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

Искусственный интеллект (ИИ) стал неотъемлемой частью инфраструктуры многих компаний, что породило новые вызовы в информационной области безопасности. Быстрое развитие ИИ-технологий требует развитие новых подходов к аудиту информационных систем, учитывающих специфику и уязвимости ИИ. Для повышения информационной безопасности необходимо оценивать угрозы, прогнозировать действия злоумышленников и адаптировать методики аудита к текущим реалиям.

Диссертация, представленная соискателем, нацелена на решение актуальных задач выявления актуальных этапов атак, при наступлении которых злоумышленник реализует атакующие воздействия, что позволяет повысить качество аудита безопасности информационных систем с учетом интеграции ИИ.

Автореферат отличается ясностью и логичностью изложения. В работе четко сформулированы цели, задачи и результаты. Основные научные достижения диссертации включают:

1. Разработку моделей для выявления опасных последовательностей действий злоумышленников при атаках на системы ИИ. Приведенные модели позволяют учитывать уровень детализации этапов атак, действия атакующего, современные метрики уязвимости и базы знаний о действиях злоумышленников.

2. Создание методики применения приводимых моделей в рамках аудита информационной безопасности систем ИИ предприятий и организаций.

3. Разработку алгоритма реализации моделей для повышения эффективности аудита с использованием предложенных моделей.

Приведенные результаты не только обладают научной новизной, но и имеют практическую значимость для повышения уровня защищенности информационных систем с элементами ИИ.

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

Однако, из автореферата не вполне ясно, почему связь классов атак на системы ИИ с предлагаемыми моделями основывается на степени известности моделей ИИ.

Указанное замечание не снижает высокого уровня проведенной соискателем работы, из чего следует, 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 отвечает 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.

Подпись Шевцовой Г.А. заверяю
Заместитель директора Департамента
по управлению персоналом и социальным
вопросам
Н.Н. Толстых
10 НОЯ 2025

Кандидат исторических наук, доцент,
директор Института информационных наук
и технологий безопасности,
заведующий кафедрой Информационной безопасности
Федерального государственного автономного
образовательного учреждения высшего образования
«Российский государственный гуманитарный университет»

Шевцова Галина Александро

Даю согласие на обработку персональных данных

Адрес места основной работы: 117534, г. Москва, ул. Кировоградская, д. 25, корп. 2, рабочий телефон: +7 (495) 388-08-88
Адрес эл. почты: ib@rggu.ru