ЗАКЛЮЧЕНИЕ

экспертной комиссии диссертационного совета 24.1.206.01 по кандидатской диссертации Крибеля Александра Михайловича на тему: «Выявление аномалий и классификация компьютерных атак в сети передачи данных на основе применения фрактального анализа и методов машинного обучения», научный руководитель – д.т.н., профессор кафедры Комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С. О. Макарова Лаута О.С.

Экспертная комиссия диссертационного совета 24.1.206.01 в составе: д.т.н., проф. Саенко И.Б. (председатель), д.т.н., проф. Осипова В.Ю., д.т.н., проф. Котенко И.В. после ознакомления с кандидатской диссертацией Крибеля Александра Михайловича на тему: «Выявление аномалий и классификация компьютерных атак в сети передачи данных на основе применения фрактального анализа и методов машинного обучения» сделала вывод о том, что диссертационная работа Крибеля А.М. посвящена решению актуальной научной задачи: разработка аналитической модели и методик выявления аномалий и классификация компьютерных атак в сетевом трафике сети передачи данных на основе применения фрактального анализа и методов машинного обучения.

Целью исследования является повышение эффективности выявления аномалий и классификации компьютерных атак в сетевом трафике сети передачи данных. Значительная практическая значимость и недостаточная научная проработка проблемы определили выбор темы, ее актуальность, цель, задачи, основные направления и содержание диссертационной работы.

Практическую значимость исследования составляют разработанные аналитическая модель и методики представляют собой научно-методическую основу, практическая реализация которой позволяет описать различные типы трафика в сетях передачи данных, определять аномальные активности, основываясь на принципах самоподобия, и, исходя из типа трафика с применением различных методов машинного обучения, выявлять компьютерные атаки. Разработанные методики являются математической основой системы раннего обнаружения компьютерных атак, основанные на обнаружении аномалий в сетях передачи данных и принятии эффективных мероприятий по защите с применением нейронной сети автокодировщика, состоящей из ячеек с долгой краткосрочной памятью и управляющим рекуррентным блоком. При этом повышается оперативность, точность и полнота выявления аномалий в сетях передачи данных, что позволяет на практике эффективно применять разработанный подход в системах глубокой проверки сетевых пакетов в сетях передачи данных.

Результаты проведенного исследования нашли практическое применение в разработках, в которых автор принимал личное участие. О реализации основных результатов проведенного исследования имеются 3 акта о реализации в НИР «Корвет», «Потенциал-2018», «Свертка-СМ» (ФГКВОУ ВО «Военная орденов Жукова и Ленина Краснознаменная академия связи им. С.М. Буденного») и 1 акт о реализации в ОКР «Опорник» (ПАО «Информационные и теле-коммуникационные технологии»

Достоверность и обоснованность научных положений, основных выводов и результатов диссертации подтверждаются результатами вычислительных экспериментов, их сравнением с результатами других исследователей, практической апробацией разработанных модели и методик, а также одобрением основных положений диссертации на научно-технических конференциях, публикациями в ведущих рецензируемых журналах, внедрением результатов работы.

Материалы и основные результаты кандидатской диссертации Крибеля А.М. удовлетворяют паспорту специальности: 2.3.6 – «Методы и системы защиты информации, информационная безопасность», по которой диссертационному совету 24.1.206.01 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 17 работ, среди которых 6 статей, индексируемые в международных базах данных Web of Science и/или Scopus; 10 статей в рецензируемых научных изданиях, входящих в перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук (журналы «Электросвязь»; «Известия Тульского государственного университета. Технические науки»; «Наукоемкие технологии в космических исследованиях Земли»; «Робототехника и техническая кибернетика»; «Первая миля»); одно свидетельство о государственной регистрации программы для ЭВМ.

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 СПб ФИЦ РАН.

Объем оригинального текста диссертационной работы составляет не менее 87%; 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 Крибеля А.М. к защите на диссертационном совете 24.1.206.01 как соответствующую профилю диссертационного совета по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность (технические системы).
2. В качестве официальных оппонентов назначить специалистов по данной проблеме: д.т.н., проф. Гречишников Е.В., д.т.н., проф. Бирюкова Д.Н.
3. В качестве ведущей организации утвердить Акционерное общество «Информационные технологии и коммуникационные системы».
4. Разрешить Крибелю А.М. опубликовать автореферат и утвердить список рассылки авторефератов.
5. Защиту диссертации назначить на «18» мая 2023 г.

Члены комиссии:

д.т.н., проф. Саенко И.Б.

д.т.н., проф. Осипов В.Ю.

д.т.н., проф. Котенко И.В.