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 стремительной цифровизации корпоративные информационные системы претерпевают значительные трансформации, обусловленные активным внедрением искусственного интеллекта (ИИ) в качестве дополнительной подсистемы. Это, в свою очередь, предъявляет новые требования к методологии и инструментам обеспечения информационной безопасности, что ставит перед специалистами в данной области ряд сложных задач. Традиционные подходы к аудиту и мониторингу, несмотря на свою эффективность в предшествующие периоды, требуют существенной модернизации для адекватного реагирования на вызовы, связанные с развитием ИИ.

Современная парадигма кибербезопасности акцентирует внимание не только на оперативном выявлении текущих угроз, но и на прогнозировании, а также определении особенностей развития потенциальных атак, что требует от аудиторов применения передовых аналитических методов. В этом контексте адаптация аудиторских методик к новым реалиям становится критически важной задачей.

Диссертационное исследование Владислава Владимировича Подтопельного посвящено комплексному анализу актуальных вопросов связанных с выявлением последовательностей атакующих воздействий, что позволяет повысить качество превентивного аудита информационных систем с учетом специфики, обусловленной внедрением ИИ. Автореферат данной работы демонстрирует высокий уровень научной проработки и логической структурированности, включая все ключевые разделы, такие как цели, задачи, методология и результаты исследования.

Основные научные достижения автора включают:

1. Разработка комплексного набора моделей, направленных на выявление критических действий злоумышленников при атаках на элементы систем ИИ. Эти модели базируются на современных метриках уязвимостей, детализированных характеристиках атак и обширной базе знаний (MITRE ATLAS) о действиях злоумышленников как международных, так и отечественных киберпреступников.

2. Формирование методики применения разработанных моделей на различных этапах аудита информационной безопасности. Данная методика позволяет оптимизировать процесс оценки рисков и повысить уровень защищенности корпоративных информационных систем с элементами ИИ.

3. Создание алгоритма имплементации моделей в процесс аудита, что значительно повышает его эффективность и точность выявления потенциальных угроз и уязвимостей, связанных с работой ИИ-систем.

Однако, в работе можно отметить недостатки:

1. внимание акцентируется на атаках, производимых злоумышленником на модели ИИ, в то время как атаки на вычислительную инфраструктуру ИИ рассматриваются опосредованно;

2. в обозначении некоторых величин отсутствует единообразие, в частности, используется одинаковое обозначение «R» для различных сущностей – действий злоумышленника по возврату в пройденные состояния (курсивом - *R*) и функции вознаграждения (без курсива - R), что вносит определённую путаницу, т.к. в табл. 1 автореферата в первом столбце функция вознаграждения (R), вероятность переходов (P) и множество действий (A) вводятся без курсива, а дальше по тексту *A* и *P* используются с курсивом, а R без курсива, кроме второго столбца табл. 1.

Указанные замечания не снижают общую оценку диссертационного исследования. Работа является законченной научно-квалификационной работой, удовлетворяющей критериям Положения о порядке присуждения учёных степеней, а её автор, Подтопельный Владислав Владимирович, заслуживает присвоения ученой степени кандидата технических наук по научной специальности 2.3.6 — Методы и системы защиты информации, информационная безопасность.

С.н.с. Института системной интеграции
и безопасности ТУСУР, к.т.н., доцент [redacted] Конев А.А.

07.11.2025

Подпись Конева А.А. удостоверяю
Учёный секретарь ТУСУР [redacted] Прокопчук Е.В.

Электронная почта: kaa@fb.tusur.ru; контактный телефон: +7(3822) 70-15-29

Федеральное государственное автономное образовательное учреждение высшего образования «Томский государственный университет систем управления и радиоэлектроники», 634050, г. Томск, пр. Ленина, 40.