ОТЗЫВ

на автореферат диссертации **Подтопельного Владислава Владимировича** на тему «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 настоящее время система искусственного интеллекта является частью общей инфраструктуры множества различных предприятий. Взрывной характер развития искусственного интеллекта породил множество различных проблем, связанных с безопасностью их эксплуатации. При обеспечении безопасности используемых информационных систем важно определять степень опасности угроз, понимать, каким образом злоумышленник может повлиять на инфраструктуру предприятия, в которых используются системы искусственного интеллекта. Таким образом встаёт важная проблема модернизации процесса аудита информационных систем с учётом внедрения новых технологий на основе искусственного интеллекта.

Именно эти актуальные задачи и решает в своём диссертационном исследовании соискатель. Исходя из положений, сформулированных в автореферате, можно заключить, что структура работы выстроена последовательно и логично, автор реферат диссертации содержит все необходимые разделы, характеризуются четкой формулировкой цели, задач и результатов. К наиболее значимым результатам диссертации, имеющим элементы научной новизны, можно отнести следующее:

1. Разработку и обоснование моделей, позволяющих определить последовательности действий злоумышленника при атаке на системы искусственного интеллекта, выявить наиболее опасные из них.

2. Методику применения предложенных моделей с учётом последовательности этапов проведения аудита информационной безопасности инфраструктуры предприятия и организаций.

3. Алгоритм применения моделей, предложенных соискателем.

Данные положения является не только результатами, обладающими научной новизной, но и имеет практическое значение для повышения уровня защищённости информационных систем со встроенными элементами системы

искусственного интеллекта при проведении обследования предприятия на предмет обеспечения защищённости его инфраструктуры.

Судя по автореферату, автор успешно решает поставленные задачи, а достоверность и обоснованность результатов определяется использованием аналитической информации, а также информации, использованной в международных источниках и авторитетных изданиях, как российских, так и зарубежных.

В качестве недостатка по автореферату следует отметить: в исследовании не описывается подробно специфика применения моделей в сопряжении с другими подходами, которые используются сегодня в современных системах аудита и методиках аудитов; не достаточно проанализирована таблица 2 и последовательность работы программного решения – рисунок 5, что связано, скорее всего, с ограниченным объёмом автореферата.

В целом автореферат позволяет сделать вывод о том, что представленная диссертация **Владислава Владимировича Подтопельного** представляет собой законченное научное исследование, имеет практическую ценность и соответствует требованиям п. 9, предъявляемым к кандидатским диссертациям по действующему «Положению о порядке присуждения ученых степеней», а её автор заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 – **Методы и системы защиты информации, информационная безопасность**.

Кандидат физико-математических наук, доцент,
заведующий кафедрой безопасности информационных систем,
федеральное государственное автономное образовательное учреждение высшего образования «Самарский национальный исследовательский университет имени академика С. П. Королёва» (Самарский университет)

[redacted] Осипов Михаил Николаевич

.Подпись заверяю

11. 11. 2025 г.

Адрес места основной работы: 443011, г. Самара, ул. Академика Павлова, 1, Самарский университет, корпус 22, к. 411
Рабочий телефон: +7 (846) 334-79-41
Адрес Эл. osipov7@yandex.ru

Подпись Осипова М.Н. удостоверяю.
Начальник отдела сопровождения деятельности диссертационных советов Самарского университета
Бояркина Бояркина У.В.
11 » ноября 2025 г.