Экз. № ___

УТВЕРЖДАЮ
Заместитель начальника училища
по учебной и научной работе
доктор технических наук, профессор
А.Крупенин
«24» 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 по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

Начало XXI века охарактеризовалось переходом ведущих государств мира к информационному воздействию (ИВ) на системы управления различного назначения. Причина этого – качественный скачок в развитии средств обеспечения управления и обмена информацией, на основе информационно-телекоммуникационных технологий. Определяющую роль в ИВ играют целенаправленные воздействия, так называемые компьютерные атаки (КА) – действия, которые осуществляются в соответствующих сетях для уничтожения важной информации в компьютерах и компьютерных сетях или же вывода из строя самих компьютеров (сетей).

В связи с этим важной задачей является обеспечение достаточной степени защищенности сетей передачи данных (СПД) от воздействий КА. Анализ показал, что существующие средства защиты не позволяют обеспечить высокие требования, предъявляемые к уровню защищенности СПД при воздействии КА, т.е. в сложившейся ситуации, существующие СПД не отвечают предъявляемым требованиям по защищенности.

Поэтому актуальность выбранного соискателем направления исследования, его темы и научной задачи, не вызывает сомнения и представляет интерес для специалистов в предметной области.

Для достижения цели в диссертационной работе поставлены и решены следующие частные задачи по:

1) анализу существующих моделей воздействия компьютерных атак в сети передачи данных;

2) анализу существующих алгоритмов выявления компьютерных атак, систем мониторинга и методик противодействия компьютерным атакам в сети передачи данных;

3) разработке аналитической модели выявления аномалий в сетевом трафике сети передачи данных в условиях компьютерных атак;

4) разработке методики раннего обнаружения аномалий в сетевом трафике сети передачи данных;

5) разработке методики классификации компьютерных атак в сетевом трафике сети передачи данных;

6) разработке архитектуры и программных прототипов компонентов системы раннего обнаружения и классификации компьютерных атак в сетевом трафике сети передачи данных, экспериментальная и теоретическая оценка эффективности предложенных моделей, методик и архитектуры.

В ходе исследования автором получены следующие новые научные результаты, 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.

Теоретическая значимость результатов исследования определяется тем, что разработанные научно-методические положения позволяют прогнозировать стратегию КА злоумышленника и, базируясь на этих результатах, обосновать

архитектуру защиты, что представляет собой существенный вклад в развитие теории информационной безопасности.

Практическая значимость результатов исследования заключается в том, что разработанные научно-методические положения представляют собой научно-методическую основу, практическая реализация которой позволяет описать различные типы трафика в СПД, определять аномальные активности, основываясь на принципах самоподобия, и, исходя из типа трафика с применением различных методов машинного обучения, выявлять КА. Разработанные методики являются математической основой системы раннего обнаружения КА, основанные на обнаружении аномалий в СПД 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 СПД, что позволяет на практике эффективно применять разработанный подход в системах глубокой проверки сетевых пакетов в СПД.

Обоснованность и достоверность полученных научных результатов и выводов основывается на всестороннем анализе выполненных ранее научно-исследовательских работ в предметной области, корректной постановке задач исследования и применении апробированного научно-методического аппарата, а также подтверждается верификацией теоретических данных и результатов экспериментов.

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

1) В автореферате недостаточно подробно раскрыт вопрос обоснования выбора показателя самоподобия в качестве критерия аномальности нестационарного трафика по отношению к использованию классических моделей временных рядов и методов машинного обучения.

2) Из автореферата не совсем ясно, как оценивалась эффективность разработанных научно-технических предложений.

Указанные недостатки имеют частный характер и не оказывают существенного влияния на результаты работы. Судя по автореферату, диссертационная работа является законченным научным трудом. Автор показал

умение самостоятельно вести исследования в определенном научном направлении с доведением их до практических рекомендаций. Результаты работы в достаточной степени опубликованы, апробированы и реализованы. Автореферат написан грамотным техническим языком, имеет логичную структуру, оформлен в соответствии с требованиями.

ВЫВОД: исходя из содержания автореферата, диссертационная работа Крибеля А.М. соответствует требованиям п.п. 9, 10, 11 и 13 «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:
Сотрудник Федерального государственного казенного военного образовательного учреждения высшего образования «Краснодарское высшее военное орденов Жукова и Октябрьской революции Краснознаменное училище имени генерала армии С.М. Штеменко» Министерства обороны Российской Федерации

доктор технических наук, профессор

Максимов Роман Викторович

«17» апреля 2023 г.

Отзыв на автореферат обсужден и одобрен на заседании кафедры защищенных информационных технологий. Протокол № 14 от 17 апреля 2023 г.

Начальник кафедры защищенных информационных технологий

кандидат технических наук, доцент

Медведев Андрей Николаевич

«17» апреля 2023 г.

Федеральное государственное казенное военное образовательное учреждение высшего образования «Краснодарское высшее военное орденов Жукова и Октябрьской революции Краснознаменное училище имени генерала армии С.М. Штеменко» Министерства обороны Российской Федерации
Почтовый адрес:
350005, г. Краснодар, ул. Грибоедова, д. 18.
Адрес электронной почты:
kvvu@mil.ru
Телефон:
8 (861) 258-10-30