МИНИСТЕРСТВО ОБОРОНЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБОРОНЫ РОССИИ)
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
КАЗЕННОЕ ВОЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОЕННЫЙ
ОРДЕНА ЖУКОВА
УНИВЕРСИТЕТ
РАДИОЭЛЕКТРОНИКИ»
МИНИСТЕРСТВА ОБОРОНЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Советский проспект, д. 126, г. Череповец,
Вологодская обл., 162622,
факс: 8 (8202) 55-68-41

«04» 04 2023 г. № 1/317

На № _____

Экз. № 1

УТВЕРЖДАЮ

Заместитель начальника Военного
университета радиоэлектроники
по учебной и научной работе

О.Родионов

«__» апреля 2023 г.

ОТЗЫВ
НА АВТОРЕФЕРАТ 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», ПРЕДСТАВЛЕННОЙ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА ТЕХНИЧЕСКИХ НАУК
(СПЕЦИАЛЬНОСТЬ 2.3.6 – «МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»)

В современных условиях стремительно меняющейся обстановки на поле боя высокий уровень информационного обеспечения боевых действий войск становится определяющим фактором достижения стратегического и оперативно-тактического превосходства над противником. Решающую роль в этом имеют революционные изменения в области обработки информации, внедрение технологий искусственного интеллекта в военные системы связи и управления. Объединение вычислительных ресурсов и построение на их основе центров обработки данных, повседневное внедрение технологий виртуализации постепенно послужило причиной пересмотра особенностей подходов к построению сети передачи данных специального назначения (СПД), которая глубоко интегрирована в сеть связи общего пользования (ССОП).

Сеть связи общего пользования достаточно глубоко интегрирована в мировое информационное пространство. Телекоммуникационное оборудование, используемое операторами услуг, в основном является импортным. Это предоставляет широкие возможности для активной деятельности злоумышленников по реализации компьютерных атак (КА) Используемое в СПД сетевое оборудование узлов связи обладает высокой контрастностью по отношению к элементам других систем связи, функционирующих в том же фрагменте ССОП, в связи с чем оно может быть выявлено с высокой вероятностью.

Это обуславливает актуальность исследования, проводимого Крибелем А.М.

В ходе решения научной задачи Крибелем А.М. получены следующие положения, выносимые на защиту:

1. Аналитическая модель выявления аномалий в сетевом трафике СПД в условиях КА.

2. Методика раннего обнаружения аномалий в сетевом трафике СПД.

3. Методика классификации КА в сетевом трафике СПД.

4. Архитектура и программные компоненты системы раннего обнаружения и классификации КА в сетевом трафике СПД.

Полученные научные результаты основываются на всестороннем анализе выполненных ранее научно-исследовательских работ в предметной области, корректной постановке задач исследования и применении апробированного научно-методического аппарата, а также подтверждаются верификацией теоретических данных и результатов экспериментов.

Из автореферата следует, что научная новизна выполненного исследования состоит в следующем:

1. Модель выявления аномалий в сетевом трафике сетей передачи данных в условиях компьютерных атак позволяет рассматривать не только стационарный, но и нестационарный сетевой трафик и обосновывает выбор фрактального метода выявления аномалий в интересах дальнейшей классификации компьютерных атак в зависимости от типа трафика.

2. Методика раннего обнаружения аномалий в сетевом трафике сетей передачи данных позволяет прогнозировать и обнаруживать известные и неизвестные компьютерные атаки на раннем этапе их проявления благодаря совместному применению методов фрактального анализа и рекуррентной нейронной сети с долгой краткосрочной памятью, в результате чего существенно сокращается время выявления аномалий и уменьшается количество ложных срабатываний.

3. Методика классификации компьютерных атак в сетевом трафике сетей передачи данных позволяет обнаруживать компьютерные атак с использованием генеративно-состязательной сети.

4. Архитектура и программный прототип компонентов системы раннего обнаружения и классификации компьютерных атак в сетях передачи данных

ориентированы на раннее обнаружение как известных, так и неизвестных компьютерных атак с минимальным количеством ложных срабатываний.

Теоретическая значимость результатов диссертации обоснована тем, что разработанные методики представляют собой научно-методическую основу, практическая реализация которых позволяет выявлять аномалии, вызванные КА в режиме реального времени, на основе интеграции фрактального анализа и рекуррентной искусственной нейронной сети с долгой краткосрочной памятью.

Практическая значимость работы отмечена в автореферате тем, что научно-технические предложения (4 глава диссертации), доведенные до реализации в виде программного комплекса, позволяют за счет раннего обнаружения КА и применения средств противодействия КА повысить защищенность СПД. Разработана программа, на которую получено свидетельство о государственной регистрации программ для ЭВМ, рекомендованная к использованию должностными лицами при планировании и выполнении мероприятий по информационной безопасности.

Научные результаты, выносимые на защиту, апробированы на научно-практических конференциях и опубликованы в рекомендованных ВАК изданиях, в том числе в единоавторстве.

Изложение материала в автореферате в целом выполнено грамотно и позволяет уяснить основные положения и научные результаты диссертационной работы.

Однако, несмотря на общее положительное впечатление о диссертации, необходимо отметить следующее в качестве замечаний:

1. Недостаточно обоснованы показатели защищенности СПД и показатель Херста в условиях КА.

2. В автореферате не раскрыто, каким образом в методике вычисляются аномальные всплески в трафике.

3. В автореферате не в полной мере раскрыты возможности программного комплекса раннего обнаружения КА: он только по нейтрализации или только выявления КА.

Данные недостатки не оказывают существенного влияния на результаты исследования. Судя по автореферату, диссертационная работа является законченным научным трудом. Крибель А.М. показал умение самостоятельно вести исследования в выбранном научном направлении с доведением их до практической реализации. Результаты работы в достаточной степени опубликованы, апробированы и реализованы. Сам автореферат имеет логичную структуру, написан грамотным техническим языком, оформлен по ГОСТу.

ВЫВОД: исходя из содержания автореферата, проведенное исследование Крибеля Александра Михайловича соответствует требованиям п.п. 9, 10, 11 и 14 «Положения о присуждении ученых степеней», предъявляемым к кандидатским диссертациям. Содержание диссертации соответствует специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность». По

новизне, уровню научной проработки и практической ценности полученных результатов соискатель заслуживает присуждения ему ученой степени кандидата технических наук.

Отзыв подготовил:
Доцент 32 кафедры, кандидат технических наук

Пермяков Александр Сергеевич

С отзывом согласен:
Начальник 32 кафедры, кандидат педагогических наук, доцент

Тихомиров Вадим Анатольевич

«24» апреля 2023 г.

Отзыв на автореферат обсужден и одобрен на заседании 32 кафедры. Протокол № 9 от 20 апреля 2023 г.

Начальник 32 кафедры, кандидат педагогических наук, доцент

Тихомиров Вадим Анатольевич

«24» апреля 2023 г.