Экз. ___

# ОТЗЫВ

официального оппонента доктора технических наук, доцента,
начальника кафедры Систем сбора и обработки информации
ФГБВОУ ВО «Военно-космическая академия имени А.Ф. Можайского»
Министерства обороны Российской Федерации
БИРЮКОВА Дениса Николаевича
на диссертационную работу КРИБЕЛЯ Александра Михайловича
по теме: «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»

**1. Актуальность темы диссертации.**

Последние десятилетия XXI века в сфере вооруженной борьбы охарактеризованы переходом технологически развитых государств мира к осуществлению атакующих воздействий на системы связи. Причина этого – качественный скачок в развитии средств обеспечения управления и обмена информацией, на основе информационно-телекоммуникационных технологий.

Определяющую роль в качественном проведении атакующих воздействий играют принципы и средства воздействия компьютерных атак. Под компьютерной атакой (КА) принято понимать специально подготовленную, согласованную по месту, времени и формам деятельность, направленную на организацию доступа, перехват, сбор, анализ, изменение и уничтожение данных, обрабатываемых в сетях передачи данных.

Таким образом, для обеспечения требуемого уровня защищенности сеть передачи данных (СПД) должна обладать эффективной системой защиты, способной решать задачи по выявлению и выбору контрмер, направленных на срыв осуществления КА. Обнаружение может быть выполнено за счет своевременного выявления аномальных проявлений (как, например, всплесков запросов по протоколу *SNMP*, *ICMP* и др.).

Проведенный автором анализ применяемых в настоящее время способов и средств обеспечения защищенности СПД в условиях КА показал, что существующие методики и средства не позволяют обеспечивать требуемый уровень защищенности СПД.

В связи с этим тема и научная задача диссертационной работы Крибеля А.М. являются **актуальными**.

**2. Новизна, теоретическая и практическая значимость полученных научных результатов.**

Новыми **научными результатами**, самостоятельно полученными автором в результате проведенных исследований и выносимыми на защиту, являются:

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.

Диссертационная работа обладает научной новизной, при этом для первого результата, выносимого на защиту, она определяется тем, что модель позволяет на ранних этапах выявлять КА, вызванных аномальной активностью сетевого трафика.

Научная новизна второго результата определяется тем, что разработанная методика раннего обнаружения аномалий в сетевом трафике сети передачи данных в отличие от известных позволяет обнаруживать КА на раннем этапе их проявления с помощью методов машинного обучения для стационарного сетевого трафика СПД и фрактального анализа для нестационарного.

Новизна третьего научного результата заключается в разработке методики классификации компьютерных атак в сетевом трафике сети передачи данных, выявлять и классифицировать КА на основе применения гибридной нейронной сети, состоящей из классификатора и

автокодировщика. Особенностью методики является возможность выявлять не только известные КА, но и атаки «нулевого дня».

Научная новизна четвертого результата заключается в разработке архитектуры и программного компонента системы раннего обнаружения и классификации компьютерных атак в сетевом трафике сети передачи данных, которые ориентированы на мгновенное обнаружение как известных, так и неизвестных КА, с минимальным количеством ложных срабатываний, их классификацию и выбор доступных контрмер.

Кроме того, новизна четвертого результата подтверждается одним свидетельством о государственной регистрации программ для ЭВМ.

**Практическая значимость** полученных автором результатов заключается в том, что в результате решения задачи обнаружения КА обоснована структура системы защиты СПД, которая включает подсистему раннего обнаружения и классификации компьютерных атак в сетевом трафике сети передачи данных. Разработанная архитектура основана на разработанной гибридной нейронной сети и содержит базу данных с информацией о КА с целью их классификации, позволяющая повысить защищенность контролируемого сегмента СПД за счет своевременного выявления и нейтрализации КА.

**Теоретическая значимость** результатов исследования определяется тем, что разработанные научно-методические положения позволяют выявить КА в СПД в режиме реального времени и прогнозировать этапы функционирования СПД. В дальнейшем, базируясь на этих результатах предлагаются исследования и разработки систем поддержки принятия решения.

Теоретическая и практическая значимость разработанных методик и научно-технических предложений подтверждается наличием актов реализации в ОКР «Опорник» (ПАО «Информационные и телекоммуникационные технологии», Санкт-Петербург) и 3 акта о реализации в НИР«Корвет» (ВАС, Санкт-Петербург), НИР «Потенциал-2018» (ВАС, Санкт-Петербург), НИР «Свертка-2018-ВАС» (ВАС, Санкт-Петербург).

Структурно диссертация состоит из четырех глав, введения, заключения, списка сокращений и списка литературы, а также пяти приложений. Изложение материала в диссертационной работе выполнено логично и грамотно, стиль изложения доказателен, текст с достаточной полнотой иллюстрирован, содержит необходимые ссылки на заимствованные

положения. По каждой главе и диссертации в целом сделаны выводы, обобщающие и конкретизирующие выполненные исследования, проведена оценка полученных результатов.

Личный вклад автора диссертации заключается в обосновании нового подхода, который позволяет на ранних этапах классифицировать и выявлять компьютерные атаки, тем самым научно обосновывая пути повышения защищенности СПД за счет преждевременных контрмер, а также реализации новых научно-методических предложений на практике.

**3. Степень обоснованности и достоверности научных положений, выводов и рекомендаций, сформулированных в диссертации.**

Обоснованность сформулированных автором научных положений, выводов и предложений обеспечивается корректностью использованных исходных данных, допущений и ограничений, строгостью математических преобразований, доказательств и расчетов, а также правильностью применения апробированного математического аппарата исследований.

Достоверность полученных научных результатов подтверждается их ясной физической трактовкой и непротиворечивостью теоретических положений и выводов диссертации непротиворечащим результатам научных работ, выполненным ранее другими авторами.

**4. Публикации, реализация и апробация научных положений.**

По тематике диссертации опубликованы 17 работ, среди которых шесть статей, индексируемые в международных базах данных Web of Science и/или Scopus; десять статей в 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; одно свидетельство о государственной регистрации программы для ЭВМ.

Основные научные и практические результаты работы докладывались и обсуждались на 10 научно-технических и научно-практических конференциях с 2017 по 2022 гг.

**5. Оценка содержания диссертации, степень ее завершенности.**

Диссертационная работа Крибеля А.М представляет законченный научно-квалификационный труд, имеющий внутреннее единство составных

частей, направленных на решение поставленной задачи исследования. К числу недостатков и замечаний, касающихся работы, на которые необходимо обратить внимание соискателю в его дальнейшей научно-исследовательской деятельности, отмечаю следующие:

1. В первом разделе работы упоминаются такие программные решения, как *Entercept* и *RealSecureServerSensor,* являющиеся программными продуктами конца 90-х годов прошлого века, и непонятно, почему соискатель не рассмотрел современные средства, технологии и их возможности (см. *SIEM*, *NTA*, *EDR*, *ThreatIntelligence*).

2. Во втором разделе (п.2.5.) не полностью описаны условия, при которых производилось вычисление и оценка показателя Херста (какой канал, протоколы, какой объем данных считается большим, как были получены эталонные выборки, как был смоделирован аномальный трафик).

3. В третьем разделе (п.3.1) при рассмотрении вопросов обнаружения аномалий в нестационарном сетевом трафике (а это передача данных с коммутацией пакетов – см. стр.53-54) сети передачи данных с помощью фрактального анализа указано: «С целью оценки аномальности предложено использовать не полезное содержимое пакетов, а взять за основу предложение Унтерова Д.С. [130] о том, что информации из заголовков пакетов будет достаточно», но при таком заявлении нужно указать с каким классом КА имеем дело, так как при реализации *sqli* или *xss* это предположение спорно;

4. Третье положение, выносимое на защиту звучит как «Методика классификации компьютерных атак в сетевом трафике сети передачи данных», однако в практической части рассмотрены только атаки, осуществляемые через протокол HTTP (см. рис. 4.1 стр. 91), что не в полном объеме отражает значимость представленного подхода.

5. В четвертой главе на стр. 124 приводится, что «Архитектура содержит оригинальные компоненты выявления аномалий в сетевом трафике и обучения разработанной нейронной сети, базу данных с информацией о КА с целью их классификации», но нигде в работе не описана упомянутая база данных и даже требования к ней.

6. Из содержания п.п.4.4 не совсем понятно, как обучить нейросеть выявлению различных атак типа sqli или xss в HTTP трафике.

7. Ряд описанных в работе экспериментов изложено недостаточно подробно для понимания и верификации полученных результатов:

- на стр. 123 указано, что «Вероятность обнаружения известных КА равна 0,96, а атаки «нулевого дня» - 0,8», но без указания того, на каких СПД и в рамках каких сетей (объектов) производились исследования, приведенные оценки мало информативны, так как одно дело контролировать магистральный канал провайдера с большим потенциальным разнообразием трафика, а другое – контролировать трафик, идущий к конкретному web-серверу с конкретными полями на web-странице;

- на стр. 127 отмечается, что «Совокупное применение разработанных модели и методик, по сравнению со многими другими подходами, позволит увеличить скорость обнаружения компьютерных атак в 14 раз путем выявления аномалий в трафике любого вида», однако понять на основании чего такой вывод был сделан невозможно (исходя из таблицы 4.1 таких выводов сделать нельзя, а других данных в работе не приводится).

8. Работа содержит ряд синтаксических, орфографических и оформительских ошибок (см. стр. 4, 13, 36, 37, 69, 100, 106; рис. 1.2, 4.2 – не соответствует содержанию, и др.).

Вместе с тем стоит отметить, что указанные недостатки не снижают общей научной и практической ценности работы, а большая часть недостатков связана с тем, что в работе отсутствует подробное описание модели объекта защиты (с указанием настроек, возможностей и порядка функционирования, каналов связи, используемых протоколов передачи данных и т.п.), а также явно не указан класс компьютерных атак, от которых предполагается защищаться, так как одно дело выявлять аномалии связанные с реализацией DDOS атак, и совсем другое – выявление аномалий в байткоде, передаваемом посредством прикладных протоколов.

**6. Автореферат** достаточно полно отражает содержание работы, полученные научные и практические результаты, соответствует основным идеям и выводам диссертации.

## ЗАКЛЮЧЕНИЕ

Представленная диссертационная работа написана на актуальную тему и является завершенным научно-квалификационным трудом. В ней получено новое решение научной задачи, заключающейся в разработке 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.

Содержание работы соответствует специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность». Автореферат кратко и в достаточной мере отражает содержание диссертации, включает перечень основных научных работ автора, связанных с темой исследования.

По научной новизне полученных научных результатов, теоретической и практической значимости, а также обоснованности и достоверности результатов, диссертация отвечает критериям, установленным пп. 9–14 «Положения о присуждении ученых степеней» (утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 года №842), предъявляемым к кандидатским диссертациям, а ее автор, Крибель Александр Михайлович, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент
Начальник кафедры Систем сбора
и обработки информации
ФГБВОУ ВО «Военно-космическая
Академия имени А.Ф. Можайского»
Министерства обороны
Российской Федерации,
доктор технических наук, доцент

«25» 04 2023г. Бирюков Денис Николаевич

Подпись официального оппонента доктора технических наук доцента Бирюкова Дениса Николаевича заверяю.

Начальник отдела кадров

Г.В.Плотников