УДК 004.056.2 Вестник УрФО № 1(51) / 2024, с. 53–59

Плаван А.И.

DOI: 10.14529/secur240107

МЕТОД ВЫЯВЛЕНИЯ АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ НА ОСНОВЕ ФИЛЬТРА КОЛМОГОРОВА-ВИНЕРА

В данной работе исследуется возможность применения оптимального линейного фильтра Колмогорова-Винера для задачи обнаружения аномалий в трафике. Метод основывается на возможности вычисления минимальной среднеквадратической ошибки фильтрации случайных процессов с известными автокорреляционными функциями.

Рассматриваются существующие статистические методы обнаружения аномалий, включая кибератаки, в сетевом трафике и предлагается новый метод обнаружения аномалий на основе среднеквадратической ошибки фильтрации.

Для оценки метода обнаружения аномалий используются записи трафика MAWI WIDE, строятся графики ROC-кривой и кривой Precision-Recall (точности-полноты) при различных пороговых значениях.

Продемонстрировано, что среднее значение метрики площади под кривой (AUC), равное 0,6 слишком мало для эффективного обнаружения аномалий в сетевом трафике и не позволяет использовать предложенный метод самостоятельно.

Предложено использовать числовые значения среднеквадратической ошибки фильтрации, получаемые в результате работы метода, в качестве дополнительного признака для повышения эффективности других методов на основе машинного обучения.

Ключевые слова: *обнаружение аномалий, сетевой трафик, фильтрация трафика, классификация трафика, среднеквадратическая ошибка, ROC-кривая, фильтр Колмогорова-Винера.*

Plavan A.I.

A METHOD FOR ANOMALY DETECTION IN NETWORK TRAFFIC BASED ON THE KOLMOGOROV-WIENER FILTER

This paper investigates the possibility of applying the optimal linear Kolmogorov-Wiener filter to the problem of anomaly detection in network traffic. The method is based on the capability of computing the minimum mean square error to filter random processes with known autocorrelation functions.

The existing statistical methods for detecting anomalies, including cyberattacks, in network traffic are reviewed and a new anomaly detection method based on mean square filtering error is proposed.

MAWI WIDE traffic records are used to evaluate the anomaly detection method, and the ROC and Precision-Recall curves are plotted at different threshold values.

It is demonstrated that the average value of the area under curve (AUC) metric of 0.6 is too small to effectively detect anomalies in network traffic and does not allow the proposed method to be used on its own.

It is suggested that the numerical values of mean square error obtained as a result of method execution can be used as an additional feature to improve the efficiency of other machine learning-based methods, which is to be further verified.

Keywords: *anomaly detection, network traffic, traffic filtering, traffic classification, MSE, ROC curve, Wiener filter.*

Введение

В современном информационном обществе сетевые технологии стали неотъемлемой частью повседневной жизни, обеспечивая передачу данных и обмен информацией на глобальном уровне. Однако с ростом зависимости от цифровых технологий также возрастает и риск кибератак, направленных на нарушение конфиденциальности, целостности и доступности данных. В этом контексте обеспечение безопасности сетей и выявление вторжений в сетевом трафике становятся критическими задачами. Одним из ключевых методов выявления вторжений является анализ сетевого трафика с использованием различных алгоритмов и техник.

Зачастую злоумышленники используют сеть в качестве транспорта для доставки вредоносных программ до целевой системы или для доступа к конфиденциальным данным, расположенным на недостаточно защищенных сетевых ресурсах. Один из принципов, на которых основаны системы обнаружения вторжений и другие средства защиты информации, состоит в том, что получить доступ к сетевому ресурсу невозможно, не повлияв на трафик в сети, то есть, не установив соединение с некоторым сервером и не послав пакеты с некоторыми данными. Возникновение нового источника трафика приводит к изменению общего состояния и значений статистических характеристик сети. Необычный трафик также может быть вызван ошибками в настройках сетевого оборудования. Такой трафик называется аномальным, или просто аномалией.

Обнаружение аномалий применяется не только в задачах выявления вредоносного трафика, но и во многих других областях, например, выявление мошенничества в банках. Методы, используемые при этом, можно разделить на две группы: обнаружение злоупотреблений (специфичных сигнатур) или обнаружений аномалий [1]. Основным преимуществом второй группы является то, что такие методы могут обнаруживать ранее неизвестные атаки. К таким методам относятся: классификация k-средних, метод главных компонент, метод «случайного леса» на основе ансамбля решающих деревьев и другие методы машинного обучения и нейронных сетей [2–4].

Целью данной статьи является исследование потенциала среднеквадратической ошибки фильтрации как признака наличия аномалий, включая кибератаки, в сетевом трафике.

Обзор литературы

Существует несколько уровней, на которых можно выполнять классификацию данных с целью обнаружения аномалий в трафике: на уровне отдельных пакетов, потоков (однонаправленных или двунаправленных), сетевых интерфейсов или всего трафика в целом [5].

Предварительно трафик необходимо специальным образом подготовить, разбив на набор наблюдений, которые и будет классифицированы. Обычно выделяют наборы сетевых потоков, идентифицируемых по следующим признакам [6]: IP-адрес отправителя, IP-адрес получателя, Порт отправителя, Порт получателя, Идентификатор протокола (опционально).

В работе [3] предлагается метод на основе классификации отдельных HTTP запросов с использованием гибридной нейронной сети для применения на уровне WAF (Web Application Firewall).

Для применения статистических методов требуется объем данных достаточного разме-

ра, чтобы выявить статистические закономерности. Объем сетевых потоков, измеряемый в количестве пакетов, может быть недостаточным для этой цели. Например в [7] было выявлено, что типичная длина TCP-потока составляет 122 пакета. Более предпочтительным является рассмотрение срезов общего трафика (пакетов всех потоков) за определенный интервал времени.

Известно, что сетевой трафик обладает свойством самоподобия, или фрактальности [8]. Этим свойством обладают как интервалы времени между поступлениями пакетов (inter-arrival times), так и суммарное количество пакетов или байт в единицу времени [9]. Самоподобие предполагает наличие автокорреляционной функции (АКФ) определенного вида. Соответственно, можно предположить, что ожидаемый трафик некоторой сети в определенное время суток может быть охарактеризован АКФ конкретного вида. Знание об этих закономерностях сетевого трафика должно учитываться при разработке новых способов обнаружения аномалий и атак для повышения их эффективности.

В [10] приводится обзор существующих подходов к обнаружению сетевых аномалий на основе методов фрактального и мультифрактального анализа, исходя из того, что сетевой трафик проявляет фрактальные свойства и может быть охарактеризован некоторыми значениями показателя Херста. При возникновении аномалии значения показателя Херста и фрактальной размерности могут отклоняться от ожидаемого.

В работе [11] предлагается метод на основе корреляции между значениями переменных MIB (Management Information Base) протокола SNMP. В течение периода обучения записывается матрица корреляции в каждый момент времени. Для обнаружения аномалий используется значение нормализованной минимальной среднеквадратической ошибки (СКО) фильтра Колмогорова-Винера, называемого также фильтром Винера. Пороговые значения индикатора вычисляются из собственных векторов корреляционной матрицы при нормальном режиме работы сети. Превышение этих значений СКО является признаком наличия аномалий в трафике.

В [12] также предлагается использовать метод на основе среднеквадратической ошибки (СКО) фильтрации, но применительно к последовательности интервалов времени между поступлениями пакетов. Значение импульсной характеристики фильтра может быть не оптимальным, и в этом случае ошибка будет отлична от нуля. Для случая оптимального фильтра ошибка должна быть равна нулю. Индикатором аномалии служит отклонение значения СКО от эталонного значения, полученного в течение периода обучения. Также в работе предлагается упрощенный вариант метода, основанный на сравнении корреляционных функций эталонного и текущего трафика в точке $\tau = 0$, но и в точке $\tau = \tau_0$, соответствующей интервалу корреляции.

В данной работе исследуется возможность применения оптимального линейного фильтра Винера для задачи обнаружения аномалий в трафике. При этом также учитывается «шум» наблюдений нормального трафика, вызванный изменениями в загрузке сети, значений MTU (maximum transmission unit, максимальный размер полезной нагрузки пакета), использованием альтернативных путей между отправителем и получателем и т.д.

Методология

Сетевой трафик, выражаемый в виде интервалов времени между поступлением пакетов, или количества пакетов или байт в единицу времени можно представить в виде случайной последовательности

$$x_k = \xi_k + \eta_k \quad k \in \{1,\ldots,N\},$$

где ξ_k – нормальный трафик, η_k – шум (случайная составляющая временного ряда), N – количество отсчетов.

Шум можно оценить с использованием одного из методов, рассмотренных в работе [13]. В данной работе шум будет рассматриваться как некоррелированный гауссовский процесс с оцениваемой дисперсией.

Фильтр Винера, позволяет получить оптимальную по критерию СКО оценку стационарного сигнала по аддитивной смеси полезного сигнала с шумом. При этом неизбежно возникает ошибка оценивания (фильтрации), которая определяется как

$$\varepsilon = \frac{1}{N}\sum_{k=1}^{N}\left(\hat{\xi}_k - \xi_k\right)^2,$$

где $\hat{\xi}_k$ – оценка k – го отсчёта нормального трафика.

Выражение для вычисления импульсной переходной функции $\mathbf{h} = \{h_1, h_2, \ldots, h_M\}$ фильтра Винера с порядком M в матричной форме выглядит следующим образом [14]

$$\mathbf{h} = \mathbf{B}_{\mathbf{x}}^{-1} \cdot \mathbf{b}_{\mathbf{x}\xi},$$

где $\mathbf{b}_{\mathbf{x}^{\xi}}$ – вектор взаимной корреляции между входным и ожидаемым полезным сигналом, представляющим нормальный трафик,

$$\mathbf{b}_{\mathbf{x}^{\xi}} = \left\{B_{x\xi}(0), B_{x\xi}(1), \ldots, B_{x\xi}(M)\right\},$$

здесь $B_{x\xi}(m)$ – корреляция значений отсчётов сигнала на входе фильтра и отсчётов сигнала, представляющего нормальный трафик,

$$B_{x\xi}(m) = E\left[(x_k - E[x])(\xi_{k+m} - E[\xi])\right],$$

$\mathbf{B}_{\mathbf{x}}$ – корреляционная матрица входного сигнала

$$\begin{pmatrix} B_x(0) & B_x(1) & \cdots & B_x(M) \\ B_x(1) & B_x(0) & \cdots & B_x(M-1) \\ \vdots & \vdots & \ddots & \vdots \\ B_x(M) & B_x(M-1) & \cdots & B_x(0) \end{pmatrix}.$$

При этом минимальная СКО фильтра записывается в виде

$$\varepsilon^2_{\min} = \boldsymbol{\sigma}^2_{\boldsymbol{\xi}} - \mathbf{h}^{\mathbf{T}} \cdot \mathbf{B}_{\mathbf{x}} \cdot \mathbf{h},$$

или (без использования импульсной переходной функции [14])

$$\varepsilon^2_{\min} = \boldsymbol{\sigma}^2_{\boldsymbol{\xi}} - \mathbf{b}^{\mathbf{T}}_{\mathbf{x}} \cdot \mathbf{B}^{-1}_{\mathbf{x}\boldsymbol{\xi}} \cdot \mathbf{b}_{\mathbf{x}\boldsymbol{\xi}}.$$

При дисперсии шума, близкой к нулю, минимальная СКО фильтра Винера тоже будет стремится к нулю. В случае отсутствия шума как такового, минимальная СКО будет равна нулю, но и сам фильтр при этом будет пропускать сигнал на входе без изменений, то есть фильтрация не будет производится. Импульсная характеристика фильтра в данном случае будет выглядеть как единичный импульс [15, 16], т.е.

$$\lim_{\sigma^2_{\eta} \to 0} \varepsilon^2_{min} = 0,$$

где σ^2_{η} – дисперсия шума.

Во время периода обучения производятся наблюдения нормального трафика. Трафик разбивается на интервалы, в течение которых он сохраняет стационарность. Будем считать, что в течение определенного времени суток трафик остается стационарным. Для каждого интервала определяется АКФ и дисперсия трафика. На основе этих характеристик синтезируется оптимальный линейный фильтр и определяется его минимальная СКО. Для определения аномалий, к трафику, наблюдаемому на текущем временном интервале, применяется соответствующий фильтр. Для сигнала на выходе фильтра вычисляется СКО и сравнивается с минимальным значением СКО для фильтра. Отклонение значения ошибки фильтрации от порогового значения служит признаком аномалии.

Для определения пороговых значений возможно использовать значение СКО, нормализованное относительно дисперсии нормального трафика [14]

$$m^2_{min} = 1 - \frac{\hat{\sigma}^2_{\xi}}{\sigma^2_{\xi}},$$

где $\hat{\sigma}^2_{\xi}$ – дисперсия оценки сигнала на выходе фильтра, σ^2_{ξ} – дисперсия ожидаемого сигнала, соответствующего нормальному трафику.

Таким образом задается верхняя граница допустимых значений, равная единице. Нижней границей является нормализованное значение минимальной СКО

$$m^2_{min} = \frac{\varepsilon^2_{min}}{\sigma^2_{\xi}}.$$

Преобразовав вычисленное для текущего трафика значение СКО из диапазона значений $\left[m^2_{min}\right]$ к диапазону [0, 1]

$$m^2_{norm} = \frac{m^2 - \varepsilon^2_{min}}{1 - \varepsilon^2_{min}},$$

и изменяя пороговое значение δ между 0 и 1, можно влиять на чувствительность классификатора и вероятность ложноположительных срабатываний. Таким образом, формулу для индикатора аномалий можно записать как:

$$m^2_{norm} = \begin{cases} > 1 & - \text{ аномалия} \\ \leq \delta & - \text{ нет аномалии} \\ < m^2_{min} & - \text{ аномалия} \end{cases}. \quad (1)$$

Результаты

Метод был проверен на наборе 15-минутных записей сетевого трафика из архива MAWI WIDE, собранного с 11 по 17 октября 2021 года. Трафик был разбит на минутные интервалы, каждый из которых рассматривался отдельно. Каждому интервалу была присвоена метка аномальности на основе того, присутствуют ли на этом интервале аномалии в исходном датасете. Аномальными были признаны 64 из 105 (60%) интервалов, то есть датасет является практически сбалансированным.

На записях трафика, собранных в один день, производилось «обучение модели» (синтез фильтров для каждого минутного интервала). Можно сказать, что для каждой минуты использовалась своя собственная модель. Шум считался гауссовским с дисперсией = σ^2_{ξ}. Для каждой соответствующей минутной записи за другие дни было вычислено значение индикатора по формуле (1). По ним были построены графики ROC-кривой и кривой Precision-Recall (точности-полноты) при различных значениях порогового значения δ, которые представлены на рис. 1.

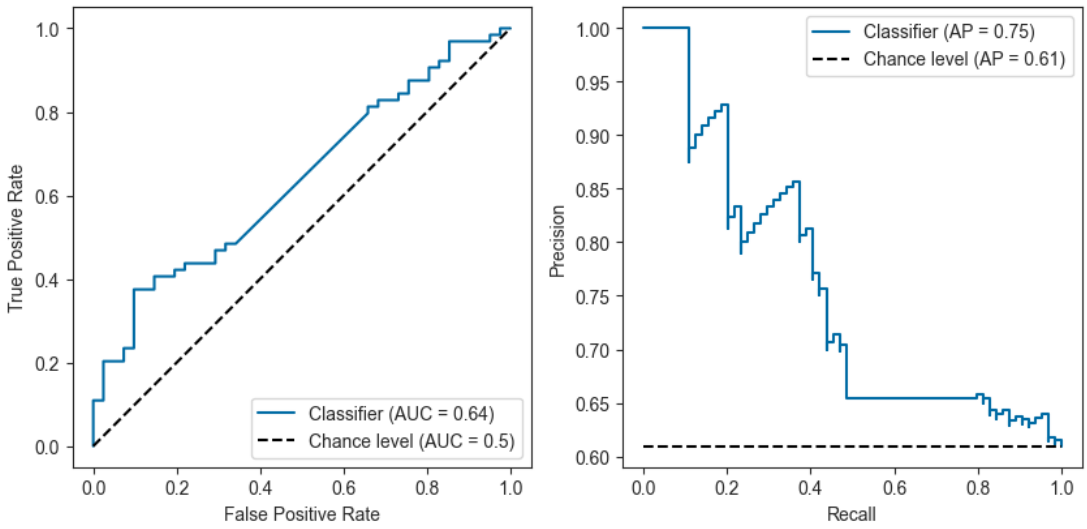

Рис. 1. Графики ROC-кривой и кривой Precision-Recall. Classifier – значения для предлагаемого метода, Chance level – значения для слепого угадывания, AUC – площадь под кривой, AP – средняя точность.

Обсуждение

ROC-кривая, или кривая рабочей характеристики приемника, первоначально появилась в теории обнаружении сигналов и использовалась для наглядной иллюстрации связи между относительным количеством правильных попаданий (детектировании сигнала при наличии шума) и ложных тревог (детектировании сигнала при его отсутствии). Аналогичным образом, ROC-кривая применяется для иллюстрации чувствительности бинарных классификаторов.

Классификатор с высокой точностью, но низким показателем полноты будет обнаруживать мало аномалий, но большинство предсказанных ей меток аномальности будут верными. Модель с высоким показателем полноты и низкой точностью наоборот будет отмечать много аномальных результатов, но при этом многие результаты будут ложноположительными. Это должно учитываться при выборе порогового значения δ.

Стоит отметить, что внешний вид графиков отличается в зависимости от того, для трафика какого дня производилось обучение. Но во всех случаях метрика площади под кривой (AUC) составляет около 0,6. Это говорит о том, что метод обладает предсказательной способностью, пусть и не очень высокой. Более того, при использовании методов машинного обучения обычно рассматривается несколько признаков [2, 3] в совокупности, здесь же рассматривается всего один. Можно предположить, что производительность существующих методов машинного обучения можно улучшить, добавив этот новый признак на основе минимальной СКО.

Также стоит отметить, что в случаях, когда обучение производилось для записей трафика, собранных в выходные дни (16 и 17 октября), метрика AUC оказывалась даже меньше 0,5. Это может говорить о том, что в выходные дни корреляционная структура трафика меняется (трафик не является стационарным), и для таких периодов необходимо использовать отдельные модели.

Вывод

В данной работе был предложен новый метод обнаружения аномалий в сетевом трафике на основе фильтра Колмогорова-Винера. Метод заключается в вычислении импульсной характеристики и минимальной СКО фильтра для последовательностей интервалов между поступлениями пакетов. Для каждого временного интервала, на котором эти интервалы сохраняют стационарность, вычисляется свой фильтр. Затем фильтр применяется к текущему трафику, полученная СКО нормируется и сравнивается с пороговым значением.

Полученное значение AUC не позволяет использовать данный метод для обнаружения аномалий самостоятельно, но, предположительно, получаемые значения могут быть использованы в качестве дополнительного признака для повышения эффективности других методов на основе машинного обучения.

Литература

1. Шелухин О.И. Обнаружение вторжений в компьютерные сети [сетевые аномалии] / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. – М.: Горячая линия-Телеком, 2018. – 220 с.

2. Обзор методов обнаружения аномалий в потоках данных / В.П. Шкодырев [и др.] // Second Conference on Software Engineering and Information Management (SEIM-2017). – Санкт-Петербург, 2017. – С. 50

3. Методика раннего обнаружения компьютерных атак в сетевом трафике сети передачи данных / О.С. Лаута [и др.] // Сборник научных статей по материалам IV Всероссийской научно-технической конференции «Безопасность информационных технологий». – Пенза: ПГУ, 3 апреля 2022 г. – Т. 1. – С. 126

4. Дик Д.И. Обнаружение аномалий пользовательских сеансов веб-приложений с использованием рекуррентных нейронных сетей / Д.И. Дик, В.В. Москвин // Материалы II национальной научной конференции. Отв. редактор Е.Н. Полякова. НАУКА XXI ВЕКА: ТЕХНОЛОГИИ, УПРАВЛЕНИЕ, БЕЗОПАСНОСТЬ. – Курган: Курганский государственный университет, 21 апреля 2022 г. – С. 55-61

5. MAWILab: combining diverse anomaly detectors for automated anomaly labeling and performance benchmarking / R. Fontugne [и др.] // Proceedings of the 6th International Conference Co-NEXT '10: Conference on emerging Networking Experiments and Technologies. – Philadelphia Pennsylvania: ACM, 2010. – MAWILab. – С. 1-12, DOI: https://doi.org/10.1145/1921168.1921179

6. Волков Д. Энтропия и выявление аномалий сетевого трафика [электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/neoflex/articles/561438/ (дата обращения: 05.08.2023)

7. Jurkiewicz P. Flow length and size distributions in campus Internet traffic / P. Jurkiewicz, G. Rzym, P. Boryło // Computer Communications. – 2021. – Т. 167. – С. 15-30, DOI: https://doi.org/10.1016/j.comcom.2020.12.016

8. On the self-similar nature of Ethernet traffic / W.E. Leland [и др.] // Conference proceedings on Communications architectures, protocols and applications. – 1993. – С. 183-193

9. Плаван А.И. Моделирование самоподобного трафика с использованием модели Poisson-Pareto-Burst-Process в симуляторе ns-3 / А.И. Плаван // XXVII Международная научно-техническая конференция «Современные средства связи». – Минск, Республика Беларусь: Белорусская государственная академия связи, 27–28 октября 2022 г. – С. 197-199

10. Басараб М.А. Обнаружение аномалий в информационных процессах на основе мультифрактального анализа / М.А. Басараб, И.С. Строганов // Вопросы кибербезопасности. – 2014. – № 4 (7). – С. 30-40

11. Al-Kasassbeh M. Network intrusion detection with wiener filter-based agent / M. Al-Kasassbeh // World Appl. Sci. J. – 2011. – Т. 13. – № 11. – С. 2372-2384

12. Карташевский В.Г. Фильтрация наблюдаемого трафика как способ обнаружения вторжений / В.Г. Карташевский, И.С. Поздняк // Вестник УрФО. – 2019. – Т. 19. – № 1 (31). – С. 17-22, DOI: https://doi.org/10.14529/secur190103

13. Копырин А.С. Технологии обработки и очистки данных, выявления и устранения шумов на временном ряду / А.С. Копырин, Е.В. Видищева // Вестник Академии знаний. – 2020. – № 4 (39). – С. 220-228

14. Haykin S.S. Adaptive filter theory / S.S. Haykin. – 4th ed. – Upper Saddle River, N.J: Prentice Hall, 2002. – 920 с.

15. Плаван А.И. Выявление аномалий в сетевом трафике по критерию среднеквадратической ошибки фильтрации линейного преобразования / А.И. Плаван, И.С. Поздняк // VII Всероссийская научно-техническая конференция «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности». – Таганрог: Южный федеральный университет, 5–11 апреля 2021 г. – С. 70-74

16. Плаван А.И. Среднеквадратическая ошибка фильтрации как критерий обнаружения аномалий сетевого трафика / А.И. Плаван, В.Г. Карташевский // Вестник Российского нового университета. Серия: Сложные системы модели, анализ и управление. – 2023. – № 1. – С. 94-101, DOI: https://doi.org/10.18137/RNU.V9187.23.01.P.94

References

1. Shelukhin O.I. Obnaruzhenie vtorzheniy v komp'yuternye seti [setevye anomalii] / O.I. Shelukhin, D.Zh. Sakalema, A.S. Filinova. – M.: Goryachaya liniya-Telekom, 2018. – 220 s.

2. Obzor metodov obnaruzheniya anomaliy v potokakh dannykh / V.P. Shkodyrev [et al.] // Second Conference on Software Engineering and Information Management (SEIM-2017). – Sankt-Peterburg, 2017. – S. 50

3. Metodika rannego obnaruzheniya komp'yuternykh atak v setevom trafike seti peredachi dannykh / O.S. Lauta [et al.] // Sbornik nauchnykh statey po materialam IV Vserossiyskoy nauchno-tekhnicheskoy konferentsii «Bezopasnost' informatsionnykh tekhnologiy». – Penza: PGU, 3 aprelya 2022 g. – T. 1. – S. 126

4. Dik D.I. Obnaruzhenie anomaliy pol'zovatel'skikh seansov veb-prilozheniy s ispol'zovaniem rekurrentnykh neyronnykh setey / D.I. Dik, V.V. Moskvin // Materialy II natsional'noy nauchnoy konferentsii. Otv. redaktor E.N. Polyakova. NAUKA XXI VEKA: TEKhNOLOGII, UPRAVLENIE, BEZOPASNOST". – Kurgan: Kurganskiy gosudarstvennyy universitet, 21 aprelya 2022 g. – S. 55-61

5. MAWILab: combining diverse anomaly detectors for automated anomaly labeling and performance benchmarking / R. Fontugne [et al.] // Proceedings of the 6th International Conference Co-NEXT '10: Conference on emerging Networking Experiments and Technologies. – Philadelphia Pennsylvania: ACM, 2010. – MAWILab. – S. 1-12, DOI: https://doi.org/10.1145/1921168.1921179

6. Volkov D. Entropiya i vyyavlenie anomaliy setevogo trafika [elektronnyy resurs]. – Rezhim dostupa: https://habr.com/ru/companies/neoflex/articles/561438/ (data obrashcheniya: 05.08.2023)

7. Jurkiewicz P. Flow length and size distributions in campus Internet traffic / P. Jurkiewicz, G. Rzym, P. Boryło // Computer Communications. – 2021. – T. 167. – S. 15-30, DOI: https://doi.org/10.1016/j.comcom.2020.12.016

8. On the self-similar nature of Ethernet traffic / W.E. Leland [et al.] // Conference proceedings on Communications architectures, protocols and applications. – 1993. – S. 183-193

9. Plavan A.I. Modelirovanie samopodobnogo trafika s ispol'zovaniem modeli Poisson-Pareto-Burst-Process v simulyatore ns-3 / A.I. Plavan // XXVII Mezhdunarodnaya nauchno-tekhnicheskaya konferentsiya «Sovremennye sredstva svyazi». – Minsk, Respublika Belarus': Belorusskaya gosudarstvennaya akademiya svyazi, 27–28 oktyabrya 2022 g. – S. 197-199

10. Basarab M.A. Obnaruzhenie anomaliy v informatsionnykh protsessakh na osnove mul'tifraktal'nogo analiza / M.A. Basarab, I.S. Stroganov // Voprosy kiberbezopasnosti. – 2014. – № 4 (7). – S. 30-40

11. Al-Kasassbeh M. Network intrusion detection with wiener filter-based agent / M. Al-Kasassbeh // World Appl. Sci. J. – 2011. – T. 13. – № 11. – S. 2372-2384

12. Kartashevskiy V.G. Fil'tratsiya nablyudaemogo trafika kak sposob obnaruzheniya vtorzheniy / V.G. Kartashevskiy, I.S. Pozdnyak // Vestnik UrFO. – 2019. – T. 19. – № 1 (31). – S. 17-22, DOI: https://doi.org/10.14529/secur190103

13. Kopyrin A.S. Tekhnologii obrabotki i ochistki dannykh, vyyavleniya i ustraneniya shumov na vremennom ryadu / A.S. Kopyrin, E.V. Vidishcheva // Vestnik Akademii znaniy. – 2020. – № 4 (39). – S. 220-228

14. Haykin S.S. Adaptive filter theory / S.S. Haykin. – 4th ed. – Upper Saddle River, N.J: Prentice Hall, 2002. – 920 s.

15. Plavan A.I. Vyyavlenie anomaliy v setevom trafike po kriteriyu srednekvadraticheskoy oshibki fil'tratsii lineynogo preobrazovaniya / A.I. Plavan, I.S. Pozdnyak // VII Vserossiyskaya nauchno-tekhnicheskaya konferentsiya «Fundamental'nye i prikladnye aspekty komp'yuternykh tekhnologiy i informatsionnoy bezopasnosti». – Taganrog: Yuzhnyy federal'nyy universitet, 5–11 aprelya 2021 g. – S. 70-74

16. Plavan A.I. Srednekvadraticheskaya oshibka fil'tratsii kak kriteriy obnaruzheniya anomaliy setevogo trafika / A.I. Plavan, V.G. Kartashevskiy // Vestnik Rossiyskogo novogo universiteta. Seriya: Slozhnye sistemy modeli, analiz i upravlenie. – 2023. – № 1. – S. 94-101, DOI: https://doi.org/10.18137/RNU.V9187.23.01.P.94

ПЛАВАН Алексей Игоревич, аспирант кафедры информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Поволжский государственный университет телекоммуникаций и информатики». 443010, г. Самара, ул. Л. Толстого, д. 23. E-mail: aleksej-plavan@ya.ru

PLAVAN Aleksey Igorevich, Postgraduate student of the Department of Information Securityof the Federal State Budgetary Educational Institution of Higher Education "Povolzhskiy State University of Telecommunications and Informatics". 443010, Samara, L. Tolstoy str., 23. E-mail: aleksej-plavan@ya.ru