Приложение 1
к Протоколу заседания
учебно-методического совета НИУ ВШЭ
от 15.12.2025 № 021 (082)

ЗАКЛЮЧЕНИЕ

временной экспертной комиссии по рассмотрению документов образовательной программы «Информационная безопасность систем искусственного интеллекта» (направление подготовки: 10.04.01 Информационная безопасность; уровень высшего образования: магистратура), онлайн-программа (платформа реализации: https://edu.hse.ru)

Сформированная УМС (протокол № 019 (080) от 04.12.2025) временная экспертная комиссия (ВЭК) по рассмотрению поступивших в УМС НИУ ВШЭ документов образовательной программы «Информационная безопасность систем искусственного интеллекта» (направление подготовки: 10.04.01 Информационная безопасность; уровень высшего образования – магистратура) в составе Дегтярева К.Ю.(руководитель комиссии), Силаева Ю.В.(член комиссии), Ясницкого Л.Н. (член комиссии) и Максименковой О.В. (член комиссии) внимательно изучила представленный разработчиками пакет документов ОП. В целом, члены ВЭК согласились с тем, что предлагаемая разработчиками программа попадает в актуальную нишу критически важного для бизнеса и рядовых пользователей направления ИИ-безопасности, развития методологии интеграции аспектов безопасности в жизненный цикл систем машинного обучения (MLSecOps); кроме того, как следует из представленных документов, направленность программы хорошо перекликается со стратегией НИУ ВШЭ в области развития и использования технологий искусственного интеллекта.

Одновременно, члены ВЭК представили свои комментарии и сформулировали замечания, которые можно свести к следующему:

1. Можно согласиться с тем, что предлагаемый учебный план вполне соответствует целям разработчиков, но при этом, сразу же обращает на себя внимание «семейный кластер» родственных ОП, связанных со сферами информационной безопасности и искусственного интеллекта. В частности, магистерская программа «Информационная безопасность и технологии искусственного интеллекта» как представитель пула программ МИЭМ НИУ ВШЭ по целям, названию и набору дисциплин достаточно сильно пересекается с вынесенной на рассмотрение ОП. Несмотря на имеющиеся различия, аспекты MLSecOps обращают на себя внимание. По мнению членов ВЭК, в документах программы недостаточно четко проведена граница, которая позволила бы судить о том, чем именно данная ОП принципиально отличается от уже реализуемых программ по информационной безопасности в ИИ-системах и смежных областях – например, чем отличается ‘портрет’ будущих абитуриентов и выпускников от профессиональных характеристик тех, кто сделает выбор в пользу иной программы? Где не прослеживаются пересечения по наполнению программы и рынку, ожидающего выпускников? Что уникального будет предлагать ОП, чего нельзя будет получить на программах-конкурентах? Наверное, можно согласиться с тем, что текущие утверждения, касающиеся уникальности и отсутствие дублирования пока (комиссия руководствовалась исключительно представленным пакетом документов и собственным взглядом на его содержание) выглядят более приближенными к

составляющим аргументации «по смыслу», нежели к аналитически строгому разбору имеющихся пересечений и выделяемых отличий. Представляется важным четко ‘развести’ предлагаемую программу с уже существующей(-щими) на уровне концепции.

2. У членов ВЭК сложилось впечатление, что цели программы сформулированы достаточно широко (подготовка специалистов по проектированию, разработке и эксплуатации безопасных ML-систем), связь между целями и конкретными показателями их достижения (какими задачами могут заниматься выпускники программы, какие позиции на рынке труда они могут занимать, чем они отличаются от выпускников уже существующих программ по инфобезопасности и ИИ-программ) могла бы быть прописана более конкретно и в более проверяемых формулировках,
3. (раздел «Партнерство с индустрией») Одновременно, было высказано мнение, что разработка и реализация программы при участии внешних организаций (VK, Ozon и др.), с одной стороны, важны и полезны для ОП, но, с другой стороны, этот факт усиливает зависимость программы от конкретных корпоративных партнеров. При независимой экспертизе документов это воспринимается как фактор риска, требующий аккуратного мониторинга и возможного наращивания внутреннего кадрового ядра в среднесрочной перспективе. Предлагаемая структура рабочей команды ОП выглядит сбалансированной по компетенциям, но достаточно хрупкой по количеству людей, напрямую специализирующихся именно в MLSecOps и ИИ-безопасности (не в целом в информационной безопасности или машинном обучении). Из текущих документов складывается ощущение, что кадров хватит для старта и первых наборов ОП, однако резерв по расширению проектной и научной составляющих, по сопровождению потенциально возможных нескольких потоков учащихся и по развитию собственных научно-педагогических школ в MLSecOps пока не очень просматривается. По сути, члены ВЭК обратили внимание на вопросы устойчивости и масштаба реализации программы. Отраженное в документах кадровое обеспечение подтверждает высокое качество ‘точечных’ специалистов, однако, в составе НПР ОП сейчас просматривается небольшое ядро штатных преподавателей и заметная доля внутренних и внешних совместителей, что потенциально создает риски при изменении кадровой или корпоративной ситуации,
4. (раздел «Партнерство с индустрией») Выше было отмечено участие в ОП ключевых технологических компаний (VK, Ozon и др.), что позволит обеспечить доступ к реальным кейсам, данным и экспертным знаниям. Однако, определенная специфика этих компаний отличается от особенностей большого числа других компаний реального сектора экономики – речь здесь может идти о серийном производстве промышленных изделий, атомной промышленности, космоса, медицины и т.п. Во всех этих сферах проблемы информационной безопасности ИИ-систем крайне остры и требуют повышенного внимания. Члены ВЭК отметили, что утверждение о том, что “… выпускники программы смогут создавать промышленные ML-системы” звучит пока не совсем убедительно; оно должно быть подкреплено привлечением специалистов и из других областей экономики,
5. Некоторые члены экспертной комиссии обратили внимание на отсутствие в пакете документов ОП явной, четко артикулированной стратегии использования ИИ-инструментов студентами в учебном процессе. На уровне ВШЭ действуют регламенты по использованию инструментов ИИ и академической честности; с учетом профиля программы (безопасность ИИ, MLSecOps), как раз и ожидается присутствие в документах продуманной и четко прописанной политики

(определение форм и границ допустимого использования ИИ в письменных и проектных работах, подходов к “обогащению образовательного опыта” за счет применения ИИ-инструментов с минимизацией читинга, фабрикации результатов и плагиата), а её отсутствие формально выглядит как серьёзное упущение,

6. По единодушному мнению членов ВЭК, подобная программа актуальна, но если кинуть взгляд в перспективу и задуматься о завтрашнем дне (первые выпускники программы могут появиться не раньше середины 2028 года), то здесь есть определенные опасения. Дело в том, что очень быстро набирают силу большие языковые модели (LLM), базовые модели (FM), соответственно, развиваются технологии промт-программирования (промт-инжиниринга), составляющие конкуренцию уже привычному программированию на языке Python. Интерес и практическое использование промт-программ растёт (здесь и интегрированные в среды разработки (IDE) помощники по написанию кода, и чат-боты, которые обобщают результаты исследований – этим всё не ограничивается; сам процесс промт-программирования имеет свою существенную специфику). Члены экспертной комиссии считают, что без охвата программой этих технологий, есть риск её быстрого устаревания и снижения интереса к ней со стороны потенциальных абитуриентов,
7. Также было отмечено, что структурная часть программ учебных дисциплин (ПУД) отличается неоднородностью, т.е. далеко не во всех дисциплинах в одинаковой мере (и форме) прописаны пререквизиты и постреквизиты, местами выстраивание логической цепочки «… что для чего является базой … » больше угадывается из здравого смысла и сопровождающей пакет документов диаграммы связей дисциплин БУП, чем считывается прямо из текста описаний дисциплин. По мнению членов экспертной комиссии, этот факт снижает прозрачность целостности ОП для экспертов, знакомящихся с документами впервые, т.е. общая логика выстроена, но по имеющемуся пулу аннотаций её можно реконструировать лишь частично,
8. Члены ВЭК также обратили внимание на то, что весьма актуальная ОП ориентирована, в первую очередь, на национальную повестку (российские нормативные требования в области информационной безопасности и ИИ, взаимодействие с российскими индустриальными партнерами, предлагаемый онлайн-формат программы на русском языке). Понятны все имеющиеся сейчас сложности по внешнему контуру, но, в целом, НИУ ВШЭ обладает достаточно развитой сетью международных связей и работающими механизмами академической мобильности. В проекте рассматриваемой ОП этот потенциал практически не задействован – например, не предлагаются англоязычные модули или совместные дисциплины с иностранными университетами по крайне востребованной тематике ИИ-безопасности и MLSecOps. Как следствие, возможные перспективы международного сотрудничества при реализации ОП выглядят сильно ограниченными при том, что тематика ОП уже является значимой точкой её (ОП) возможного роста и активного развития.

В результате, руководитель и члены комиссии представили заполненные чек-листы (обновленная версия) с соответствующими оценками вынесенного на рассмотрение пакета документов ОП по различным параметрам со своими замечаниями и комментариями. После подсчета выставленных членами ВЭК оценок, средний балл по всем критериям оказался равен 61,2 (наиболее низкие баллы в чек-листах были выставлены членами экспертной комиссии в пп. 1.6 (отсутствие программ-конкурентов в НИУ ВШЭ, особенно в том же кампусе, в котором планируется открытие рассматриваемой программы), 1.7 (имеющийся задел международного сотрудничества

и его перспективы при реализации образовательной программы), 2.3 (отсутствие дублирования уже реализуемых в НИУ ВШЭ образовательных программ), 3.2 (включение в программы учебных дисциплин пререквизитов и постреквизитов, позволяющих оценить логику построения образовательной программы и её целостность), 3.3 (включение в программы учебных дисциплин образовательной программы перечней основной и актуальной литературы), 4.1 (учет активного развития решений на основе ИИ и определение стратегии их использования в программе, нацеленной на обогащение образовательного опыта студентов при минимизации проблем читинга и плагиата в письменных работах) и 5.2 (оптимальное соединение возможностей кадрового потенциала НИУ ВШЭ и внешних организаций).

Несмотря на то, что полученный средний балл формально позволяет согласовать представленный пакет документов, тем не менее, по мнению большинства членов ВЭК, отмеченные выше замечания и комментарии все-таки подводят к необходимости доработать представленные документы ОП. Временная экспертная комиссия рекомендует УМС направить документы программы «Информационная безопасность систем искусственного интеллекта» (направление подготовки: 10.04.01 Информационная безопасность; уровень высшего образования – магистратура) на доработку.