DOI 10.37882/2223-2966.2025.06-2.36

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ АЛГОРИТМА КЛОНАЛЬНОГО ОТБОРА В ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМАХ ДЛЯ ОБНАРУЖЕНИЯ АТАК ТИПА ОТКАЗА В ОБСЛУЖИВАНИИ

MATHEMATICAL MODELING OF THE CLONAL SELECTION ALGORITHM IN ARTIFICIAL IMMUNE SYSTEMS FOR THE DETECTION OF DENIAL-OF-SERVICE ATTACKS

A. Sokolov
S. Artemova
D. Potapova
A. Brysin

Summary. In the article, a mathematical model of the clonal selection algorithm, adapted for detecting denial-of-service (DDoS) attacks within the framework of artificial immune systems, is presented. The process of formalizing the feature spaces of network traffic and the principles of interaction between detectors (antibodies) and network events (antigens) is described. Special attention is given to the mechanisms of cloning, mutation, and selection of detectors, as well as their adaptation to the dynamic conditions of the network environment. The model takes into account the temporal characteristics of network traffic and implements adaptive updating of detectors, ensuring resilience against new and multi-phase attacks. An experimental analysis of the model's effectiveness was conducted using classification quality metrics. The obtained results confirm the applicability of the proposed approach for real-time detection of DDoS attacks.

Keywords: artificial immunity, clonal selection, DDoS attacks, mathematical modeling, anomaly detection, network traffic, information security.

Соколов Александр Сергеевич
МИРЭА=Российский технологический университет
Sokols601@gmail.com
Артемова Светлана Валерьевна
Доктор технических наук, доцент, МИРЭА=Российский технологический университет
artemova_s@mirea.ru
Потапова Дарья Александровна
преподаватель, старший научный сотрудник, МИРЭА=Российский технологический университет
Potapova.daria1998@yandex.ru
Брысин Андрей Николаевич
Кандидат технических наук, доцент, Институт машиноведения им. А.А. Благонравова РАН, МИРЭА=Российский технологический университет
brysin@rambler.ru

Аннотация. В статье представлена математическая модель алгоритма клонального отбора, адаптированная для обнаружения атак типа отказа в обслуживании (DDoS) в рамках концепции искусственных иммунных систем. Описан процесс формализации пространств признаков сетевого трафика и принципов взаимодействия между детекторами (антителами) и сетевыми событиями (антигенами). Особое внимание уделено механизмам клонирования, мутации и селекции детекторов, а также их адаптации к динамическим условиям сетевой среды. Модель учитывает временные характеристики сетевого трафика и реализует адаптивное обновление детекторов, что обеспечивает устойчивость к новым и многофазным атакам. Проведён экспериментальный анализ эффективности модели с применением метрик качества классификации. Полученные результаты подтверждают применимость предложенного подхода для обнаружения DDoS-атак в реальном времени.

Ключевые слова: искусственный иммунитет, клональный отбор, DDoS-атаки, математическое моделирование, обнаружение аномалий, сетевой трафик, информационная безопасность.

Введение

Распределенные атаки типа отказа в обслуживании (DDoS) являются одной из наиболее серьезных угроз в области кибербезопасности. [1, с. 212] Они нацелены на нарушение доступности сетевых ресурсов. Эти атаки характеризуются массовой отправкой запросов к целевому серверу, что приводит к его перегрузке и отказу в обслуживании. В условиях стремительного роста объемов сетевого трафика и усложнения методов атак разработка эффективных систем обнаружения становится критически важной задачей.

Искусственные иммунные системы (ИИС) [2, с. 344] предлагают перспективный подход к обнаружению DDoS-атак благодаря их способности моделировать биологические процессы иммунитета. Алгоритм клонального отбора, лежащий в основе ИИС, имитирует процесс

выбора и размножения антител, наиболее эффективный для распознавания патогенов. Данный механизм позволяет системе адаптироваться к новым угрозам, включая атаки нулевого дня.

Алгоритм клонального отбора базируется на принципах биологического иммунитета, где антитела с высокой аффинностью к антигенам проходят процесс клонирования и мутации для улучшения своей эффективности. В контексте обнаружения DDoS-атак сетевой трафик рассматривается как совокупность антигенов, а детекторы — как антитела, распознающие аномалии. Такой подход позволяет моделировать сложные сетевые взаимодействия в терминах биологических процессов.

Целью данного исследования является разработка математической модели алгоритма клонального отбора, адаптированной для обнаружения атак типа отказа в обслуживании. Модель должна учитывать динамичность сетевого трафика и обеспечивать высокую точность распознавания аномалий. [2, с. 344] Особое внимание уделяется способности системы обновлять свои детекторы для противодействия атакам. Понимание механизмов клонального отбора, заимствованных из биологии, позволяет формализовать процессы распознавания аномалий в сетевом трафике для построения математической модели для данного процесса.

Теоретическое обоснование

Искусственная иммунная система (ИИС) представляет собой вычислительный подход, основанный на принципах работы биологической иммунной системы, которая защищает организм от патогенов. Биологическая иммунная система функционирует как распределенная адаптивная система, способная распознавать и нейтрализовать патогены посредством сложных механизмов взаимодействия клеток. Одним из процессов является клональный отбор, при котором В-лимфоциты, продуцирующие антитела с высокой аффинностью к антигенам, размножаются и подвергаются мутациям. Этот процесс представлен на рисунке 1 как цикл, включающий распознавание, клонирование, мутацию и отбор.

В искусственных иммунных системах антигены представляют собой характеристики сетевого трафика, такие как частота запросов, объем данных или временные интервалы между пакетами. Антитела, или детекторы, являются математическими конструкциями, которые сопоставляются с этими характеристиками. Для иллюстрации принципа клонального отбора построим двумерную модель пространства признаков с детекторами аномального поведения. На ней антигены изображаются точками в многомерном пространстве (например, на плоскости с осями «частота запросов» и «объем данных»), где нормальный трафик образует плотные кластеры, а аномалии располагаются обособленно. Детекторы, обозначаемые как d покрывают области аномалий, но не пересекаются с зонами нормальной активности. Модель, продемонстрированная на рисунке 2, наглядно демонстрирует, как система «обучается»: детекторы адаптируются, чтобы точнее выявлять угрозы и минимизировать ложные срабатывания.

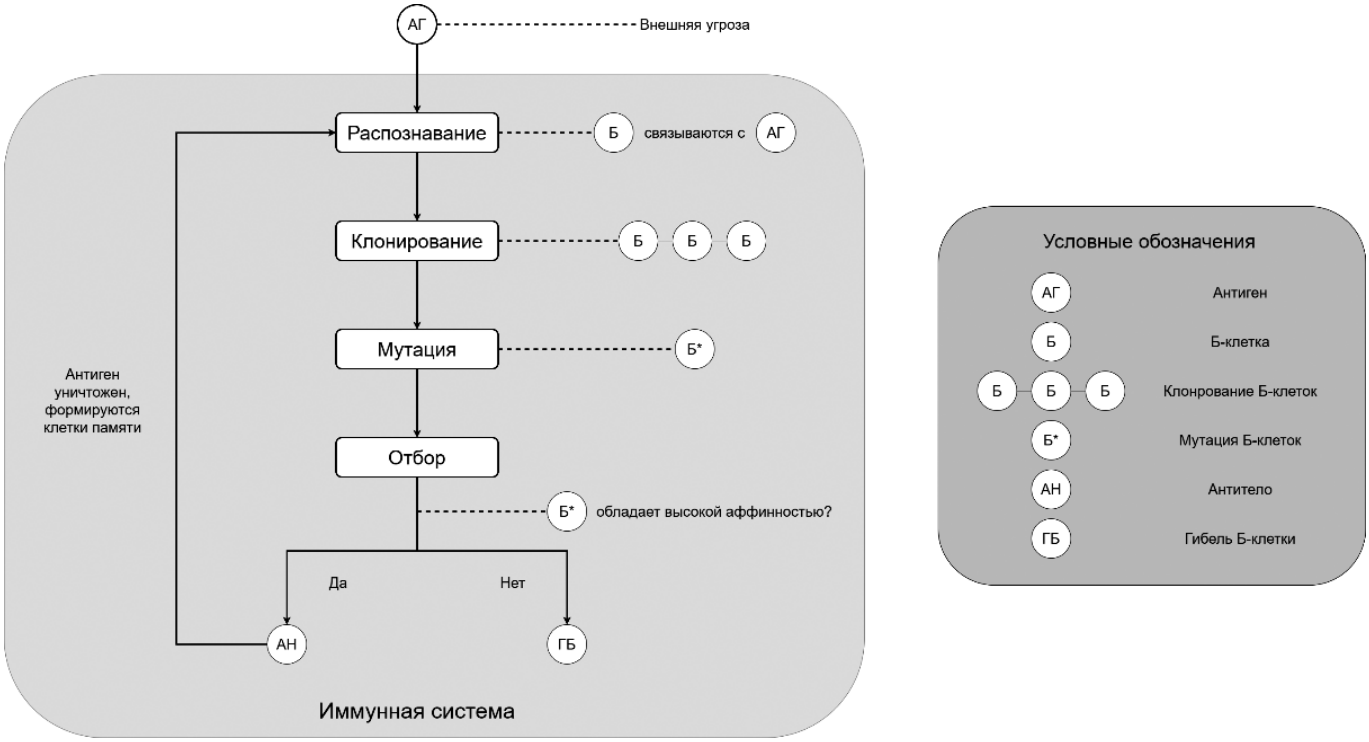

Рис. 1. Алгоритм клонального отбора

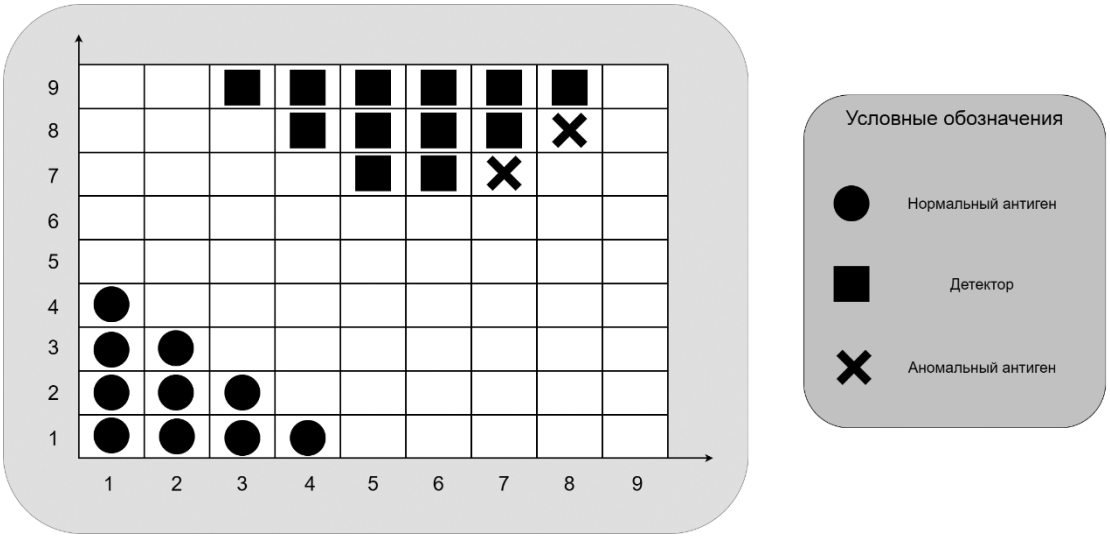

Рис. 2. Двумерная модель пространства признаков с детекторами аномального поведения

На основе модели пространства признаков [3, с. 41] формализуем процесс клонального отбора, что позволит количественно описать взаимодействие детекторов и антигенов в математических терминах.

Математическая формализация клонального отбора начинается с определения пространства признаков сетевого трафика. Например, трафик можно представить как вектор:

$$x = (x_1, x_2, \ldots, x_n)$$

где x_i — это метрики, такие как интенсивность пакетов или размер заголовков, а n — размерность пространства признаков, определяемая количеством выбранных метрик.

Аффинность между детектором d и антигеном x рассчитывается как расстояние, например, евклидово:

$$aff(d, x) = \sqrt{\sum_{i=1}^{n} (d_i - x_i)^2}$$

Детекторы с низким значением расстояния (высокой аффинностью) отбираются для клонирования.

Адаптация модели к задаче обнаружения DDoS-атак [4, с. 551] требует учета динамики сетевого трафика. Детекторы должны иметь ограниченный период существования, чтобы система могла обновляться в ответ на изменения. Например, каждый детектор может быть ассоциирован с параметром времени жизни τ, который уменьшается с каждым циклом анализа.

Математическая модель алгоритма клонального отбора

На основе теоретической формализации клонального отбора, описанной ранее, где сетевой трафик представлен как векторы характеристик в многомерном пространстве признаков, разработаем математическую модель алгоритма клонального отбора. Эта модель формализует процессы распознавания аномалий, клонирования, мутации и селекции детекторов, обеспечивая адаптацию к динамической природе DDoS-атак [4, с. 555].

Математическая модель клонального отбора начинается с формализации представления сетевого трафика как множества антигенов:

$$Ag = \{x_1, x_2, \ldots, x_m\},$$

где каждый $x_i \in R^n$. Детекторы формируют множество $Ab = \{d_1, d_2, \ldots, d_k\}$, где каждый детектор d_j характеризуется центром $c_j \in R^n$ и радиусом r_j. Задача состоит в том, чтобы покрыть пространство аномального трафика, минимизируя ложные срабатывания на нормальный трафик.

Для определения соответствия между антигенами и детекторами используется функция аффинности, которая измеряет близость между ними. В данной модели аффинность вычисляется как евклидово расстояние:

$$aff(x_i, d_j) = x_i - c_j.$$

Детектор активируется, если $aff(x_i, d_j) \leq r_j$, сигнализируя о возможной аномалии. Этот подход позволяет точно выделять области пространства признаков, где сосредоточены аномальные паттерны.

Процесс клонирования усиливает способность модели к распознаванию аномалий. Детекторы с высокой аффинностью (низким расстоянием до антигенов) создают N_c копий, где $N_c = \beta \times aff(x_i, d_j)^{-1}$, а β — коэффициент,

регулирующий интенсивность клонирования. Клонирование как указано в работе [5, с. 305] увеличивает плотность детекторов в областях, где аномалии наиболее вероятны, улучшая точность обнаружения.

Клоны подвергаются мутации для исследования новых областей пространства признаков и предотвращения переобучения на известные аномалии. Мутация моделируется как случайное возмущение центра детектора:

$$c_j' = c_j + \epsilon,$$

где $\epsilon \sim \mathcal{N}(0, \sigma^2)$. Параметр σ адаптируется в зависимости от плотности антигенов, обеспечивая баланс между исследованием новых паттернов и сохранением обобщающей способности модели.

Селекция детекторов направлена на выбор наиболее эффективных элементов, способных распознавать аномалии с минимальным перекрытием нормального трафика. Это достигается через минимизацию функции потерь:

$$L(d_j) = \sum_{x_i \in Ag} \left(aff(x_i, d_j) \le r_j \right) - \lambda \sum_{x_i \in Norm} \left(aff(x_i, d_j) \le r_j \right),$$

где λ — коэффициент штрафа за ложные срабатывания. Итеративная оптимизация функции потерь обеспечивает сходимость модели к оптимальному покрытию.

Адаптивность модели к изменяющимся DDoS-атакам реализуется через механизм обновления детекторов [6]. Каждый детектор имеет время жизни τ, которое уменьшается с каждым циклом анализа. Если детектор d_j не активируется в течение τ_j, он удаляется, а новый генерируется в области с низким покрытием. Этот процесс позволяет системе реагировать на новые типы атак, такие как многофазные DDoS-атаки.

Для повышения эффективности модель оптимизирует гиперпараметры, такие как β, σ и τ, с использованием методов градиентного спуска или эвристических алгоритмов. Оптимизация направлена на максимизацию точности и полноты обнаружения при минимизации вычислительных затрат. Такой подход делает модель применимой в реальных сетевых средах с высокими объемами трафика.

Визуализация и интерпретация модели

Для оценки эффективности разработанной математической модели клонального отбора была проведена серия экспериментов, направленных на анализ её способности обнаруживать DDoS-атаки в условиях динамического сетевого трафика. Основной задачей визуализации является демонстрация сходимости модели, выраженной через уменьшение функции потерь в процессе итеративной оптимизации. Визуализация позволяет интерпретировать поведение модели, выявляя её адаптивность и точность при распознавании аномалий.

Эффективность модели оценивалась с использованием метрик точности (Precision), полноты (Recall) и F1-меры. Точность определялась как доля правильно идентифицированных аномалий среди всех событий, классифицированных как аномальные:

$$Precision = \frac{TP}{TP + FP},$$

где *TP* — истинно положительные срабатывания, *FP* — ложноположительные.

Полнота измеряла долю обнаруженных аномалий из всех реальных аномалий:

$$Recall = \frac{TP}{TP + FN},$$

где *FN* — ложноотрицательные случаи [7].

F1-мера, рассчитываемая как

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall},$$

обеспечивала сбалансированную оценку. Эти метрики позволили объективно оценить качество обнаружения и минимизировать субъективные суждения о нормальности работы модели.

Процесс визуализации начинается с построения графика зависимости функции потерь *L* от номера итерации, что отражает динамику обучения модели. Функция потерь оценивает качество детекторов, балансируя между покрытием аномального трафика и минимизацией ложных срабатываний. Для эксперимента было выполнено 50 итераций, в ходе которых значения *L* фиксировались для каждого цикла.

В качестве входных данных использовались синтетические наборы данных, имитирующие сетевой трафик с нормальными и аномальными характеристиками. Антигены представляли собой векторы признаков, включающие метрики, такие как интенсивность пакетов и энтропия заголовков. Параметры модели, включая коэффициент клонирования $\beta = 10$, дисперсию мутации $\sigma^2 = 0{,}5$ и штраф за ложные срабатывания $\lambda = 0{,}5$, были предварительно оптимизированы для обеспечения устойчивости результатов.

На начальном этапе эксперимента значение функции потерь составило около 100 условных единиц, что

указывает на низкую начальную точность детекторов и большое число ложных срабатываний. С каждой итерацией, благодаря процессам клонирования [8, с. 8642], мутации и селекции, функция потерь экспоненциально уменьшалась, достигая уровня около 10 единиц к 50-й итерации. Это демонстрирует способность модели к самообучению и адаптации к сложным паттернам аномального трафика.

Для построения графика зависимости функции потерь от номера итерации значения L были рассчитаны по формуле:

$$L_t = L_0 \times e^{-kt} + C,$$

где $L = 100$, $k = 0{,}05$, $C = 10$, а t — номер итерации.

Интерпретация графика показывает, что модель быстро улучшает качество покрытия аномального трафика в первые 20 итераций, после чего скорость уменьшения функции потерь замедляется, достигая минимального уровня. Это подтверждает высокую эффективность алгоритма клонального отбора в задаче обнаружения DDoS-атак. Достижение низкого уровня функции потерь соответствует увеличению F1-меры до 0.92, как это показано на рисунке 3 к 50-й итерации, что указывает на оптимальный баланс между точностью и полнотой обнаружения.

Визуализация также позволяет оценить адаптивность модели к новым типам атак. График сходимости, продемонстрированный на рисунке 4, показывает, что модель успешно обновляет детекторы систем обнаружения вторжений [9], сохраняя низкий уровень функции потерь даже при изменении характера трафика, что подтверждает её применимость в реальных условиях.

Заключение

Полученные результаты исследования позволяют утверждать, что разработанная математическую модель алгоритма клонального отбора в искусственных иммунных системах может использоваться для обнаружения атак типа отказа в обслуживании. Визуализация процесса сходимости функции потерь демонстрирует способность модели к самообучению, обеспечивая точное распознавание аномального сетевого трафика при минимальном уровне ложных срабатываний. Предложенный подход может быть рекомендован специалистам в области кибербезопасности как перспективный метод обнаружения угроз, в сочетании с другими алгоритмами машинного обучения.

Рис. 3. Динамика F1-меры при обучении модели клонального отбора

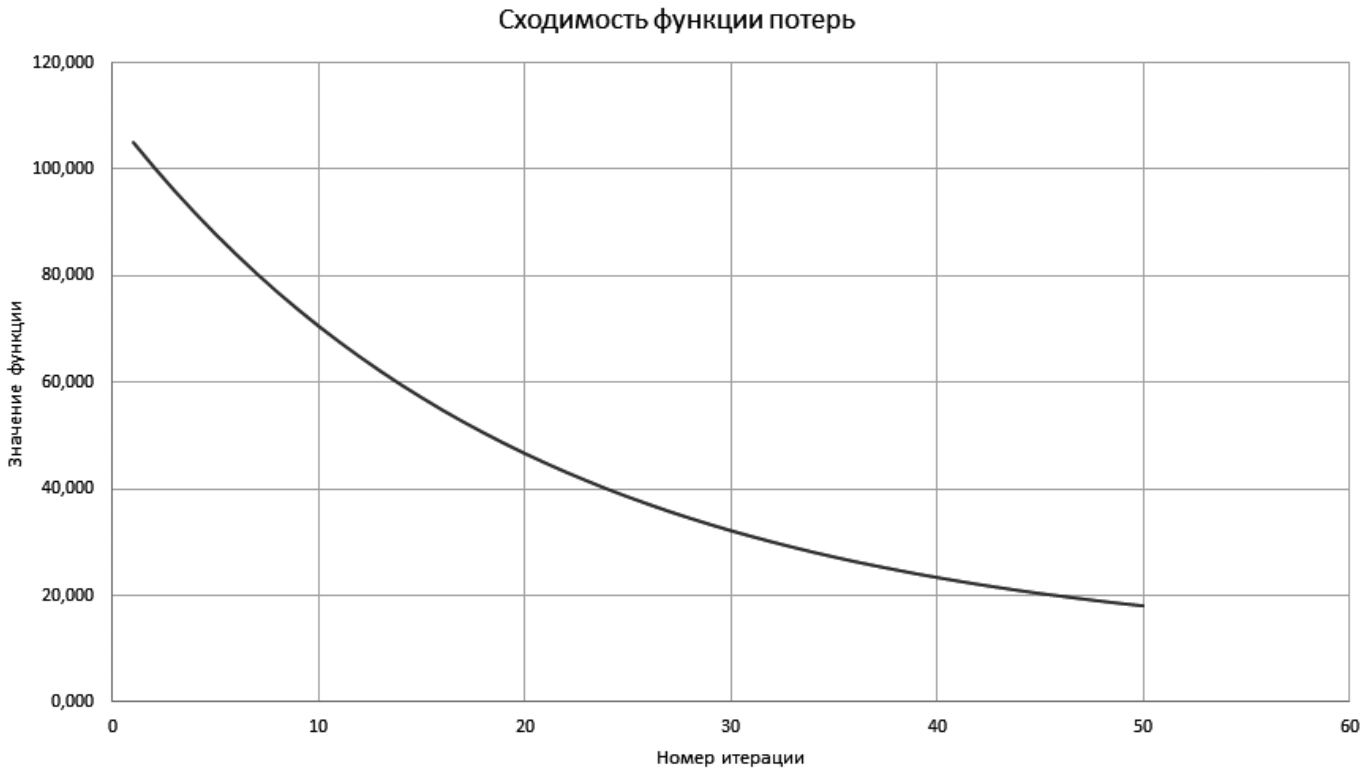

Рис. 4. Сходимость функции потерь

ЛИТЕРАТУРА

1. Скобцов Ю.А. Введение в искусственные иммунные системы: учебное пособие. — М., СПб.: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2022. — 212 с. [Дата обращения: 29.04.2025].
2. Дасгупта В. Введение в искусственные иммунные системы: учебное пособие. — Букинист, 2006. — 344 с. [Дата обращения: 29.04.2025].
3. Митяков Е.С., Максимова Е.А., Артемова С.В., Бакаев А.А., Вегера Ж.Г. Моделирование процессов управления инцидентами информационной безопасности на предприятии // Russian Technological Journal. — 2019. — С. 39–47. [Дата обращения: 30.04.2025].
4. Калашников А.О., Максимовский А.Ю. Развитие автоматных моделей мониторинга информационной безопасности сетевых объектов // Информация и безопасность. — ФГБОУ ВО «Воронежский государственный технический университет», 2019. — С. 549–556. [Дата обращения: 30.04.2025].
5. Потапова Д.А., Ушаков Д.А Применение генетических алгоритмов для оптимизации систем защиты информации. Кибербезопасность: технические и правовые аспекты защиты информации // Сборник научных трудов I Национальной научно-практической конференции. — С. 304–309. [Дата обращения: 30.04.2025].
6. Apostu, A., Gheorghe, S., Hîji, A., Cleju, N., Pătraşcu, A., Rusu, C., Ionescu, R., Irofti, P. Detecting and Mitigating DDoS Attacks with AI: A Survey [Электронный ресурс] // arXiv.org. — 2025. — 22 марта. — Режим доступа: https://arxiv.org/abs/2503.17867 (дата обращения: 01.05.2025).
7. de Melo L.H., Bertoli G.C., Nogueira M., dos Santos A.L., Pereira Junior L.A. Anomaly-Flow: A Multi-domain Federated Generative Adversarial Network for Distributed Denial-of-Service Detection [Электронный ресурс] // arXiv.org. — 2025. — 18 марта. — Режим доступа: https://arxiv.org/abs/2503.14618 (дата обращения: 01.05.2025).
8. Ramzan M., Shoaib M., Altaf A., Arshad S., Iqbal F., Castilla Á.K., Ashraf, I. Distributed Denial of Service Attack Detection in Network Traffic Using Deep Learning Algorithm [Электронный ресурс] // Sensors. — 2023. — Т. 23, № 20. — С. 8642. — DOI: https://doi.org/10.3390/s23208642 (дата обращения: 03.05.2025).
9. Gautam R., Padmavathy R. Distributed denial of service attack detection using machine learning classifiers [Электронный ресурс] // International Journal of Ad Hoc and Ubiquitous Computing. — 2024. — Режим доступа: https://www.inderscienceonline.com/doi/abs/10.1504/IJAHUC.2024.140032 (дата обращения: 04.05.2025).

© Соколов Александр Сергеевич (Sokols601@gmail.com); Артемова Светлана Валерьевна (artemova_s@mirea.ru);
Потапова Дарья Александровна Potapova.daria1998@yandex.ru); Брысин Андрей Николаевич (brysin@rambler.ru)
Журнал «Современная наука: актуальные проблемы теории и практики»