УДК 004.056
doi:10.31799/1684-8853-2026-4-28-40
EDN: HRWBEL

Научные статьи
Articles

Теоретико-игровая модель адаптивного управления защищенностью распределенных IoT/IoRT-систем на основе обнаружения аномалий и прогнозирования уязвимости безопасности

В. А. Липатников[a], *доктор техн. наук, профессор, orcid.org/0000-0002-3736-4743, lipatnikovanl@mail.ru*
В. А. Задбоев[a], *младший научный сотрудник, orcid.org/0009-0003-9362-1307*
Д. В. Макаренко[a], *адъюнкт, orcid.org/0009-0002-4732-2990*
И. А. Андреев[a], *оператор роты (научной), orcid.org/0009-0007-3617-3439*
[a]*Военная академия связи им. Маршала Советского Союза С. М. Буденного, Тихорецкий пр., 3, Санкт-Петербург, 193232, РФ*

Введение: *современные распределенные IoT/IoRT-системы непрерывно функционируют в условиях нестационарного трафика, ограниченных ресурсов периферийных узлов и изменяющихся многоэтапных киберугроз, что требует перехода от реактивных схем контроля к превентивному управлению защищенностью. Особую сложность представляет необходимость сохранять устойчивость функционирования при одновременном воздействии всех указанных факторов. При этом традиционные механизмы контроля не всегда позволяют своевременно учитывать динамику атаки и изменение состояния системы.* ***Цель:*** *разработать теоретико-игровую модель адаптивного управления защищенностью распределенных IoT/IoRT-систем, объединяющую обнаружение аномалий, прогнозирование краткосрочной уязвимости безопасности и превентивный выбор режима контроля при ограниченных ресурсах.* ***Результаты:*** *построена модель конфликта «Злоумышленник–Защитник», в которой решение о выборе режима контроля принимается по минимаксному критерию с учетом текущей аномальности, накопленной аномальности, прогноза уязвимости и остатка ресурса безопасности. Предложенный подход обеспечивает повышение качества управленческих решений в условиях неопределенности действий нарушителя и позволяет рассматривать защиту как непрерывный процесс адаптации к изменяющимся условиям функционирования системы. Экспериментальная проверка на данных N-BaIoT показала, что теоретико-игровая стратегия обеспечивает меньший средний и накопленный ущерб по сравнению со статической, пороговой и риск-ориентированной стратегиями, что подтверждает целесообразность использования адаптивного выбора режима контроля для снижения последствий многоэтапных кибервоздействий.* ***Практическая значимость:*** *возможно построение вычислительно реализуемых средств превентивного управления защищенностью распределенных IoT/IoRT-систем на стандартной аппаратной платформе.*

Ключевые слова *— IoT, IoRT, защищенность, обнаружение аномалий, прогнозирование уязвимости, теоретико-игровая модель, превентивное управление, киберугрозы, многоэтапные атаки, ресурсные ограничения.*

Для цитирования: Липатников В. А., Задбоев В. А., Макаренко Д. В., Андреев И. А. Теоретико-игровая модель адаптивного управления защищенностью распределенных IoT/IoRT-систем на основе обнаружения аномалий и прогнозирования уязвимости безопасности. *Информационно-управляющие системы*, 2026, № 4, с. 28–40. doi:10.31799/1684-8853-2026-4-28-40, EDN: HRWBEL
For citation: Lipatnikov V. A., Zadboev V. A., Makarenko D. V., Andreev I. A. Game-theoretic model of adaptive security management for distributed IoT/IoRT systems based on anomaly detection and security vulnerability forecasting. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 4, pp. 28–40 (In Russian). doi:10.31799/1684-8853-2026-4-28-40, EDN: HRWBEL

Введение

Распределенные системы интернета вещей (IoT) и интернета вещей робототехнических комплексов (IoRT) широко применяются в задачах мониторинга, управления и обмена данными в реальном времени. Рост числа периферийных узлов, неоднородность каналов связи и изменение характера сетевого взаимодействия усложняет обеспечение защищенности таких систем, особенно в условиях многоэтапных и изменяющихся атакующих воздействий [1–4].

Для IoT/IoRT-сред характерно сочетание трех факторов: нестационарного трафика, ограниченных вычислительных и энергетических ресурсов периферийных узлов и высокой изменчивости киберугроз. Поэтому традиционные средства контроля безопасности, основанные на статических правилах, сигнатурах и фиксированных порогах, нередко оказываются недостаточно гибкими: они хуже адаптируются к новым типам атак, чувствительны к несбалансированности данных и не всегда обеспечивают своевременную реакцию при развитии сложных сценариев вторжения [5–9].

Особую сложность представляют многоэтапные и коррелированные во времени атаки, при которых вредоносное воздействие формируется не одним событием, а последовательностью взаимосвязанных действий [10–13]. В таких условиях недостаточно фиксировать только текущее отклонение от нормы. Необходимо учитывать накопление признаков угрозы во времени, прогнозировать

изменение состояния безопасности и выбирать режим контроля с упреждением относительно следующей фазы атаки.

Однако трудность состоит в том, что усиление контроля безопасности чаще всего сопровождается более жесткими режимами мониторинга и реагирования, которые в свою очередь повышают вычислительные, коммуникационные и организационные затраты. В то же время попытки ослабить контроль увеличивают вероятность успешной реализации атаки [14–20]. Следовательно, задача выбора режима безопасности имеет конфликтный характер: защитная сторона стремится уменьшить ущерб с минимальными затратами ресурсов, в то время как атакующая сторона стремится увеличить ущерб и перевести систему в неблагоприятное состояние.

Именно в этом смысле рассматриваемая в статье модель является теоретико-игровой. Ее центральный элемент состоит не просто в вычислении показателей аномальности или прогноза уязвимости, а в том, что выбор режима контроля формализуется как задача двух игроков в виде Злоумышленника и Защитника с противоположными целями. Защитник выбирает подходящие режимы контроля безопасности, минимизируя потери в наихудшем допустимом сценарии атакующего воздействия, тогда как Злоумышленник рассматривается как сторона, стремящаяся провести атаку с максимально возможным ущербом. Тем самым обнаружение аномалий и прогнозирование уязвимости в данной работе выступают не самостоятельной целью, а информационной основой для игрового выбора защитного действия. Работы [21–23] используются не как источник вводимых далее формул, а как предметные аналоги активной защиты и сетевого контроля, относительно которых уточняется предлагаемая игровая постановка.

Такой подход позволяет перейти от реактивной схемы к превентивной. Если пороговые и статические методы усиливают контроль уже после заметного роста аномальности, то в предлагаемой модели решение принимается с учетом не только текущего отклонения, но и накопленной аномальности, прогноза краткосрочной уязвимости и ресурсного состояния системы, что в свою очередь позволяет интерпретировать действия Защитника как опережающие в конфликте «Злоумышленник – Защитник».

В связи с этим в статье рассматривается задача построения теоретико-игровой модели адаптивного управления защищенностью, в которой показатели аномальности и прогноза уязвимости используются как информационная основа для выработки оптимальной стратегии контроля безопасности в конфликте «Злоумышленник – Защитник».

Постановка задачи

В настоящей статье вводится самостоятельная система обозначений и соотношений теоретико-игровой модели адаптивного управления защищенностью распределенной IoT/IoRT-системы. Работы [21–23] используются как предметная основа для сопоставления с активной защитой, сетевым контролем и многоэтапными атаками, но математическая постановка, обозначения (табл. 1) и правила выбора режима контроля формируются непосредственно в данной работе.

С учетом конфликтного характера взаимодействия и интегральной оценки риска выбор режима контроля формулируется как минимаксная задача.

Минимаксная постановка используется как робастный вариант выбора режима контроля в условиях неполной информации о текущем намерении нарушителя. При этом Злоумышленник не предполагается обладателем всего возможного арсенала атак на каждом шаге: множество допустимых стратегий формируется как сценарное множество, согласованное с наблюдаемыми признаками, уровнем аномальности, накоплением угрозы и ресурсным состоянием системы:

$$r_t^* = \arg\min_{r_t \in R} \max_{h_t \in H_t} L\left(r_t, h_t, R_t, B_t\right). \qquad (1)$$

В соответствии с выражением (1) на каждом шаге выбирается такой режим контроля, который минимизирует потери Защитника при наиболее неблагоприятном допустимом сценарии воздействия. Такая запись не исключает использования статистической информации: если апостериорные вероятности сценариев атак доступны и достаточно устойчивы, минимаксное правило заменяется байесовской формой [см. (15)]. В базовом варианте статьи выбран минимаксный критерий, поскольку для распределенных IoT/IoRT-систем в переходных эпизодах «нормальный трафик → атакующий трафик» априорное распределение действий нарушителя, как правило, неполно, нестационарно и зависит от текущей конфигурации системы.

Теоретико-игровая модель адаптивного управления защищенностью распределенных IoT/IoRT-систем

Теоретико-игровая модель строится как контур, объединяющий формирование текущей аномальности, накопление признаков угрозы, прогнозирование краткосрочной уязвимости и минимаксный выбор режима контроля безопасности.

■ ***Таблица 1.*** Основные обозначения и базовые соотношения модели
■ ***Table 1.*** Main symbols and basic relations of the model

Обозначение	Описание	Определение/условие
t	Дискретное время функционирования системы	$t \in \{1, 2, \ldots, T\}$
$\mathbf{x}_t$	Вектор наблюдаемых признаков на шаге t	$\mathbf{x}_t = (x_{t1}, x_{t2}, \ldots, x_m)$
A_t	Показатель текущей аномальности	$A_t \in [0, 1]$
$\hat{V}_{t+1}$	Прогнозный показатель уязвимости на следующем шаге	$\hat{V}_{t+1} \in [0, 1]$
R_t	Интегральная оценка риска	$R_t = \alpha A_t + \eta S_t + (1 - \alpha - \eta)\hat{V}_{t+1}$, $\alpha, \eta \geq 0$, $\alpha + \eta \leq 1$
r_t	Режим контроля безопасности, выбираемый Защитником	$r_t \in R = \{R_1, R_2, \ldots, R_k\}$
R_1, R_2, R_3	Режимы контроля безопасности	R_1 – минимальный, R_2 – усиленный, R_3 – критический
B_t	Остаток ресурса безопасности на шаге t	$B_{t+1} = \min(B_{\max}, \max(0, B_t - c(r_t) + u_t))$
$c(r_t)$	Расход ресурса при выбранном режиме	$c(r_t) \geq 0$
u_t	Восстановление или пополнение ресурса	$u_t \geq 0$
B_{crit}	Критический порог ресурса безопасности	При $B_t < B_{crit}$ система переходит в зону ресурсного дефицита
h_t	Сценарий/стратегия атакующего воздействия Злоумышленника	$h_t \in H_t$
H_t	Множество допустимых сценариев/стратегий нарушителя на шаге t	Включает низкоинтенсивные, всплесковые и многоэтапные воздействия
$D_t(r_t, h_t, B_t)$	Ущерб (потери Защитника) на шаге t	Зависит от режима контроля, сценария атаки и остатка ресурса
J	Целевой функционал защитной стороны	$J = \sum_{t=1}^{T} \left(D_t(r_t, h_t, B_t) + \lambda c(r_t) \right)$, $\lambda \geq 0$
$L(\cdot)$	Локальная функция потерь	Учитывает риск, ущерб, стоимость режима и текущее ресурсное состояние системы

Формирование показателя аномальности наблюдаемого поведения

Для описания нормального режима работы системы вводится профиль нормального состояния, т. е. параметризованное описание типичных значений наблюдаемых признаков и допустимых отклонений от них:

$$\mu_t = \beta \mu_{t-1} + (1 - \beta) x_t, \ \beta \in [0, 1]. \quad (2)$$

Для оценки отклонения текущего состояния от профиля нормы используется нормированная ошибка.

Под профилем нормального состояния в работе понимается векторная характеристика штатного поведения системы, включающая сглаженные оценки средних значений признаков и их допустимой изменчивости. Параметр β является коэффициентом памяти профиля: при $\beta > 1$ профиль изменяется медленнее и сильнее учитывает предыдущее состояние, при $\beta > 0$ профиль быстрее адаптируется к новым штатным наблюдениям. Символ μ обозначает оценку среднего значения признака в профиле нормы. Обновление профиля выполняется только для интервалов, не отнесенных к аномальным, что снижает риск включения атакующего поведения в норму:

$$e_t = \frac{1}{m} \sum_{j=1}^{m} \left| x_{tj} - \mu_{tj} \right|. \quad (3)$$

Тогда показатель текущей аномальности определяется как

$$A_t = \min\left(1, \frac{e_t}{\theta_t}\right), \quad (4)$$

где динамический порог нормализации задает допустимый уровень отклонения текущего признакового вектора от профиля нормального состояния.

Значение порога адаптируется по истории нормальных отклонений и используется для приведения ошибки к сопоставимой шкале аномальности.

Для адаптации порога к изменяющимся условиям среды используется правило:

Коэффициент адаптации порога определяет скорость реакции на изменение штатного трафика: малые значения обеспечивают устойчивость к выбросам, большие значения ускоряют перестройку порога при изменении нормального режима. Порог не обновляется по интервалам, для которых текущая аномальность превышает допустимую границу:

$$\theta_t = \gamma\theta_{t-1} + (1-\gamma)e_t,\ \gamma \in [0,1]. \quad (5)$$

Поскольку единичные выбросы не всегда соответствуют реальной атаке, вводится накопленный показатель аномальности:

Коэффициент памяти накопленного показателя задает вклад предшествующих интервалов наблюдения. Поэтому единичный выброс оказывает ограниченное влияние, а последовательность слабых отклонений приводит к росту накопленной аномальности и отражает развитие многоэтапного воздействия:

$$S_t = \rho S_{t-1} + (1-\rho)A_t,\ \ \rho \in [0,1]. \quad (6)$$

В отличие от мгновенной оценки текущей аномальности накопленный показатель аномальности позволяет учитывать последовательные и многоэтапные воздействия, развивающиеся во времени [20–23].

Прогнозирование уязвимости безопасности распределенной IoT/IoRT-системы

Для перехода к превентивному управлению вводится показатель прогнозной уязвимости безопасности $\hat{V}_{t+1}$, формируемый по краткой истории аномальности и ресурсного состояния системы:

$$\hat{V}_{t+1} = \sigma\left(w_1 S_t + w_2 \Delta S_t + w_3\left(1 - \frac{B_t}{B_{\max}}\right) + b\right), \quad (7)$$

где $\sigma(\cdot)$ — логистическая функция; B_t — остаток ресурса безопасности; $B_{\max}$ — максимальный доступный ресурс; w_1, w_2, w_3 — весовые коэффициенты вклада накопленной аномальности, текущего изменения аномальности и ресурсного дефицита; b — свободный параметр модели. Весовые коэффициенты задаются неотрицательными и нормируются при настройке модели, а b используется для смещения границы перехода к высокому прогнозному риску. Здесь $\Delta S_t = S_t - S_{t-1}$ характеризует изменение накопленного уровня признаков угрозы между соседними шагами наблюдения.

В соответствии с выражением (7) прогноз уязвимости возрастает при увеличении накопленной аномальности и с приближением системы к ресурсному дефициту.

Интегральная оценка риска учитывает мгновенное отклонение, накопленную аномальность и краткосрочный прогноз угрозы.

Форма интегральной оценки риска выбрана как агрегирующая функция трех независимых по смыслу компонент: мгновенного отклонения, накопления признаков угрозы и прогноза уязвимости. Такая последовательность введения показателей необходима для того, чтобы затем построить матрицу потерь игры: риск не заменяет игру, а входит в локальную функцию потерь Защитника как один из факторов ожидаемого ущерба:

$$R_t = \alpha A_t + \eta S_t + (1-\alpha-\eta)\hat{V}_{t+1},$$
$$\alpha, \eta \ge 0,\ \ \alpha + \eta \le 1. \quad (8)$$

Теоретико-игровая модель конфликта «Злоумышленник – Защитник»

На каждом шаге t модель Злоумышленника задается сценарным множеством H_t допустимых стратегий воздействия. Это множество включает не весь теоретически возможный арсенал атак, а те сценарии, которые согласуются с текущим состоянием наблюдений: низкоинтенсивное воздействие, всплесковую активность, сканирование, развитие многоэтапной атаки или интенсивное ботнет-воздействие. Защитник выбирает режим контроля безопасности из множества допустимых режимов. Для каждого сочетания «режим контроля — стратегия нарушителя» вводится функция локального ущерба:

$$D_t(r_t, h_t, B_t) = q(h_t)\big(1 - e(r_t)\big)\big(1 + \Psi(B_t)\big), \quad (9)$$

где $q(h_t)$ — базовая интенсивность ущерба для стратегии нарушителя h_t; $e(r_t)$ — защитный эффект выбранного режима контроля; $\Psi(B_t)$ — множитель деградации защиты при снижении доступного ресурса.

Множитель деградации определяется как

$$\Psi_t(B_t) = \begin{cases} 0, & B_t \ge B_{crit}, \\ \delta\left(1 - \dfrac{B_t}{B_{crit}}\right), & B_t < B_{crit}, \end{cases} \quad \delta \ge 0. \quad (10)$$

Стоимость применения режима контроля задается функцией

$$C_t = c(r_t)(1 + \chi R_t),\ \ \chi \ge 0, \quad (11)$$

где $c(r_t)$ — базовая стоимость режима.

Локальная функция потерь защищающейся стороны определяется как

$$L_t(r_t, h_t) = \omega_1 D_t + \omega_2 C_t + \omega_3 M_t,$$
$$\omega_i \geq 0, \sum_{i=1}^{3} \omega_i = 1, \quad (12)$$

где M_t — штраф за частое переключение режимов контроля, отражающий дополнительные организационные и вычислительные потери при необоснованной смене защитного режима.

В простейшем случае

$$M_t = I(r_t \neq r_{t-1}), \quad (13)$$

где $I(\cdot)$ — индикаторная функция.

Правило выбора режима контроля безопасности

При заданных R_t и B_t Защитник выбирает режим по минимаксному критерию:

$$r_t^* = \arg\min_{r_t \in R} \max_{h_t \in H_t} L_t(r_t, h_t). \quad (14)$$

Если для рассматриваемой системы доступна устойчивая статистическая оценка распределения сценариев атак, правило (14) может быть записано в байесовской форме:

$$r_t^* = \arg\min_{r_t \in R} \sum_{h_t \in H_t} \pi(h_t \mid \mathbf{z}_t) L_t(r_t, h_t), \quad (15)$$

где $\pi(h_t|\mathbf{z}_t)$ — апостериорная вероятность сценария атаки h_t при текущем состоянии $\mathbf{z}_t$.

Для практической части используется правило (14), поскольку переходные эпизоды атаки характеризуются неполной и нестационарной информацией о намерении нарушителя. Байесовская форма (15) рассматривается как расширение модели для случая, когда распределение сценариев атак может быть надежно оценено по данным эксплуатации.

После выбора режима ресурс безопасности обновляется по выражению

$$B_{t+1} = \min\left(B_{\max}, \max(0, B_t - c(r_t^*) + u_t)\right), \quad (16)$$

где u_t — частичное восстановление ресурса за шаг. Восстановление выполняется при снижении уровня угрозы и отсутствии необходимости удерживать усиленный или критический режим; пополнение ресурса описывает приток доступного вычислительного, энергетического или коммуникационного бюджета. Верхняя граница задается исходным ресурсом $B_0 = B_{\max}$, поэтому после обновления выполняется ограничение $B_{t+1} \leq B_0$. Нижняя граница исключает отрицательные значения ресурса безопасности.

Выражения (2)–(16) образуют единый контур обнаружения, прогноза, оценки риска и выбора режима контроля безопасности.

Алгоритм реализации и программная схема экспериментального исследования конфликта «Злоумышленник – Защитник»

Общая логика алгоритма

Предлагаемая модель реализуется как дискретный адаптивный цикл, в котором по вектору наблюдений $\mathbf{x}_t$ формируются показатели A_t, S_t, $\hat{V}_{t+1}$, R_t, после чего по минимаксному правилу (14) выбирается режим контроля r_t^* и обновляется ресурс безопасности по формуле (16). Для компактной записи общий алгоритм представим отображением

$$Y_t = \Psi(\mathbf{x}_t, \mathbf{z}_{t-1}, B_t), \quad (17)$$

где $Y_t = \left\{H_t, \hat{V}_{t+1}, R_t, r_t^*, B_{t+1}\right\}$ — множество вычисляемых на шаге t выходных величин; $\mathbf{z}_{t-1} = \{\mu_{t-1}, \theta_{t-1}, S_{t-1}, B_{t-1}, r_{t-1}\}$ — вектор внутреннего состояния подсистемы безопасности.

Пошаговая алгоритмическая процедура

На шаге t вычисления выполняются в следующем порядке. Сначала по входному вектору наблюдений $\mathbf{x}_t$ обновляется адаптивный профиль нормы μ_t по формуле (2). Затем по выражению (3) рассчитывается усредненная ошибка отклонения e_t, на основе которой динамический порог θ_t уточняется согласно формуле (5). После этого текущая аномальность A_t определяется по выражению (4), а накопленный показатель аномальности S_t — по формуле (6). На следующем этапе рассчитывается прогнозный показатель уязвимости $\hat{V}_{t+1}$ в соответствии с выражением (7), а затем интегральный риск R_t формируется по формуле (8). Далее для каждого допустимого режима контроля $r_t \in R$ вычисляются локальный ущерб D_t, стоимость C_t и функция потерь L_t по выражениям (9)–(13). На основе полученных значений выбирается оптимальный режим r_t^* согласно минимаксному критерию (14), после чего ресурс безопасности обновляется по формуле (16).

С учетом указанной последовательности шагов алгоритм выбора режима можно записать в виде

$$r_t^* = \arg\min_{r_t \in R} \max_{h_t \in H_t} \left[\omega_1 D_t(r_t, h_t, B_t) + \omega_2 C_t(r_t, R_t) + \omega_3 M_t(r_t, r_{t-1})\right]. \quad (18)$$

Формула (18) является алгоритмической реализацией теоретико-игрового выбора режима и непосредственно используется в программной модели при пошаговом переборе множества режимов R и сценарного множества допустимых стратегий нарушителя H_t.

Программная схема реализации модели

Для практической проверки предложенного подхода использована модульная программная схема на языке Python, включающая модуль подготовки данных, модуль обнаружения аномалий M_{det}, модуль прогнозирования уязвимости M_{pred}, игровой модуль выбора режима M_{game} и модуль оценки результатов M_{eval}. Общая структура реализации задается последовательностью

$$x_t \to M_{det} \to M_{pred} \to M_{game} \to M_{eval}. \quad (19)$$

Программная реализация имеет линейно-модульную структуру, удобную для поэтапной отладки и для замены отдельных блоков без изменения общей логики метода. Такая схема обеспечивает воспроизводимую реализацию метода на стандартной аппаратной платформе без использования специализированных вычислителей.

Сценарий вычислительного эксперимента

Экспериментальное исследование предлагается проводить в дискретном времени на горизонте T шагов. Для каждого шага используются наблюдаемые данные $\mathbf{x}_t$, значения внутреннего состояния системы и остаток ресурса безопасности B_t. В качестве начальных условий задаются: начальный профиль нормы μ_0, начальный порог θ_0, начальная накопленная аномальность S_0, исходный режим контроля r_0, полный доступный ресурс $B_0 = B_{\max}$, а также параметры α, η, ρ, β, γ, w_1, w_2, w_3, b, χ, ω_1, ω_2, ω_3 и δ. Коэффициенты w_1, w_2, w_3 относятся к прогнозному показателю уязвимости, тогда как ω_1, ω_2, ω_3 задают веса компонент локальной функции потерь.

Полный вычислительный прогон эксперимента можно представить как последовательное выполнение отображения

$$\{x_t, B_t, z_{t-1}\}_{t=1}^{\mathrm{T}} \to \left\{H_t, \hat{V}_{t+1}, R_t, r_t^*, D_t, C_t, B_{t+1}\right\}_{t=1}^{\mathrm{T}}. \quad (20)$$

Из выражения (20) следует, что на каждом шаге сохраняются не только текущие управляющие решения, но и промежуточные величины, необходимые для последующего анализа качества обнаружения, прогноза и управления защищенностью.

Метрики оценки качества обнаружения и управления защищенностью

Для подтверждения заявленной цели статьи метрики должны отражать не только качество обнаружения, но и влияние метода на защищенность и ресурсное состояние системы. В рамках вычислительного эксперимента предлагается использовать следующие показатели.

Средняя величина ущерба, приходящаяся на один шаг функционирования системы:

$$\bar{D} = \frac{1}{T}\sum_{t=1}^{T} D_t. \quad (21)$$

Накопленный ущерб рассматривается как суммарная величина потерь Защитника на всем горизонте наблюдения и непосредственно связан с уровнем поддерживаемой защищенности:

$$D_{\Sigma} = \sum_{t=1}^{T} D_t. \quad (22)$$

Суммарный расход ресурса безопасности, характеризующий общую стоимость реализованной защитной стратегии:

$$C_{\Sigma} = \sum_{t=1}^{T} c\left(r_t^*\right). \quad (23)$$

Доля времени функционирования системы в зоне ресурсного дефицита, которая отражает, насколько часто система переходит в состояние пониженной защищенности из-за истощения доступного ресурса:

$$P_{def} = \frac{1}{T}\sum_{t=1}^{T} I(B_t < B_{crit}). \quad (24)$$

В практической части статьи основное внимание уделяется метрикам, непосредственно отражающим влияние метода на защищенность и ресурсное состояние системы: среднему ущербу, накопленному ущербу, суммарному расходу ресурса и доле времени в зоне ресурсного дефицита.

Экспериментальная часть моделирования адаптивного управления защищенностью распределенных IoT/IoRT-систем

Постановка вычислительного эксперимента

Экспериментальная проверка предложенной модели выполнена на реальных данных сетевого трафика IoT-устройств. В качестве основного источника данных использован датасет N-BaIoT: Data for Network Based Detection of IoT Botnet Attacks, содержащий записи нормального и вредоносного трафика для ряда IoT-устройств (N-BaIoT Dataset to Detect IoT Botnet Attacks. https://www.kaggle.com/datasets/mkashifn/nbaiot-dataset), в том числе при атаках семейства Mirai. В базовом сценарии исследования выбрано устройство Danmini_Doorbell, для которого доступны как записи штатного функционирования, так и данные о сетевой активности при нескольких типах ботнет-атак.

Исходный набор данных был сформирован из файлов атакующего трафика семейства Mirai: ack, scan, syn, udp, udpplain. После объединения подмножеств получен массив объемом 701 648 наблюдений, включающий 49 548 “benign”-наблюдений и 652 100 “attack”-наблюдений.

На этапе предварительной обработки были выделены числовые признаки, удалены константные столбцы и выполнено заполнение пропущенных значений медианами. В дальнейшем использовалось 115 числовых признаков, формирующих вектор наблюдений $\mathbf{x}_t$, введенный в первом разделе.

В работе исходные данные использовались не для прямой бинарной классификации, а для построения последовательного контура обнаружения, прогноза и управления. Сначала по “benign”-подмножеству формировался модуль обнаружения аномалий, вычисляющий показатель текущей аномальности A_t. Далее по формулам (6)–(8) определялись накопленная аномальность S_t, прогноз краткосрочной уязвимости $\hat{V}_{t+1}$ и интегральный риск R_t. Тем самым реальный сетевой трафик преобразовывался в последовательность сигналов, непосредственно используемых в теоретико-игровом модуле выбора режима контроля безопасности.

Для проверки превентивных свойств модели из общего временного ряда были сформированы переходные эпизоды типа «нормальный трафик → атакующий трафик». Такая постановка позволяет анализировать не только поведение системы в установившемся атакующем режиме, но и момент перехода от нормального состояния к развитию угрозы, когда Защитник должен выполнить опережающий выбор режима контроля. Длина каждого эпизода составляла 2000 шагов наблюдения, а всего было сформировано 20 эпизодов, различающихся положением точки начала атаки внутри окна.

В качестве сравниваемых стратегий управления использовались четыре варианта.

1. Статическая стратегия, в которой режим контроля выбирается заранее и не изменяется во времени. Такая стратегия служит нижней базовой линией для оценки адаптивных решений.

2. Пороговая стратегия, в которой режим контроля определяется только текущим значением аномальности и заранее заданных порогов.

Именно такой тип сравнения уже применялся в работах, посвященных активной защите сетей, обработке результатов сетевого контроля и анализу поведения системы при многоэтапных атаках.

3. Риск-ориентированная стратегия, использующая прогнозный показатель риска $\hat{V}_{t+1}$, но не включающая теоретико-игровой механизм выбора. Такая стратегия позволяет отделить вклад самого прогностического блока от вклада теоретико-игрового механизма выбора.

4. Теоретико-игровая стратегия, в которой выбор режима контроля выполняется на основе теоретико-игрового критерия с учетом текущей аномальности, накопленной аномальности, прогноза уязвимости и ресурсного состояния системы.

Во всех вариантах использовалось одно и то же множество режимов контроля

$$r_t \in R = \{R_1, R_2, R_3\}, \tag{25}$$

где R_1 соответствует минимальному режиму контроля, R_2 — усиленному, а R_3 — критическому режиму с максимальной интенсивностью мониторинга и реагирования.

В базовом эксперименте начальный ресурс безопасности B_0 принимался 5000, критический порог дефицита B_{crit} — 1000, а восстановление ресурса на каждом шаге задавалось постоянной величиной. Дополнительно выполнялся стресс-анализ, в котором отношение B_{crit}/B_0 варьировалось в диапазоне от 0,20 до 0,45. В качестве основных критериев эффективности использовались показатели: средний ущерб $\bar{D}$ (21), накопленный ущерб D_Σ (22), суммарный расход ресурса C_Σ (23), доля времени в зоне дефицита P_{def} (24) и число переключений режимов контроля.

Таким образом, вычислительный эксперимент обеспечивает сопоставление реактивных и превентивных стратегий управления защищенностью в конфликте «Злоумышленник – Защитник».

Результаты основного эксперимента на переходных эпизодах типа «нормальный трафик → атакующий трафик»

Эксперимент на переходных эпизодах «нормальный трафик → атакующий трафик» ориентирован на анализ поведения модели в момент перехода от нормального функционирования к развитию вредоносной активности. В такой постановке важно не только зафиксировать отклонение от нормы, но и своевременно усилить режим контроля до полной реализации следующей фазы атаки.

Результаты основного вычислительного эксперимента получены на 20 переходных эпизодах длиной 2000 шагов. На каждом шаге по наблюдаемому трафику вычислялись текущая аномальность A_t, накопленная аномальность S_t и прогноз краткосрочной уязвимости $\hat{V}_{t+1}$. Далее на основе интегрального риска R_t выполнялся выбор режима контроля безопасности по правилу (14) для теоретико-игровой стратегии и по упрощенным правилам для базовых подходов. Эффективность сравнивалась по показателям $\bar{D}$, D_Σ, C_Σ, P_{def} и числу переключений режима.

Сводные результаты основного эксперимента представлены в табл. 2.

Теоретико-игровая стратегия показала наименьший накопленный и средний ущерб среди всех сравниваемых подходов, что указывает на устойчивое преимущество теоретико-игрового механизма выбора режима контроля.

■ ***Таблица 2.*** Результаты основного эксперимента на переходных эпизодах «нормальный трафик → атакующий трафик»
■ ***Table 2.*** Results of the main experiment on benign → attack transition episodes

Стратегия	$\bar{D}$	D_Σ	Остаточный ресурс B_{last}	Минимальный ресурс $B_{\min}$	Число переключений	C_Σ	P_{def}
Теоретико-игровая	0,233	9325,758	4875,227	4427,2	6840	79 434,4	0,0
Риск-ориентированная	0,275	10 989,231	4936,109	4520,0	2357	70 878,4	0,0
Статическая	0,398	15 939,417	5000,000	5000,0	20	56 000,0	0,0
Пороговая	0,401	16 045,683	4942,233	4522,0	2562	53 576,4	0,0

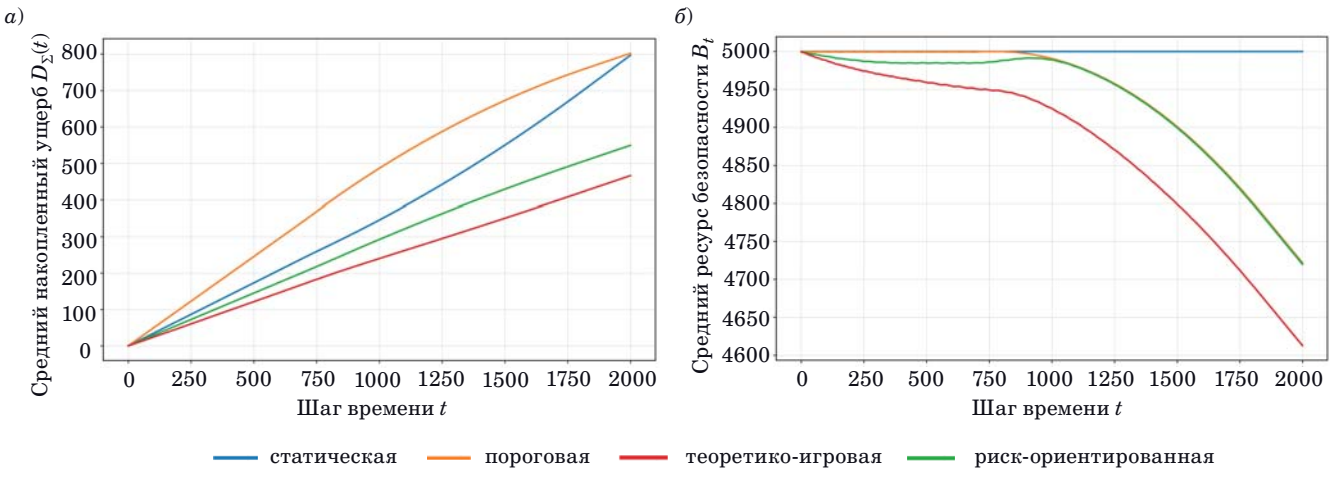
Важно, что теоретико-игровая стратегия превосходит не только статическую и пороговую схемы, но и риск-ориентированную стратегию, уже использующую прогноз $\hat{V}_{t+1}$. Следовательно, выигрыш объясняется не только наличием прогностического блока, но и тем, что прогноз используется в конфликтной постановке «Злоумышленник – Защитник» для превентивного выбора режима контроля.

Для наглядного сопоставления динамики стратегий используется рис. 1, *а*, на котором видно, что кривая теоретико-игровой стратегии располагается ниже остальных на всем протяжении эпизода. Различие с риск-ориентированной стратегией становится устойчивым после начала атакующего участка и сохраняется до завершения эпизода. Статическая и пороговая стратегии накапливают ущерб заметно быстрее, что указывает на их меньшую приспособленность к переходным сценариям развития атаки.

Наряду с уменьшением ущерба важно оценить затраты от этого выигрыша (рис. 1, *б*).

Теоретико-игровая стратегия использует ресурс безопасности наиболее интенсивно, что согласуется с логикой модели: при росте показателей A_t, S_t и $\hat{V}_{t+1}$ Защитник заранее переводит систему в более жесткий режим контроля, уменьшая ожидаемый ущерб ценой более высокого расхода ресурса. В базовом режиме эксперимента это не приводит к переходу в зону дефицита, поскольку для всех подходов выполняется $P_{def} = 0$, однако суммарный расход ресурса у теоретико-игровой стратегии выше, чем у пороговой и статической схем.

Таким образом, основной эксперимент на переходных эпизодах «нормальный трафик → атакующий трафик» показывает, что предлагаемая теоретико-игровая стратегия превентивного управления снижает как средний, так и накопленный ущерб по сравнению со статической, пороговой и риск-ориентированной стратегиями. При этом выигрыш относительно риск-ориентированной стратегии отражает вклад именно игрового механизма выбора режима, а не только эффект использования прогноза уязвимости.



■ ***Рис. 1.*** Усредненные накопленный ущерб $D_\Sigma(t)$ (*а*) и динамика ресурса безопасности B_t (*б*) для сравниваемых стратегий на переходных эпизодах «нормальный трафик → атакующий трафик»
■ ***Fig. 1.*** Average cumulative damage $D_\Sigma(t)$ (*а*) and dynamics of the security resource B_t (*б*) for comparing strategies during transitional episodes benign → attack

Результаты стресс-анализа при варьировании B_{crit}/B_0

Для проверки устойчивости полученных результатов в условиях ужесточения ресурсных ограничений выполнен стресс-анализ, в котором варьировалось отношение критического порога дефицита ресурса к начальному ресурсу безопасности:

$$\frac{B_{crit}}{B_0} \in \{0,20;|0,25;|0,30;|0,35;|0,40;|0,45\}. \quad (26)$$

В отличие от базового эксперимента, где для всех стратегий наблюдалось $P_{def} = 0$, в стрессовом режиме параметры расхода и восстановления ресурса были выбраны так, чтобы система действительно входила в зону дефицита. Это позволило оценить устойчивость сравниваемых стратегий при более жестких ресурсных условиях.

Сводные результаты стресс-анализа представлены в табл. 3. Для сокращения объема в таблицу включены три характерных значения отношения B_{crit}/B_0, отражающие нижнюю, промежуточную и верхнюю области исследованного диапазона.

При увеличении отношения B_{crit}/B_0 все стратегии демонстрируют ожидаемое ухудшение характеристик: возрастают средний ущерб $\bar{D}$, накопленный ущерб D_Σ и доля времени в зоне дефицита ресурса P_{def}. Это означает, что при ужесточении порога ресурсной устойчивости даже кратковременное снижение остатка ресурса начинает сильнее влиять на результат управления защищенностью.

Несмотря на общее ухудшение показателей теоретико-игровая стратегия сохраняет наименьший ущерб на всем исследованном диапазоне. При $B_{crit}/B_0 = 0,20$ средний ущерб для нее составляет около 0,3498, тогда как для риск-ориентированной стратегии — около 0,3934, для пороговой — около 0,4355, а для статической — около 0,5461. При $B_{crit}/B_0 = 0,45$ значения ущерба возрастают у всех стратегий, однако преимущество теоретико-игровой стратегии сохраняется: $\bar{D}$ увеличивается лишь до 0,3577, тогда как у риск-ориентированной — до 0,4224, у пороговой — до 0,4484, а у статической — до 0,5984.

■ ***Таблица 3.*** Результаты стресс-анализа при варьировании отношения B_{crit}/B_0

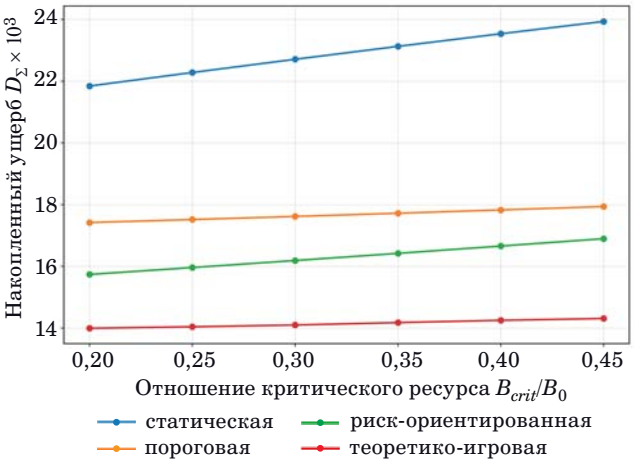
■ ***Table 3.*** Stress-analysis results for varying the ratio B_{crit}/B_0

Стратегия	$\bar{D}$	D_Σ	C_Σ	P_{def}
$B_{crit}/B_0 = 0,20$				
Теоретико-игровая	0,350	13 991,861	110 211,6	0,572
Риск-ориентированная	0,393	15 737,471	94 317,6	0,461
Пороговая	0,435	17 419,163	70 710,8	0,156
Статическая	0,546	21 842,075	72 000,0	0,333
$B_{crit}/B_0 = 0,30$				
Теоретико-игровая	0,352	14 097,891	110 950,8	0,626
Риск-ориентированная	0,405	16 187,750	94 317,6	0,528
Пороговая	0,440	17 616,008	70 710,8	0,195
Статическая	0,567	22 709,425	72 000,0	0,416
$B_{crit}/B_0 = 0,45$				
Теоретико-игровая	0,358	14 308,894	111 820,8	0,707
Риск-ориентированная	0,422	16 894,827	94 317,6	0,631
Пороговая	0,448	17 936,557	70 710,8	0,257
Статическая	0,598	23 935,354	72 000,0	0,541

Наиболее наглядно это проявляется для накопленного ущерба D_Σ (рис. 2).

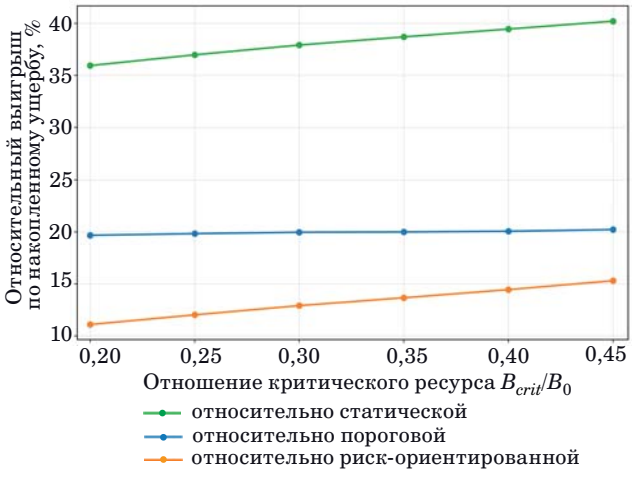
Теоретико-игровая стратегия остается лучшей по накопленному ущербу при всех рассмотренных значениях B_{crit}/B_0. Для количественной интерпретации результата на рис. 3 приведен относительный выигрыш теоретико-игровой стратегии по накопленному ущербу по сравнению с базовыми подходами.

Согласно полученным данным, выигрыш теоретико-игровой стратегии по накопленному ущербу относительно пороговой составляет примерно 19,7–20,2 % на всем исследованном диапазоне B_{crit}/B_0. Относительно риск-ориентированной стратегии выигрыш возрастает примерно от 11,1 до 15,3 %, а относительно статической — от 35,9 до 40,2 %.



■ ***Рис. 2.*** Зависимость накопленного ущерба D_Σ от отношения B_{crit}/B_0

■ ***Fig. 2.*** Dependence of accumulated damage D_Σ on the ratio B_{crit}/B_0



■ ***Рис. 3.*** Относительный выигрыш теоретико-игровой стратегии по накопленному ущербу по сравнению с базовыми подходами

■ ***Fig. 3.*** Relative gain of the game-theoretic strategy in terms of accumulated damage compared to baseline approaches

При этом уменьшение ущерба достигается ценой более интенсивного использования ресурса безопасности, например, для теоретико-игровой стратегии значения C_Σ и P_{def} выше, чем у пороговой и статической. Следовательно, предлагаемую стратегию следует интерпретировать как средство приоритетной минимизации ущерба, а не как универсальный минимум по всем метрикам одновременно.

Таким образом, стресс-анализ подтверждает, что теоретико-игровая стратегия сохраняет преимущество по ущербу в широком диапазоне ресурсных условий и остается устойчивой при ужесточении эксплуатационных ограничений.

Обсуждение результатов

Полученные результаты показывают, что предлагаемая теоретико-игровая модель превентивного управления защищенностью распределенных IoT/IoRT-систем обеспечивает снижение ущерба на переходных сценариях «нормальный трафик → атакующий трафик». В отличие от статической, пороговой и риск-ориентированной стратегий, теоретико-игровая стратегия использует текущее отклонение от профиля нормы, накопленную аномальность, прогноз краткосрочной уязвимости и ресурсное состояние системы, что позволяет Защитнику заранее усиливать режим контроля.

Существенно, что выигрыш достигается не только по сравнению с простыми базовыми подходами, но и по сравнению с риск-ориентированной стратегией, уже использующей прогноз $\hat{V}_{t+1}$. Это означает, что эффект связан не только с наличием прогностического блока, но и с включением прогноза в теоретико-игровой механизм выбора режима. Основными ограничениями исследования остаются использование одного устройства из датасета N-BaIoT, облегченная форма прогнозного блока и дискретное множество режимов контроля.

Заключение

В статье предложена теоретико-игровая модель адаптивного управления защищенностью распределенных IoT/IoRT-систем, объединяющая обнаружение аномалий, прогнозирование краткосрочной уязвимости и превентивный выбор режима контроля безопасности при ограниченных ресурсах периферийных узлов. Экспериментальная проверка на данных N-BaIoT показала, что теоретико-игровая стратегия обеспечивает меньший накопленный ущерб по сравнению со статической, пороговой и риск-ориентированной стратегиями на переходных эпизодах «нормальный трафик → атакующий трафик». Стресс-анализ при варьировании отношения B_{crit}/B_0 подтвердил сохранение этого преимущества при ужесточении ресурсных ограничений. Практическая значимость работы связана с построением воспроизводимой вычислительной схемы, пригодной для реализации на стандартной аппаратной платформе.

Литература

1. **Rose S., Borchert O., Mitchell S., Connelly S.** *Zero Trust Architecture*. Gaithersburg, National Institute of Standards and Technology, 2020. 54 p. doi:10.6028/NIST.SP.800-207
2. **Bast C., Yeh K.-H.** Emerging authentication technologies for zero trust on the Internet of Things. *Symmetry*, 2024, vol. 16, no. 8, art. 993. doi:10.3390/sym16080993
3. **Nie S., Ren J., Wu R., Han P., Han Z., Wan W.** Zero-trust access control mechanism based on blockchain and inner-product encryption in the Internet of Things in a 6G environment. *Sensors*, 2025, vol. 25, no. 2, art. 550. doi:10.3390/s25020550
4. **DeMedeiros K., Hendawi A., Alvarez M.** A survey of AI-based anomaly detection in IoT and sensor networks. *Sensors*, 2023, vol. 23, no. 3, art. 1352. doi:10.3390/s23031352
5. **Belay M. A., Blakseth S. S., Rasheed A., Salvo Rossi P.** Unsupervised anomaly detection for IoT-based multivariate time series: Existing solutions, performance analysis and future directions. *Sensors*, 2023, vol. 23, no. 5, art. 2844. doi:10.3390/s23052844
6. **Aldhaheri A., Alwahedi F., Ferrag M. A., Battah A.** Deep learning for cyber threat detection in IoT networks: A review. *Internet of Things and Cyber-Physical Systems*, 2024, vol. 4, pp. 110–128. doi:10.1016/j.iotcps.2023.09.003
7. **Fan Y., Fu T., Listopad N. I., Liu P., Garg S., Hassan M. M.** Utilizing correlation in space and time: Anomaly detection for Industrial Internet of Things (IIoT) via spatiotemporal gated graph attention network. *Alexandria Engineering Journal*, 2024, vol. 106, pp. 560–570. doi:10.1016/j.aej.2024.08.048
8. **Issa A. S. A., Sonuç E.** CLSTMNet: A Deep learning model for intrusion detection. *Journal of Physics: Conference Series*, 2021, vol. 1973, art. 012244. doi:10.1088/1742-6596/1973/1/012244
9. **Friji H., Mavromatis I., Sanchez-Mompo A., Carnelli P., Olivereau A., Khan A.** Multi-stage attack detection and prediction using graph neural networks: An IoT feasibility study. *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2023, pp. 614–621. doi:10.1109/TrustCom60117.2023.00095
10. **Liu W., Gao P., Zhang H., Li K., Yang W., Wei X., Shu J.** Detecting complex multi-step attacks with explainable graph neural network. *arXiv*, 2024, arXiv:2405.11335v2 [cs.CR]. doi:10.48550/arXiv.2405.11335
11. **Perales Gómez A. L., Martínez Beltrán E. T., Sánchez Sánchez P. M., Huertas Celdrán A.** TemporalFED: A software module for detecting cyberattacks in Industry 4.0 time-series data using decentralized federated learning. *arXiv*, 2025, arXiv:2308.03554v2 [cs.CR]. doi:10.48550/arXiv.2308.03554
12. **Danish M.** Enhancing cyber security through predictive analytics: Real-time threat detection and response. *International Journal of Advanced Computer Science and Applications*, 2025, vol. 16, no. 8, pp. 27–35. doi:10.14569/IJACSA.2025.0160804
13. **Jiang Y., Oo N., Meng Q., Lin L., Niyato D., Xiong Z., Lim H. W., Sikdar B.** CyGATE: Game-theoretic cyber attack-defense engine for patch strategy optimization. *arXiv*, 2025. doi:10.48550/arXiv.2508.00478
14. **Datar M., Dujardin Y.** Adaptive learning for moving target defence: Enhancing cybersecurity strategies. *arXiv*, 2025. arXiv:2508.17945v1 [cs.GT].
15. **Spyrou E. D., Kappatos V., Stylios C.** Game-theoretic secure socket transmission with a zero trust model. *Applied Sciences*, 2025, vol. 15, no. 19, art. 10535. doi:10.3390/app151910535
16. **Исаева О. С., Кулясов Н. В., Исаев С. В.** Инфраструктура сбора данных и имитации угроз безопасности сети интернета вещей. *Сибирский аэрокосмический журнал*, 2025, Т. 26, № 1, с. 8–20. doi: 10.31772/2712-8970-2025-26-1-8-20, EDN: OPICJJ
17. **Федоров Н. А., Сычев П. П.** Исследование вопросов информационной безопасности систем «Интернета вещей». *Системный анализ в науке и образовании*, 2023, № 2, с. 27–35. EDN: FGJBSV
18. **Васильев В. И., Гвоздев В. Е., Шамсутдинов Р. Р.** Обнаружение аномалий в системах промышленного Интернета вещей на основе искусственной иммунной системы. *Доклады ТУСУР*, 2021, Т. 24, № 4, с. 40–45. doi: 10.21293/1818-0442-2021-24-4-40-45, EDN: YKHKPJ
19. **Тергеуов О. С., Маликова Ф. У.** Обнаружение и устранение DDoS-атаки IoT-ботнетов на основе SIEM. *Universum: технические науки*, 2022, № 4-1 (97), с. 54–63. EDN: WJNKHL
20. **Уринов Н. Т., Мамадалиев С. С., Бахрамова М. Б., Алижонов Ш. А., Неъматжонов А. У., Акбарова М. Ш.** Определение информативных признаков и формализация базы знаний для идентификации кибератаки Stuxnet на систему Интернета вещей. *Потомки Аль-Фаргани*, 2025, т. 1, вып. 2, с. 80–85. https://doi.org/10.5281/zenodo.15580978. https://al-fargoniy.uz/ (дата обращения: 15.05.2025).
21. **Липатников В. А., Мелехов К. В., Задбоев В. А.** Способ активной защиты информационно-вычислительных сетей от многоэтапных атак. *Сборник трудов международной и межрегиональной конференции «Региональная информатика и информационная безопасность»,* Санкт-Петербург, 1–4 апреля 2024 г. СПб., с. 112–114.
22. **Липатников В. А., Мелехов К. В.** Способ обработки результатов сетевого контроля при поддержке принятия решения администратора безопасности информации. *Тр. XXVII Всерос. науч.-практ. конф. «Актуальные проблемы защиты и безопасности»*, СПб., 2024, *с.* 306–310.
23. **Липатников В. А., Мелихов И. А., Мелехов К. В.** Особенности сетевого контроля в сети передачи данных в условиях многоэтапных атак. *Технологии. Инновации. Связь: сб. матер. науч.-практ. конф.*, СПб., 2023, с. 171–174.

UDC 004.056
doi:10.31799/1684-8853-2026-4-28-40
EDN: HRWBEL

Game-theoretic model of adaptive security management for distributed IoT/IoRT systems based on anomaly detection and security vulnerability forecasting

V. A. Lipatnikov[a], Dr. Sc., Tech., Professor, orcid.org/0000-0002-3736-4743, lipatnikovanl@mail.ru
V. A. Zadboev[a], Junior Researcher, orcid.org/0009-0003-9362-1307
D. V. Makarenko[a], Post-Graduate Student, orcid.org/0009-0002-4732-2990
I. A. Andreev[a], Scientific Company Operator, orcid.org/0009-0007-3617-3439
[a]S. M. Budenny Military Academy of Communication, 3, Tikhoretskii Pr., 190064, Saint-Petersburg, Russian Federation

Introduction: Modern distributed IoT/IoRT systems operate continuously under conditions of non-stationary traffic, limited resources of edge nodes, and evolving multi-stage cyber threats, which necessitates a transition from reactive control schemes to preventive security management. A particular challenge is the need to maintain operational stability under the simultaneous influence of all the above-mentioned factors. At the same time, traditional control mechanisms do not always allow timely consideration of attack dynamics and changes in the system state. **Purpose:** To develop a game-theoretic model for adaptive security management in distributed IoT/IoRT systems that integrates anomaly detection, short-term security vulnerability prediction, and preventive selection of a control mode under resource constraints. **Results:** We construct an "Attacker–Defender" conflict model, in which the decision on selecting a control mode is made according to the minimax criterion, taking into account the current anomaly level, accumulated anomaly level, vulnerability forecast, and the remaining security resource. The proposed approach improves the quality of management decisions under uncertainty regarding the attacker's actions and makes it possible to consider security as a continuous process of adaptation to changing system operating conditions. Experimental validation on the N-BaIoT dataset shows that the game-theoretic strategy provides lower average and cumulative damage as compared to static, threshold-based, and risk-oriented strategies, which confirms the feasibility of using adaptive control mode selection to reduce the consequences of multi-stage cyber impacts. **Practical relevance:** The practical significance lies in the possibility of developing computationally feasible tools for preventive security management of distributed IoT/IoRT systems on a standard hardware platform.

Keywords – IoT, IoRT, security, anomaly detection, vulnerability forecasting, game-theoretic model, preventive control, cyber threats, multi-stage attacks, resource constraints.

For citation: Lipatnikov V. A., Zadboev V. A., Makarenko D. V., Andreev I. A. Game-theoretic model of adaptive security management for distributed IoT/IoRT systems based on anomaly detection and security vulnerability forecasting. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 4, pp. 28–40 (In Russian). doi:10.31799/1684-8853-2026-4-28-40, EDN: HRWBEL

References

1. Rose S., Borchert O., Mitchell S., Connelly S. *Zero Trust Architecture*. Gaithersburg, National Institute of Standards and Technology, 2020. 54 p. doi:10.6028/NIST.SP.800-207
2. Bast C., Yeh K.-H. Emerging authentication technologies for zero trust on the Internet of Things. *Symmetry*, 2024, vol. 16, no. 8, art. 993. doi:10.3390/sym16080993
3. Nie S., Ren J., Wu R., Han P., Han Z., Wan W. Zero-trust access control mechanism based on blockchain and inner-product encryption in the Internet of Things in a 6G environment. *Sensors*, 2025, vol. 25, no. 2, art. 550. doi:10.3390/s25020550
4. DeMedeiros K., Hendawi A., Alvarez M. A survey of AI-based anomaly detection in IoT and sensor networks. *Sensors*, 2023, vol. 23, no. 3, art. 1352. doi:10.3390/s23031352
5. Belay M. A., Blakseth S. S., Rasheed A., Salvo Rossi P. Unsupervised anomaly detection for IoT-based multivariate time series: Existing solutions, performance analysis and future directions. *Sensors*, 2023, vol. 23, no. 5, art. 2844. doi:10.3390/s23052844
6. Aldhaheri A., Alwahedi F., Ferrag M. A., Battah A. Deep learning for cyber threat detection in IoT networks: A review. *Internet of Things and Cyber-Physical Systems*, 2024, vol. 4, pp. 110–128. doi:10.1016/j.iotcps.2023.09.003
7. Fan Y., Fu T., Listopad N. I., Liu P., Garg S., Hassan M. M. Utilizing correlation in space and time: Anomaly detection for Industrial Internet of Things (IIoT) via spatiotemporal gated graph attention network. *Alexandria Engineering Journal*, 2024, vol. 106, pp. 560–570. doi:10.1016/j.aej.2024.08.048
8. Issa A. S. A., Sonuç E. CLSTMNet: A Deep learning model for intrusion detection. *Journal of Physics: Conference Series*, 2021, vol. 1973, art. 012244. doi:10.1088/1742-6596/1973/1/012244
9. Friji H., Mavromatis I., Sanchez-Mompo A., Carnelli P., Olivereau A., Khan A. Multi-stage attack detection and prediction using graph neural networks: An IoT feasibility study. *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2023, pp. 614–621. doi:10.1109/TrustCom60117.2023. 00095
10. Liu W., Gao P., Zhang H., Li K., Yang W., Wei X., Shu J. Detecting complex multi-step attacks with explainable graph neural network. *arXiv*, 2024, arXiv:2405.11335v2 [cs.CR]. doi:10.48550/arXiv.2405.11335
11. Perales Gómez A. L., Martínez Beltrán E. T., Sánchez Sánchez P. M., Huertas Celdrán A. TemporalFED: A software module for detecting cyberattacks in Industry 4.0 time-series data using decentralized federated learning. *arXiv*, 2025, arXiv:2308.03554v2 [cs.CR]. doi:10.48550/arXiv.2308.03554
12. Danish M. Enhancing cyber security through predictive analytics: Real-time threat detection and response. *International Journal of Advanced Computer Science and Applications*, 2025, vol. 16, no. 8, pp. 27–35. doi:10.14569/IJACSA.2025.0160804
13. Jiang Y., Oo N., Meng Q., Lin L., Niyato D., Xiong Z., Lim H. W., Sikdar B. CyGATE: Game-theoretic cyber attack-defense engine for patch strategy optimization. *arXiv*, 2025. doi:10.48550/arXiv.2508.00478
14. Datar M., Dujardin Y. Adaptive learning for moving target defence: Enhancing cybersecurity strategies. *arXiv*, 2025. arXiv:2508.17945v1 [cs.GT].
15. Spyrou E. D., Kappatos V., Stylios C. Game-theoretic secure socket transmission with a zero trust model. *Applied Sciences*, 2025, vol. 15, no. 19, art. 10535. doi:10.3390/app151910535
16. Isaeva O. S., Kulyasov N. V., Isaev S. V. Infrastructure for collecting data and simulating security threats in the Internet of Things networks. *Siberian Aerospace Journal*, 2025, vol. 26, no. 1, pp. 8–20 (In Russian). doi:10.31772/2712-8970-2025-26-1-8-20, EDN: OPICJJ
17. Fedorov N. A., Sychov P. P. A study of security issues of Internet of Things (IoT) systems. *Sistemnyy analiz v nauke i obrazovanii*, 2023, no. 2, pp. 27–35 (In Russian). EDN: FGJBSV
18. Vasilyev V. I., Gvozdev V. E., Shamsutdinov R. R. Network anomaly detection based on artificial immune system for industrial Internet of Things. *Proceedings of the TUSUR University*, 2021, vol. 24, no. 4, pp. 40–45 (In Russian). doi:10.21293/1818-0442-2021-24-4-40-45, EDN: YKHKPJ

19. Tergeuov O. S., Malikova F. U. Detection and elimination of IoT botnets based on SIEM DDoS attacks. *Universum: tekhnicheskie nauki*, 2022, no. 4-1 (97), pp. 54–63 (In Russian). EDN: WJNKHL
20. Urinov N. T., Mamadaliev S. S., Bakhramova M. B., Alizhonov Sh. A., Ne'matzhonov A. U., Akbarova M. Sh. Definition of informative features and formalization of the knowledge base for identification of the Stuxnet cyber attack on the Internet of Things system. *Al-Farg'onyi avlodlari*, 2025, vol. 1, iss. 2, pp. 80–85. https://doi.org/10.5281/zenodo.15580978. Available at: https://al-fargoniy.uz/ (accessed 15 May 2025) (In Russian).
21. Lipatnikov V. A., Melekhov K. V., Zadboev V. A. Method of active protection of information and computing networks against multi-stage attacks. *Sbornik trudov Sankt-Peterburgskoj mezhdunarodnoj konferencii i Sankt-Peterburgskoj mezhregional'noj konferencii "Regional'naya informatika i informacionnaya bezopasnost'"* [Proc. Saint Petersburg International and Interregional Conf. "Regional Informatics and Information Security"]. Saint Petersburg, 2024, pp. 112–114 (In Russian).
22. Lipatnikov V. A., Melekhov K. V. Method for processing network control results in support of decision-making by an information security administrator. *Trudy XXVII Vserossijskoj nauchnoj-prakticheskoj konferencii "Aktual'nye problemy zashchity i bezopasnosti"* [Proc. XXVII All-Russian Sci. and Pract. Conf. "Current issues of protection and security"]. Saint Petersburg, 2024, pp. 306–310 (In Russian).
23. Lipatnikov V. A., Melikhov I. A., Melekhov K. V. Features of network control in a data transmission network under conditions of multi-stage attacks. *Materialy nauchno-prakticheskoj konferencii "Tekhnologii. Innovacii. Svyaz'"* [Mater. of the Sci. and Pract. Conf. "Technologies. Innovations. Communications"]. Saint Petersburg, 2023, pp. 171–174 (In Russian).