ОТЗЫВ

На автореферат диссертации Ушакова Игоря Александровича «Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

В настоящее время наблюдается стремительный рост атак на информационные структуры предприятий. Все больше организаций сталкиваются с инсайдерскими атаками – когда злоумышленник выполняет деструктивные действия, находясь внутри периметра организации, часто маскируя свои действия под действия легитимных пользователей. Следовательно, становится значительно сложнее обнаруживать нарушителей и, соответственно, организации несут значительные финансовые и репутационные убытки. Таким образом, диссертационное исследование, которое направлено на обнаружение инсайдеров в компьютерных сетях с использованием комбинированного подхода на основе экспертных правил, методов машинного обучения и обработки больших данных является крайне актуальным.

Теоретическая значимость диссертационной работы определяется ее вкладом в дальнейшее развитие теории и методов информационной безопасности. В частности, автор выносит на защиту следующие положения:

1. Модель представления больших данных об инсайдерских атаках в формате NoSQL, обеспечивающая хранение и анализ признаков пользователей в компьютерных сетях в различные моменты времени.
2. Модель и алгоритмы комбинированного применения экспертных правил и методов машинного обучения в интересах обнаружения инсайдерских атак.
3. Методика обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных.
4. Архитектура и программная реализация системы обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных.

Полученные результаты могут применяться при формировании систем обеспечения информационной безопасности предприятий.

Обоснованность и достоверность результатов подтверждается рядом экспериментов по оценке показателя обоснованности каждого из вариантов комбинирования алгоритмов для каждой группы сценариев, апробацией результатов работы на конференциях всероссийского и международного уровня, а также публикацией основных научных результатов в 40 печатных работах, в том числе 9 – в рецензируемых изданиях из перечня ВАК, 2 – в изданиях, индексируемых в

международных базах Scopus и Web of Science, наличием 3 свидетельств о регистрации программ для ЭВМ.

По содержанию автореферата имеются следующие замечания:

1. В автореферате при описании алгоритма, основанного на экспертных правилах указано, что правила создаются экспертами с учетом собственного накопленного опыта и существующих «лучших практик». Однако, непонятно какой квалификацией должны обладать эксперты и по какому принципу они выбирались.
2. В тексте автореферата не раскрыты атрибуты пользователей, входящих в кортеж $Users_i$.

Указанные недостатки не снижают теоретической и практической ценности полученных результатов.

В целом, судя по автореферату и публикациям, диссертация Ушакова И.А., выполненная на тему: «Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных» представляет собой самостоятельную научно-квалификационную работу, в которой представлена и решена актуальная научная задача по разработке модельно-методического аппарата для обнаружения инсайдеров в КС на основе комбинированного использования экспертных правил, методов машинного обучения и обработки больших данных.

Исследование Ушакова И.А. удовлетворяет требованиям п. 9-14 Положения о присуждении учёных степеней, утвержденного постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 года, предъявляемым к кандидатским диссертациям.

Считаю, что Ушаков И.А. заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Советник генерального [redacted] АО «ЭВРИКА»
д.т.н., доцент Суханов Андрей Вячеславович
03.04.2020

Почтовый адрес: 19608[redacted] сковский пр., д. 118
Тел.: (812) 718-61-91
E-mail: avsuhanov@eureca.ru

Подпись Суханова А.В. удостоверяю
Начальник управления кадров и
документационного обеспечения АО «ЭВ

А.В. Дмитриченко