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 ключевую роль, интегрируясь в технологическую инфраструктуру множества предприятий и организаций. Быстрый рост технологий ИИ породил ряд значительных проблем, связанных с обеспечением безопасности функционирования систем с элементами искусственного интеллекта.

В контексте кибербезопасности информационных систем критически важно адекватно оценивать потенциальные угрозы и прогнозировать возможные векторы атак злоумышленников на инфраструктуру с применением технологий ИИ. Это актуализирует необходимость модернизации подходов к аудиту информационных систем с учётом внедрения инновационных решений, учитывающих специфику 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, чётко формулирующие цели, задачи и результаты исследования.

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

1. Разработку и теоретическое обоснование моделей, направленных на выявление наиболее опасных последовательностей атакующих действий злоумышленников на системы ИИ. Модели учитывают уровень детализации анализа атакующих сценариев, а также интеграцию современных метрик оценки уязвимостей и баз знаний о методах атак злоумышленников как международного, так и отечественного происхождения.

2. Разработку методики применения предложенных моделей в контексте последовательности этапов проведения аудита информационной безопасности корпоративной инфраструктуры и организаций.

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

В качестве недостатков работы можно отметить следующие:

1. Описание применения моделей с учетом методики аудита рассматривается либо в контексте MITRE ATLAS, либо в её альтернативах.
2. В ATLAS представлено 56 техник, а в ATT&CK 196, это может не охватывать все возможные угрозы для сложной ИИ-систем.
3. Угрозы в области ИИ быстро эволюционируют, ATLAS требует регулярного обновления. Задержки в добавлении новых техник могут снижать его актуальность.

Вместе с тем, указанные недостатки не снижают значимости полученных результатов и не влияют на общую положительную оценку диссертационной работы В.В. Подтопленного.

Заключение, автореферат позволяет сделать вывод, что диссертация **Владислава Владимировича Подтопельного** 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.

Заведующий кафедрой «Защита информации» Калужского филиала федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана», доктор технических наук, профессор (специальность 05.13.19), mazinav@yandex.ru; телефон: +7 9109155825.

Мазин Анатолий Викторович

« 11 » ноября 2025 года

Адрес организации: 248000, Калужская область, г.о. «Город Калуга», г. Калуга, ул. Университетский Городок, соор.1;

Подпись Мазина А.В. заверяю:
Начальник управления научно-технической политики
КФ МГТУ им. Н.Э. Баумана
к.ф-м.н., доцент Е.В. Вершинин

« 11 » ноября 2025 года