Отзыв на автореферат диссертации

Подтопельного Владислава Владимировича

«Модели и методика определения последовательностей атакующих воздействий на системы искусственного интеллекта при аудите информационной безопасности», представленную на соискание учёной степени кандидата технических наук по научной специальности

2.3.6. – Методы и системы защиты информации, информационная безопасность

В современной информационной экосистеме искусственный интеллект (ИИ) играет важную роль, поскольку он интегрируется в инфраструктуру множества предприятий и организаций. Экспоненциальный рост технологий ИИ породил ряд существенных проблем, связанных с обеспечением безопасности их функционирования. В контексте обеспечения кибербезопасности информационных систем, критически важно адекватно оценивать потенциальные угрозы и прогнозировать возможные векторы атак злоумышленников на инфраструктуру, где применяются технологии ИИ. Это актуализирует необходимость модернизации подходов к аудиту информационных систем с учетом внедрения инновационных решений на базе ИИ.

Диссертационное исследование соискателя направлено на решение этих актуальных задач. Анализ автореферата позволяет сделать вывод о том, что структура работы выстроена методически грамотно и логически последовательно, а текст реферата содержит все необходимые разделы, четко формулирующие цели, задачи и результаты исследования.

Среди наиболее значимых научных достижений диссертации, обладающих элементами новизны, можно выделить следующие:

1. Разработку и теоретическое обоснование моделей на основе марковских процессов принятия решений, направленных на выявление наиболее опасных последовательностей атакующих действий злоумышленников на системы ИИ. Модели учитывают уровень детализации последовательностей действий нарушителя для последующего анализа сценариев атак.

2. Предложенную методику, которая позволяет использовать модели в процессе проведения аудита информационной безопасности корпоративной инфраструктуры и организаций.

3. Формализацию алгоритма реализации предложенных моделей, обеспечивающего их практическую применимость и эффективность в процессе аудита информационной безопасности.

Материал автореферата подтверждает, что автор успешно решает поставленные задачи и обосновывает достоверность результатов, опираясь на аналитическую информацию, а также данные из международных и отечественных источников.

Однако имеются следующие замечания:

1) По нашему мнению, положения, выносимые на защиту диссертации, должны быть привязаны к пунктам специальности 2.3.6, что чётко показывает результаты автора в представленном диссертационном исследовании.
2) В работе можно отметить некоторую ограниченность исследования, связанную с использованием MITRE ATLAS, как основы построения моделей.
3) В пунктах научной новизны отсутствуют количественные показатели предлагаемых методик, алгоритмов. Отмечаются только качественные параметры:

1.....Это позволит улучшить совместную работу смежных систем контроля и поиска событий безопасности (за счет введения методов анализа на основе МППР), **повысить качество** аудита ИБ

3. Разработаны модели, методика и алгоритм определения атакующих последовательностей для сценариев атак на ПИИ, формируемых в процессе аудита ИБ ПИИ.

Однако, указанные замечания не снижают общей оценки диссертационного исследования.

ЗАКЛЮЧЕНИЕ: на основании вышеизложенного считаем, что диссертационная работа В. В. Подтопельного «Модели и методика определения последовательностей атакующих воздействий на системы искусственного интеллекта при аудите информационной безопасности» является завершенной научно-квалификационной работой. Полученные автором результаты являются

достаточно новыми, обоснованными и достоверными. Автореферат полностью соответствует содержанию диссертации.

Работа удовлетворяет требованиям ВАК и соответствуют паспорту специальности 2.3.6 - Методы и системы защиты информации, информационная безопасность. Диссертационная работа соответствует всем требованиям п. 9 - 14 «Положения о присуждении ученых степеней», утвержденным постановлением Правительства Российской Федерации от 24.09.2013 г. № 842, а ее автор, Подтопельный Владислав Владимирович, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6. – Методы и системы защиты информации, информационная безопасность.

И.о. зав. кафедрой безопасности информации и технологий ГБОУ ВПО «Сибирский государственный университет телекоммуникаций и информатики», д.т.н. (05.13.19), доцент

С.Н.Новиков

10.11.2025 г.

630102, г. Новосибирск, ул. Кирова, 86. Тел. 8-913-923-7-234; e-mail: snovikov@ngs.ru

Подпись заверяю : и.о. начальника отдела кадров Цветкова А.В.