DOI: 10.15514/ISPRAS-2026-38(3)-46

Динамическая модель информационной системы с пороговым оператором адаптивной защиты

М.Д. Полин, ORCID: 0009-0001-1471-6638 <polin.md@edu.spbstu.ru>
А.А. Ефремов, ORCID: 0000-0002-0224-2412 <artem.efremov@spbstu.ru>
Санкт-Петербургский политехнический университет Петра Великого,
Россия, 195251, г. Санкт-петербург, ул. Политехническая, 29.

Аннотация. В работе исследуется задача обеспечения устойчивости информационных систем при воздействии аномально высокой нагрузки, характерной для распределённых атак типа «отказ в обслуживании» (DDoS). Предложена безразмерная детерминированная динамическая модель, основанная на теории массового обслуживания и описывающая взаимосвязанную динамику длины очереди запросов, уровня адаптивной защиты и загрузки вычислительных ресурсов – центрального процессора и сетевого канала. Модель учитывает нелинейный эффект насыщения скорости обработки при перегрузке, что отражает реальное снижение эффективности серверной инфраструктуры при росте числа одновременных запросов. Ключевым элементом является алгоритм адаптивной защиты, реализованный через пороговый оператор, который активируется только при превышении критического уровня очереди и автоматически отключается после нормализации нагрузки. Такой подход минимизирует риск блокировки легитимного трафика и исключает ложные срабатывания в штатном режиме работы. Выполнен анализ устойчивости на основе спектра матрицы Якоби, подтвердивший асимптотическую устойчивость системы при условии, что интенсивность штатного трафика не превышает пропускную способность обработки. Численное моделирование выполнено для трёх типов сценариев: кратковременного всплеска интенсивности, многоэтапной атаки с повторяющимися волнами и скрытой атаки типа с последующим резким усилением. Для повышения адекватности модели в неё введён механизм условного вовлечения резервных вычислительных ресурсов, активируемый только после завершения атаки и при сохраняющейся перегрузке. Валидация модели на данных публичного набора данных CICDDoS2019 подтвердила её приемлемую точность: достигнуто качественное и количественное соответствие. Полученные результаты демонстрируют практическую применимость модели для проектирования систем прогнозирующей защиты в облачных и распределённых средах, а также для оптимизации параметров адаптивных механизмов в реальных информационных инфраструктурах.

Ключевые слова: DDoS-атака; динамическое моделирование; теория массового обслуживания; адаптивная защита; оператор динамики; безразмерный анализ; устойчивость; кибербезопасность.

Для цитирования: Полин М.Д., Ефремов А.А. Динамическая модель информационной системы с пороговым оператором адаптивной защиты. Труды ИСП РАН, том 38, вып. 3, часть 4, 2026 г., стр. 59-70. DOI: 10.15514/ISPRAS–2026–38(3)–46.

Dynamic model of an information system with a threshold adaptive protection operator

M.D. Polin, ORCID: 0009-0001-1471-6638 <polin.md@edu.spbstu.ru>
A.A. Efremov, ORCID: 0000-0002-0224-2412 <artem.efremov@spbstu.ru>
Peter the Great St. Petersburg Polytechnic University
29, Politekhnicheskaya Street, St. Petersburg, 195251, Russia.

Abstract. This paper investigates the problem of ensuring the stability of information systems under anomalous load conditions characteristic of Distributed Denial-of-Service (DDoS) attacks. A deterministic dynamic model is proposed, grounded in queueing theory and describing the coupled dynamics of the request queue length, the level of adaptive protection, and the utilization of computational resources–namely, the central processing unit and the network channel. The model incorporates a nonlinear saturation effect in request processing under overload, which accurately reflects the degradation of server infrastructure efficiency as the number of concurrent requests increases. The core component of the model is an adaptive protection algorithm implemented through a threshold-based operator that activates only when the queue exceeds a critical threshold and automatically deactivates once the load normalizes, thereby minimizing the risk of blocking legitimate traffic and eliminating false positives during normal operation. To ensure universality of the analysis, the system of differential equations is transformed into a dimensionless form, which enables the identification of key dimensionless parameter groups and eliminates dependence on specific units of measurement. A rigorous stability analysis based on the spectrum of the Jacobian matrix confirms the asymptotic stability of the system, provided that the intensity of normal traffic does not exceed the processing capacity. Numerical simulations were conducted for three distinct attack scenarios: a short-term burst, a multi-stage attack with repeated waves, and a low-and-slow attack followed by a sharp surge. To enhance model adequacy, a mechanism for conditional engagement of reserve computational resources was introduced, activated only after the cessation of the attack and in the presence of persistent overload. Model validation against the public CICDDoS2019 dataset confirmed its high accuracy, demonstrating both qualitative and quantitative agreement. The obtained results highlight the model's practical applicability for designing predictive protection systems in cloud and distributed environments, as well as for optimizing the parameters of adaptive mechanisms in real-world information infrastructures.

Keywords: DDoS attack; dynamic modeling; queueing theory; adaptive protection; dynamic operator; dimensionless analysis; stability; cybersecurity.

For citation: Polin M.D., Efremov A.A. Dynamic model of an information system with a threshold adaptive protection operator. Trudy ISP RAN/Proc. ISP RAS, vol. 38, issue 3, part 4, 2026, pp. 59-70 (in Russian). DOI: 10.15514/ISPRAS-2026-38(3)-46.

1. Введение

По данным Cloudflare (от 2023 года), объём DDoS-атак за год вырос на 42 %, а пиковые значения превысили 1 Тбит/с – уровень, сопоставимый с суммарной нагрузкой на крупнейшие центры обработки данных [1]. Особенную важность представляет рост целевых атак на критически важные секторы: согласно статье по отчёту ENISA (от 2024г.), DDoS-инциденты составили 41 % от всех киберугроз в сфере здравоохранения [2]. В таких условиях даже кратковременная недоступность телемедицинских сервисов может повлечь за собой необратимые последствия.

Современные DDoS-атаки отличаются не только масштабом, но и высокой адаптивностью. Злоумышленники используют уязвимости в новых протоколах (например, HTTP/3), которые позволяют обходить традиционные сигнатурные фильтры [3]. Широкое распространение Интернета вещей (IoT-устройств) создаёт новые возможности для формирования мощных ботнетов: в 2024 году атака, организованная с помощью 500 тыс. скомпрометированных камер и роутеров, достигла мощности 2.3 Тбит/с и нарушила работу облачного провайдера OVHcloud [4]. Ещё одно направление – применение методов машинного обучения для

генерации трафика, имитирующего поведение реальных пользователей, что затрудняет его детекцию классическими средствами [5].

Традиционные методы защиты – такие как статические правила сетевого экрана или ручное масштабирование ресурсов – всё чаще оказываются неэффективными против быстро эволюционирующих угроз [6]. Это обуславливает необходимость перехода к адаптивным, прогнозирующим системам защиты, способным анализировать динамику атаки в реальном времени и оперативно корректировать стратегию противодействия.

В литературе для описания подобных систем применяются три основных типа моделей. Стохастические модели, основанные на теории вероятностей и случайных процессах (например, классические СМО типа M/M/1), хорошо подходят для анализа средних характеристик – таких как среднее время ожидания или вероятность отказа [7-8]. Однако они плохо приспособлены для задач синтеза управления и прогнозирования критических состояний в реальном времени. Гибридные модели пытаются совместить стохастический и детерминированный подходы, но зачастую становятся чрезмерно сложными для анализа и интерпретации [9-10]. Детерминированные модели, построенные на системах обыкновенных дифференциальных уравнений, занимают промежуточное положение: они достаточно просты для качественного анализа (включая исследование устойчивости), но при этом позволяют явно описывать причинно-следственные связи между трафиком, ресурсами и защитой.

В рамках детерминированного подхода можно выделить два направления исследований. Первым направлением является теоретико-игровое моделирование, где взаимодействие злоумышленника и системы защиты рассматривается как динамическая игра [11]. Хотя такой подход теоретически строг, на практике он требует знания стратегии противника, что в условиях реальных кибератак недостижимо.

Вторым направлением является использование модели теории массового обслуживания (СМО), где динамика длины очереди $L(t)$ описывается балансовым уравнением $L^{\cdot} = \lambda - \mu$, где λ – интенсивность входящего потока, а μ – скорость обслуживания. Такая модель отражает «вид спереди» на систему, но не учитывает механизмы защиты. Для их включения используется подход с обратной связью [12].

Цель настоящей работы – разработка динамической модели в операторной форме для синтеза адаптивной защиты информационной системы от DDoS-атак. В работе использован детерминированный подход. Он обеспечивает оптимальный баланс между физической интерпретируемостью, математической простотой и пригодностью для дальнейшего использования в системах прогнозирующей защиты.

2. Синтез дифференциального оператора информационной системы

Объектом моделирования выступает серверная инфраструктура информационной системы, подверженная DDoS-атаке. Её состояние описывается четырьмя переменными:

$L(t)$ – длина очереди запросов (число задач, ожидающих обработки);

$R(t)$ – уровень адаптивной защиты, интерпретируемый как порог фильтрации трафика;

$C(t)$ – нормированная загрузка центрального процессора;

$B(t)$ – нормированная загрузка сетевого канала.

Общий входящий трафик складывается из законного и атакующего компонентов:

$$\alpha(t) = \alpha_{legit} + \alpha_{attack}(t), \tag{1}$$

где α_{attack} задаётся как кусочно-постоянная функция, активная в интервале $[t_s, t_e]$.

Скорость обработки запросов снижается при перегрузке из-за конкуренции за ресурсы. Этот эффект моделируется нелинейной зависимостью [13]:

$$\mu(L) = \mu_0 \cdot \frac{L}{L+1}. \tag{2}$$

При малой очереди система работает с максимальной эффективностью, а при росте очереди скорость обработки стремится к предельному значению μ_0, но задержки возрастают.
Динамика очереди описывается балансовым уравнением:

$$\frac{dL}{dt} = \alpha(t) - \mu_0 \cdot \frac{L}{L+1}. \tag{3}$$

Для учёта адаптивной защиты вводится механизм обратной связи. Защита активируется только при превышении критического уровня очереди L_{crit}:

$$\frac{dR}{dt} = \max(L - L_{crit}, 0) - \gamma(t) R, \tag{4}$$

где коэффициент затухания $\gamma(t)$ зависит от фазы атаки:

$$\gamma(t) = \begin{cases} \gamma_{active}, & t \le t_e, \\ \gamma_{cooldown} & t > t_e. \end{cases}$$

Загрузка вычислительных ресурсов связана с длиной очереди через линейные дифференциальные уравнения первого порядка:

$$\frac{dC}{dt} = \eta_1 (L - C),$$

$$\frac{dB}{dt} = \eta_2 (L - B),$$

где η_1, η_2 – коэффициенты, характеризующие инерционность CPU и сети.
Модель информационной системы представляет собой систему обыкновенных именованных дифференциальных уравнений. Эту систему можно записать в операторной форме:

$$\frac{d\mathbf{X}}{dt} = \mathrm{A}\left(\mathbf{X}(t), \alpha_{attack}(t)\right), \tag{5}$$

где $\mathbf{X} = \begin{bmatrix} L & R & C & B \end{bmatrix}^T$ – вектор состояния, а A – оператор динамики, интегрирующий процессы обработки, защиты и реакции ресурсов.
Далее система именованных дифференциальных уравнений приведена к безразмерной форме. В качестве масштабирующих величин выбраны характерная длина очереди $L_0 = L_{crit}$ и характерное время $t_0 = 1/\mu_0$.
Вводятся безразмерные переменные:

$$l = \frac{L}{L_0}, \quad \tau = \frac{t}{t_0} = \mu_0 t, \quad r = \frac{R}{L_0}, \quad c = C, \quad b = B.$$

Подстановка безразмерные переменных в систему именованных уравнений (5) позволяет получить безразмерную форму модели информационной системы:

$$\begin{cases} \dfrac{dl}{d\tau} = a_l + a_a(\tau) - \dfrac{l}{l+1} - \delta \cdot H(\tau - \tau_e) \cdot H(l-1), \\ \dfrac{dr}{d\tau} = \begin{cases} \max(l-1, 0) - \gamma_{active} r, & \tau \le \tau_e, \\ -\gamma_{cooldown} r, & \tau > \tau_e, \end{cases} \\ \dfrac{dc}{d\tau} = \dot{\eta}_1 (l - c), \\ \dfrac{db}{d\tau} = \dot{\eta}_2 (l - b), \end{cases} \tag{6}$$

где введены безразмерные параметры:

$$a_l = \frac{\alpha_{legit}}{\mu_0 L_{crit}}, \quad a_a = \frac{\alpha_{attack}}{\mu_0 L_{crit}}, \quad \dot{\eta}_1 = \eta_1 t_0, \quad \dot{\eta}_2 = \eta_2 t_0.$$

Дифференциальный оператор информационной системы (6) принимает вид:

$$\frac{d\mathbf{X}}{d\tau} = \mathbf{M}\mathbf{X} + \mathbf{N} + \mathbf{F}(\mathbf{X}), \tag{7}$$

где

$$\mathbf{X} = \begin{bmatrix} l \\ r \\ c \\ b \end{bmatrix}, \quad \mathbf{M} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & -\gamma & 0 & 0 \\ 0 & 0 & -\dot{\eta}_1 & 0 \\ 0 & 0 & 0 & \dot{\eta}_2 \end{bmatrix}, \quad \mathbf{N} = \begin{bmatrix} a_l + a_a(\tau) \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad \mathbf{F}(\mathbf{X}) = \begin{bmatrix} -\frac{l}{l+1} - \delta \cdot H(\tau - \tau_e) \cdot H(l-1) \\ \max(l-1, 0) \\ \dot{\eta}_1 l \\ \dot{\eta}_2 l \end{bmatrix}.$$

Предложенный оператор включает алгоритм адаптивной защиты, который реализует следующую логику управления: защита активируется только при превышении критического уровня очереди $l > L_{\text{crit}}$. Реализация выполнена через нелинейную функцию

$$F_{act}(l) = \max(l-1, 0).$$

Коэффициент затухания защиты γ переключается в зависимости от фазы атаки:

- Во время атаки ($\tau \le \tau_e$): $\gamma = \gamma_{\text{active}}$. Это обеспечивает устойчивость защиты к кратковременным флуктуациям трафика и предотвращает «дрожание» порога.
- После атаки ($\tau > \tau_e$): $\gamma = \gamma_{\text{cooldown}}$. Это гарантирует быстрое отключение защиты, минимизируя риск блокировки легитимного трафика в период после атаки.

После завершения атаки, если очередь остаётся выше критического уровня, система автоматически подключает дополнительные вычислительные мощности. Этот механизм описывается слагаемым:

$$\delta H(\tau - \tau_e) \cdot H(l-1),$$

где $H(\cdot)$ – функция Хевисайда. Таким образом, резервные ресурсы включаются только тогда, когда они действительно необходимы для ускорения восстановления. Данный алгоритм отражает принципы работы современных облачных платформ, где некоторая пороговая активация соответствует правилам сетевого экрана, используя двухрежимное затухание быстро возвращает стандартную политику фильтрации. Однако есть допущения по эластичному масштабированию, за счёт привлечения дополнительных ресурсов.

3. Анализ устойчивости оператора информационной системы

Анализ устойчивости является центральным этапом исследования динамических систем, поскольку позволяет определить способность информационной системы возвращаться в рабочее состояние после внешнего возмущения – в данном случае, DDoS-атаки. Устойчивость понимается в смысле Ляпунова: малые отклонения от равновесного состояния не приводят к неограниченному росту очереди или полному отказу в обслуживании. Рассматривается поведение системы после завершения атаки, когда внешний атакующий поток отсутствует ($a_a = 0$). В этом случае динамика защиты упрощается: поскольку $l < 1$ вблизи равновесия, выполняется $\max(l - 1,0) = 0$, и уравнение для r принимает вид:

$$\frac{dt}{d\tau} = -\gamma_{cooldown} r.$$

Следовательно, $r(\tau) \to 0$ экспоненциально быстро, и в окрестности стационарной точки можно положить $r^* = 0$.

Таким образом, стационарное состояние системы определяется решением уравнения:

$$0 = a_l - \frac{l^*}{l^* + 1}. \tag{8}$$

Решая его, получается:

$$l^* = \frac{a_l}{1 - a_l}, \quad a_l < 1. \tag{9}$$

Это условие имеет простой физический смысл: законный трафик не должен превышать пропускную способность системы в нормальном режиме. Если $a_l \ge 1$, система не имеет устойчивого равновесия даже без атаки, что соответствует перманентной перегрузке. Для анализа устойчивости проводится линеаризация системы в окрестности стационарной точки (l^*, $r^* = 0$, $c^* = l^*$, $b^* = l^*$). Частные производные правых частей уравнений:

Для очереди:

$$f_l(l) = a_l - \frac{l}{l+1} \quad \Rightarrow \quad \left.\frac{\partial f_l}{dl}\right|_{l^*} = -\frac{1}{(l^*+1)^2}.$$

Для защиты:

$$f_r(l, r) = -\lambda_{cooldown} r \quad \Rightarrow \quad \frac{\partial f_r}{\partial l} = 0, \frac{\partial f_r}{\partial r} = -\gamma_{cooldown}.$$

Для ресурсов:

$$\frac{\partial f_c}{dl} = \eta_1^{'}, \quad \frac{\partial f_c}{\partial c} = -\eta_1^{'}, \quad \frac{\partial f_b}{\partial l} = \eta_2^{'}, \quad \frac{\partial f_b}{\partial b} = -\eta_2^{'}.$$

Матрица Якоби принимает вид:

$$J = \begin{bmatrix} -\frac{1}{(l^*+1)^2} & 0 & 0 & 0 \\ 0 & -\gamma_{cooldown} & 0 & 0 \\ \eta_1^{'} & 0 & -\eta_1^{'} & 0 \\ \eta_2^{'} & 0 & 0 & -\eta_2^{'} \end{bmatrix}. \tag{10}$$

Собственные значения этой матрицы:

$$\lambda_1 = -\frac{1}{(l^*+1)^2} \quad \lambda_2 = -\gamma_{cooldown} \quad \lambda_3 = -\eta_1^{'} \quad \lambda_4 = -\eta_2^{'}.$$

Все собственные значения строго отрицательны при $a_l < 1$, что означает, что стационарная точка является асимптотически устойчивой. Система не только возвращается в равновесие, но и делает это экспоненциально быстро.

Физическая интерпретация собственных значений:

- λ_1 – скорость стабилизации очереди (зависит от загрузки);
- λ_2 – скорость отключения защиты;
- λ_3, λ_4 – инерционность CPU и сети.

4. Вычислительный эксперимент

Для оценки эффективности предложенной модели и алгоритма адаптивной защиты было проведено численное моделирование в трёх различных сценариях DDoS-атак. Все эксперименты выполнены при одинаковых параметрах системы, значения которых приведены в табл. 1 и соответствуют условиям, использованным при реализации оператора на языке Python.

Табл. 1. Параметры моделирования.
Table 1. Model parameters.

Параметр	Обозначение	Значение
Законный трафик	a_l	1,0
Атакующий трафик	a_a	1,5
Критический уровень очереди	L_{crit}	1,0
Коэффициент затухания (атака)	γ_{active}	0,3
Коэффициент затухания (после атаки)	$\gamma_{cooldown}$	1,5
Коэффициент вовлечения ресурсов	δ	0,5
Начальные условия	$l(0)$, $r(0)$, $c(0)$, $b(0)$	0,1 / 0 / 0.5 / 0.5

Рассмотрим несколько сценариев DDoS-атак.

Сценарий 1: Импульсная атака

Атака представляет собой однократный всплеск интенсивности трафика в интервале $\tau \in [5,15]$. Результаты моделирования (рис. 1) показывают:

- При начале атаки очередь l начинает расти, достигая пика ≈ 18 к моменту её окончания.
- Защита r активируется постепенно, достигая значения ≈ 25 .
- Сразу после окончания атаки (τ >15) защита быстро спадает до нуля за счёт высокого коэффициента $\gamma_{cooldown}$ = 1.5.
- Одновременно включаются резервные ресурсы (δ = 0.5), что приводит к резкому снижению очереди – она падает с 18 до 6 за 5 единиц времени.
- Система стабилизируется на уровне l ≈ 5.0, что соответствует равновесному состоянию при a_l = 1.

Этот сценарий демонстрирует корректную работу всех компонентов алгоритма: пороговая активация, быстрое отключение защиты и ускоренное восстановление.

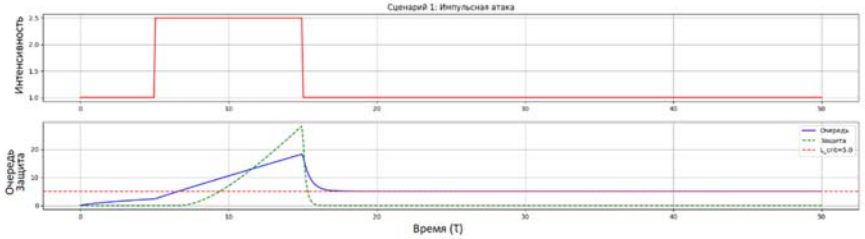

Рис. 1. Графики компонент состояний при импульсной атаке.
Fig 1. State component graphs under a pulse attack.

Сценарий 2: Многоэтапная атака

Атака состоит из трёх волн: (5, 10, 1.2), (15, 20, 1.8), (25, 30, 1.0). Результаты (рис. 2) показывают:

- При каждой волне защита активируется и затем быстро спадает после её окончания, что подтверждает работоспособность механизма с двумя режимами затухания.

- Между волнами очередь не успевает полностью восстановиться, что приводит к более высокому пиковому значению на третьей волне (l ≈ 25).
- После окончания третьей волны резервные ресурсы включаются, и очередь быстро снижается до уровня l ≈ 5.

Этот сценарий подтверждает, что модель способна адаптироваться к повторным атакам без ложных срабатываний защиты между волнами.

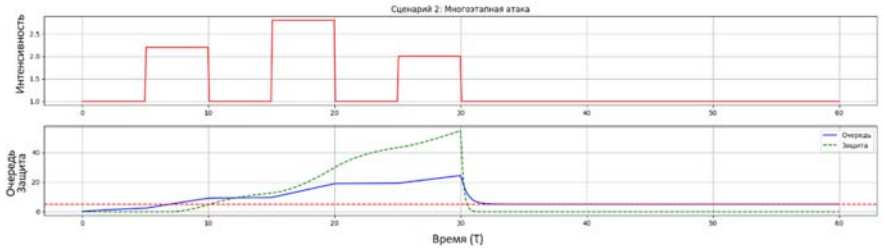

Рис. 2. Графики компонент состояний при волновой атаке.
Fig. 2. State component graphs during a wave attack.

Сценарий 3: Скользящая атака

Сценарий включает медленную атаку в течение 40 единиц времени (a_a=0.3), за которой следует резкий всплеск ($\tau \in [40,45]$, a_a = 2.0). Результаты (рис. 3) показывают:

- Во время атаки очередь медленно растёт, но остаётся ниже критического уровня (l < 1), поэтому защита не активируется. Это соответствует реальной ситуации, когда атака маскируется под легитимный трафик.
- При резком увеличении трафика (τ = 40) очередь скачкообразно растёт до l ≈ 25, что вызывает мгновенную активацию защиты.
- После всплеска очередь снижается медленнее, чем в предыдущих сценариях, поскольку перед всплеском уже была накоплена скрытая перегрузка. Время восстановления составляет ≈ 15 единиц времени.

Этот сценарий наиболее близок к реальным атакам и подтверждает, что модель способна выявлять скрытую перегрузку и реагировать на неожиданные всплески.

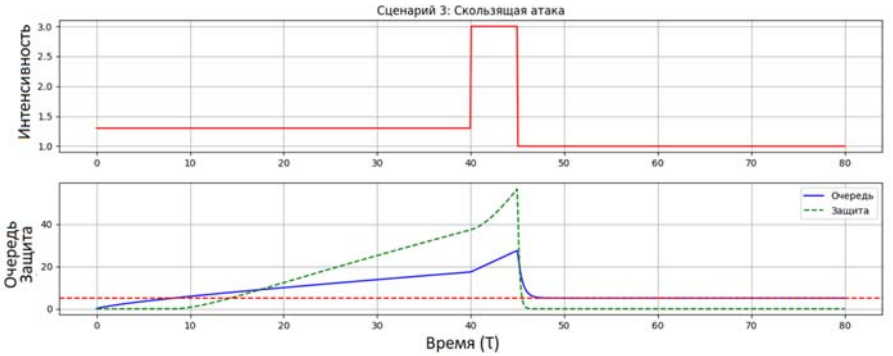

Рис. 3. Графики компонент состояний при скользящей атаке.
Fig. 3. State component graphs during a "slow-low" attack.

5. Валидация модели

Для подтверждения адекватности предложенной динамической модели была проведена её валидации. Валидация модели проведена по двум направлениям: функциональная (соответствие выходных данных реальным измерениям) и структурная (корректность внутренних механизмов и связей). На основе публичного набора данных CICDDoS2019, разработанного Канадским институтом кибербезопасности. Этот набор является общепризнанным эталоном для оценки моделей анализа DDoS-атак и содержит трафик реальных атак, собранный в контролируемой лабораторной среде [14].

В качестве эталонных данных выбран сценарий DrDoS/UDP, представляющий собой распределённую атаку с использованием протокола UDP. Из исходных CSV-файлов набора были извлечены следующие параметры для каждого сетевого потока:

- временная метка начала потока;
- длительность потока, мкс;
- общее число пакетов от атакующего;
- общий объём данных, байт.

На основе этих данных был построен временной ряд интенсивности трафика в пакетах в секунду. Для этого каждый поток был равномерно «распределён» по своей длительности, а затем агрегирован в 1-секундные временные интервалы. Полученный профиль PPS был нормирован на уровень легитимного трафика в спокойном режиме (≈200 пакетов/с), что позволило перейти к безразмерной интенсивности:

$$a_{total}^{real}(\tau) = \frac{PPS(T)}{PPS_{normal}}. \quad (11)$$

Этот нормированный профиль использовался в качестве входного воздействия $a_a(\tau)$ в предложенную модель. Все остальные параметры (табл. 1) оставались неизменными. Численное интегрирование системы ОДУ проводилось на интервале, соответствующем длительности атаки в наборе данных (~100 с).

Результаты моделирования были сопоставлены с нормированным профилем из набора данных CICDDoS2019. Получено качественное совпадение формы кривых: оба профиля демонстрируют резкий всплеск нагрузки, плато во время атаки и экспоненциальное снижение после её окончания. Отметим, что значение квадратного корня из средней квадратичной ошибки RMSE=0.18 следует интерпретировать в контексте детерминированной природы модели. В различных работах для гибридных стохастико-детерминированных моделей DDoS-атак достигаются значения RMSE в диапазоне 0.08–0.15, однако ценой значительно большей вычислительной сложности. Таким образом, предложенная модель представляет собой компромисс между точностью и вычислительной эффективностью, что делает её пригодной для применения в условиях ограниченных вычислительных ресурсов или требований к быстрому реагированию.

Структурная валидация подтверждается анализом устойчивости и корректностью поведения в предельных режимах.

6. Вывод / Conclusion

В результате синтезирована и исследована детерминированная модель информационной системы, подверженной воздействию аномально высокой нагрузки. Модель интегрирует три ключевых процесса: нелинейную насыщаемость обработки запросов, адаптивный механизм защиты и реакцию вычислительных ресурсов. Путём приведения системы к безразмерной форме обеспечена её универсальность и выделены ключевые безразмерные группы параметров. Выполнен анализ устойчивости, подтвердивший асимптотическую стабильность

системы при условии, что интенсивность штатного трафика не превышает пропускную способность обработки. Численное моделирование для трёх сценариев и валидация на структурированном наборе данных CICDDoS2019 подтверждает приемлемое поведение модели. Предложенный оператор динамики, включающий пороговый механизм адаптивной защиты и условное вовлечение резервных ресурсов, обеспечивает эффективную стабилизацию системы без ложных срабатываний. Демонстрируется принципиальная возможность построения прогнозирующих систем защиты на основе детерминированных моделей.

Основное допущение заключается в детерминированном характере модели, которая не учитывает стохастические компоненты динамической информационной системы и реального трафика. Это делает модель менее пригодной для анализа систем с низкой интенсивностью атак или в условиях смешанного легитимного и вредоносного трафика с высокой степенью случайности.

Дальнейшее развитие модели предполагает интеграцию стохастических компонентов, учет многоуровневой архитектуры и оптимизацию параметров модели методами теории автоматического управления.

Список литературы / References

[1]. Cloudflare. DDoS Threat Report for 2023 Q4: Cloudflare Blog, 2023. Available at: https://blog.cloudflare.com/ddos-threat-report-for-2023-q4/, accessed дата обращения: 18.12.2025.

[2]. ENISA Threat Landscape 2024: European Union Agency for Cybersecurity, 2024. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024, accessed: 18.12.2025

[3]. Козырева Н. И. Современные методы предотвращения DDoS-атак и защиты веб-серверов, 2025. Available at: https://cyberleninka.ru/article/n/sovremennye-metody-predotvrascheniya-ddos-atak-i-zaschity-veb-serverov, accessed 18.12.2025.

[4]. OVHcloud. A brief retrospective of network-layer DDoS attacks in 2024: OVHcloud Blog, 2025. Available at: https://blog.ovhcloud.com/a-brief-retrospective-of-network-layer-ddos-attacks-in-2024-at-ovhcloud/, accessed 18.12.2025.

[5]. Лапина М.А. Применение технологий машинного обучения для обнаружения вторжений и атак в веб-среде. Вестник компьютерных и информационных технологий, 2024, № 4, стр. 92-103. Доступно по ссылке: https://cyberrus.info/wp-content/uploads/2024/07/vokib-2024-4-st10-s092-103.pdf, дата обращения: 18.12.2025.

[6]. Горбачёв А.А. Алгоритм имитации динамических характеристик сетевого трафика веб-сервисов с использованием методов машинного обучения. Вестник компьютерных и информационных технологий, 2024, № 4, стр. 104-115. Доступно по ссылке: https://cyberrus.info/wp-content/uploads/2024/08/vokib-2024-4-st11-s104-115.pdf, дата обращения: 18.12.2025.

[7]. MITRE. Adversarial ML Threat Matrix. MITRE, 2020. Доступно по ссылке: https://github.com/mitre/advmlthreatmatrix, дата обращения: 21.12.2025.

[8]. Mishra P., Varadharajan V., Tupakula U., Pilli E.S. A Detailed Investigation and Analysis of DDoS Attacks in Cloud Computing Environment. Journal of Network and Computer Applications, 168 (2020), 102736.

[9]. Петрива Н.В. Гибридная система массового обслуживания с повторными вызовами. Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2021, № 1 (55), стр. 136-145. Доступно по ссылке: https://vital.lib.tsu.ru/vital/access/services/Download/koha:000721432/SOURCE1, дата обращения: 25.10.2025.

[10]. Васильев В.И., Вульфин А.М. Гибридные модели в задачах обнаружения сетевых атак: проблемы реального времени и интерпретации. Вестник компьютерных и информационных технологий, 2024, № 6, стр. 117-129. Доступно по ссылке: https://cyberrus.info/wp-content/uploads/2024/12/vokib-2024-6-st10-s117-129.pdf, дата обращения: 18.12.2025.

[11]. Калашников А.О. Пример использования теоретико-игрового подхода в задачах обеспечения кибербезопасности информационных систем с использованием «ложных» информационных объектов. Вестник компьютерных и информационных технологий, 2014, № 1, стр. 49-54. Доступно по ссылке: https://cyberrus.info/wp-content/uploads/2014/03/49-54.pdf, дата обращения: 18.12.2025.

[12]. Осипов Г.С. Компьютерное моделирование систем массового обслуживания с ограничениями. Современные наукоемкие технологии, 2025, № 1, стр. 1-10. Доступно по ссылке: https://top-technologies.ru/article/view?id=37874, дата обращения 16.12.2025.

[13]. Головко Н.И. Исследование моделей систем массового обслуживания в информационных сетях // Сибирский журнал индустриальной математики, 2008, т. 11, № 1, стр. 45-56. Доступно по ссылке: https://www.mathnet.ru/php/getFT.phtml?jrnid=sjim&paperid=500&what=fullt, дата обращения: 18.12.2025.

[14]. Talukder M. A., Uddin M. CIC-DDoS2019 Dataset (version 1), 2023. [Dataset]. Mendeley Data. DOI: 10.17632/ssnc74xm6r.1.

Информация об авторах / Information about authors

Максим Дмитриевич ПОЛИН – студент бакалавриата по направлению подготовки «Информационные системы и технологии», Института компьютерных наук и кибербезопасности, СПБПУ Петра Великого. Сфера научных интересов: моделирование информационных систем, решение задач оптимизации, экстремальных задач, разработка программных продуктов.

Maksim Dmitrievich POLIN – undergraduate student in the field of Information Systems and Technologies at the Institute of Computer Science and Cybersecurity of Peter the Great St. Petersburg Polytechnic University. Research interests: information systems modeling, solving optimization and extremal problems, software development.

Артём Александрович ЕФРЕМОВ – кандидат физико-математических наук, доцент, руководитель ООП «Информационные системы и технологии», Института компьютерных наук и кибербезопасности, СПБПУ Петра Великого. Сфера научных интересов: синтез сложных динамических систем, оптимизация, управление.

Artem Aleksandrovich EFREMOV – Cand. Sci. (Phys.-Math), Assoc. Prof., Head of the Information Systems and Technology Training Department at the Institute of Computer Science and Cybersecurity of Peter the Great St. Petersburg Polytechnic University. Research interests: synthesis of complex dynamic systems, optimization, control.