Общество с ограниченной ответственностью
НИЕНШАНЦ - ЗАЩИТА

07.05.2020 г.
г. Санкт-Петербург

Генеральный директор
Е. Баранов

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»

Обнаружение инсайдеров в компьютерных сетях является крайне актуальной задачей. Развитие информационных технологий и разработка современного программного обеспечения позволяют злоумышленникам использовать новые методы для выполнения сетевых атак. Комбинирование алгоритмов на основе экспертных правил и методов машинного обучения одновременно с технологиями обработки больших данных позволяет эффективно решать задачу обнаружения инсайдерских сессий в компьютерных сетях с учетом роста трафика пользователей.

В диссертации выполнено исследование применения комбинированного подхода на основе экспертных правил, методов машинного обучения и обработки больших данных для обнаружения инсайдеров в компьютерных сетях. С этой целью получено четыре научных результата, обладающих новизной и практической значимостью. Это подтверждается выполненным анализом современного состояния затронутой темы, наличием девяти работ, опубликованных в рецензируемых изданиях из перечня ВАК, а также двух работах в изданиях, индексируемых в международных базах Scopus и Web of Science. Кроме того, автором получено три свидетельства о государственной регистрации программ для ЭВМ.

Среди выявленных в автореферате недостатков отмечаю следующие:

1. Из автореферата не понятна роль применяемого MapReduce алгоритма во втором этапе разработанной методики.
2. Не ясно отличие используемых терминов "инсайдер КС" и "внутренний нарушитель КС".

3. На рисунке 1 на блок схеме определения аномалий в качестве проверки используется критерий "нестандартное устройство", однако отсутствует описание методики классификации устройств на стандартные и нестандартные.

Указанные выше недостатки не влияют на положительное восприятие полученных автором результатов. Выполненное исследование является логически завершенным и содержит непротиворечивые выводы. На основе полученных экспериментальных результатов поставленная автором цель достигается.

Считаю, что представленная в автореферате диссертационная работа соответствует требованиям п. 9-14 «Положения о присуждении учёных степеней», предъявляемым к кандидатским диссертациям, а ее автор Ушаков Игорь Александрович заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Начальник производственно-технического отдела
ООО «Ниеншанц-Защита»
Кандидат технических наук Мурашов Сергей Викторович

07.05.2020 г.

Почтовый адрес: 194044, Санкт-Петербург, Б. Сампсониевский пр.,64
Тел.: (812) 542-91-46
E-mail: info@n-z.spb.ru