

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 настоящее время искусственный интеллект (ИИ) интегрирован в инфраструктуру множества предприятий, что породило ряд существенных проблем, связанных с безопасностью их эксплуатации. Экспоненциальный рост ИИ-технологий выявил необходимость разработки новых подходов к аудиту информационных систем (ИС), учитывающих специфику и потенциальные уязвимости, связанные с внедрением ИИ. В контексте обеспечения информационной безопасности (ИБ) критически важно оценивать угрозы ИБ, прогнозировать возможные действия злоумышленников и адаптировать существующие методики аудита ИБ к новым реалиям.

Диссертационная работа, представленная соискателем, направлена на решение части актуальных задач аудита ИБ ИС с учетом интеграции в них ИИ. Решаемые задачи в работе связаны с выявлением наиболее опасных действий, совершаемых во время атаки злоумышленником.

Автореферат демонстрирует структурированность и логичность работы, включающей все необходимые разделы, четко сформулированные цели, задачи и результаты. К ключевым научным достижениям диссертации можно отнести следующие:

1. Разработку моделей, позволяющих выявлять опасные последовательности действий злоумышленников при атаках на системы ИИ. При этом учитываются: уровень детализации действий, специфика современных метрик уязвимостей, а также международных и отечественных баз знаний о действиях злоумышленников.

2. Методику применения предложенных моделей в рамках последовательности этапов аудита ИБ инфраструктуры предприятий и организаций.

3. Алгоритм использования предложенных моделей для повышения результативности аудита ИБ.

Эти результаты не только обладают научной новизной, но и имеют практическую значимость для повышения уровня защищенности ИС с системами ИИ.

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

В качестве замечания следует отметить: из материала автореферата недостаточно ясно, какова специфика прототипов, с которыми производится сравнение разработанных автором моделей.

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 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.

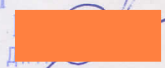
Отзыв подготовила:

Профессор кафедры информационной безопасности банковских систем института интеллектуальных кибернетических систем НИЯУ МИФИ,
доктор технических наук, доцент,
Тел. +79166776599, email: NGMiloslavskaya@mephi.ru

 Милославская Наталья Георгиевна

Докторская диссертация защищена по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Даю согласие на обработку персональных данных.

Подпись Милославской Н.Г.  заверяю:



МК ОТДЕЛА
УВ
ОВА

26 октября 2025 г.

Адрес места основной работы:

Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский ядерный университет «МИФИ»,
НИЯУ МИФИ

115409, г. Москва, Каширское шоссе, д. 31,

www.mephi.ru, тел. +74957885699, email: info@mephi.ru