УДК 004.02

ПРОГРАММНАЯ СИСТЕМА ИДЕНТИФИКАЦИИ АНОМАЛЬНОЙ АКТИВНОСТИ СУБЪЕКТОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Родионов В.Д., Соловьев Н.А.

ФГБОУ ВО «Оренбургский государственный университет», Оренбург, e-mail: vvvdddrrr@gmail.com

Статья посвящена разработке программной системы, предназначенной для идентификации аномальной активности субъектов информационно-телекоммуникационной сети. Для достижения этой цели проведен системный анализ, который позволил выявить необходимость автоматизации информационных процессов, а также актуальность создания новой системы защиты, основанной на анализе аналогов существующих средств информационной безопасности. Основой для этой системы послужил спектральный анализ сетевого трафика, который позволяет обнаружить аномалии и сетевые атаки. Для обнаружения аномалий в данной системе используется расчет коэффициентов корреляции Пирсона, которые показывают степень схожести частотных показателей сетевого трафика на разных временных интервалах. Для расчета этих коэффициентов используется дискретное оконное преобразование Фурье. В статье показан алгоритм работы программной системы, который позволяет достичь требуемой эффективности обнаружения аномалий в информационно-телекоммуникационной сети. Для проверки достоверности проводимых расчетов сравниваются коэффициенты корреляции Пирсона в предложенной системе и в программной среде MatLab при аналогичных входных данных. Исследование показало, что разработанная система обеспечивает высокую точность в обнаружении аномалий объектов информационно-телекоммуникационной сети. Программа может определить как аномалию, так и конкретную атаку, сравнив частотные показатели текущего сетевого трафика с записанным шаблоном.

Ключевые слова: обнаружение аномалий, сетевой трафик, Фурье-анализ, коэффициент корреляции Пирсона, информационная безопасность

SOFTWARE SYSTEM FOR IDENTIFICATION OF ABNORMAL ACTIVITY OF SUBJECTS OF THE INFORMATION AND TELECOMMUNICATION NETWORK

Rodionov V.D., Solovyov N.A.

Orenburg state university, Orenbug, e-mail: vvvdddrrr@gmail.com

This article is devoted to the development of a software system designed to identify abnormal activity of subjects of the information and telecommunications network. To achieve this goal, a system analysis was carried out, which revealed the need for automation of information processes, as well as the relevance of creating a new security system based on the analysis of analogues of existing information security tools. The basis for this system was the spectral analysis of network traffic, which allows you to detect anomalies and network attacks. To detect anomalies in this system, the calculation of Pearson correlation coefficients is used, which show the degree of similarity of the frequency indicators of network traffic at different time intervals. A discrete windowed Fourier transform is used to calculate these coefficients. The article shows the algorithm of the developed software system, which allows to achieve high efficiency in detecting anomalies in the information and telecommunications network. To verify the reliability of the calculations carried out, the Pearson correlation coefficient was calculated in the MatLab software environment with similar input data. The study showed that the developed system works efficiently and provides high accuracy in detecting anomalies in the information and telecommunications network. The program can determine both an anomaly and a specific attack by comparing the frequency indicators of the current network traffic with the recorded pattern.

Keywords: anomaly detection, network traffic, Fourier analysis, Pearson correlation coefficient, information security

С каждым годом вопрос использования средства обнаружения сетевых атак становится все актуальнее, так как растет количество сфер, в которых применяются сетевые технологии, а также увеличивается количество пользователей, использующих сетевые технологии. Рост сетевых технологий влияет на рост количества методов сетевых атак. Использование средств, обнаруживающих сетевые атаки по заранее прописанным правилам, становится неактуальным, так как новые типы атак не будут идентифицированы.

Компания Positive Techonologies в статье «Обнаружение распространенных угроз ИБ в сетевом трафике» приводит результаты исследования угроз в 60 организациях за 2021–2022 годы. Доля компаний, в которых была обнаружена подозрительная сетевая активность, составляет 93% [1].

Без использования средств обнаружения сетевых атак компании рискуют потерять прибыль и доверие у своих пользователей из-за таких последствий, как отказ в обслуживании и утечка данных.

Оперативное обнаружение защищает от последствий сетевых атак, что доказывает необходимость разработки программной среды, способной обнаруживать аномалии и новые типы сетевых атак.

Чаще всего для защиты информационно-телекоммуникационной сети применяются системы обнаружения сетевых атак Snort и Surricata. Они используют правила-шаблоны, которые контролируют сетевые пакеты, и уведомляют администратора, если сетевой трафик соответствует заранее прописанным правилам. Такой подход исключает выявление новых типов сетевых атак, а также требует жесткой редактуры правил, что осложняет администрирование таких средств.

Цель исследования – автоматизация информационных процессов обнаружения сетевых атак на основе анализа сетевого трафика. Для этого определены показатели, которые используются при обнаружении сетевых атак, создана математическая модель процесса идентификации сетевых атак и аномалий и разработано программное средство, реализующее предложенный метод.

Методы обнаружения сетевых атак

При рассмотрении методов обнаружения сетевых атак по способу интерпретации входных данных можно выделить два класса [2]:

− обнаружение аномалий;

− обнаружение злоупотреблений.

Методы обнаружения аномалий подразумевают поиск отклонений от обычного трафика внутри сети. Сложность данного метода заключается в определении допустимого отклонения и нормальной активности.

Методы обнаружения злоупотреблений заключаются в идентификации несанкционированных действий путем сравнения с шаблоном атаки. Шаблон атаки – совокупность действий, соответствующих поведению конкретной атаки. Параметры сетевого трафика отправляются на проверку, в которой происходит сравнение с различными шаблонами атаки и определяется, осуществляется атака или нет. Данный метод позволяет сразу узнать тип атаки, так как для каждой атаки разрабатывается свой шаблон, но это создает и определенные проблемы: нужно описывать каждую атаку, что является трудоемким процессом. Если атака не описана, то никаких предупреждений не будет выдано, так как все тесты будут пройдены.

Обнаружение аномалий может происходить двумя способами:

− проверка на соответствие шаблонам;

− спектральный анализ.

Спектральный анализ – метод обработки сетевого трафика, который позволяет описать частотный состав исследуемого трафика [3]. Быстрое преобразование Фурье переводит временные характеристики сетевого трафика в частотный вид [4].

Использование спектрального анализа позволяет выявлять скрытые закономерности сетевого трафика.

Для обнаружения аномалий в сетевом трафике фрагмент трафика T длиною N отсчетов сравнивается с предыдущим фрагментом T-1 такой же длины.

Для сравнения трафика составляются последовательности, которые могут состоять из:

− количества пакетов, распределенных по типу протоколов;

− количества всех пакетов за одну секунду;

− размера сетевого трафика за секунду;

− размера трафика определенного протокола за секунду;

− количества хостов, обнаруженных в сетевом трафике.

С помощью быстрого дискретного преобразования Фурье числовая одномерная последовательность длиною N преобразуется в частотный вид (1). После этого рассчитывается коэффициент корреляции Пирсона, который позволяет оценить схожесть частотных показателей сетевого трафика (2).

$$y(k)=\sum_{n=0}^{N-1}x(n)e^{-2\pi j\frac{kn}{N}} \quad (1)$$

$$R_{XY}=\frac{\sum\left(X-\overline{X}\right)\left(Y-\overline{Y}\right)}{\sqrt{\sum\left(X-\overline{X}\right)^2\sum\left(Y-\overline{Y}\right)^2}} \quad (2)$$

Здесь X – количество сетевых пакетов за секунду фрагмента T-1; $\overline{X}$ среднее – арифметическое пакетов в секунду для фрагмента T–1; Y – количество сетевых пакетов за секунду фрагмента T; $\overline{Y}$ – среднее арифметическое пакетов в секунду для фрагмента T.

Пороговые значения коэффициентов корреляции и оптимальный период измерений сетевого трафика выявлены экспериментальным путем [5]:

− оптимальный период измерений сетевого трафика – 10 секунд;

− лучший коэффициент корреляции для обнаружения аномалии – 0,3;

− лучший коэффициент корреляции для обнаружения атаки – 0,7.

Разработка программного средства

Понимание функционала разрабатываемой программы отражается в функциональной схеме. Функции разрабатываемой системы представляются в виде специальных объектов и утверждений.

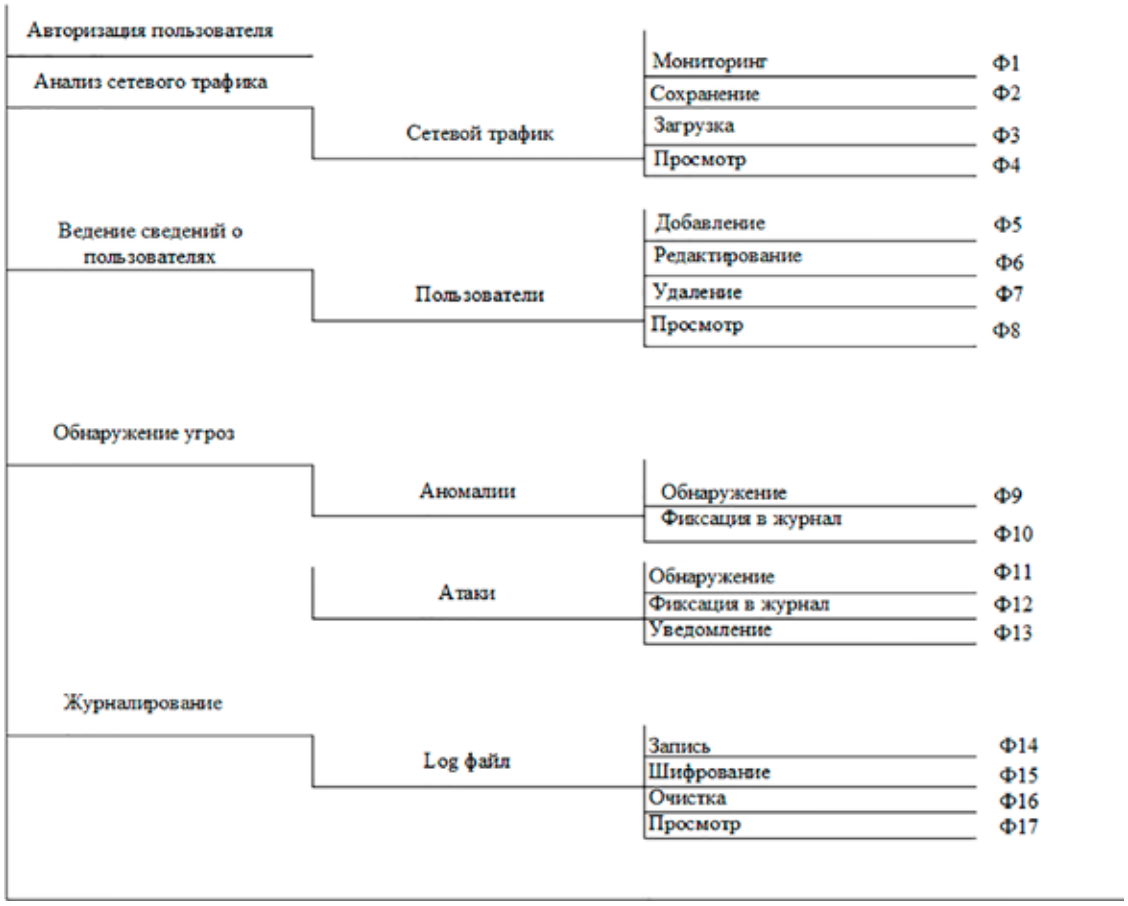

Рис. 1. Иерархия функций разрабатываемой программы

Основными функциями разрабатываемого программного средства являются:

− авторизация пользователей;
− анализ сетевого трафика;
− ведение сведений о пользователях;
− обнаружение угроз;
− журналирование.

Функции, реализуемые разрабатываемой программы, отображены в иерархии функций (рис. 1).

Функции взаимодействуют с зашифрованным журналом событий (.log файлом), с записанным сетевым трафиком (.pcap файл) и базой данных, в которой хранятся сведения о правах и аутентификационные данные пользователей.

Исходя из иерархии функции, построена диаграмма состояний, подробно описывающая процесс работы программы (рис. 2).

На основе выявленных функций и описания состояний была разработана программа на языке программирования Python 3.10 (рис. 3). На главном окне программы показаны четыре графика. Верхний левый график показывает количество пакетов в секунду за прошлый период в 10 секунд. Верхний правый график показывает количество пакетов за текущий период. Преобразованные в частотный вид показатели отображены на нижнем графике. Коэффициент корреляции Пирсона, рассчитанный между частотными показателями двух периодов, показан ниже графиков. Если коэффициент меньше 0,3, то происходит сравнение с частотными показателями, записанными во время атак. При сравнении с шаблонами атак, если коэффициент больше 0,7, появляется окно с оповещением об атаке, в ином случае появляется окно с оповещением об аномалии.

С главного окна пользователю доступна справочная информация о программе: Окна «Помощь», «О программе». Также пользователю доступна загрузка .pcap файла во вкладке «Файл», после которой произойдет анализ выбранного файла.

Во вкладке «Учетные записи» реализовано управление учетными записями системы. Пользователям системы доступны редактирование существующих учетных записей, создание новых и удаление старых.

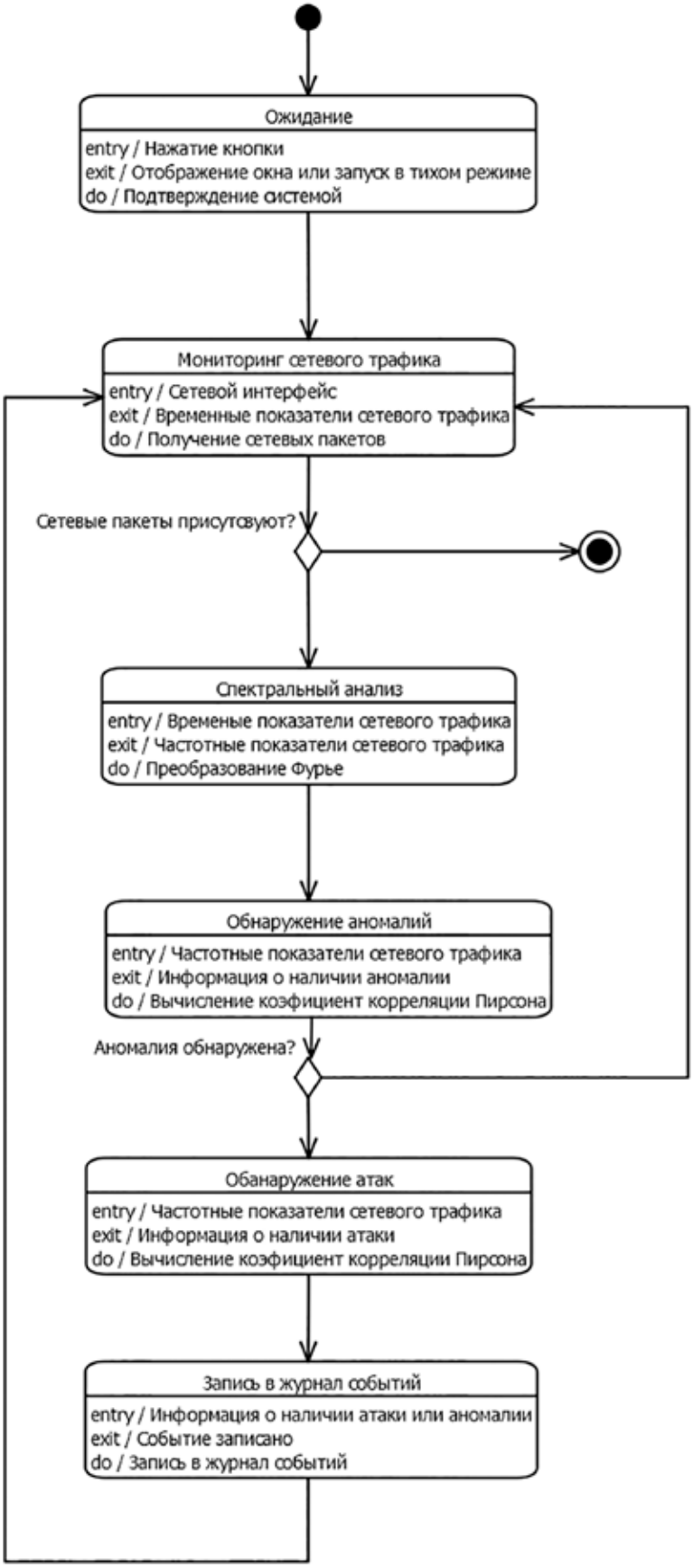

Рис. 2. Диаграмма состояний

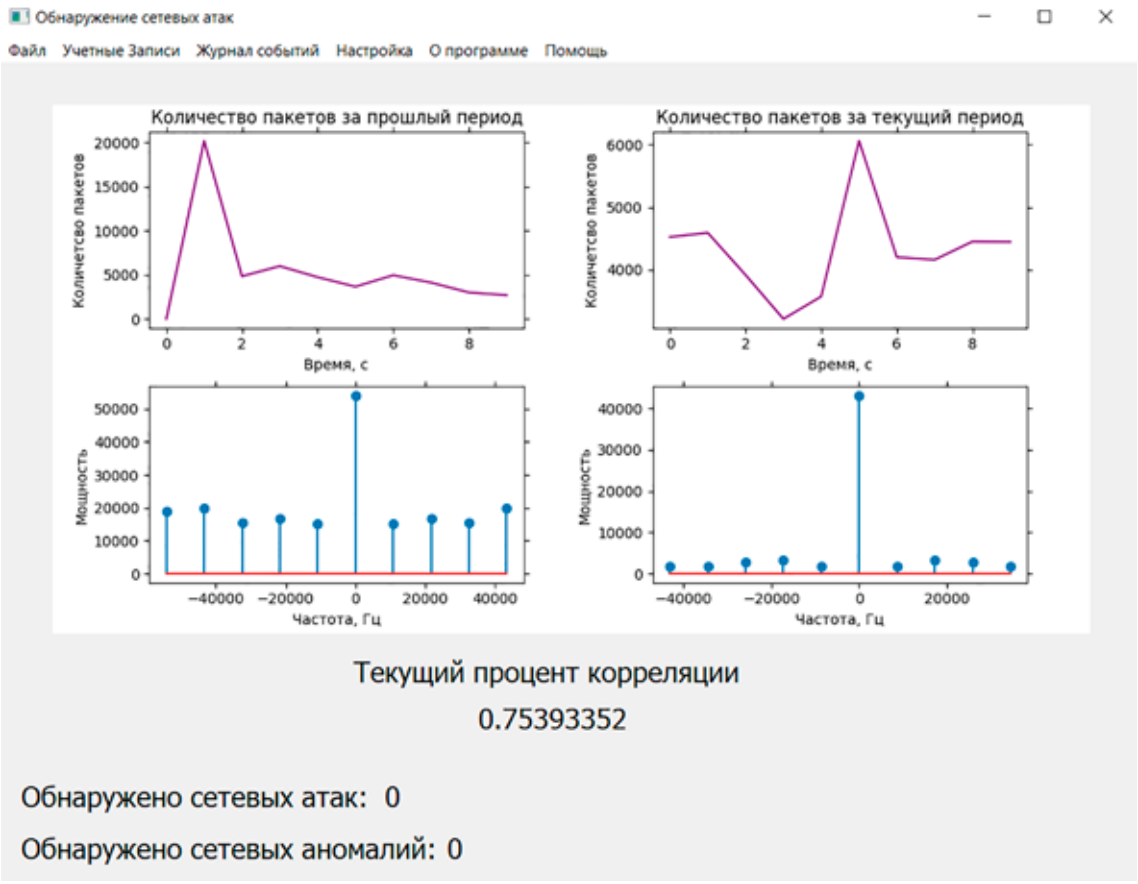

Рис. 3. Интерфейс АИС

$$MAS := [0\ \ 20170\ \ 4833\ \ 5981\ \ 4729\ \ 3656\ \ 4951\ \ 4116\ \ 2998\ \ 2690]$$

$$MAS2 := [4523\ \ 4590\ \ 3914\ \ 3211\ \ 3570\ \ 6061\ \ 4199\ \ 4158\ \ 4450\ \ 4446]$$

$$F := \mathrm{dft}(MAS) \qquad D := \mathrm{dft}(MAS2)$$

$$F1 := \mathrm{Re}(F) \qquad F2 := \mathrm{Re}(D)$$

$$CORC := \mathrm{Re}(\mathrm{corr}(F, D))$$

$$CORC = 0.754$$

Рис. 4. Результат расчета в MathCAD

Вкладка «Журнал событий» вызывает окно с отображением событий, записанных программой в .log файл. Пользователь может очистить журнал событий, если у него есть соответствующие права на данное действие.

Для проверки результатов, выдаваемых программным средством, произведено сравнение с результатами, рассчитанными в MathCAD. В качестве исходных данных представлены следующие массивы с количеством пакетов за T-1 и T:

[0, 20170, 4833, 5981, 4729, 3656, 4951, 4116, 2998, 2690]
[4523, 4590, 3914, 3211, 3570, 6061, 4199, 4158, 4450, 4446]

Выходным значением программы является коэффициент корреляции Пирсона (рис. 3). Программа выдала: 0,7539. Встроенная функция в MathCAD dft выполняет преобразование Фурье, а функция corr рассчитывает коэффициент корреляции Пирсона (рис. 4).

MathCAD выдал округленный результат 0,754, что доказывает точность выдаваемого результата разработанного программного средства.

Заключение

Данная статья описывает метод обнаружения сетевых атак и аномалий, основанный на спектральном анализе сетевого трафика. Также описывается разработанное программное средство, которое реализует предложенный метод обнаружения аномалий с помощью спектрального анализа. Основные функции программы включают авторизацию пользователей, анализ сетевого трафика, обнаружение угроз и журналирование.

Список литературы

1. Обнаружение распространенных угроз ИБ в сетевом трафике. [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/network-traffic-analysis-2022/ (дата обращения: 15.02.2023).

2. Лукацкий А.В. Обнаружение атак. СПб.: БХВ-Петербург, 2003. 608 с.

3. Браницкий А.А. Обнаружение аномальных сетевых соединений на основе гибридизации методов вычислительного интеллекта: дис. … канд. тех. наук. Санкт-Петербург, 2018. 305 с.

4. Медведев С.Ю. Преобразование Фурье и классический цифровой спектральный анализ. [Электронный ресурс]. URL: http://www.vibration.ru/preobraz_fur.shtml (дата обращения: 15.02.2023).

5. Родионов В.Д. Экспериментальное исследование защиты информационно-телекоммуникационной системы на основе спектрального анализа сетевого трафика // Научные исследования студентов и учащихся: сборник статей VIII Международной научно-практической конференции, Пенза, 07 февраля 2023 года. Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2023. С. 75-78.