Акционерное общество
«Информационные технологии
и коммуникационные системы»
(АО «ИнфоТеКС»)
Юридический адрес:
улица Мишина, дом 56, стр.2,
этаж 2, пом. IX, комната 29
Москва, 127083
Почтовый адрес:
а/я № 80, улица Отрадная, дом 2Б, стр. 1
Москва, 127273
Тел. (495)737-61-92, факс (495)737-72-78
e-mail: soft@infotecs.ru
http://www.infotecs.ru
ОГРН 1027739185066
ИНН/КПП 7710013769/771401001

25 АПР 2023 № 11-2023-0345/1

На №.....от.....

УТВЕРЖДАЮ:
Генеральный директор
АО «ИнфоТеКС»

А.А. Чапчаев

«25» апреля 2023 г.

005178

ОТЗЫВ

ведущей организации АО «Информационные технологии и коммуникационные системы» на диссертацию Крибеля Александра Михайловича на тему «Выявление аномалий и классификация компьютерных атак в сети передачи данных на основе применения фрактального анализа и методов машинного обучения», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

На сегодняшний день сети передачи данных (СПД), относящиеся к сетям связи общего пользования (ССОП), это сложные системы, которые осуществляют или обеспечивают выполнение функционала, нарушение выполнения которого может привести к необратимым негативным последствиям в социальной, экономической, политической, информационной, экологической и иных сферах.

В силу специфики развития и масштабирования сети передачи данных предоставляют практически неограниченные возможности для активной деятельности технической компьютерной разведки (ТКР). Проводимый анализ показывает, что система ТКР способна перехватывать большие объемы сетевого

трафика, анализировать его и выявлять демаскирующие признаки (ДМП) элементов функционирующих систем связи критически важных объектов. Таким образом, беспрепятственный сбор информации об СПД вероятным противником ведет к осуществлению компьютерных атак (КА), направленных на вывод из строя злоумышленниками систем, поддерживающих жизнеобеспечение человечества и возникновению глобальных техногенных катастроф.

Всё вышеизложенное определяет актуальность диссертационной работы, базирующейся на классических и современных достижениях теории систем, теории вероятностей, теории математического моделирования и статистики, теории искусственных нейронных сетей.

Диссертация Крибеля А.М. представляет собой самостоятельную научно-квалификационную работу, направленную на решение актуальной научной задачи, заключающейся в разработке научно-методического аппарата, позволяющего исследовать процесс функционирования сети передачи данных в условиях компьютерных атак.

В ходе решения научной задачи разработаны следующие положения, выносимые на защиту:

1. Модель выявления аномалий в сетевом трафике сети передачи данных в условиях компьютерных атак.

2. Методика раннего обнаружения аномалий в сетевом трафике сети передачи данных.

3. Методика классификации компьютерных атак в сетевом трафике сети передачи данных.

4. Архитектура и программные компоненты системы раннего обнаружения и классификации компьютерных атак в сетевом трафике сети передачи данных.

Объектом исследования в работе выбраны сети передачи данных в условиях компьютерных атак.

Предметом исследования являются модели, методики и алгоритмы выявления аномалий и классификации компьютерных атак в сетях передачи данных.

Во **введении** автором обоснована актуальность работы, определены объект и предмет исследования, сформулирована цель, раскрыто содержание научной задачи, перечислены результаты, выносимые на защиту, раскрыта их научная новизна, теоретическая и практическая значимость, представлены сведения об апробации, публикациях и реализации результатов исследования.

Основным содержанием **первой главы** является анализ предметной области, заключающийся в исследовании особенностей функционирования СПД в условиях КА. Рассмотрены роль и место СПД как технической основы информационного обмена, представлена модель угроз ресурсам сети передачи данных.

Сформулирована вербальная модель КА и определены основные узлы СПД, на которые оказывается последовательное воздействие в виде компьютерных атак (КА), целью которых является выявление перечня критических уязвимостей в системе информационной безопасности СПД.

Проанализированы системные недостатки используемого научно-методологического аппарата СПД в условиях КА. Обоснованы постановка задачи и границы исследования. На основе проведенного анализа и выявленных противоречий определена структура работы, намечены основные пути решения частных задач исследования.

Вторая глава диссертации посвящена рассмотрению первого научного результата, выносимого на защиту. Его суть заключается в разработке модели выявления аномалий в сетевом трафике СПД в условиях КА, которая позволяет обрабатывать как стационарный, так и нестационарный сетевой трафик в режиме близкого к реальному времени, выявлять аномалии сетевого трафика, вызванные ведением КА.

В процессе изложения модели выявления аномалий в сетевом трафике СПД в условиях КА автор предположил, что воздействие компьютерных атак приводит к появлению в СПД аномальной активности трафика. Для обнаружения

аномальной активности трафика в СПД необходимо учитывать наличие большого количества сетевых маршрутов, на которых периодически возникают резкие колебания задержки в передаче данных и большие потери пакетов, появление новых свойств сетевого трафика.

В предложенной модели первым этапом на основе применения теста Дики-Фуллера проверяется стационарность временного ряда, далее методом нормированного размаха (*R/S*-анализ) определяется степень самоподобия сетевого трафика. С помощью разработанных программных средств проведена серия экспериментов для различных параметров сетевого трафика, которые подтвердили наличие свойств самоподобия, а также их нарушение при воздействии компьютерных атак.

Научная новизна первого научного результата состоит в том, что разработанная модель позволяет обрабатывать как стационарный, так и не стационарный сетевой трафик (временной ряд), выявлять аномалии в режиме близкого к реальному масштабу времени и на основе этого прогнозировать этапы компьютерной атаки.

Второй научный результат, выносимый на защиту, представлен в **третьей главе**. Автор разработал методику раннего обнаружения аномалий в сетевом трафике СПД, позволяющую обнаруживать КА на раннем этапе их проявления с помощью методов машинного обучения для стационарного сетевого трафика СПД и фрактального анализа для нестационарного. Для методики были определены исходные данные, показатели, критерии и допущения.

С помощью программных средств получены численные значения точности классификации КА для стационарного сетевого трафика СПД с помощью методов машинного обучения и результаты фрактального анализа для нестационарного.

Научная новизна второго результата состоит в том, что разработанная система раннего обнаружения аномалий в сетевом трафике СПД в отличие от известных позволяет с минимальным количеством ложных срабатываний

определить КА, а также способность выявлять КА в режиме времени, близкого к реальному. Особенностью методики является модель автокодировщика, позволяющая выявлять КА «нулевого дня».

В четвертой главе диссертации раскрывается третий и четвёртый научный результат, выносимый на защиту. В данном разделе представлены: методика классификации компьютерных атак в сетевом трафике сети передачи данных, а также архитектура и программные компоненты системы раннего обнаружения и классификации компьютерных атак в сетевом трафике сети передачи данных. Спецификой предложенной методики является то, что обнаружение КА производится с использованием автокодировщика, обученного на основе эталонных данных работы СПД, информационного обмена в ней и классификатора, учитывающего все отклонения от штатной работы сети, а предложенная архитектура и программные прототипы компонентов системы раннего обнаружения и классификации КА в сетевом трафике СПД ориентированы на быстрое обнаружение как известных, так и неизвестных КА, с минимальным количеством ложных срабатываний и их классификацию.

Научная новизна третьего результата заключается в том, что разработанная методика классификации компьютерных атак в сетевом трафике СПД использует нейронную сеть, в процессе работы которой классификатор дополнительно обучается на скрытых латентных представлениях, полученных автокодировщиком, обученном на основе нормальных данных функционирования сетей передачи данных. Предложенная архитектура и программные прототипы компонентов системы раннего обнаружения и классификации компьютерных атак в сетях передачи данных ориентированы на быстрое обнаружение как известных, так и неизвестных компьютерных атак, с минимальным количеством ложных срабатываний и их классификацию при возможности.

Значимость полученных автором диссертации результатов для развития отрасли технических наук заключается в том, что разработанные методики позволяют превентивно выявлять КА, тем самым задействовать контрмеры, и являются математической основой системы раннего обнаружения компьютерных атак, которая базируется на обнаружении аномалий в сетях передачи данных 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 применять разработанный подход в системах обнаружения и предотвращения вторжений.

Рекомендации по использованию результатов и выводов, приведенных в диссертации. Разработанные в диссертационной работе методики и алгоритм имеют высокую скорость и точность обнаружения КА. В то же время они сохраняют свою эффективность при работе с нестационарным трафиком, что наиболее характерно для сетевого трафика существующих СПД.

Следует отметить, что результаты проведенных Крибелем А.М. исследований могут быть использованы в системах обнаружения вторжений (IDS) и системах предотвращения вторжений (IPS).

Обоснованность и достоверность полученных результатов обеспечивается применением апробированного математического аппарата, корректностью вводимых ограничений и допущений, непротиворечивостью полученных теоретических результатов экспериментам, адекватностью выбранного математического аппарата, описывающего функционирование СПД в условиях КА. Достоверность подтверждается положительными отзывами и одобрениями, полученными при апробации новых научных результатов на научно-технических и научно-практических конференциях и семинарах, а также реализацией в рамках выполненных ОКР и НИР (ОКР «Опорник» ПАО «Информационные и

телекоммуникационные технологии», Санкт-Петербург), НИР «Корвет», НИР «Потенциал-2018» «Свертка-СМ» (ФГКВОУ ВО «Военная орденов Жукова и Ленина Краснознаменная академия связи им. С.М. Буденного»), одним свидетельством о государственной регистрации программ для ЭВМ.

Уверенное знание автором предмета исследований в сочетании с активным применением современных математических методов свидетельствует о высокой специальной подготовке диссертанта.

Вместе с тем, указав на полезность полученных результатов, считаем необходимым отметить **ряд недостатков, имеющихся в представленной диссертации.**

Общие недостатки и замечания:

1. В работе недостаточно описаны тестовые данные – что они из себя представляют количественно и качественно, источники данных, способы их обработки и нормализации. Также, слабо описаны план и детали экспериментов, а иногда эта информация и вовсе отсутствует.
2. Стоило явно указать в работе, что понимается под «реальным временем» и «ранним обнаружением» - терминами, которые фигурируют, в том числе, и в научной новизне.
3. Результаты экспериментов, приведенные в таблице 4.1, не верифицируемы, и нет ссылки на источник. Кроме того, нельзя говорить, что сигнатурные методы неспособны работать с нестационарным трафиком. Сигнатуры не зависят от типа трафика.
4. Отсутствуют подписи осей у графиков на рисунках 2.4 – 2.8, что затрудняет их понимание.
5. Есть несоответствие ссылок на литературу и самих источников.

Однако отмеченные недостатки принципиально не влияют на проведенные в диссертационной работе исследования и выносимые на защиту положения.

Заключение: Диссертационная работа Крибеля А.М. является законченной научно-квалификационной работой, в которой решена актуальная научная задача, заключающаяся в разработке аналитической модели и методик выявления аномалий и классификации компьютерных атак в сетевом трафике сети передачи данных на основе применения фрактального анализа и методов машинного обучения, имеющая существенное значение для построения защищенных СПД.

Диссертация характеризует автора как сформированного специалиста, способного самостоятельно исследозвать широкий круг теоретических и практических вопросов, получать обоснованные выводы и рекомендации. Содержание работы соответствует специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

Задачи, поставленные в диссертационной работе, решены в полном объеме. Диссертация и автореферат изложены грамотным, четким и доказательным языком технических публикаций.

В целом диссертационная работа Крибеля А.М. соответствует требованиям пп. 9–14 «Положение о присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24.09.2013г. №842 (в редакции от 26.01.2023г. №101),предъявляемым к кандидатским диссертациям, а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

Диссертационная работа и отзыв обсуждены и одобрены на расширенном семинаре центра научных исследований и перспективных разработок АО «Информационные технологии и коммуникационные системы» протокол №1 от 25 апреля 2023г., на котором присутствовало 6 сотрудников, в т.ч. 4 кандидата технических наук, 1 кандидат физико-математических наук.

Заместитель генерального директора
по науке и инновациям
АО «ИнфоТеКС», к.ф-м.н.
127273, г. Москва, ул. Отрадная,
дом 2Б, строение 1
Urivskiy@infotecs.ru
+7 (495) 737-61-92, доб. 5249

Уривский
Алексей Викторович

Старший исследователь
Центра научных исследований
и перспективных разработок
АО «ИнфоТеКС», к.т.н.
127273, г. Москва, ул. Отрадная,
дом 2Б, строение 1
Oleg.Guzev@infotecs.ru
+7 (495) 737-61-92, доб. 4272

Гузев
Олег Юрьевич