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

Интеграция ИИ в корпоративные системы (КИС) сегодня обострила проблемы в области информационной безопасности, как систем ИИ, так и КИС. Существующие методы аудита и мониторинга не справляются с современными киберугрозами, поэтому необходимы инновационные подходы к оценке и управлению рисками в процессе аудита информационных систем. Диссертация В. В. Подтопельного посвящена анализу атак на системы ИИ и их влиянию на аудит информационной безопасности. Работа отличается чёткой структурой, ясными целями и задачами, а также обоснованными результатами. Цель исследования — детализировать и уточнить описание последовательности действий при предполагаемых атаках на системы ИИ при аудите их безопасности. Для этого были разработаны модели и методика углублённого анализа уязвимостей.

Автореферат демонстрирует высокий уровень структурированности и логическую последовательность работы, включая все необходимые разделы, а также чётко сформулированные цели, задачи и результаты исследования.

Диссертация В. В. Подтопельного «Модели и методика определения последовательностей атакующих воздействий на системы искусственного интеллекта при аудите информационной безопасности» включает оригинальные результаты из трех областей: информационной безопасности, математического моделирования и разработки программ. Основной результат – возможность определения наиболее опасных последовательностей атакующих воздействий, что улучшает качество аудита ИБ систем ИИ.

Диссертация состоит из введения, четырех глав, заключения, списка литературы и приложений. Ее объем — 250 страниц, включая 50 рисунков и 20 таблиц.

Во введении представлены ключевые элементы исследования: обозначены объект и предмет изучения, чётко сформулированы цели и задачи работы, перечислены применяемые методы, а также основные тезисы,

которые выносятся на защиту. Кроме того, дано краткое описание структуры работы по главам.

Первая глава посвящена исследованию потенциала моделирования атакующих воздействий посредством марковских процессов принятия решений (МППР). В ней проанализированы:

– особенности проведения аудита систем ИИ;

– классическая постановка задачи моделирования атак;

– сравнительный анализ различных методик.

Во второй главе раскрывается специфика использования МППР для моделирования атак на системы ИИ. Здесь:

– определены функция ценности и функция вознаграждения;

– изложены математические принципы построения графа атаки;

– выделены два режима моделирования — online (с возможностью возврата в предыдущие состояния) и offline (без имитации действий злоумышленника).

Третья глава содержит описание моделей формирования последовательностей атак на базе МППР. В ней представлены:

– типовая модель;

– упрощённые модели;

– подробные модели.

Каждая из моделей предусматривает два режима применения. Ключевым результатом главы стало формальное описание сценария атаки, а также разработка методики аудита систем ИИ.

В четвёртой главе выполнена экспериментальная проверка предложенных моделей. Оценка полноты описания атак проводилась по следующим критериям:

– учёт всех возможных состояний системы;

– охват различных типов действий;

– анализ обратных действий;

– перебор возможных последовательностей атак.

В заключении обобщены результаты проведённого исследования, сформулированы основные выводы и практические рекомендации.

Итогом диссертационной работы стали:

– новые модели, методика, алгоритм определения последовательности атакующих воздействий на системы ИИ при проведении аудита информационной безопасности ИИ систем;

– программные комплексы, реализующие разработанные алгоритмы.

Результаты исследования опубликованы в 17 научных работах, в том числе:

– 5 статей в изданиях, входящих в перечень ВАК;

– 7 свидетельств о государственной регистрации программ.

Научная новизна результатов исследования заключается в следующем (все результаты, выносимые на защиту, являются новыми):

1. Использование аппарата марковских процессов принятия решений (МППР) для обоснования сценариев атак, прогнозирования событий безопасности и улучшения контроля работы систем защиты. Это повысит качество управления информационной безопасностью и оперативность реагирования на угрозы.

2. Совмещение методов анализа признаков событий безопасности для выявления ранее необнаруженных этапов атак на системы с персональными данными. Учитываются топология сети, архитектура подсистем ИИ и методики описания действий атакующего.

3. Разработка моделей и методики определения атакующих последовательностей для сценариев атак на системы с персональными данными, формируемых в процессе аудита информационной безопасности.

Обоснованность и достоверность научных выводов, представленных в диссертации, достигаются благодаря тщательному анализу современных исследований в этой области. Это подтверждается тем, что результаты, полученные с помощью компьютерной реализации, согласуются с теоретическими положениями.

Однако, в материале автореферата недостаточно подробно описаны свойства MITRE ATLAS, которые важны для формирования предлагаемых моделей.

Указанное замечание не снижает общую оценку 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. № 842. Автор заслуживает присуждения ученой степени

кандидата технических наук, что подтверждает его высокий уровень компетентности и фундаментальное знание в области информационной безопасности.

Заведующий кафедрой Информационной безопасности

д.т.н., доцент [redacted] Шакурский Максим Викторович

Федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный университет телекоммуникаций и информатики»
443010, г. Самара, ул. Льва Толстого, д. 23
+7 (846) 333 58 56
info@psuti.ru

Отдел документационного обеспечения

Собственноручную (ые) подпись (и) Шакурского М.В.

Заверяю: начальник ОДО ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики» И.В. Плеханова

12.11 2025