ЗАКЛЮЧЕНИЕ

экспертной комиссии диссертационного совета Д.002.199.01 по кандидатской диссертации Браницкого Александра Александровича на тему: «Обнаружение аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта», 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. Осипова В.Ю. (председатель), д.т.н., проф. Воробьева В.И., д.т.н., проф. Молдовяна Н.А. после ознакомления с кандидатской диссертацией Браницкого Александра Александровича на тему: «Обнаружение аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта» сделала вывод о том, что диссертационная работа Браницкого А.А. посвящена решению актуальной научной задачи: обнаружения аномальных соединений в сетевом трафике с использованием подхода, основанного на комбинировании разнородных классификаторов и направленного на повышение показателей эффективности функционирования системы обнаружения атак.

Целью исследования является повышение эффективности функционирования системы обнаружения атак на основе подхода «гибридизация методов вычислительного интеллекта». Выбор темы, ее актуальность, цель, задачи, направления и содержание диссертационного исследования обусловлены необходимостью разработки гибкой методики объединения разнородных классификаторов в контексте обнаружения аномальных сетевых соединений.

Практическую значимость исследования составляют разработанные в диссертации модель, алгоритм и методика, которые обеспечивают решение актуальной научно-технической задачи, направленной на повышение эффективности функционирования системы обнаружения атак за счет использования методики, позволяющей выбрать наилучшую схему комбинирования классификаторов, и вносят значительный вклад в развитие принципов построения систем обнаружения атак и оценки эффективности их функционирования. Результаты исследования используются в рамках европейского проекта программы TEMPUS и внедрены в СПбГУТ и ИТМО.

Использование разработанной методики гибридизации бинарных классификаторов обеспечивает возможность объединения разнородных средств обнаружения сетевых атак, таких как сигнатурный анализ и адаптивные методы вычислительного интеллекта, для построения распределенной системы обнаружения атак. Согласно разработанной методике интеллектуальное ядро системы обнаружения атак адаптируется под выявление разнообразных типов атак, позволяет комбинировать бинарные классификаторы, разрешать конфликты, формировать входные сигналы для классификаторов, выполнять обход дерева классификаторов для соотнесения подозрительного сетевого соединения к тому или иному классу.

Достоверность и обоснованность научных положений, основных выводов и результатов диссертации обеспечиваются детальным анализом современного состояния исследований в рассматриваемой области, подтверждаются согласованностью теоретических результатов с экспериментальными результатами, публикацией в ведущих рецензируемых российских и зарубежных журналах, регистрацией программ для ЭВМ.

Материалы и основные результаты кандидатской диссертации Браницкого А.А. удовлетворяют паспорту 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 опубликована 21 научная работа, в том числе 6

статей в периодических журналах, рекомендованных ВАК (журналы «Информационно-управляющие системы», «Проблемы информационной безопасности. Компьютерные системы», «Труды СПИИРАН», «Защита информации. Инсайд»).

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 95%; 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 Браницкого А.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., доц. Комашинского В.И., д.т.н., доц. Шерстюка Ю.М.
3. В качестве ведущей организации утвердить ОАО «Информационные телекоммуникационные технологии».
4. Разрешить Браницкому А.А. опубликовать автореферат и утвердить список рассылки авторефератов.
5. Защиту диссертации назначить на «09» октября 2018 г.

Члены комиссии:

роф. Осипов В.Ю.

роф. Воробьев В.И.

роф. Молдовян Н.А.