Экз. №2

АКЦИОНЕРНОЕ ОБЩЕСТВО
«НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР
«АТЛАС»
(АО «НТЦ «Атлас»)
Пензенский филиал

Проспект Победы, д. 69, г. Пенза, 440028
Тел. (8412) 64-38-63, Факс (8412) 47-78-80
e-mail: atlas@atlas-pf.ru

УТВЕРЖДАЮ

Директор ПФ АО «НТЦ «Атлас»

_ Юранов Ю.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")

Информационные технологии активно развиваются, проникая во все сферы жизни общества. Актуальность вопросов информационной безопасности сетевых технологий постоянно растет. Появление новых угроз, совершенствование методов атак требует разработки новых подходов к реализации механизмов защиты, обеспечивающих своевременную реакцию на действие злоумышленников.

В настоящее время существенно увеличился объем обрабатываемой информации, значительный объем информации хранится и обрабатывается в электронном виде, что существенно затрудняет ее защиту. Необходимость в разработке новых подходов к защите информации также связана с ростом возможностей вычислительной техники и развитием сетевых технологий.

Массовое использование сети Интернет значительно увеличило актуальность защиты от удаленных атак. В настоящее время удаленные атаки на информационные системы занимают лидирующие место среди угроз информационной безопасности. Атакам может подвергаться не только информация, хранящаяся на локальных накопителях, но и информация при ее передаче через сеть.

Используя существующие методы и средства информационной безопасности невозможно достичь максимального уровня защищенности. При этом с ростом уровня защищенности той или иной сети возникают определенные неудобства, ограничения и трудности для пользователей. Часто необходимо выбрать оптимальный вариант защиты сети, который бы существенно не снижал удобство использования средств сетевого обмена и, одновременно, обеспечивал высокий уровень защиты информации. Создание подобных решений является достаточно сложной задачей.

Таким образом, в условиях постоянного развития угроз информационной безопасности сетевых технологий, рассматриваемая в представленной диссертации тема является актуальной и имеет важное практическое значение.

В автореферате представлены следующие полученные автором результаты, выносимые на защиту:

1) аналитическая модель выявления аномалий в сетевом трафике сети передачи данных (СПД) в условиях компьютерных атак (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.

Научная новизна полученных результатов состоит в том, что:

а) разработанная аналитическая модель выявления аномалий в сетевом трафике СПД в условиях КА, в отличие от известных, описывает не только стационарный, но и нестационарный сетевой трафик и обосновывает выбор фрактального метода выявления аномалий для целей дальнейшей классификации КА в зависимости от типа трафика;

б) разработанная методика раннего обнаружения аномалий в сетевом трафике СПД, в отличие от известных, способна проводить прогнозирование и обнаружение не только известных, но и неизвестных КА на раннем этапе их проявления, благодаря совместному применению методов фрактального анализа и искусственной нейронной сети LSTM-типа, в результате чего существенно

сокращается время выявления аномалий и уменьшается количество ложных срабатываний;

в) разработанная методика классификации КА в сетевом трафике СПД отличается от известных тем, что в ней обнаружение КА выполняется с использованием генеративно-состязательной сети, которая производит дообучение классификатора на скрытых латентных представлениях, полученных автокодировщиком, исходя из анализа данных о функционировании СПД;

г) предложенная архитектура и программные прототипы компонентов системы раннего обнаружения и классификации КА в СПД отличаются от известных тем, что они ориентированы на раннее обнаружение как известных, так и ранее неизвестных КА с минимизацией ложных срабатываний за счет реализации методов фрактального анализа и искусственной нейронной сети LSTM-типа.

Теоретическая и практическая значимость результатов исследования заключается в том, что разработанные аналитическая модель и методики 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 мер 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 эффективно применять разработанный подход в системах глубокой проверки сетевых пакетов в СПД.

Представленный на отзыв автореферат позволяет понять основные принципы и научные результаты проведенного исследования. Подходы, представленные в диссертации, опубликованы и достаточно полно описаны в рецензируемых журналах, включенных в перечень ВАК, индексируемых в международных базах данных Web of Science и/или Scopus.

К незначительным недостаткам представленного на отзыв автореферата можно отнести следующие:

– в автореферате неполно описана разработанная аналитическая модель: не указаны предположения, положенные в ее основу, отсутствуют объяснения условных обозначений в формулах, не указаны границы изменения параметров в формулах и границы их применимости;

– в автореферате не приведено обоснование выбора фрактального метода анализа в качестве математического аппарата для выявления аномалий в сетевом трафике СПД;

– в автореферате не приведены условия, при которых были получены достаточно высокие значения вероятностей обнаружения КА.

Диссертационная работа Крибеля А.М. является завершенной научной квалификационной работой, отличающейся актуальностью и полнотой проведенных исследований, в которой в значительной мере решена актуальная научная задача, имеющая важное практическое значение. Работа отвечает пп. 9, 10, 11 и 14 требований «Положения о присуждении ученых степеней», а ее автор заслуживает присуждения ему ученой степени кандидата технических наук по специальности 2.3.6 (Методы и системы защиты информации, информационная безопасность).

д.т.н. Егорова Наталья Алексеевна
Научный сотрудник ПФ АО «НТЦ «Атлас»
Проспект Победы, д. 69, г. Пенза, 440028
atlas@atlas-pf.ru 8(8412)64-38-30
к.т.н. Безяев Александр Викторович
Ведущий научный сотрудник ПФ АО «НТЦ «Атлас»
Проспект Победы, д. 69, г. Пенза, 440028
atlas@atlas-pf.ru 8(8412)64-38-17
Отзыв рассмотрен на НТС.
Протокол заседания от 17.04.2023 г. № 5.
Ведущий научный консультант ПФ АО «НТЦ «Атлас»
Десятов Владимир Дмитриевич