

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 цифровой трансформации и активного внедрения искусственного интеллекта в корпоративные информационные системы, методология и инструменты обеспечения кибербезопасности претерпевают значительные изменения. Это предъявляет новые, более сложные требования к специалистам в данной области, вынуждая их адаптироваться к изменяющимся реалиям и разрабатывать инновационные подходы к проведению аудита и мониторинга систем искусственного интеллекта. Традиционные методы, хотя и были эффективны в прошлом, в настоящем не способны адекватно реагировать на вызовы, связанные с усложнением угроз.

Современная концепция информационной безопасности акцентирует внимание не только на оперативном выявлении текущих угроз, но и на прогнозировании потенциальных атак. Это требует применения передовых аналитических и прогностических моделей. В этой связи адаптация аудиторских методик к специфике искусственного интеллекта в корпоративных информационных системах приобретает критическое значение, требуя разработки новых алгоритмов и моделей для оценки рисков и уязвимостей.

Диссертационное исследование Владислава Владимировича Подтопельного представляет собой всесторонний анализ актуальных вопросов аудита информационных систем с учетом особенностей, связанных с интеграцией искусственного интеллекта в данные системы.

Автореферат исследования демонстрирует высокий уровень научной проработки и четкой структурированности, включая ключевые разделы, такие как цели, задачи, методология и результаты работы.

Основные научные достижения автора включают:

1. Разработку комплексного набора моделей для выявления действий злоумышленников при атаках на информационные системы, содержащие элементы искусственного интеллекта. Эти модели основаны на новейших метриках уязвимостей, детальном анализе характеристик атак и обширной базе знаний о действиях киберпреступников MITRE ATLAS.

2. Формирование методики использования указанных моделей на различных этапах аудита информационной безопасности, что позволяет оптимизировать процесс оценки рисков и повысить уровень защищенности корпоративных информационных систем.

3. Создание алгоритма применения разработанных моделей в процесс аудита, что существенно повышает эффективность и точность выявления потенциальных угроз и уязвимостей, связанных с функционированием систем, основанных на технологиях искусственного интеллекта.

Однако, из автореферата не ясно, каким образом в моделях учитывается специфика распространенных в России подходов и методик формирования сценариев атак.

Указанное замечание не снижает общую оценку диссертационного исследования. 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 представленной диссертационной работы, В.В. Подтопельный, заслуживает присуждения ученой степени кандидата технических наук, что подтверждает его высокий уровень компетентности и фундаментальное знание в области информационной безопасности.

Заведующий кафедрой основ радиотехники и защиты информации,
кандидат технических наук, доцент



Петров Виктор Иванович

ФГБОУ ВО «Московский государственный технический университет гражданской авиации» (МГТУ ГА)

Почтовый адрес: Кронштадтский бульвар, д. 20, Москва, 125993.

Тел. (499) 459-0701. Сайт: www.mstuca.ru.

Email: info@mstuca.ru

Подпись заведующего кафедрой основ радиотехники и защиты информации
ФГБОУ ВО "Московский государственный технический университет гражданской

технических наук,
ГБОУ МГТУГА,

1911,

О.Г. Феоктистова