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 условиях стремительного развития цифровых технологий и внедрения искусственного интеллекта (ИИ) в бизнес-процессы, вопросы информационной безопасности становятся особенно актуальными. Существующие методы аудита часто оказываются недостаточными для противодействия новым киберугрозам, что требует разработки инновационных подходов к управлению рисками. Кибербезопасность сегодня выходит за рамки простого обнаружения текущих угроз и включает прогнозирование будущих атак. В связи с этим адаптация методов аудита к работе с ИИ приобретает критическое значение. Диссертация Владислава Владимировича Подтопельного посвящена ключевым аспектам аудита информационных систем, включающих подсистемы ИИ.

Автореферат диссертации имеет чёткую структуру, содержит цели, задачи, результаты исследования. Работа направлена на повышение степени полноты описания атакующих действий злоумышленника для последующего анализа атак на системы, использующие ИИ. Исследование направлено на создание алгоритмов для выявления скрытых угроз и предсказания атак, что способствует повышению уровня защиты корпоративных информационных систем.

Основные задачи исследования включают:

1. Анализ существующих методов и инструментов оценки безопасности ИИ в условиях неполных данных.

2. Оценка данных для моделирования атак и определение ключевых метрик.

3. Разработка моделей для анализа и прогнозирования атак.

4. Создание методик и алгоритмов для моделирования атакующего воздействия.

5. Разработка программного решения для автоматизации оценки защитных механизмов.

Цель исследования — создание научно обоснованных моделей методики и формирования атакующих последовательностей при исследовании безопасности ИИ-систем. Диссертация Владислава Подтопельного объединяет результаты исследований в области информационной безопасности, математического моделирования и разработки программного обеспечения.

Структура диссертации состоит из введения, четырёх глав, заключения, списка литературы и приложений и занимает 250 страниц. В работе представлено 50 рисунков и 20 таблиц.

Во введении определены объект и предмет исследования, цели и задачи, а также основные положения и краткое содержание каждой главы. В первой главе рассматриваются цели и возможности моделирования атак с использованием марковских процессов принятия решений (МППР), а также особенности аудита ИИ-систем. Вторая глава посвящена применению МППР для моделирования атак на ИИ, включая функции ценности, вознаграждения и построение графов атак. Третья глава рассматривает модели последовательностей атак на основе МППР и методику аудита. Четвёртая глава представляет экспериментальную оценку разработанных моделей. В заключении подводятся итоги исследования и формулируются основные выводы.

Научная новизна заключается в следующем:

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.

Обоснованность выводов подтверждается анализом современных исследований и согласованием теоретических положений с практической реализацией.

Однако, из материала автореферата недостаточно ясно, как влияет предложенная функция вознаграждения на модели с учетом специфики применяемого режима моделирования.

Указанное замечание не снижает общей оценки диссертационного исследования. В заключение, автореферат позволяет сделать вывод, что диссертация **Владислава Владимировича Подтопельного** представляет собой качественную научно-квалификационную работу, сочетающую актуальность темы, новизну подхода и практическую значимость. Работа удовлетворяет требованиям ВАК и соответствуют паспорту научной 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. N° 842. Автор заслуживает присуждения ученой степени кандидата технических наук, что подтверждает его высокий уровень компетентности и фундаментальное знание в области информационной безопасности.

Директор института оптики и
технологии информационной
безопасности, доктор экономический наук,
доцент

Шабурова Аэлита Владимировна

13.11.2025

Организация: ФГБОУ ВО «СГУГиТ», inst.oot@ssga.ru
Адрес: ул. Плахотного, д.10, Новосибирск, 630108
Email: aelita_shaburova@mail.ru

Подпись заверяю

ПОДПИСЬ Шабурова А.В.
ЗАВЕРЯЮ Специалист по персоналу
Е.С. Мартынова