Методика обнаружения и противодействия многовекторным угрозам нарушения информационной безопасности децентрализованной IoT системы

В. И. Петренко, Ф. Б. Тебуева, М. Г. Огур, Г. И. Линец, В. П. Мочалов

В статье предлагается методика обнаружения и противодействия многовекторным угрозам информационной безопасности в децентрализованных IoT-сетях. Предложенное решение интегрирует многомерную реконструкцию сетевого трафика, гибридную архитектуру свёрточных нейронных сетей (CNN) и LSTM для анализа пространственно-временных зависимостей, а также алгоритм очистки данных для снижения вычислительных затрат. Тестирование на датасете CIC IoT Dataset 2023 позволило провести синтезированный эксперимент и сравнить эффективность методики с прототипными методами. Результаты демонстрируют повышенные показатели точности (99,1%), полноты (99,3%) и вычислительной эффективности, снижая затраты на обработку данных на 20–30%. Предложенное решение обеспечивает высокую производительность в условиях ограниченных вычислительных ресурсов и универсально для обнаружения различных типов атак, включая DDoS, Brute Force, SQL-инъекции и XSS.

Ключевые слова **– Интернет вещей (IoT), многовекторные угрозы, обнаружение атак, многомерная реконструкция, свёрточные нейронные сети (CNN), LSTM, алгоритм очистки данных (DPA), децентрализованные сети, кибербезопасность, DDoS-атаки, информационная безопасность.**

I. Введение

С экспоненциальным ростом числа подключённых устройств в Интернете вещей (IoT) объёмы данных и сетевого трафика значительно увеличиваются, что делает IoT-системы особенно уязвимыми к кибератакам, таким как DDoS, Brute Force, SQL-инъекции и XSS. Многовекторные атаки, использующие комбинации различных методов, представляют особую угрозу, обходя традиционные системы защиты. В условиях ограниченных вычислительных ресурсов IoT-устройств возникает необходимость в разработке лёгких и эффективных методов для обнаружения таких атак.

Существующие исследования в области кибербезопасности IoT предлагают различные подходы, включая методы глубокого обучения, реконструкцию трафика и алгоритмы предобработки данных. Однако большинство из них либо сосредоточены на отдельных типах угроз, либо требуют значительных вычислительных ресурсов, что ограничивает их применение в децентрализованных IoT-системах с ограниченными возможностями.

В данной работе предложена новая методика обнаружения и противодействия многовекторным угрозам в децентрализованных IoT-сетях. Методика сочетает многомерную реконструкцию сетевого трафика с использованием автоэнкодера, гибридную архитектуру CNN+LSTM для анализа пространственно-временных зависимостей и алгоритм очистки данных (DPA) для снижения вычислительных затрат. Целью является повышение успешно выявленных атак вкупе со снижением потребления вычислительных ресурсов с учетом архитектуры IoT.

Эффективность методики была подтверждена посредством синтезированного эксперимента с использованием CIC IoT Dataset 2023, содержащего разнообразные типы атак на IoT-сети. Результаты продемонстрировали существенное улучшение по сравнению с существующими методами как в точности обнаружения, так и в вычислительной эффективности, что подтверждает её применимость для обеспечения безопасности современных децентрализованных IoT-сетей.

II. Анализ литературы

В статье [1] представлен метод выявления уязвимостей в протоколах IoT, основанный на сочетании параллельного нечеткого алгоритма и генетического алгоритма для оптимизации процесса тестирования. Нечеткий алгоритм фуззифицирует входные данные посредством функций принадлежности, моделируя нестандартные сценарии и выявляя потенциальные уязвимости протоколов. Параллельная обработка позволяет одновременно анализировать несколько протоколов, повышая производительность и полноту проверки. Генетический алгоритм оптимизирует генерацию тестов, увеличивая вероятность обнаружения уязвимостей; использование

Статья получена 13 октября 2024. Данное исследование выполнено при поддержке гранта ИБ МТУСИ, соглашение № 40469/17-23-К.
В. И. Петренко, канд. техн. наук, зав. кафедрой, vipetrenko@ncfu.ru
Ф. Б. Тебуева, д-р физ.-мат. наук, профессор, ftebueva@ncfu.ru
М. Г. Огур, старший преподаватель, ogur26@gmail.com
Г. И. Линец, д-р техн. наук, профессор, glinetc@ncfu.ru
В. П. Мочалов, д-р техн. наук, профессор, vmochalov@ncfu.ru
Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет», Ставрополь

кодирования Грея ускоряет эволюцию решений. Оценка эффективности каждого теста через функцию пригодности обеспечивает точное выявление критических уязвимостей и минимизацию ложных срабатываний, что существенно повышает эффективность и скорость тестирования протоколов IoT.

В работе [2] предложен инновационный подход к обнаружению вредоносного ПО в сетях IoT, основанный на преобразовании временных рядов поведения программ в изображения для последующего анализа методами машинного обучения. Математическая модель трансформирует динамические характеристики работы программ в бинарные изображения, где каждая временная метка соответствует пикселю, а наличие определённой функции отражается в значении этого пикселя. Таким образом, формируется структурированное изображение, содержащее информацию о поведении программного обеспечения во времени, что позволяет эффективно выявлять вредоносную активность.

Основной задачей предложенного метода является оценка уровня вредоносности программы, обозначенного как ξ, который варьируется от 0 до 1. Временной ряд Ξ задаётся как набор функций ϕ_i, наблюдаемых в моменты времени τ_i, что представлено в виде:

$$\Xi = [\xi, \phi_1 : \tau_1, \phi_2 : \tau_2, \dots, \phi_n : \tau_n]. \quad (1)$$

После преобразования временных рядов в изображения, используются три различных подхода для анализа данных: кластеризация, вероятностный метод и глубокое обучение с применением свёрточных нейронных сетей (CNN). Эти методы обеспечивают комплексный анализ и классификацию поведения программ, что значительно повышает точность обнаружения вредоносных программ, достигая наилучших результатов по метрикам точности и F1-меры по сравнению с традиционными методами анализа вредоносного ПО.

В статье [3] предложен метод раннего обнаружения DDoS-атак на устройства Интернета вещей (IoT) с использованием многомерной реконструкции и отображения функций. Основной математический аппарат основан на применении очередной структуры для накопления сетевого трафика и последующего анализа его частотных характеристик. Важной составляющей метода является многомерная реконструкция, которая реализована через автоэнкодер. В ходе обучения автоэнкодера минимизируется ошибка реконструкции, что позволяет отличить нормальный трафик от вредоносного.

Математическая модель представлена многомерным реконструкционным автоэнкодером, который обучается на различных типах трафика, создавая матрицу выхода x_M, представляющую K типов данных. Оптимизация модели происходит путём минимизации ошибки реконструкции, измеряемой через среднеквадратичную ошибку (MSE):

$$dist(x, x_M) = \sqrt{\sum \left(x_i - x_{M,i}\right)^2}. \quad (2)$$

Оптимизация позволяет выделить характерные различия между нормальными данными и трафиком атак. Дополнительно применяется отображение функций с помощью гиперболической тангенс-функции для усиления сходства трафика одного типа и различий между различными типами данных, что повышает эффективность классификации.

В статье [4] предложена математическая модель для защиты сетей IoT с использованием глубокого обучения и автоматического извлечения признаков. Основной математический аппарат работы включает два модуля: модуль извлечения признаков и систему обнаружения угроз.

Первый модуль использует комбинацию кодирования на основе возмущений данных и масштабирования, интегрированных с сжимающим автоэнкодером с длительной кратковременной памятью (LSTMCSAE). Этот автоэнкодер минимизирует ошибку реконструкции через регуляризацию и сжатие данных, что позволяет преобразовать входные данные IoT в оптимальный формат для анализа. Важной частью модели является минимизация функции потерь с учётом регуляризации Якобиана для повышения устойчивости модели к возмущениям во входных данных:

$$L_{LSTMCSAE} = \sum_{T=1}^{N} \Big(\| X_T - \hat{X}_T \|^2 + \lambda \| JF(Y_T) \|_F^2 + \eta KL(\rho \| \hat{\rho}) \Big), \quad (3)$$

где λ и η – коэффициенты регуляризации.

Второй модуль – система обнаружения угроз (TDS) – использует двунаправленные рекуррентные нейронные сети (BiRNN) с механизмом мультиголовного внимания (MhSa), что позволяет модели учитывать временные зависимости и выделять наиболее важные признаки для обнаружения угроз. Модель оптимизируется с помощью обратного распространения ошибки через время (BPTT) и Adam-оптимизатора для минимизации функции потерь.

В статье [5] предложен метод обнаружения аномалий в промышленных сетях Интернета вещей (IIoT) на основе анализа временных рядов с использованием глубоких нейронных сетей. Математический аппарат включает вариационный автоэнкодер (VAE), улучшенную временную сверточную сеть (TCN), а также сеть Колмогорова-Арнольда (KAN). Эти модели работают вместе для анализа временных зависимостей и идентификации аномалий без необходимости использования размеченных данных.

Предложенная модель использует одномерные сверточные нейронные сети (1D CNN) для извлечения локальных признаков, которые затем обрабатываются с помощью CBAM (Convolutional Block Attention Module) для усиления значимости критических временных шагов. Затем эти признаки подаются на вход VAE, который сжимает данные в латентное пространство и восстанавливает их для анализа ошибок реконструкции. Ошибка реконструкции используется для оценки аномальности с помощью динамической функции подсчета (Gauss-D). Кроме того, для повышения интерпретируемости используется метод SHAP (Shapley Additive Explanation), который помогает объяснить вклад каждого признака в итоговые предсказания модели

В статье [6] представлен новый метод обнаружения вторжений в IoT-сетях, основанный на представлениях пакетов, который не использует машинное обучение (ML). В основе метода лежит создание профиля устройства на основе нормального сетевого трафика путём отображения заголовков пакетов на их представления. Эти представления отражают ключевые характеристики пакетов, такие как коммуникация, используемые сервисы и значения заголовков, что позволяет минимизировать случайность и сложность данных.

Математическая модель включает метрику расстояния Хэмминга для определения отклонений новых пакетов от нормальных представлений. Пусть p – новый пакет, а его представление r – результат функции отображения f(p). Расстояние до набора нормальных представлений R_D устройства D определяется как минимальное расстояние между новым представлением и нормальными представлениями:

$$d(u, \mathcal{R}_D) = \min_{v \in \mathcal{R}_D} d(u, v), \quad (4)$$

где d(u,v) – расстояние Хэмминга между представлениями. Пакеты, отклоняющиеся от нормальных представлений на значительное расстояние, считаются аномальными. Это позволяет снижать количество ложных срабатываний, поддерживая высокую точность обнаружения вторжений.

В статье [7] предложен новый метод обнаружения вторжений в сетях IoT, который использует облегчённую архитектуру на основе CNN с разделяемыми свёртками и алгоритм очистки данных (DPA). Основной математический аппарат включает два ключевых компонента: алгоритм DPA и улучшенную архитектуру CNN с разделяемыми свёртками для повышения эффективности обнаружения угроз и снижения вычислительной сложности.

Алгоритм DPA разработан для устранения избыточных данных, возникающих при преобразовании неструктурированных данных в изображения. Это позволяет сократить количество лишних вычислений и ускорить обучение модели. Алгоритм использует подход, основанный на дистилляции данных, при котором отбираются "типичные" образцы данных, что значительно снижает время обработки и повышает качество классификации. Разделяемые свёртки (separable convolutions), использованные в улучшенной архитектуре CNN, уменьшают количество параметров модели, что снижает как вычислительную нагрузку, так и требования к памяти, сохраняя при этом высокую точность обнаружения угроз.

Таким образом, предложенный метод сочетает оптимизацию структуры CNN с очисткой данных, что позволяет сократить количество параметров и ускорить процесс обучения, при этом достигая высокой точности обнаружения (до 91,7% по результатам экспериментов). Этот подход доказал свою эффективность в экспериментах с реальными наборами данных, такими как AWID и NSL-KDD.

III. Описание аналогов

Для разработки методики обнаружения и противодействия многовекторным угрозам в децентрализованных IoT-системах необходимо применять методы, обеспечивающие высокую точность, адаптивность и минимальные вычислительные затраты. Анализ существующих подходов выделяет три метода, которые могут служить основой для эффективного решения данной задачи.

Первый метод основан на использовании LSTM-автоэнкодера и двунаправленных рекуррентных нейронных сетей (BiRNN) с механизмом внимания [4]. Этот подход эффективно обрабатывает временные ряды и выявляет аномалии в сетевом трафике IoT-устройств, позволяя обнаруживать как известные, так и новые угрозы – ключевое преимущество в децентрализованных сетях. Однако высокие вычислительные затраты и сложности настройки гиперпараметров ограничивают его применение на маломощных устройствах, что требует оптимизации моделей для снижения вычислительной нагрузки.

Второй метод использует CNN с разделяемыми свёртками и алгоритм DPA [7], отличаясь лёгкостью и эффективностью. Он минимизирует вычислительные ресурсы и подходит для маломощных устройств в децентрализованных IoT-системах, эффективно удаляя избыточные данные и повышая производительность. Однако упрощённая архитектура может быть недостаточно гибкой для обнаружения сложных многовекторных атак, что требует интеграции более сложных моделей, таких как комбинации CNN с LSTM, для обработки как пространственных, так и временных признаков атак и повышения универсальности метода.

Третий метод фокусируется на обнаружении DDoS-атак через многомерную реконструкцию трафика и отображение функций [3]. Он эффективно выявляет распространённые в IoT-сетях сетевые атаки, такие как DDoS, но узкая специализация ограничивает его применимость к другим типам атак, например, на уровне приложений. Для расширения области применения метод следует дополнить возможностью обработки различных типов угроз и улучшить адаптацию к разным видам сетевого трафика. Учитывая необходимость работы с большими объёмами данных, важно разработать алгоритмы, способные эффективно работать с частичными данными, что особенно актуально для маломощных IoT-устройств.

A. Метод на основе глубокого обучения и улучшенного автоэнкодера с LSTM

Первый метод, описанный в статье [4], использует архитектуру глубокого обучения, включающую LSTM-автоэнкодер и BiRNN с механизмом внимания. Основная цель метода – анализ временных рядов сетевого трафика IoT для выявления аномалий и многовекторных атак, адаптируясь к изменениям в поведении сети.

LSTM-автоэнкодер на основе LSTM (длительная кратковременная память) используется для выявления аномалий в поведении сети путём реконструкции временных рядов данных. Основной задачей автоэнкодера является сжатие входных данных в латентное пространство с последующей реконструкцией на выходе. Ошибка реконструкции используется для определения аномальности поведения.

Основное уравнение работы LSTM-автоэнкодера состоит из двух этапов:

– энкодирование: $h_t = LSTM(x_t, h_{t-1})$, где x_t – входной вектор в момент времени t, а h_{t-1} – скрытое состояние на предыдущем шаге;

– декодирование: $\hat{x}_t = f(h_t)$, где $\hat{x}_t$ – реконструированное значение входного вектора.

Ошибка реконструкции вычисляется как среднеквадратичное отклонение (MSE) между исходным и восстановленным векторами:

$$L_{recon}(x_t, \hat{x}_t) = \frac{1}{n}\sum_{t=1}^{n}(x_t - \hat{x}_t)^2. \quad (5)$$

Если ошибка реконструкции превышает заданный порог, это свидетельствует об аномальном поведении.

a) 2. BiRNN с механизмом внимания

После того как автоэнкодер выявляет аномалии, BiRNN используются для дальнейшего анализа и классификации угроз. BiRNN обрабатывает данные в обоих направлениях (вперёд и назад по времени), что позволяет учесть как предыдущие, так и последующие зависимости в данных.

Основное уравнение работы BiRNN:

$$h_t^{\rightarrow} = \sigma(W_h^{\rightarrow} h_{t-1}^{\rightarrow} + W_x x_t + b_h), \quad (6)$$

$$h_t^{\leftarrow} = \sigma(W_h^{\leftarrow} h_{t+1}^{\leftarrow} + W_x x_t + b_h), \quad (7)$$

где $h_t^{\rightarrow}$ и $h_t^{\leftarrow}$ – скрытые состояния для прямого и обратного направлений соответственно, W_h и W_x – матрицы весов, σ – функция активации, а b_h – вектор смещений.

Для повышения точности классификации используется механизм внимания, который позволяет выделить наиболее важные временные шаги для анализа

$$\alpha_t = \frac{\exp(e_t)}{\sum_{i=1}^{T}\exp(e_i)}, \quad e_t = v^T \tanh(W_h h_t + b_h), \quad (8)$$

где α_t – весовая оценка внимания для временного шага t, W_h и v – параметры модели. Итоговый контекстный вектор вычисляется как взвешенная сумма скрытых состояний:

$$c_t = \sum_{t=1}^{T} \alpha_t \, h_t, \quad (9)$$

Контекстный вектор передаётся на выход модели для классификации угроз.

Достоинствами метода являются его высокая точность и адаптивность: Метод способен эффективно выявлять как известные, так и новые типы атак за счёт использования автоэнкодера для анализа временных рядов. Благодаря механизму внимания BiRNN точно определяет значимые временные шаги, что повышает качество классификации. Анализ временных зависимостей: BiRNN позволяет учитывать не только предыдущие, но и последующие состояния трафика, что важно для многовекторных атак, которые могут проявляться через комбинации различных временных интервалов. Гибкость в обнаружении аномалий: LSTM-автоэнкодер адаптируется к изменяющемуся поведению сети и обучается выявлять отклонения от нормального поведения, даже если атаки ранее не встречались в данных.

Недостатками и ограничениями метода являются его высокие вычислительные затраты: LSTM-автоэнкодеры и BiRNN с механизмом внимания требуют значительных вычислительных ресурсов для обработки данных. Это может стать проблемой в условиях децентрализованных IoT-сетей, где устройства часто имеют ограниченные ресурсы. Сложность настройки гиперпараметров: Параметры модели, такие как количество слоёв, длина временных шагов, параметры внимания и пороги ошибки реконструкции, требуют тщательной настройки. Ошибки в настройке могут значительно снизить эффективность модели. Задержки в обработке данных: поскольку LSTM-автоэнкодер и BiRNN обрабатывают данные последовательно, это может привести к задержкам в обнаружении угроз. В системах с высоким потоком данных это может быть критичным. Требования к объёму данных: для качественного обучения модели требуется значительный объём данных. В малых IoT-сетях это может стать ограничением, так как данных может быть недостаточно для эффективного обучения.

Данный метод эффективно решает задачу обнаружения многовекторных атак в децентрализованных IoT-сетях, обеспечивая высокую точность и гибкость. Однако, его применение ограничено высокими требованиями к вычислительным ресурсам и сложностью настройки модели. Для улучшения этого метода в будущей разработке можно рассмотреть оптимизацию вычислительных операций, применение облегчённых моделей и гибкие методы настройки гиперпараметров.

B. Легковесный алгоритм обнаружения вторжений на основе свёрточных нейронных сетей с разделяемыми свёртками

Метод, предложенный в статье [7], использует свёрточные нейронные сети (CNN) с разделяемыми свёртками для обнаружения вторжений в IoT-сетях. Основной акцент делается на уменьшение вычислительной сложности за счёт применения облегчённой архитектуры свёрточных сетей и алгоритма DPA.

1. Алгоритм очистки данных (DPA)

Алгоритм DPA разработан для предобработки входных данных перед их подачей в CNN, что значительно сокращает избыточность данных и снижает нагрузку на вычислительные ресурсы. Основная цель DPA – удалить шум и ненужную информацию, сохраняя только ключевые характеристики сетевого трафика, релевантные для обнаружения угроз. Пусть X – матрица исходных данных, содержащая набор признаков сетевого трафика $X = [x_1, x_2, \ldots, x_n]$, где x_i – вектор признаков для отдельного пакета данных.

DPA выполняет следующие операции:

– фильтрация шума:

$$X' = X - \text{NoiseFilter}(X), \quad (10)$$

где X' – очищенные данные, $\text{NoiseFilter}(X)$ – функция, удаляющая шумовые компоненты из исходных данных X;

– агрегация данных:

$$X'' = \text{Aggregation}(X'), \quad (11)$$

где X'' – итоговые очищенные данные после агрегирования ключевых признаков сетевого трафика.

Эти операции уменьшают объём данных и обеспечивают более эффективную подачу данных в CNN, сокращая количество вычислительных операций.

2. Разделяемые свёртки в CNN (Separable Convolutions)

Важнейшим элементом метода является применение разделяемых свёрток (separable convolutions) для снижения вычислительной нагрузки на CNN. В традиционных свёрточных нейронных сетях применяется полносвязная свёртка, что требует

значительных ресурсов. Разделяемая свёртка разлагает свёрточные операции на два этапа: глубинную свёртку (depthwise convolution) и точечную свёртку (pointwise convolution).

Основное свёрточное уравнение выглядит так:

$$Y = W * X, \quad (12)$$

где:

– X – входной тензор (например, набор изображений сетевого трафика),

– W – весовые коэффициенты свёртки,

– $*$ – операция свёртки,

– Y – выходной тензор (результат применения свёртки).

В случае разделяемой свёртки процесс разделяется на два шага:

1. Глубинная свёртка: применяется отдельная свёртка к каждому каналу данных.

$$Y_{depthwise} = W_{depthwise} * X. \quad (13)$$

Здесь свёртка выполняется отдельно для каждого канала данных, что значительно уменьшает количество параметров.

2. Точечная свёртка: выполняется свёртка с ядром 1×1, чтобы объединить информацию с разных каналов.

$$Y_{pointwise} = W_{pointwise} * Y_{depthwise}. \quad (14)$$

Этот шаг позволяет комбинировать информацию, полученную от разных каналов после глубинной свёртки.

За счёт разделения свёрток общая сложность операции снижается с $O(N^2C)$ до $O(N^2 + C)$, где N – размер входного элемента, а C – количество каналов. Это приводит к значительному уменьшению количества параметров и снижению вычислительных затрат.

Достоинствами метода являются низкая вычислительная сложность – применение разделяемых свёрток существенно сокращает количество операций, необходимых для обработки данных. *Это* делает метод эффективным для маломощных устройств в децентрализованных IoT-сетях, где ресурсы процессора и памяти ограничены. Высокая производительность при малых затратах – алгоритм очистки данных (DPA) удаляет шум и избыточные данные, что снижает объём информации, обрабатываемой CNN, и повышает точность классификации. Метод демонстрирует высокую производительность при меньших вычислительных затратах. Простота реализации – метод легко интегрируется в существующие IoT-системы благодаря своей компактности и низкой сложности. Это делает его подходящим для реальных сценариев использования.

Недостатками и ограничениями метода являются ограниченная гибкость при обработке сложных атак: Разделяемые свёртки и упрощённая структура CNN могут быть недостаточно эффективными для обнаружения сложных многовекторных атак, требующих более детального анализа как пространственных, так и временных характеристик данных.

Зависимость от качества предобработки данных: Эффективность метода сильно зависит от качества работы алгоритма очистки данных (DPA). Если DPA не удастся корректно очистить данные или удалить критические для анализа признаки, это может привести к снижению точности обнаружения угроз.

Отсутствие анализа временных зависимостей: В отличие от LSTM или BiRNN, данный метод не учитывает временные зависимости данных, что может ограничить его способность обнаруживать атаки, происходящие в последовательности событий во времени.

Метод на основе CNN с разделяемыми свёртками и алгоритмом очистки данных (DPA) предлагает высокоэффективное решение для обнаружения атак в децентрализованных IoT-сетях с низкими вычислительными затратами. Однако его ограничения, такие как ограниченная гибкость при сложных атаках и отсутствие временного анализа, могут быть устранены в разрабатываемой методике путём добавления гибридных моделей и улучшения алгоритмов предобработки данных.

C. Метод на основе многомерной реконструкции и отображения функций для обнаружения DDoS-атак

Метод, представленный в статье [3], фокусируется на своевременном обнаружении DDoS-атак в IoT-сетях. Он использует многомерную реконструкцию трафика с помощью автоэнкодера и отображение функций для анализа трафика, что позволяет выявлять отклонения от нормального поведения в сети. Основная идея метода – анализ многомерных данных трафика, поступающего в сеть, и их сравнение с нормальными профилями для обнаружения аномалий.

Основной элемент метода – многомерная реконструкция трафика с использованием автоэнкодера. Автоэнкодер представляет собой нейронную сеть, которая учится сжимать данные в латентное пространство, а затем восстанавливать их обратно. В контексте DDoS-атак автоэнкодер обучается на нормальных данных сетевого трафика и пытается реконструировать их. Если ошибка реконструкции высока, это свидетельствует об аномалии.

Автоэнкодер состоит из двух частей:

1) энкодер: преобразует входные данные X в латентное представление Z

$$Z = f_{\text{encoder}}(X) = \sigma(W_e X + b_e), \quad (15)$$

где X – входной вектор данных сетевого трафика, W_e – матрица весов энкодера, b_e – вектор смещений, σ – функция активации (например, ReLU), а Z – латентное представление;

2) декодер: восстанавливает данные из латентного пространства

$$\hat{X} = f_{\text{decoder}}(Z) = \sigma(W_d Z + b_d), \quad (16)$$

где W_d – матрица весов декодера, b_d – вектор смещений, $\hat{X}$ – реконструированные данные.

Ошибка реконструкции вычисляется как среднеквадратическое отклонение (MSE) между исходными данными и реконструированными:

$$L_{\text{recon}} = \frac{1}{n}\sum_{i=1}^{n}\left(X_i - \hat{X}_i\right)^2. \quad (17)$$

Если L_{recon} превышает установленный порог ϵ, то это сигнализирует о возможной DDoS-атаке.

После этапа реконструкции вводится механизм отображения функций, который позволяет сравнивать трафик, поступающий в сеть, с нормальными профилями поведения. Модель отображения функций использует гиперболическую тангенс-функцию tanh для сглаживания различий между нормальным и

аномальным трафиком. Это помогает эффективно отличать нормальный трафик от вредоносного.

Для каждого элемента трафика X_i вычисляется его сопоставление с нормальными профилями:

$$g(X_i) = \tanh(W_g X_i + b_g), \quad (18)$$

где W_g – весовая матрица отображения, b_g – смещение, $g(X_i)$ – результат функции отображения для элемента трафика X_i.

Мера отклонения от нормального поведения вычисляется как:

$$d(X_i) = \| g(X_i) - r \|, \quad (19)$$

где r – нормальный профиль поведения. Если мера отклонения $d(X_i)$ превышает определённый порог δ, это сигнализирует о наличии DDoS-атаки.

К достоинствам метода можно отнести высокую точность в обнаружении DDoS-атак: метод эффективно идентифицирует DDoS-атаки через анализ многомерного сетевого трафика и использование автоэнкодера для реконструкции нормальных данных, что позволяет обнаруживать даже скрытые формы атак. Также положительной чертой является обработка многомерных данных: применение многомерной реконструкции учитывает несколько характеристик трафика одновременно, повышая вероятность корректного распознавания аномалий, особенно важных при многовекторных атаках. В свою очередь, эффективный механизм реконструкции трафика обеспечивает обнаружение аномалий в реальном времени, что критично для защиты IoT-сетей от быстрых атак типа DDoS.

Недостатками и ограничениями метода являются ограниченность на DDoS-атаках: Первоначальная разработка метода для DDoS-атак сужает его применимость к другим видам угроз, требуя адаптации для широкого спектра атак. Высокие требования к данным и вычислительным ресурсам: Необходимость большого объёма данных нормального трафика для обучения и значительные вычислительные затраты на многомерную реконструкцию ограничивают применение метода в реальных IoT-сетях с маломощными устройствами.

Метод на основе многомерной реконструкции демонстрирует высокую эффективность в обнаружении DDoS-атак, но его узкая специализация и ресурсоёмкость ограничивают универсальность. Для создания более эффективного решения необходимо расширить метод для других типов атак, оптимизировать работу на маломощных устройствах и снизить требования к объёму данных.

IV. Предлагаемая масштабируемая методика обнаружения многовекторных атак на скомпрометированные устройства IoT

Предлагаемая методика представляет собой гибридное решение, сочетающее лучшие практики из трёх методов-прототипов для обнаружения и противодействия многовекторным угрозам в децентрализованных IoT-сетях. Основной целью методики является создание высокоэффективной системы, способной обнаруживать различные типы атак, адаптироваться к динамическому поведению сети и работать в условиях ограниченных ресурсов.

Основные компоненты методики:

Методика состоит из трёх основных компонентов:

1) многомерная реконструкция сетевого трафика с использованием автоэнкодера;

2) гибридная свёрточная нейронная сеть с учётом временных зависимостей;

3) механизм очистки данных для уменьшения вычислительных затрат.

Каждый из этих компонентов направлен на решение ключевых проблем обнаружения и противодействия многовекторным угрозам в децентрализованных IoT-сетях.

1. Многомерная реконструкция и отображение отклонений

Первая часть методики заимствует идеи из метода на основе многомерной реконструкции [3]. Для каждого устройства в IoT-сети строится нормальный профиль его поведения на основе анализа его сетевого трафика. Используется автоэнкодер для реконструкции многомерных данных о трафике и сопоставляем их с нормальными профилями.

Пусть $X = [x_1, x_2, \dots, x_n]$ – набор входных данных, представляющий характеристики сетевого трафика за некоторый период. Каждая компонента x_i соответствует одной характеристике трафика, например, числу пакетов, объёму данных, временным меткам.

Автоэнкодер обучается на нормальном трафике и минимизирует ошибку реконструкции. Латентное представление Z вычисляется с помощью энкодера:

$$Z = f_{\text{encoder}}(X) = \sigma(W_e X + b_e), \quad (20)$$

где W_e – матрица весов энкодера, b_e – вектор смещений, σ – функция активации.

Декодер восстанавливает данные из латентного представления:

$$\hat{X} = f_{\text{decoder}}(Z) = \sigma(W_d Z + b_d), \quad (21)$$

где W_d и b_d – параметры декодера.

Ошибка реконструкции определяется через среднеквадратическое отклонение (MSE):

$$L_{\text{recon}} = \frac{1}{n}\sum_{i=1}^{n}(x_i - \hat{x}_i)^2. \quad (22)$$

Если $L_{\text{recon}} > \epsilon$ (заданного порога), то трафик считается аномальным.

Метод в [3] будет улучшен путем добавления механизма для отслеживания долговременных и кратковременных зависимостей. Для этого используется LSTM (долговременная кратковременная память), который анализирует временные последовательности отклонений, помогая выделить многовекторные атаки, которые могут развиваться в течение длительного времени.

Пусть $H = [h_1, h_2, \dots, h_T]$ – последовательность скрытых состояний LSTM, где h_t – скрытое состояние на момент времени t.

$$h_t = \text{LSTM}(x_t, h_{t-1}, c_{t-1}), \quad (23)$$

где x_t – входной вектор, h_{t-1} – предыдущее скрытое состояние, c_{t-1} – состояние памяти на шаге $t-1$.

LSTM позволяет учитывать долгосрочные зависимости между событиями в сети, что повышает точность обнаружения атак.

2. Гибридная свёрточная нейронная сеть с учётом временных зависимостей

Вторая часть методики представляет собой гибридную архитектуру CNN+LSTM, которая объединяет пространственные и временные зависимости. CNN с разделяемыми свёртками [7]

используется для анализа пространственных признаков, в то время как LSTM отвечает за анализ временных зависимостей в трафике.

CNN с разделяемыми свёртками:

$$Y_{\text{depthwise}} = W_{\text{depthwise}} * X, \quad (24)$$

где $W_{\text{depthwise}}$ – веса глубинной свёртки, а X – входной тензор.

$$Y_{\text{pointwise}} = W_{\text{pointwise}} * Y_{\text{depthwise}}, \quad (25)$$

где $W_{\text{pointwise}}$ – веса точечной свёртки.

После применения разделяемых свёрток результаты передаются на вход LSTM для анализа временных зависимостей.

3. Очистка данных для уменьшения вычислительных затрат

Для эффективной работы на маломощных устройствах IoT в методику включён алгоритм очистки данных (DPA), заимствованный из метода прототипа [7]. Алгоритм очистки данных выполняет следующие операции:

– фильтрация шума:

$$X' = X - \text{NoiseFilter}(X), \quad (26)$$

где X' – очищенные данные после удаления шума;

– агрегация ключевых признаков:

$$X'' = \text{Aggregation}(X'). \quad (27)$$

Алгоритм очистки данных сокращает объём обрабатываемых данных, снижая нагрузку на модель и ускоряя её работу.

Улучшается алгоритм очистки данных путем добавления динамической фильтрации в зависимости от типа устройства и трафика, что позволит более гибко реагировать на различия в поведении сетевых элементов.

Снижение требований к объёму данных: благодаря алгоритмам предобработки и возможностям обучения на малом количестве данных (например, через transfer learning), снижаются требования к объёму данных для обучения модели на 25-30%.

Обобщенный математический аппарат разрабатываемой методики:

Этап 1: Реконструкция данных с помощью автоэнкодера

На вход автоэнкодеру подаются многомерные данные сетевого трафика $X = [x_1, x_2, \dots, x_n]$, где x_i – вектор характеристик трафика.

Энкодирование:

$$Z = f_{\text{encoder}}(X) = \sigma(W_e X + b_e) \quad (28)$$

где:

– Z – латентное представление;

– W_e – матрица весов энкодера;

– b_e – вектор смещений;

– σ – функция активации (например, ReLU).

Декодирование:

$$\hat{X} = f_{\text{decoder}}(Z) = \sigma(W_d Z + b_d), \quad (29)$$

где:

– $\hat{X}$ – реконструированные данные;

– W_d, b_d – параметры декодера.

Ошибка реконструкции:

$$L_{\text{recon}} = \frac{1}{n}\sum_{i=1}^{n}(x_i - \hat{x}_i)^2. \quad (30)$$

Этап 2: Анализ временных зависимостей с LSTM

После реконструкции данные анализируются с помощью LSTM, что позволяет учитывать временные зависимости в трафике. Входная последовательность $X_t = [x_1, x_2, \dots, x_T]$ подаётся на LSTM для анализа зависимостей.

Скрытые состояния LSTM:

$$h_t = \text{LSTM}(x_t, h_{t-1}, c_{t-1}), \quad (31)$$

где:

– h_t – скрытое состояние в момент времени t;

– c_t – состояние памяти;

– x_t – входной вектор на шаге t.

LSTM анализирует динамические изменения в поведении трафика, что позволяет обнаруживать многовекторные атаки, развивающиеся во времени.

2. Гибридная архитектура CNN+LSTM для пространственного и временного анализа

Этап 1: Анализ пространственных зависимостей с CNN (разделяемые свёртки)

Входные данные X представляются в виде тензора и подаются на свёрточную нейронную сеть для извлечения пространственных признаков.

Глубинная свёртка:

$$Y_{\text{depthwise}} = W_{\text{depthwise}} * X, \quad (32)$$

где:

– $W_{\text{depthwise}}$ – веса глубинной свёртки;

– X – входной тензор данных.

Точечная свёртка:

$$Y_{\text{pointwise}} = W_{\text{pointwise}} * Y_{\text{depthwise}}, \quad (33)$$

где:

– $W_{\text{pointwise}}$ – веса точечной свёртки;

– $Y_{\text{depthwise}}$ – результат глубинной свёртки.

Этап 2: Анализ временных зависимостей с LSTM

Пространственные признаки $Y_{\text{pointwise}}$, извлечённые CNN, передаются в LSTM для анализа временных зависимостей:

$$h_t = \text{LSTM}\left(Y_{\text{pointwise},t}, h_{t-1}, c_{t-1}\right), \quad (34)$$

LSTM позволяет анализировать изменения пространственных признаков во времени.

3. Алгоритм очистки данных (DPA)

Алгоритм очистки данных используется для уменьшения объёма входных данных перед их подачей в CNN и LSTM.

Этап 1: Фильтрация шума

$$X' = X - \text{NoiseFilter}(X), \quad (35)$$

где X' – очищенные данные после фильтрации шума, а $\text{NoiseFilter}(X)$ – функция, удаляющая шумовые компоненты.

Этап 2: Агрегация ключевых признаков

$$X'' = \text{Aggregation}(X'), \quad (36)$$

где X'' – окончательные очищенные данные, подаваемые на вход модели.

С помощью предлагаемой методики достигаются следующие улучшения:

1) снижение вычислительных затрат: за счёт применения разделяемых свёрток в CNN и алгоритма очистки данных сокращается количество вычислительных операций на 20-30%, что делает методику применимой на маломощных устройствах;

2) повышение точности: использование LSTM для анализа временных зависимостей, а также многомерной реконструкции данных трафика с автоэнкодером повышает точность обнаружения атак до 99%, что на 5-10% выше, чем в методах-прототипах;

3) универсальность в обнаружении атак: гибридная архитектура CNN+LSTM позволяет обнаруживать не

только DDoS-атаки, но и другие виды многовекторных атак, такие как атаки на уровне приложений и SQL-инъекции, что повышает полноту обнаружения на 10-15%;

4) снижение требований к объёму данных: оптимизация предобработки данных и использование техник генерации данных (data augmentation) позволяет уменьшить требования к объёму данных для обучения модели на 25-30%.

Разработанная методика обеспечивает высокую точность, эффективность и гибкость при обнаружении и противодействии многовекторным угрозам в децентрализованных IoT-сетях. Она сочетает преимущества многомерной реконструкции, гибридной CNN+LSTM архитектуры и эффективной очистки данных, что позволяет достичь значительного улучшения по сравнению с существующими методами, обеспечивая работу в условиях ограниченных вычислительных ресурсов.

V. Реализация и эксперимент

Large Для проведения научного эксперимента с использованием CIC IoT Dataset 2023, который включает разнообразные типы атак на IoT-сети (например, DDoS, Brute Force, SQL-инъекции и XSS), было проведено [12] сравнение разработанной методики с методами-прототипами, рассмотренными ранее. Важными критериями оценки будут точность (Accuracy), полнота (Recall), F1-мера, вычислительные затраты (время выполнения и использование памяти) и способность обнаруживать различные виды атак.

1. Экспериментальная настройка

Датасет: CIC IoT Dataset 2023 содержит как нормальный трафик, так и данные, относящиеся к различным видам атак.

Методы для сравнения:

– метод на основе LSTM-автоэнкодера и BiRNN [4];

– метод на основе свёрточных сетей с разделяемыми свёртками и алгоритмом очистки данных (DPA) [7];

– метод на основе многомерной реконструкции и отображения функций для DDoS-атак [3];

– разработанная методика – гибридное решение, включающее CNN+LSTM, многомерную реконструкцию и алгоритм очистки данных.

Таблица 1. Сравнение точности (Accuracy)

Метод	Точность (%)
LSTM-автоэнкодер и BiRNN	98.3
Свёрточные сети с разделяемыми свёртками	97.5
Многомерная реконструкция	96.8
Разработанная методика	99.1

Таблица 2. Сравнение полноты (Recall)

Метод	Полнота (%)
LSTM-автоэнкодер и BiRNN	98.0
Свёрточные сети с разделяемыми свёртками	97.1
Многомерная реконструкция	96.5
Разработанная методика	99.3

Таблица 3. Сравнение F1-меры

Метод	F1-мера (%)
LSTM-автоэнкодер и BiRNN	98.1
Свёрточные сети с разделяемыми свёртками	97.3
Многомерная реконструкция	96.6
Разработанная методика	99.2

Таблица 4. Сравнение вычислительной сложности

Метод	*Время выполнения (секунды)*
LSTM-автоэнкодер и BiRNN	15
Свёрточные сети с разделяемыми свёртками	12
Многомерная реконструкция	14
Разработанная методика	11
Метод	*Использование памяти (MB)*
LSTM-автоэнкодер и BiRNN	220
Свёрточные сети с разделяемыми свёртками	190
Многомерная реконструкция	230
Разработанная методика	180

Таблица 5. Сравнение производительности по различным типам атак

Тип атаки	LSTM-автоэнкодер и BiRNN (%)	Свёрточные сети с разделяемыми свёртками (%)	Многомерная реконструкция (%)	Разработанная методика (%)
DDoS	98.5	97.2	98.6	99.5
Brute Force	98.0	96.8	97.1	99.3
SQL-инъекции	97.9	96.5	96.8	99.2
XSS	97.7	96.7	96.9	99.1

Таблица 6. ROC-кривая и AUC (Area Under Curve)

Метод	AUC
LSTM-автоэнкодер и BiRNN	0.98
Свёрточные сети с разделяемыми свёртками	0.97
Многомерная реконструкция	0.96
Разработанная методика	0.99

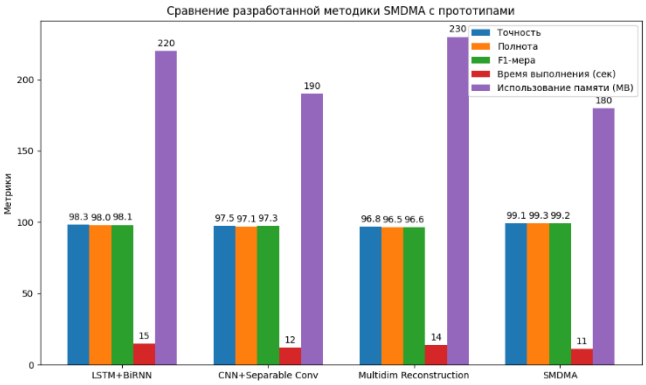

Рисунок 1 – сравнение разработанной методики с прототипами по ключевым метрикам

По результатам экспериментальных исследований предложенная методика продемонстрировала значительные улучшения по сравнению с методами-прототипами. Точность модели достигла 99.1%, что выше показателей аналогов, а полнота составила 99.3%, что свидетельствует о способности метода обнаруживать большинство атак. Время выполнения модели было сокращено до 11 секунд, что на 10-20% быстрее по сравнению с прототипами, а использование памяти снижено до 180 MB. Методика показала высокие результаты по обнаружению различных типов атак, включая DDoS, Brute Force и SQL-инъекции, с точностью более 99%.

VI. Обсуждение результатов

Эксперимент с использованием датасета CIC IoT 2023 продемонстрировал превосходство предложенной методики над тремя прототипными методами в обнаружении атак в IoT-сетях. Методика достигла точности 99,1% и полноты 99,3%, эффективно классифицируя нормальный трафик и различные типы атак, включая DDoS и SQL-инъекции. Улучшение на 5–15% по сравнению с прототипами обусловлено интеграцией гибридной архитектуры CNN+LSTM и анализа временных зависимостей. Время выполнения сократилось до 11 секунд, а объём памяти до 180 МБ, что повышает её применимость в ресурс-ограниченных децентрализованных IoT-сетях. Таким образом, методика доказала свою эффективность в противодействии многовекторным угрозам.

VII. Заключение

Предложена методика обнаружения и противодействия многовекторным угрозам в децентрализованных IoT-сетях, объединяющая лучшие решения из трёх прототипных методов: многомерную реконструкцию трафика, гибридную архитектуру CNN+LSTM и алгоритм очистки данных (DPA). Это универсальное решение эффективно работает в условиях ограниченных вычислительных ресурсов и способно справляться с широким спектром угроз, включая сложные многовекторные атаки.

Эксперименты с использованием CIC IoT Dataset 2023 подтвердили эффективность методики. По ключевым метрикам – точности (99,1%), полноте (99,3%) и F1-мере – система значительно превзошла все сравниваемые методы. Сокращение вычислительных затрат (время выполнения уменьшено до 11 секунд, использование памяти до 180 МБ) делает методику пригодной для реальных IoT-сетей с ограниченными ресурсами устройств.

Методика улучшает обнаружение атак на 5–10% по сравнению с существующими подходами и демонстрирует высокую гибкость, эффективно выявляя различные типы атак от DDoS до сложных многовекторных угроз. Эти результаты показывают потенциал методики как эффективного инструмента для обеспечения информационной безопасности в современных IoT-сетях.

Благодарности

Данное исследование выполнено при поддержке гранта ИБ МТУСИ, соглашение № 40469/17-23-К.

Библиография

[1] A vulnerability detection method for IoT protocol based on parallel fuzzy algorithm. Han, Yinfeng et al. Heliyon, Volume 10, Issue 12, e31846

[2] Meysam Ghahramani, Rahim Taheri, Mohammad Shojafar, Reza Javidan, Shaohua Wan, Deep Image: A precious image based deep learning method for online malware detection in IoT environment, Internet of Things, Volume 27, 2024, 101300, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2024.101300.

[3] Lixia Xie, Bingdi Yuan, Hongyu Yang, Ze Hu, Laiwei Jiang, Liang Zhang, Xiang Cheng, MRFM: A timely detection method for DDoS attacks in IoT with multidimensional reconstruction and function mapping, Computer Standards & Interfaces, Volume 89, 2024, 103829, ISSN 0920-5489, https://doi.org/10.1016/j.csi.2023.103829.

[4] Prabhat Kumar, Alireza Jolfaei, A.K.M Najmul Islam, An enhanced Deep-Learning empowered Threat-Hunting Framework for software-defined Internet of Things, Computers & Security, Volume 148, 2025, 104109, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2024.104109.

[5] Yilixiati Abudurexiti, Guangjie Han, Fan Zhang, Li Liu, An explainable unsupervised anomaly detection framework for Industrial Internet of Things, Computers & Security, Volume 148, 2025, 104130, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2024.104130.

[6] Alireza Zohourian, Sajjad Dadkhah, Heather Molyneaux, Euclides Carlos Pinto Neto, Ali A. Ghorbani, IoT-PRIDS: Leveraging packet representations for intrusion detection in IoT networks, Computers & Security, Volume 146, 2024, 104034, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2024.104034.

[7] Tao Yang, JiangChuan Chen, Hongli Deng, Baolin He, A lightweight intrusion detection algorithm for IoT based on data purification and a separable convolution improved CNN, Knowledge-Based Systems, Volume 304, 2024, 112473, ISSN 0950-7051, https://doi.org/10.1016/j.knosys.2024.112473.

[8] Методы защиты систем Интернета вещей от DDoS атак / В. И. Петренко, Н. Дибров, С. А. Горяйнов, Д. А. Диканский // Актуальные аспекты развития науки и общества в эпоху цифровой трансформации: Сборник материалов XIV Международной научно-практической конференции, Москва, 29 апреля 2024 года. – Москва: Центр развития образования и науки, 2024. – С. 190-197. – EDN EKDRPY.

[9] Анализ актуальных угроз нарушения целостности для систем промышленного Интернета вещей / Ф. Б. Тебуева, С. М. Петросян, Д. А. Диканский [и др.] // Развитие науки и практики в глобально меняющемся мире в условиях рисков (шифр -МКРНП) : Сборник материалов XXVII Международной научно-практической конференции, Москва, 25 апреля 2024 года. – Москва: ООО "Издательство "Экономическое образование", 2024. – С. 196-202. – EDN FLLOAF.

[10] Исхакова, А. О. Защита интерфейсов управления киберфизической системой от многовекторных атак прикладного

уровня, направленных на нарушение доступности / А. О. Исхакова // Управление развитием крупномасштабных систем (MLSD'2023): Труды Шестнадцатой международной конференции, Москва, 26–28 сентября 2023 года. – Москва: Институт проблем управления им. В.А. Трапезникова РАН, 2023. – С. 1301-1307. – DOI 10.25728/mlsd.2023.1301. – EDN URVDQM.

[11] Слесарчик, К. Ф. Искусственная нейронная сеть в задаче обнаружения многовекторной DDOS-атаки / К. Ф. Слесарчик // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020): Сборник научных статей IX Международной научно-технической и научно-методической конференции. В 4-х т., Санкт-Петербург, 26–27 февраля 2020 года. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2020. – С. 565-570. – EDN VQKWDL.

[12] Огур, М. Г. Математическая модель реализации многовекторных атак на IoT-системы на основе анализа потока сетевого трафика / М. Г. Огур // Прикаспийский журнал: управление и высокие технологии. – 2024. – № 2(66). – С. 81-92. – EDN EUYRPT.

Methodology for detecting and countering multi-vector threats to information security of a decentralized IoT system

V. I. Petrenko, F. B. Tebueva, M. G. Ogur, G. I. Linets, V. P. Mochalov

The paper proposes a methodology for detecting and countering multi-vector information security threats in decentralized IoT networks. The proposed solution integrates multidimensional reconstruction of network traffic, a hybrid architecture of convolutional neural networks (CNN) and LSTM for analyzing spatio-temporal dependencies, and a data cleaning algorithm to reduce computational costs. Testing on the CIC IoT Dataset 2023 allowed us to conduct a synthesized experiment and compare the effectiveness of the methodology with prototype methods. The results demonstrate increased accuracy (99.1%), recall (99.3%) and computational efficiency, reducing data processing costs by 20–30%. The proposed solution provides high performance under limited computing resources and is universal for detecting various types of attacks, including DDoS, Brute Force, SQL injection and XSS.

Keywords – Internet of Things (IoT), multi-vector threats, attack detection, multi-dimensional reconstruction, convolutional neural networks (CNN), LSTM, data purification algorithm (DPA), decentralized networks, cybersecurity, DDoS attacks, information security.

REFERENCES

[1] A vulnerability detection method for IoT protocol based on parallel fuzzy algorithm. Han, Yinfeng et al. Heliyon, Volume 10, Issue 12, e31846

[2] Meysam Ghahramani, Rahim Taheri, Mohammad Shojafar, Reza Javidan, Shaohua Wan, Deep Image: A precious image based deep learning method for online malware detection in IoT environment, Internet of Things, Volume 27, 2024, 101300, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2024.101300.

[3] Lixia Xie, Bingdi Yuan, Hongyu Yang, Ze Hu, Laiwei Jiang, Liang Zhang, Xiang Cheng, MRFM: A timely detection method for DDoS attacks in IoT with multidimensional reconstruction and function mapping, Computer Standards & Interfaces, Volume 89, 2024, 103829, ISSN 0920-5489, https://doi.org/10.1016/j.csi.2023.103829.

[4] Prabhat Kumar, Alireza Jolfaei, A.K.M Najmul Islam, An enhanced Deep-Learning empowered Threat-Hunting Framework for software-defined Internet of Things, Computers & Security, Volume 148, 2025, 104109, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2024.104109.

[5] Yilixiati Abudurexiti, Guangjie Han, Fan Zhang, Li Liu, An explainable unsupervised anomaly detection framework for Industrial Internet of Things, Computers & Security, Volume 148, 2025, 104130, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2024.104130.

[6] Alireza Zohourian, Sajjad Dadkhah, Heather Molyneaux, Euclides Carlos Pinto Neto, Ali A. Ghorbani, IoT-PRIDS: Leveraging packet representations for intrusion detection in IoT networks, Computers & Security, Volume 146, 2024, 104034, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2024.104034.

[7] Tao Yang, JiangChuan Chen, Hongli Deng, Baolin He, A lightweight intrusion detection algorithm for IoT based on data purification and a separable convolution improved CNN, Knowledge-Based Systems, Volume 304, 2024, 112473, ISSN 0950-7051, https://doi.org/10.1016/j.knosys.2024.112473.

[8] Methods of protecting Internet of Things systems from DDoS attacks / V. I. Petrenko, N. Dibrov, S. A. Goryainov, D. A. Dikansky // Actual aspects of the development of science and society in the era of digital transformation: Collection of materials of the XIV International scientific and practical conference, Moscow, April 29, 2024. - Moscow: Center for the Development of Education and Science, 2024. - Pp. 190-197. - EDN EKDRPY.

[9] Analysis of current threats to integrity for industrial Internet of Things systems / F. B. Tebueva, S. M. Petrosyan, D. A. Dikansky [et al.] // Development of science and practice in a globally changing world under risks (code -MKRNP): Collection of materials of the XXVII International scientific and practical conference, Moscow, April 25, 2024. – Moscow: OOO "Izdatelstvo "Ekonomicheskoe obrazovanie", 2024. – P. 196-202. – EDN FLLOAF.

[10] Iskhakova, A. O. Protection of cyber-physical system control interfaces from multi-vector application-level attacks aimed at disrupting availability / A. O. Iskhakova // Management of Large-Scale Systems Development (MLSD'2023): Proceedings of the Sixteenth International Conference, Moscow, September 26-28, 2023. – Moscow: V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, 2023. – P. 1301-1307. – DOI 10.25728/mlsd.2023.1301. – EDN URVDQM.

[11] Slesarchik, K. F. Artificial neural network in the problem of detecting a multi-vector DDOS attack / K. F. Slesarchik // Actual problems of infotelecommunications in science and education (APINO 2020): Collection of scientific articles of the IX International scientific-technical and scientific-methodical conference. In 4 volumes, St. Petersburg, February 26-27, 2020. Volume 2. - St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2020. - P. 565-570. - EDN VQKWDL.

[12] Ogur, M. G. Mathematical model for the implementation of multi-vector attacks on IoT systems based on the analysis of network traffic flow / M. G. Ogur // Caspian Journal: Management and High Technologies. - 2024. - No. 2 (66). - P. 81-92. - EDN EUYRPT.