 Определить основные меры по снижению рисков несанкционированного доступа.

Задача 3

Исходные данные:

Сканер уязвимостей выявил устаревшую версию веб-сервера, слабую парольную политику и отсутствие многофакторной аутентификации.

Требуется:

1 Распределить выявленные уязвимости по степени критичности.
2 Предложить порядок устранения выявленных уязвимостей.

Задача 4

Исходные данные:

В журнале событий сервера зафиксировано 180 неуспешных попыток входа в учетную запись администратора за 15 минут с разных IP-адресов.

Требуется:

1 Определить возможный тип атаки.
2 Предложить первичные меры реагирования на инцидент.

Задача 5

Исходные данные:

В SIEM-систему поступают события с рабочих станций, серверов, межсетевого экрана и антивирусного программного обеспечения.

Требуется:

1 Определить, какие события необходимо использовать для выявления подозрительной активности.
2 Сформулировать пример правила корреляции для SIEM-системы.

Задача 6

Исходные данные:

Для обнаружения сетевых атак построена модель машинного обучения. По результатам тестирования получены значения: TP = 90, TN = 860, FP = 35, FN = 15, где TP — верно обнаруженные атаки, TN — верно определенный нормальный трафик, FP — ложные срабатывания, FN — пропущенные атаки.

Требуется:

1 Рассчитать accuracy, precision, recall и F1-меру.
2 Сделать вывод о качестве модели обнаружения атак.

Задача 7

Исходные данные:

В наборе данных для обучения модели обнаружения атак содержится 97 % нормального сетевого трафика и 3 % атак.

Требуется:

1 Определить проблему, возникающую при обучении модели на таких данных.
2 Предложить методы устранения дисбаланса классов.

Задача 8

Исходные данные:

Организация планирует внедрить модель машинного обучения для обнаружения аномалий в сетевом трафике. Доступны признаки: IP-адрес отправителя, IP-адрес получателя, порт, протокол, длительность соединения и объем переданных данных.

Требуется:

1 Определить признаки, пригодные для обучения модели.
2 Предложить этапы предварительной обработки данных.

Задача 9

Исходные данные:

После обновления обучающего набора качество модели обнаружения вредоносного трафика снизилось. Предполагается, что в обучающие данные были добавлены искаженные примеры.

Требуется:

1 Определить возможный тип атаки на систему искусственного интеллекта.

2 Предложить меры защиты обучающих данных.

Задача 10

Исходные данные:

Злоумышленник изменяет признаки сетевого трафика так, чтобы модель машинного обучения классифицировала вредоносную активность как нормальную.

Требуется:

1 Определить тип атаки на модель искусственного интеллекта.

2 Предложить способы повышения устойчивости модели.

Задача 11

Исходные данные:

Разрабатывается программный модуль авторизации пользователей. В модуле предусмотрены логин и пароль, но отсутствуют ограничения по сложности пароля и количеству попыток входа.

Требуется:

1 Определить уязвимости проектируемого модуля.

2 Сформулировать требования к безопасной авторизации.

Задача 12

Исходные данные:

Статический анализатор кода выявил возможность SQL-инъекции, отсутствие проверки входных данных и хранение пароля в открытом виде.

Требуется:

1 Классифицировать выявленные уязвимости.

2 Предложить способы их устранения.

Задача 13

Исходные данные:

В репозитории проекта обнаружены пароли, токены доступа и ключи API, сохраненные в исходном коде.

Требуется:

1 Определить риски хранения секретов в исходном коде.
2 Предложить безопасные способы хранения конфиденциальных параметров.

Задача 14

Исходные данные:

Команда разработки внедряет CI/CD-пайплайн. Проверка безопасности программного кода проводится только перед выпуском новой версии продукта.

Требуется:

1 Определить недостатки текущего процесса разработки.
2 Предложить проверки безопасности, которые необходимо включить в CI/CD-пайплайн.

Задача 15

Исходные данные:

В базе данных информационной системы хранятся сведения о пользователях, их ролях, журналах действий и событиях безопасности. Резервное копирование выполняется один раз в неделю.

Требуется:

1 Определить риски выбранной периодичности резервного копирования.
2 Предложить меры защиты и восстановления данных.

Задача 16

Исходные данные:

После сбоя сервера база данных была восстановлена из резервной копии, созданной 72 часа назад. Данные о событиях безопасности за последние трое суток были потеряны.

Требуется:

1 Определить фактическое значение RPO и объяснить, почему выбранная схема резервного копирования не обеспечивает сохранность данных о событиях безопасности.

2 Определить, как потеря журналов событий может повлиять на расследование инцидента.

Задача 17

Исходные данные:

Организация планирует перенести часть сервисов в облачную инфраструктуру с использованием моделей IaaS и SaaS.

Требуется:

1 Определить основные угрозы безопасности облачной инфраструктуры.

2 Предложить меры защиты данных и управления доступом.

Задача 18

Исходные данные:

В облачной среде обнаружена учетная запись с правами администратора, которая не использовалась более шести месяцев. Многофакторная аутентификация для нее не включена.

Требуется:

1 Определить риски, связанные с данной учетной записью.

2 Предложить действия администратора безопасности.

Задача 19

Исходные данные:

На рабочей станции пользователя обнаружены высокая загрузка процессора, неизвестный процесс, соединение с внешним IP-адресом и изменение системных файлов.

Требуется:

1 Определить возможный тип вредоносной активности.

2 Указать, какие цифровые следы необходимо сохранить для расследования.

Задача 20

Исходные данные:

При анализе вредоносного файла установлено, что он создает копию в системной директории, изменяет параметры автозагрузки и подключается к удаленному серверу.

Требуется:

1 Определить признаки вредоносного программного обеспечения.

2 Предложить меры локализации и устранения угрозы.

Задача 21

Исходные данные:

В организации произошел инцидент: учетная запись сотрудника была использована для входа в систему в ночное время с неизвестного IP-адреса, после чего были выгружены конфиденциальные файлы.

Требуется:

1 Составить последовательность действий по расследованию инцидента.

2 Предложить меры предотвращения повторения подобной ситуации.

Задача 22

Исходные данные:

В ходе расследования инцидента имеются журналы входа пользователей, сетевые дампы, образ диска рабочей станции и список измененных файлов.

Требуется:

1 Определить порядок сбора и сохранения цифровых доказательств.

2 Сформулировать требования к обеспечению целостности доказательств.

Задача 23

Исходные данные:

По результатам анализа инцидента установлена последовательность событий: получение фишингового письма, переход по ссылке, ввод учетных данных, вход злоумышленника в систему и выгрузка конфиденциальных файлов.

Требуется:

1 Построить цепочку атаки.

2 Предложить меры защиты на каждом этапе атаки.

Задача 24

Исходные данные:

Разрабатывается интеллектуальный агент для анализа событий безопасности. Агент должен получать данные из SIEM-системы, выявлять аномалии и формировать рекомендации специалисту по информационной безопасности.

Требуется:

1 Определить основные функции автономного ИИ-агента.
2 Указать ограничения и риски автоматического реагирования на инциденты.

Задача 25

Исходные данные:

Заказчик разрабатываемой информационной системы указал только функциональные требования: регистрацию пользователей, хранение данных, поиск записей и формирование отчетов. Требования к безопасности, надежности и разграничению доступа в техническом задании не определены.

Требуется:

1 Определить, какие требования к безопасности необходимо добавить в техническое задание.
2 Разделить предложенные требования на функциональные и нефункциональные.

Задача 26

Исходные данные:

В организации отсутствуют единые правила управления доступом, реагирования на инциденты, резервного копирования, хранения журналов событий и контроля действий пользователей.

Требуется:

1 Составить перечень внутренних документов по информационной безопасности, необходимых для организации защиты информационной системы.
2 Определить назначение политики информационной безопасности.

## 7 Организация государственного экзамена и работы государственной экзаменационной комиссии

Государственный экзамен по направлению подготовки 09.04.03 «Прикладная информатика», магистерская программа «Искусственный интеллект в кибербезопасности», проводится в устной форме в виде итогового междисциплинарного экзамена с учетом требований федерального государственного образовательного стандарта высшего образования — магистратура по направлению подготовки 09.04.03 «Прикладная информатика», утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 916, а также планируемых результатов освоения образовательной программы.

Государственный экзамен проводится по ключевым дисциплинам образовательной программы, результаты освоения которых имеют определяющее значение для профессиональной деятельности выпускников в области прикладной информатики, искусственного интеллекта, машинного обучения, разработки и сопровождения защищенных информационных систем, анализа защищенности, управления рисками и расследования компьютерных инцидентов.

Не позднее чем за 30 календарных дней до дня проведения первого государственного аттестационного испытания Университет утверждает распорядительным актом расписание государственных аттестационных испытаний, в котором указываются даты, время и место проведения государственных аттестационных испытаний и предэкзаменационных консультаций. Расписание доводится до сведения обучающихся, председателя и членов государственных экзаменационных комиссий и апелляционных комиссий, секретарей государственных экзаменационных комиссий, руководителей и консультантов выпускных квалификационных работ.

При формировании расписания устанавливаются перерывы между государственными аттестационными испытаниями продолжительностью не менее 7 календарных дней.

К государственному экзамену допускается обучающийся, не имеющий академической задолженности и в полном объеме выполнивший учебный план или индивидуальный учебный план по осваиваемой образовательной программе высшего образования.

Перед государственным экзаменом проводится консультирование обучающихся по вопросам, включенным в программу государственного экзамена, — предэкзаменационная консультация.

При подготовке к сдаче государственного экзамена обучающемуся необходимо внимательно изучить программу государственного экзамена, перечень теоретических вопросов, практико-ориентированные задания, критерии оценивания, а также основную и дополнительную литературу, рекомендованную для подготовки к государственному экзамену.

При подготовке к государственному экзамену обучающемуся следует повторить материалы профильных дисциплин образовательной программы, связанных с проектированием и сопровождением информационных систем, искусственным интеллектом, машинным обучением в кибербезопасности, анализом защищенности, разработкой защищенного программного обеспечения, администрированием безопасных информационных систем, управлением информационной безопасностью и расследованием компьютерных инцидентов.

Государственный экзамен проводится по экзаменационным билетам, разработанным на основании настоящих методических указаний и программы государственного экзамена по направлению подготовки 09.04.03 «Прикладная информатика», магистерская программа «Искусственный интеллект в кибербезопасности», в соответствии с содержанием образовательной программы и рабочими программами профильных дисциплин.

Экзаменационный билет включает:

- теоретический вопрос;
- задание на проверку умений;
- практико-ориентированное задание.

Государственный экзамен принимает государственная экзаменационная комиссия, состав которой утверждается приказом ректора Университета не позднее чем за 1 месяц до даты начала государственной итоговой аттестации.

После получения экзаменационного билета обучающемуся предоставляется время для подготовки ответа в соответствии с установленным порядком проведения государственного экзамена.

После подготовки обучающийся в устной форме представляет членам государственной экзаменационной комиссии ответ на теоретический вопрос, результаты выполнения задания на проверку умений и практико-ориентированного задания.

Члены государственной экзаменационной комиссии могут задавать обучающемуся дополнительные вопросы по содержанию представленного ответа, а также по вопросам, связанным с проверкой уровня сформированности компетенций и готовности выпускника к решению профессиональных задач.

Обучающимся и лицам, привлекаемым к проведению государственного экзамена, во время его проведения запрещается иметь при себе и использовать средства связи.

## 8 Порядок оценки результатов государственного экзамена

Оценка результатов государственного экзамена осуществляется государственной экзаменационной комиссией в соответствии с критериями оценивания, установленными настоящими методическими указаниями и программой государственного экзамена.

Итоговая оценка за государственный экзамен определяется по сумме баллов, полученных обучающимся за выполнение всех элементов экзаменационного билета и ответы на дополнительные вопросы членов государственной экзаменационной комиссии.

В случае расхождения мнений членов государственной экзаменационной комиссии итоговое решение принимается простым большинством голосов членов комиссии, участвующих в заседании. При равном числе голосов председатель государственной экзаменационной комиссии обладает правом решающего голоса.

Результат государственного экзамена, проводимого в устной форме, объявляется в день его проведения.

Решение государственной экзаменационной комиссии оформляется протоколом заседания государственной экзаменационной комиссии.

## 9 Критерии оценки результатов сдачи государственного экзамена

### Показатели, критерии и оценивание компетенций

Государственный экзамен по направлению подготовки 09.04.03 «Прикладная информатика», магистерская программа «Искусственный интеллект в кибербезопасности», направлен на проверку уровня сформированности универсальных, общепрофессиональных и профессиональных компетенций выпускника, предусмотренных образовательной программой.

При оценке результатов сдачи государственного экзамена учитываются полнота и правильность ответа на теоретический вопрос, способность обучающегося применять профессиональные знания при выполнении задания на проверку умений, качество выполнения практико-ориентированного задания, обоснованность выводов, владение профессиональной терминологией, а также способность отвечать на дополнительные вопросы членов государственной экзаменационной комиссии.

| Элемент государственного экзамена | Проверяемые результаты освоения ОП ВО | Показатели оценивания | Критерии оценивания | Балл |
|---|---|---|---|---|
| Теоретический вопрос | Знать: теоретические основы прикладной информатики, ИИ и кибербезопасности. Уметь: объяснять основные методы и технологии по теме вопроса. Владеть: профессиональной терминологией и навыками аргументации ответа. | Качество ответа на теоретический вопрос экзаменационного билета после отведенного времени на подготовку к ответу. | Полный и аргументированный ответ; раскрыта суть вопроса; использована профессиональная терминология; приведены примеры по теме | 30 |
| | | | Частичный ответ; вопрос раскрыт неполно; имеются отдельные неточности; примеры и аргументация недостаточны | 1 -29 |
| | | | Ответ не раскрывает вопрос; допущены грубые ошибки; обучающийся не демонстрирует необходимых знаний или отказывается от ответа. | 0 |
| Задание на проверку умений | Знать: методы анализа профессиональной информации и формализации прикладных задач. Уметь: выбирать методы и инструменты для решения задач в области ИИ, кибербезопасности и проектирования ИС. Владеть: навыками применения выбранных методов при решении профессиональных задач. | Качество выполнения задания на проверку умений; правильность выбранного способа решения; обоснованность действий и выводов обучающегося. | Задание выполнено полностью; способ решения выбран правильно; действия и выводы обоснованы. | 30 |
| | | | Задание выполнено частично; способ решения в целом верен, но есть неточности; выводы сформулированы неполно. | 1 - 29 |
| | | | Задание не выполнено или выполнено неверно; обучающийся не демонстрирует умение применять знания к профессиональной ситуации. | 0 |
| Практико-ориентированное задание | Знать: методы анализа защищенности, | Качество выполнения практико- | Задание выполнено полностью; исходные данные | 30 |

| | | | | |
|---|---|---|---|---|
| | разработки защищенного ПО, применения ИИ в кибербезопасности и расследования инцидентов. Уметь: анализировать исходные данные, выявлять угрозы, уязвимости и признаки инцидентов. Владеть: навыками подготовки обоснованных решений и рекомендаций по защите, реагированию и устранению угроз. | ориентированного задания; полнота анализа исходных данных; обоснованность предложенных решений и выводов. | проанализированы верно; предложены обоснованные решения и выводы. | |
| | | | Задание выполнено частично; анализ исходных данных неполный; предложенные решения требуют уточнения. | 1 - 29 |
| | | | Задание не выполнено или выполнено неверно; обучающийся не демонстрирует практических навыков решения профессиональной задачи. | 0 |
| Дополнительные вопросы членов государственной экзаменационной комиссии | Знать: основные понятия и методы по теме ответа. Уметь: уточнять и обосновывать ранее представленный ответ. Владеть: профессиональной терминологией и навыками аргументированного ответа. | Способность отвечать на дополнительные вопросы членов государственной экзаменационной комиссии без предварительной подготовки. | Полные и аргументированные ответы; обучающийся уточняет и обосновывает ранее представленный ответ. | 10 |
| | | | Частичные ответы; имеются отдельные неточности, но понимание темы в целом продемонстрировано. | 1 - 9 |
| | | | Ответы отсутствуют или содержат грубые ошибки; обучающийся не демонстрирует достаточного уровня подготовки. | 0 |

Критерии оценки ответа на теоретический вопрос

30 баллов выставляется обучающемуся при полном, логичном и аргументированном ответе на вопрос билета, демонстрации системных

теоретических знаний, владении профессиональной терминологией и способности привести примеры по теме вопроса.

20–29 баллов выставляется обучающемуся при достаточно полном ответе, в котором имеются отдельные неточности или недостаточно развернутые положения. Обучающийся в целом раскрывает содержание вопроса, но нуждается в уточняющих вопросах членов государственной экзаменационной комиссии.

10–19 баллов выставляется обучающемуся при частичном раскрытии вопроса, наличии существенных пробелов в теоретических знаниях, недостаточной аргументации и ограниченном использовании профессиональной терминологии.

1–9 баллов выставляется обучающемуся при фрагментарном ответе, наличии грубых ошибок, нарушении логики изложения и отсутствии обоснованных выводов.

0 баллов выставляется при отсутствии ответа или при ответе, не имеющем отношения к вопросу экзаменационного билета.

Критерии оценки результатов выполнения задания на проверку умений

30 баллов выставляется обучающемуся, если задание выполнено полностью и правильно, выбран обоснованный способ решения, действия логичны, выводы корректны и соответствуют профессиональной задаче.

20–29 баллов выставляется обучающемуся, если задание выполнено в целом правильно, но имеются отдельные неточности, неполнота в обосновании решения или недостаточная детализация выводов.

10–19 баллов выставляется обучающемуся, если задание выполнено частично, способ решения выбран не полностью обоснованно, допущены ошибки, влияющие на полноту и качество выводов.

1–9 баллов выставляется обучающемуся, если задание выполнено неправильно, решение носит фрагментарный характер, выводы не позволяют подтвердить сформированность проверяемых умений.

0 баллов выставляется, если задание не выполнено.

Критерии оценки результатов выполнения задания на проверку навыков

30 баллов выставляется обучающемуся, если практико-ориентированное задание выполнено полностью, исходные данные проанализированы правильно, выявлены ключевые угрозы, уязвимости, признаки инцидента или иные значимые элементы профессиональной ситуации, предложены обоснованные решения и выводы.

20–29 баллов выставляется обучающемуся, если практико-ориентированное задание выполнено в целом правильно, но анализ исходных данных проведен недостаточно полно, отдельные решения требуют уточнения, выводы сформулированы не полностью.

10–19 баллов выставляется обучающемуся, если задание выполнено частично, при анализе профессиональной ситуации допущены существенные ошибки, предложенные решения недостаточно обоснованы.

1–9 баллов выставляется обучающемуся, если задание выполнено неправильно, анализ исходных данных носит фрагментарный характер, предложенные решения не соответствуют условиям задания.

0 баллов выставляется, если задание не выполнено.

Критерии оценки ответов на дополнительные вопросы членов государственной экзаменационной комиссии

10 баллов выставляется обучающемуся при полных, точных и аргументированных ответах на дополнительные вопросы, корректном

использовании профессиональной терминологии и способности обосновать ранее представленный ответ.

5–9 баллов выставляется обучающемуся при частичных ответах на дополнительные вопросы, наличии отдельных неточностей, но при общем понимании рассматриваемой профессиональной ситуации.

1–4 балла выставляется обучающемуся при фрагментарных ответах, слабой аргументации и существенных затруднениях при пояснении ранее представленного ответа.

0 баллов выставляется, если обучающийся не отвечает на дополнительные вопросы или допускает грубые ошибки, свидетельствующие о недостаточном уровне подготовки.

Полученная на государственном экзамене сумма баллов переводится в пятибалльную систему оценивания следующим образом:

- «отлично» — от 89 до 100 баллов;
- «хорошо» — от 77 до 88 баллов;
- «удовлетворительно» — от 65 до 76 баллов;
- «неудовлетворительно» — от 0 до 64 баллов.

При оценивании ответа обучающегося члены государственной экзаменационной комиссии учитывают полноту и правильность ответа, уровень владения профессиональной терминологией, логичность и грамотность изложения, способность применять теоретические знания при решении практико-ориентированных заданий, а также обоснованность выводов.

В случае расхождения мнений членов государственной экзаменационной комиссии итоговое решение принимается простым большинством голосов членов комиссии, участвующих в заседании. При равном числе голосов председатель государственной экзаменационной комиссии обладает правом решающего голоса.

Результат государственного экзамена, проводимого в устной форме, объявляется в день его проведения.

Решение государственной экзаменационной комиссии оформляется протоколом заседания государственной экзаменационной комиссии.

Протокол заседания государственной экзаменационной комиссии подписывается председателем и секретарем государственной экзаменационной комиссии.

## 10 Рекомендации обучающемуся по подготовке к государственному экзамену

Государственный экзамен проводится по утвержденной программе государственного экзамена, содержащей перечень вопросов, выносимых на государственный экзамен, практико-ориентированные задания, критерии оценивания и рекомендации обучающимся по подготовке к государственному экзамену, в том числе перечень рекомендованной литературы.

Программа государственного экзамена разрабатывается выпускающей кафедрой, рассматривается учебно-методической комиссией факультета и утверждается деканом факультета.

Перед государственным экзаменом проводится консультирование обучающихся по вопросам, включенным в программу государственного экзамена, — предэкзаменационная консультация.

При подготовке к государственному экзамену обучающемуся рекомендуется:

изучить программу государственного экзамена;

повторить теоретические вопросы, вынесенные на государственный экзамен;

проработать практико-ориентированные задания;

изучить критерии оценивания результатов государственного экзамена;

повторить материалы профильных дисциплин образовательной программы;

использовать основную и дополнительную литературу, рекомендованную для подготовки к государственному экзамену;

обратить внимание на профессиональную терминологию, используемую в области прикладной информатики, искусственного интеллекта и кибербезопасности;

отработать умение логично и последовательно излагать ответ, обосновывать выводы и приводить примеры.

Особое внимание при подготовке к государственному экзамену следует уделить вопросам проектирования и сопровождения информационных систем, применения методов искусственного интеллекта и машинного обучения в кибербезопасности, анализа защищенности компьютерных систем, разработки защищенного программного обеспечения, администрирования средств защиты информации, управления информационной безопасностью и расследования компьютерных инцидентов.

Государственный экзамен проводится в устной форме. Обучающийся получает экзаменационный билет, содержание которого соответствует утвержденной программе государственного экзамена. После получения экзаменационного билета обучающемуся предоставляется время для подготовки ответа в соответствии с установленным порядком проведения государственного экзамена.

При подготовке ответа обучающийся должен определить структуру ответа, выделить основные понятия, сформулировать ключевые положения, подготовить аргументы и примеры, а также продумать выводы по каждому вопросу или заданию.

В ходе ответа обучающийся представляет членам государственной экзаменационной комиссии ответ на теоретический вопрос, результаты выполнения задания на проверку умений и практико-ориентированного задания. После завершения ответа члены государственной экзаменационной комиссии могут задавать дополнительные и уточняющие вопросы в пределах программы государственного экзамена.

Ответ обучающегося должен быть полным, логичным, аргументированным и стилистически грамотным. При ответе необходимо использовать профессиональную терминологию, демонстрировать понимание содержания вопроса, умение применять знания к профессиональным ситуациям и способность обосновывать предлагаемые решения.

Государственный экзамен принимает государственная экзаменационная комиссия. Заседания государственной экзаменационной комиссии проводятся председателем при участии не менее двух третей состава комиссии. Решения государственной экзаменационной комиссии оформляются протоколом.

Приложения

*Приложение 1*

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1
к государственному экзамену
образовательной программы высшего образования
по направлению подготовки
09.04.03 «Прикладная информатика»,
магистерская программа «Искусственный интеллект в кибербезопасности»
на 2026-2027 учебный год

1. Теоретический вопрос

Машинное обучение в кибербезопасности: задачи, методы и показатели качества моделей обнаружения атак.

2. Задание на проверку умений

Для модели обнаружения сетевых атак получены следующие результаты тестирования: TP = 90, TN = 860, FP = 35, FN = 15, где TP — верно обнаруженные атаки, TN — верно определенный нормальный трафик, FP — ложные срабатывания, FN — пропущенные атаки.

Требуется:

Рассчитать accuracy, precision, recall и F1-меру.

Сделать вывод о качестве модели обнаружения атак.

3. Задание на проверку навыков

В организации произошел инцидент: учетная запись сотрудника была использована для входа в систему в ночное время с неизвестного IP-адреса, после чего были выгружены конфиденциальные файлы.

Требуется:

Составить последовательность действий по расследованию инцидента.

Предложить меры предотвращения повторения подобной ситуации.

И.о. декана факультета цифровых технологий

_____ /_____/