# Отзыв

на автореферат диссертации Подтопельного Владислава Владимировича на тему «Модели и методика определения последовательностей атакующих воздействий на системы искусственного интеллекта при аудите информационной безопасности»,
представленной на соискание учёной степени кандидата технических наук по научной специальности 2.3.6. – Методы и системы защиты информации, информационная безопасность

Диссертационное исследование Подтопельного В.В. посвящено актуальной проблеме в области обеспечения защиты систем искусственного интеллекта (СИИ), особенно решению задач аудита информационной безопасности СИИ.

В работе представлен детальный анализ различных методов и методик выявления и анализа вредоносных воздействий на СИИ, что позволило автору обосновать возможность, с целью своевременного выявления угроз при проведении аудита безопасности, использовать методы марковских процессов принятия решений (МППР).

Подходя к проблеме проведения аудита с позиций формализации последовательности действий злоумышленника, автор проводит анализ атакующих воздействий на СИИ, создает модели на основе МППР, позволяющие построить сценарии компьютерных атак с разным уровнем детализации действий злоумышленника, как последовательности событий безопасности. При этом учитываются особенности типовой инфраструктуры СИИ, порядок доступности инфраструктурных компонентов на логическом и физическом уровне. Автор акцентирует внимание на превосходстве методов Value Iteration над другими методами МППР при решении задач построения последовательности, как наиболее простой, с точки зрения применимости.

Очевидна научная новизна результатов диссертационного исследования, которая заключается в формировании новых подходов в сфере аудита информационной безопасности СИИ, и, в частности, в сфере построения

сценариев атак, что позволяет повысить защищенность системы путем перекрытия заранее определённых путей атакующих воздействий.

Обращаясь к теоретической базе исследования, стоит отметить проведенный автором глубокий анализ зарубежных и отечественных источников информации о действиях нарушителей (база знаний MITRE и ФСТЭК России). Особого внимания заслуживает конструирование и разработка моделей с применением последовательностей техник и тактик MITRE ATLAS.

Также следует выделить различные режимы моделирования, вносимые в методику применения моделей. Это позволяет регулировать меру точности и учитывать человеческий фактор при определении наиболее опасных последовательностей действий злоумышленника.

Практическая реализация разработанных моделей, методик и алгоритмов для оценки различных сценариев компьютерных атак позволяет, при проведении аудита информационной безопасности СИИ, своевременно выявлять возникающие угрозы. Эффективность работы предложенных алгоритмов была подтверждена при проведении имитационного моделирования, результаты которого были представлены в четвертой главе работы.

Основные положения диссертационной работы нашли отражение в публикациях в научных специализированных изданиях, в том числе 5 научных работ опубликованы в изданиях, рекомендованных ВАК РФ, в материалах международных конференций. Получено 7 свидетельств о регистрации программ для ЭВМ.

В качестве замечаний к представленной работе следует отметить, что по тексту автореферата не достаточно ясно, каким образом проверяется на значимость каждое действие с учетом его стоимости (стр.17), а также порядок определения адаптивности сравниваемых моделей (стр. 21, табл. 2).

Однако, указанные замечания не снижают общую положительную оценку диссертационной работы.

Исходя из выше изложенного, можно констатировать, что диссертация Подтопельного Владислава Владимировича является завершенной научно-

квалификационной работой, по своему содержанию соответствует требованиям «Положения о порядке присуждения ученых степеней», утвержденного Постановлением Правительства РФ от 24.09.2013 № 842, предъявляемым к кандидатским диссертациям, а соискатель Подтопельный Владислав Владимирович заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 Методы и системы защиты информации, информационная безопасность.

Профессор кафедры “Информационной безопасности”,
кандидат технических наук, доцент [redacted] Серпенинов Олег Витальевич

13.11.2025

Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)», www. rsue.ru
Адрес: ул. Большая Садовая, д. 69, г.Ростов-на-Дону, Ростовская обл., 344002
Тел.: 8(863) 263-30-80
Email: main@rsue.ru

ФГБОУ ВО «Ростовский государственный экономический университет (РИНХ)»
УДОСТОВЕРЯЮ
Начальник управления по работе с персоналом и кадровой политике
Е.В Королева