Акционерное общество
«Лаборатория противодействия промышленному шпионажу»
(АО «Лаборатория ППШ»)

199178, Россия, Санкт-Петербург, наб.реки Смоленки, д.25, лит.Е, пом.31 т. (812) 702-7383; ф.: (812)309-4509
e-mail: lab@pps.ru http://www.pps.ru

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»

Целью исследования Ушакова И.А. является повышение защищенности компьютерных сетей (КС) за счет усовершенствования моделей, алгоритмов и методики обнаружения инсайдеров в КС с использованием комбинирования экспертных правил, методов машинного обучения и способов обработки больших данных. Работа, безусловно, является актуальной, так как в случае успешной реализации инсайдерских атак организации могут понести значительные убытки. Применение предложенных методик, моделей, алгоритмов поиска и обнаружения инсайдеров в информационно-телекоммуникационных сетях с использованием методов машинного обучения, способов обработки больших данных и комбинирования экспертных правил позволяет повысить вероятность выявления инсайдеров и снизить риски нарушения сетевой безопасности организации.

В своей работе Ушаков И.А. исследует модели, алгоритмы и метод обеспечения обнаружения инсайдеров в компьютерных сетях. Основными результатами работы являются:

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.

Теоретическая значимость исследования определяется новизной полученных результатов. вкладом в дальнейшее развитие теории и методов информационной безопасности, что проявляется в следующих аспектах: расширены классы атрибутов, необходимых для обнаружения инсайдеров; предложен новый подход к комбинированию двух классов алгоритмов, основанных на экспертных правилах и на методах машинного обучения, для решения задачи обнаружения инсайдеров в КС; методика обнаружения инсайдеров реализует последовательность операций, необходимых для решения задачи обнаружения инсайдеров, основывается на модели в формате NoSQL, алгоритмах, основанных на экспертных правилах, а также алгоритмах, основанных на методах машинного обучения; архитектура программного комплекса системы обнаружения инсайдеров реализует совокупность компонентов, их взаимосвязь, процедуру их выполнения и программную реализацию для решения задачи обнаружения инсайдеров в КС; архитектура основана на модели в формате NoSQL, алгоритмах, основанных на экспертных правилах и методах машинного обучения, предложенных в диссертации.

Практическая значимость исследования подтверждается апробацией полученных результатов работы на 12-ти научных и практических конференциях, в том числе международных. По материа-

лам исследования опубликовано 40 работ, в том числе 9 – в рецензируемых изданиях из перечня ВАК, 2 – в изданиях, индексируемых в международных базах Scopus и Web of Science, получено 3 свидетельства о государственной регистрации программ для ЭВМ.

По содержанию автореферата имеются следующие замечания:

1. В автореферате модель инсайдера раскрыта на концептуальном уровне, в частности не понятны критерии определения атрибутов инсайдера, уровни доступа, квалификация инсайдера, цель инсайдера.
2. В автореферате из блок-схемы алгоритма определения аномалий на основе экспертных правил (рисунок 1) неясно, что делают Подпрограммы A, B, C, D, E.
3. Согласно рисунку 4 - сбор информации осуществляется с серверов AAA, AD, DNS, DHCP, однако в автореферате не указывается, каким образом осуществляется сбор информации и с использованием каких протоколов, а также не указывается - используются ли при этом протоколы Syslog, SNMP и Netflow / SFlow.
4. Не раскрыто понятие кибербезопасности применительно к тематике исследования.

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. Указанные недостатки не снижают теоретической и практической ценности полученных результатов. Исследование Ушакова И.А. удовлетворяет требованиям п. 9-14 Положения о присуждении учёных степеней, 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».

Заместитель генерального дирек
по научной работе АО «Лаборат
Кандидат технических наук, доц **Лысов Андрей Владимирович**

Почтовый адрес: 199178, г.Санкт-Петербург, наб. реки Смоленки, д.25, лит.Е
Тел.: (812)309-59-44, (812)702-73-83
E-mail: Lab@pps.ru