ЗАКЛЮЧЕНИЕ

экспертной комиссии диссертационного совета Д.002.199.01 по кандидатской диссертации Ушакова Игоря Александровича на тему: «Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных», научный руководитель – д.т.н., профессор, главный научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН Котенко И.В.

Экспертная комиссия диссертационного совета Д.002.199.01 в составе: д.т.н., проф. Молдовян А.А. (председатель), д.т.н., проф. Молдовян Н.А., д.т.н., проф. Саенко И.Б. после ознакомления с кандидатской диссертацией Ушакова Игоря Александровича на тему: «Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных» сделала вывод о том, что диссертационная работа Ушакова И.А. посвящена решению актуальной научной задачи: разработки модельно-методического аппарата для обнаружения нарушителей информационной безопасности в КС внутреннего периметра (инсайдеров) на основе комбинированного использования экспертных правил, методов машинного обучения и обработки больших данных.

Целью исследования 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. Значительная практическая значимость и недостаточная научная проработка проблемы определили выбор темы, ее актуальность, цель, задачи, основные направления и содержание диссертационного исследования.

Основными результатами работы являются:

1. Модель представления больших данных об инсайдерских атаках в формате NoSQL, отличающаяся от существующих возможностью обеспечения хранения и анализа признаков пользователей, полученных на базе UBA/UEBA-аналитики и характеризующих потенциальную инсайдерскую деятельность в компьютерных сетях, а также возможностью учета динамики изменения этих признаков.
2. Модель и алгоритмы комбинированного применения экспертных правил и методов машинного обучения в интересах обнаружения инсайдерских атак, отличающиеся от существующих комплексным подходом к решению задачи обнаружения инсайдеров с учетом признаков и свойств пользователей, устройств, приложений, сервисов, включая параметр времени.
3. Методика обнаружения инсайдеров, отличающаяся от существующих использованием предложенной модели представления больших данных об инсайдерских атаках, а также предложенных модели и алгоритмов комбинированного применения экспертных правил, методов машинного обучения и обработки больших данных.
4. Архитектура и программная реализация системы обнаружения инсайдеров в компьютерных сетях, отличающаяся от известных архитектур и программных средств использованием предложенной методики обнаружения инсайдеров, обеспечивающей комбинированное применение технологий обработки больших данных, экспертных правил и методов машинного обучения.

Практическая значимость диссертационной работы определяется значимостью полученных результатов и состоит в следующем:

- модель представления больших данных об инсайдерских атаках является основой для формализации данных и знаний о пользователях, устройствах, приложениях и сервисах в КС;

- модель и алгоритмы комбинированного применения экспертных правил и методов машинного обучения позволяют оперировать большими объемами данных и выявлять инсайдеров для достижения наилучших показателей эффективности; произведена настройка алгоритмов на основе методов машинного обучения по типовым сценариям инсайдеров в КС; обосновано комбинированное применение алгоритмов обнаружения инсайдеров;

- методика обнаружения инсайдеров повышает эффективность обнаружения внутренних нарушителей в КС (оперативность – за счет использования обработки больших данных; результативность – за счет совместного использования алгоритмов на основе экспертных правил и методах машинного обучения, ресурсоэкономность – за счет новых высокотехнологичных программно-аппаратных решений);

- архитектура и программная реализация способствует эффективному обнаружению инсайдеров в КС с использованием предложенной методики обнаружения инсайдеров, обеспечивающей комбинированное применение технологий обработки больших данных, экспертных правил и методов машинного обучения.

Достоверность и обоснованность научных положений, основных выводов и результатов диссертации обеспечиваются тщательным анализом состояния исследований в данной области, подтверждается согласованностью результатов, полученных при экспериментах, успешной апробацией на ряде научных конференций всероссийского и международного уровня, и публикацией в ведущих рецензируемых научных изданиях.

Материалы и основные результаты кандидатской диссертации Ушакова И.А. удовлетворяют п.3 паспорта специальности: 05.13.19 – «Методы и системы защиты информации, информационная безопасность», по которой диссертационному совету Д.002.199.01 предоставлено право проведения защит диссертаций.

Основные научные результаты диссертации удовлетворяют требованиям, предусмотренным пунктами 11 и 13 Положения о присуждении ученых степеней: по материалам диссертационной работы опубликовано 40 научных работ, в том числе 19 статей, из которых 9 статей в рецензируемых изданиях из перечня ВАК («Вопросы кибербезопасности», «Защита информации. Инсайд», «Труды СПИИРАН», «Труды учебных заведений связи»).

Недостоверные сведения о работах, в которых изложены основные научные результаты диссертации, опубликованных соискателем ученой степени, отсутствуют.

Текст диссертации, представленной в диссертационный совет, идентичен тексту диссертации, размещенной на сайте СПИИРАН.

Объем оригинального текста диссертационной работы составляет не менее 89%; цитирование оформлено корректно. Требования, установленные пунктом 14 Положения о присуждении ученых степеней, соблюдены: заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не обнаружено; научных работ, выполненных соискателем ученой степени в соавторстве, без ссылок на соавторов, не выявлено.

Комиссия предлагает:

1. Принять кандидатскую диссертацию Ушакова И.А. к защите на диссертационном совете Д.002.199.01 как соответствующую профилю диссертационного совета по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

2. В качестве официальных оппонентов назначить специалистов по данной проблеме: д.т.н., проф. Синещука Ю.И., к.т.н., доц. Ефимова В.В.
3. В качестве ведущей организации утвердить АО «Научно-исследовательский институт «Рубин».
4. Разрешить Ушакову И.А. опубликовать автореферат и утвердить список рассылки авторефератов.
5. Защиту диссертации назначить на «28» апреля 2020 г.

Члены комиссии: д.т.н., проф. Молдовян А.А.

д.т.н., проф. Молдовян Н.А.

д.т.н., проф. Саенко И.Б.