УДК 004.032.26

Воронин И.В.

старший преподаватель

ЛГПУ имени П.П. Семенова-Тян-Шанского

РФ, г. Липецк

Газин А.И., кандидат технических наук, доцент

доцент

ЛГПУ имени П.П. Семенова-Тян-Шанского

РФ, г. Липецк

Золотарева Т.А.

старший преподаватель

ЛГПУ имени П.П. Семенова-Тян-Шанского

РФ, г. Липецк

Селищев О.В.

преподаватель

ЛГПУ имени П.П. Семенова-Тян-Шанского

РФ, г. Липецк

Скуднев Д.М., кандидат технических наук, доцент

зав. кафедрой информатики, информационных технологий и защиты информации, доцент

ЛГПУ имени П.П. Семенова-Тян-Шанского

РФ, г. Липецк

МАТЕМАТИЧЕСКАЯ И ПРОГРАММНАЯ РЕАЛИЗАЦИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ ДЛЯ ИДЕНТИФИКАЦИИ СОСТОЯНИЯ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Аннотация: рассматривается практическое применение искусственной нейронной сети Хэмминга, описывается разработка интеллектуальной системы поддержки принятия решений, проводится оценка эффективности программы.

Ключевые слова: компьютерная сеть, сниффер, сигнатурный анализ, искусственная нейронная сеть, система поддержки принятия решений.

Voronin I.V.

senior lecturer

LSPU named after P.P. Semenov-Tyan-Shanskogo

Russia, Lipetsk

Gazin A.I., Candidate of Technical Sciences, docent

docent

LSPU named after P.P. Semenov-Tyan-Shanskogo

Russia, Lipetsk

Zolotareva T.A.

senior lecturer

LSPU named after P.P. Semenov-Tyan-Shanskogo

Russia, Lipetsk

Selishchev O.V.

teacher

LSPU named after P.P. Semenov-Tyan-Shanskogo

Russia, Lipetsk

Skudnev DM., Candidate of Technical Sciences, docent

Head of the Department of Computer Science, Information Technology and Information Security, docent

LSPU named after P.P. Semenov-Tyan-Shanskogo

Russia, Lipetsk

MATHEMATICAL AND SOFTWARE IMPLEMENTATION OF AN INTELLIGENT DECISION SUPPORT SYSTEM FOR IDENTIFYING THE STATE OF A LOCAL COMPUTER NETWORK

Abstract: the practical application of an artificial neural network of Hamming is considered, the development of an intelligent decision support system is described, the effectiveness of the program is evaluated.

Keywords: computer network, sniffer, signature analysis, artificial neural network, decision support system.

В настоящее время, развивающиеся корпоративные сети включают в себя большое количество мелких подсетей, которые в свою очередь объединяют огромное количество сетевых устройств. К таким устройствам можно отнести:

– автоматизированные рабочие места сотрудников организации;

– серверное оборудование;

– сетевое оборудование – коммутаторы, маршрутизаторы и др.;

– системы обеспечения безопасности организации – системы видеонаблюдения, системами контроля управления доступом (СКУД), охрано-пожарные комплексы;

– ЧПУ станки;

– Интернет вещей (IoT);

– другие сетевые устройства.

Каждое из этих устройств может привносить какие-либо сбои в нормальный режим работы сети организации. В настоящее время, в подавляющем большинстве организаций, задача выявления сетевых проблем возложена на системного администратора. В настоящее время, программные и программно-аппаратные комплексы выявления инцидентов в локальной сети разработаны для выявления событий информационной безопасности. Для выявления же инцидентов, не относящихся к событиям информационной безопасности, системному администратору, приходилось использовать снифферы, например, Wireshark, CommView, Intercepter-NG и др. Часто, в локальной сети возникают «плавающие ошибки». «Плавающие ошибки» – это те ошибки, которые возникают периодически, в результате стечения каких-то обстоятельств, и очень тяжело диагностируются.

Для выявления такого рода ошибок, необходимо длительное время накапливать статистику снифферами, практически «вручную» анализировать ее, контролировать работу всего сетевого оборудования, входящего в состав локальной сети организации. Вся эта работа займет практически все рабочее время персонала, занятого обслуживание IT-инфраструктуры организации. В целях оптимизации времени работы системного администратора, а также для сокращения временных издержек, при выполнения однотипных, рутинных операций, необходимо использовать современные технологии на рабочих местах специалистов, занимающихся сетевым анализом. Эти технологии должны быть тесно интегрированы с современной системой поддержки принятия решений (DSS) [1].

При изучении сетевого трафика, было установлено, что наиболее оптимальным будет использование нейросетевого анализатора с применением методов машинного обучения, основанных на

искусственных нейронных сетях, которые позволяют решать задачи в области обработки и распознавания различные изображения более эффективно, чем классические подходы [2].

Например, для обнаружения и классификации проблем компьютерных сетей используется сигнатурный анализ. Его основа – обнаружение совпадений найденной последовательности с базовой выборкой, путем побитового сравнения. Таким образом, есть возможность обнаружить подпись, указывающая на наличие вредоносного кода в анализируемом трафике.

При этом для использования искусственной нейронной сети (ИНС) в задачах анализа трафика компьютерных сетей, требуется обучающая выборка, позволяющая корректно идентифицировать все сбойные пакеты данных, возникающие при классификации сетевого трафика [3].

Для решения поставленной задачи, будем использовать ИНС Хэмминга, проведя классификацию бинарных векторов. В основу этой работы ИНС входят процедуры, направленные на поиск эталонного пакета данных среди всех представленных зашумленных входных векторов. ИНС Хэмминга используется, чтобы определить, принадлежит ли объект к определенному классу, который определяется вектором *X*. Этот вектор имеет биполярные особенности, которые могут принимать значения как *1* так и *-1*, и имеет *N* состояний. Предполагается, что существует *M* классов, каждый из которых характеризуется своим собственным состоянием $-X_v,\ v = 1, 2, \dots, V.$

Данные основаны на изображениях опорных векторов и векторов признаков, выбранных экспертами и которые соответствуют выбранным изображениям. ИНС Хэмминга состоит из N входов, на которые передаются биполярные характеристики объекта. В дальнейшем, происходит обработка полученных характеристик, после чего срабатывает один из *K* выходов, с указанием определенного класса, к которому

принадлежит представленный на входе объект. Количество нейронов в ИНС Хэмминга зависит от количества эталонных кадров, хранящихся в база данных, и запись нового кадра в базу данных с эталонами, сопровождается расчетом вектора признаков. Этот означает, что, помимо самих кадров, база содержит также вычисляемые вектора. Для анализа сетевого трафика и идентификации состояния сети, возможно методы машинного обучения, на пример на основе оптимизированной ИНС Хэмминга.

В рамках выполнения поставленной задачи, была разработана интеллектуальная система поддержки принятия решений (СППР) с использованием среды разработки Embarcadero Delphi. Разработанная система прошла регистрацию как программа для ЭВМ в Федеральном институте промышленной собственности (Свидетельство о государственной регистрации программы для ЭВМ «Научная обработка отчетов анализаторов сетевых трафиков» № 2021610934 от 19.01.2021 г.).

Оценка эффективности программы осуществлялась по трем главным функциональным критериям:

1). Коэффициент ошибок (в зависимости от выбранного типа сниффера). Данный параметр зависимость показывает, как отношение числа ошибочно определенных пакетов к общему числу пакетов зависит от выбора типа сниффера (тип импортируемого файла-отчета).

2). Коэффициент производительности (в зависимости от объема информации). Данный параметр показывает, как величина, обратная времени работы анализирующего программного модуля (АПМ), зависит от объема информации (число записей в журналах и пр.).

3). Коэффициент ошибок (в зависимости от типа ЛВС). Данный коэффициент показывает, как отношение числа ошибочно определенных пакетов к общему числу пакетов зависит от выбора типа ЛВС (тип оборудования, топология и т.д.).

Оценка эффективности функционирования работы анализирующего программного модуля СППР для идентификации состояния ЛВС показывает свою значимость в работе фирмы средних размеров. Были предложены как программно-технические критерии, так и экономические критерии для наиболее развернутого исследования особенностей АПМ СППР. Также были выявлены приоритеты в практическом применении подобного программного комплекса.

Работа выполнена в рамках гранта РФФИ № 19-47-480002.

Использованные источники:

1. I V Voronin, A I Gazin, V S Ziyautdinov, T A Zolotareva, D M Skudnev and O V Selishchev Identification of the local area network using machine learning // Journal of Physics: Conference Series (JPCS): Conference on Applied Physics, Information Technologies and Engineering» (APITECH-2019) – Q3. – 2019.

2. Рапопорт Г.Н. Биологический и искусственный разум. Сознание, мышление и эмоции / Г.Н. Рапопорт, А.Г. Герц, – Текст: непосредственный. - Москва: Editorial URSS, 2017. - 184 с

3. Зияутдинов, В.С. Аналитическое обеспечение интеллектуальной системы поддержки принятия решения для идентификации состояния локальной вычислительной сети / В.С. Зияутдинов, Т.А. Золотарева, И.В. Воронин, Д.М. Скуднев, – Текст: непосредственный // Фундаментальные исследования. – 2016. – № 10-2. – С. 280-284;

4. Воронин, И.В. Оценка эффективности работы интеллектуальной системы поддержки принятия решений для идентификации состояния локальных вычислительных сетей / И.В.Воронин, А.И.Газин, Т.А.Золотарева, Д.М.Скуднев, О.В.Селищев, – Текст: непосредственный // Современная наука: Актуальные проблемы теории и практики. – 2021. – №7. – С. 55-60.