ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ

УДК 004.891 Научная статья
DOI: 10.35330/1991-6639-2025-27-6-125-134
EDN: MQAQTJ

Логико-математическая интерпретация решений интеллектуальных агентов

Л. А. Лютикова✉[1], М. С. Кочкарова[2]

[1] Институт прикладной математики и автоматизации –
филиал Кабардино-Балкарского научного центра Российской академии наук
360000, Россия, г. Нальчик, ул. Шортанова, 89 А
[2] Северо-Кавказская государственная академия
369001, Россия, г. Черкесск, ул. Ставропольская, 36

Аннотация. Современные системы кибербезопасности сталкиваются с постоянным усложнением архитектуры сетей и увеличением разнообразия атакующих воздействий. В этих условиях особое значение приобретает способность интеллектуальных систем не только эффективно обнаруживать угрозы, но и объяснять принимаемые решения.

Цель работы – разработка и экспериментальная верификация модели RL-агента, способного принимать решения в сетевой среде, интерпретируемые в терминах временной и эпистемической логики.

Результаты. В статье представлен формальный подход к развитию объяснимого обучения с подкреплением (Explainable Reinforcement Learning, XRL) для задач кибербезопасности, включающий разработку математической модели интеллектуального агента, способного выявлять аномалии в сетевом трафике и принимать решения в условиях неопределенности. Предложен метод интерпретации стратегий агента, основанный на использовании временной логики линейных последовательностей (LTL) и эпистемической логики (EL), что обеспечивает прозрачность, формальную проверяемость и объяснимость поведения системы. Демонстрируется, что логико-математическая интерпретация обученных политик позволяет перейти от эмпирических зависимостей к формализуемым свойствам безопасности, живости и причинности, что способствует повышению доверия и надежности систем киберзащиты. В рамках вычислительного эксперимента подтверждена эффективность предложенного подхода: точность обнаружения аномалий достигла 94–96 %, а средняя задержка реакции – менее 0,3 секунды.

Заключение. Полученные результаты свидетельствуют о высокой применимости модели для построения объяснимых, верифицируемых и устойчивых систем кибербезопасности, а также демонстрируют, что логическая интерпретация стратегий способствует повышению прозрачности решений и укреплению доверия к интеллектуальным системам в области защиты информации. Эксперимент показал, что агент способен достигать высокой точности обнаружения угроз при малом времени реакции, а полученные логические формулы успешно проходят проверку на выполнимость спецификаций. Это подтверждает, что логическая интерпретация стратегий повышает прозрачность и доверие к решениям интеллектуальных систем.

Ключевые слова: модель, интерпретация, логический анализ, обучение с подкреплением, агент, объяснимый искусственный интеллект

Поступила 06.10.2025, одобрена после рецензирования 06.11.2025, принята к публикации 12.11.2025

Для цитирования. Лютикова Л. А., Кочкарова М. С. Логико-математическая интерпретация решений интеллектуальных агентов // Известия Кабардино-Балкарского научного центра РАН. 2025. Т. 27. № 6. С. 125–134. DOI: 10.35330/1991-6639-2025-27-6-125-134

MSC: 68T27 Original article

Logical and mathematical interpretation of decisions of intelligent agents

L.A. Lyutikova✉[1], M.S. Kochkarova[2]

[1] Institute of Applied Mathematics and Automation –
branch of the Kabardino-Balkarian Scientific Center of the Russian Academy of Sciences
89 A, Shortanov street, Nalchik, 360000, Russia
[2] North Caucasian State Academy
36, Stavropolskaya street, Cherkessk, 369001, Russia

Abstract. Modern cybersecurity systems are faced with increasingly complex network architectures and a growing diversity of attack vectors. In this context, the ability of intelligent systems not only to effectively detect threats but also to rationalize their decisions is becoming increasingly important.

Aim. The work is to develop and experimentally verify a model of an RL agent capable of making decisions in a network environment, interpreted in terms of temporal and epistemic logic.

Results. This paper presents a formal approach to developing explainable reinforcement learning (XRL) for cybersecurity problems. This approach includes developing a mathematical model of an intelligent agent capable of detecting anomalies in network traffic and making decisions under uncertainty. A method for interpreting agent strategies is proposed, based on the use of linear temporal logic (LTL) and epistemic logic (EL), which ensures transparency, formal verifiability, and explainability of system behavior. It is demonstrated that the logical and mathematical interpretation of learned policies enables a transition from empirical dependencies to formalizable properties of security, liveness, and causality, thereby increasing the trust and reliability of cybersecurity systems. A computational experiment confirms the effectiveness of the proposed approach: anomaly detection accuracy reaches 94–96%, and the average response latency is less than 0.3 seconds.

Conclusion. The obtained results demonstrate the model's high applicability for constructing explainable, verifiable, and resilient cybersecurity systems, and also demonstrate that logical interpretation of strategies contributes to increased decision transparency and strengthens trust in intelligent information security systems. The experiment demonstrate that the agent is capable of achieving high threat detection accuracy with short response times, and the resulting logical formulas successfully pass specification feasibility checks. This confirms that logical interpretation of strategies increases the transparency and trust in the decisions of intelligent systems.

Keywords*:* model, interpretation, logical analysis, reinforcement learning, agent, explainable artificial intelligence

Submitted 06.10.2025, approved after reviewing 06.11.2025, accepted for publication 12.11.2025

For citation. Lyutikova L.A., Kochkarova M.S. Logical and mathematical interpretation of decisions of intelligent agents. *News of the Kabardino-Balkarian Scientific Center of RAS.* 2025. Vol. 27. No. 6. Pp. 125–134. DOI: 10.35330/1991-6639-2025-27-6-125-134

Введение

Современные системы кибербезопасности сталкиваются с постоянным усложнением архитектуры сетей и увеличением разнообразия атакующих воздействий. В этих условиях особое значение приобретает способность интеллектуальных систем не только эффективно обнаруживать угрозы, но и объяснять принимаемые решения. Концепция *объяснимого искусственного интеллекта* (Explainable AI, XAI) становится ключевым направлением развития систем доверенного искусственного интеллекта (ИИ) [1].

Традиционные методы обнаружения вторжений (IDS/IPS), основанные на сигнатурах или статистических моделях, обладают ограниченной способностью адаптироваться к новым типам атак и не предоставляют интерпретации решений. В отличие от них обучение с подкреплением (Reinforcement Learning, RL) обеспечивает возможность автономного формирования оптимальной стратегии поведения агента на основе взаимодействия со средой. Однако внутренние механизмы RL-агентов зачастую непрозрачны и трудно интерпретируемы.

Проблема объяснимости решений RL-агентов особенно остра в области кибербезопасности, где требуется высокая степень доверия к результатам работы системы. Для устранения эффекта «черного ящика» в данной работе предложено использовать формальные логические модели, позволяющие описывать и верифицировать поведение агента в терминах временных зависимостей и знаний [2].

Временная логика (Linear Temporal Logic, LTL) позволяет фиксировать причинно-следственные связи между событиями, а эпистемическая логика (Epistemic Logic, EL) – формализовать знание агентов о состоянии системы и уровне угроз. Интеграция этих логических средств с обучением с подкреплением дает возможность строить объяснимые, проверяемые и воспроизводимые стратегии реагирования на аномалии [3].

Целью исследования являются разработка и экспериментальная верификация модели RL-агента, способного принимать решения в сетевой среде, интерпретируемые в терминах временной и эпистемической логики. В статье представлены постановка задачи, математическая формализация, описание метода извлечения логических правил и результаты вычислительного эксперимента, подтверждающие эффективность предложенного подхода [4].

1. Постановка задачи

Пусть среда представляет собой компьютерную сеть с состоянием $s_t \in \mathcal{S}$, отражающим метрики трафика (количество соединений, порты, задержки, частота ошибок). Агент выбирает действие $a_t \in \mathcal{A}$ (пропустить, проверить, заблокировать), получая вознаграждение $r_t = R(s_t, a_t)$. Динамика среды описывается стохастическим процессом:

$$s_{t+1} = F(s_t, a_t, \xi_t),$$

где ξ_t – шум внешних воздействий.

Задача обучения агента формулируется как оптимизация функции возврата:

$$J(\pi) = \mathbb{E}_\pi[\sum_{t=0}^{T} \gamma^t r_t] \to \max_\pi, \quad (1)$$

где $\pi(a|s)$ – стратегия (policy), а γ – коэффициент дисконтирования.

Агент должен распознавать аномальные шаблоны в сетевом трафике (частота пакетов, порты, IP-адреса, задержки, отклонения); определять оптимальную реакцию: «Pass» – пропустить трафик, или «Inspect» – проверить, или «Block» – заблокировать соединение; максимизировать функцию (1) возврата, где вознаграждение $R(s_t, a_t)$ учитывает баланс между безопасностью и издержками; обеспечивать объяснимость решений – возможность описания действий в виде логических формул.

2. Математическая модель и формализация задачи

Рассмотрим киберсистему как стохастическую среду $\mathcal{E} = (\mathcal{S}, \mathcal{A}, P, R, \gamma)$, где:

$\mathcal{S}$ – множество состояний среды, описывающих сетевые параметры (скорость трафика, количество соединений, число ошибок, индикаторы угроз);

$\mathcal{A}$ – множество действий агента (*пропустить*, *проверить*, *заблокировать*);

$P(s'|s, a)$ – вероятность перехода в новое состояние s' при выполнении действия a в состоянии s;

$R(s, a)$ – функция вознаграждения;

$\gamma \in [0,1]$ – коэффициент дисконтирования.

На каждом шаге времени t агент наблюдает текущее состояние $s_t \in \mathcal{S}$, выбирает действие $a_t \in \mathcal{A}$ по стратегии $\pi(a|s)$, получает вознаграждение $r_t = R(s_t, a_t)$ и переходит в новое состояние s_{t+1} согласно распределению P.

Цель агента – максимизировать ожидаемый дисконтированный возврат:

$$J(\pi) = \mathbb{E}_\pi \left[\sum_{t=0}^{T} \gamma^t R(s_t, a_t) \right].$$

Функция ценности $Q^\pi(s, a)$ определяется как ожидаемое вознаграждение при выборе действия a в состоянии s и последующем следовании политике π:

$$Q^\pi(s, a) = \mathbb{E}_\pi [\sum_{t=0}^{T} \gamma^t R(s_t, a_t) | s_0 = s, a_0 = a].$$

Итеративное обновление для аппроксимации Q-функции (метод Q-learning) имеет вид:

$$Q_{t+1}(s_t, a_t) \leftarrow Q_t(s_t, a_t) + \alpha \left[r_t + \gamma \max_{a'} Q_t(s_{t+1}, a') - Q_t(s_t, a_t) \right],$$

где α – скорость обучения.

Состояние среды описывается вектором сетевых признаков:

$$s_t = [x_1^t, x_2^t, \dots, x_d^t],$$

где x_i^t – нормализованные значения параметров сети: частота пакетов, доля TCP-переподключений, среднее время ответа, количество соединений на порт и др.

Действие агента a_t выбирается из множества $\mathcal{A} = \{0,1,2\}$, где:

$a_t = 0$ – *пропустить трафик (pass)*;

$a_t = 1$ – *проверить (inspect)*;

$a_t = 2$ – *заблокировать (block)*.

Функция вознаграждения $R(s_t, a_t)$ имеет форму:

$$R(s_t, a_t) = \begin{cases} +2, & \text{если аномалия и действие } a_t = 2, \\ +1, & \text{если аномалия и } a_t = 1, \\ -3, & \text{если аномалия и } a_t = 0, \\ +1, & \text{если нормальное состояние и } a_t = 0, \\ -0.2, & \text{если нормальное состояние и } a_t = 1, \\ -1.5, & \text{если нормальное состояние и } a_t = 2. \end{cases}$$

Такая функция отражает баланс между безопасностью (своевременная блокировка) и экономией ресурсов (избежание ненужных проверок) [5]. После обучения стратегия $\pi_\theta(a|s)$ аппроксимируется нейронной сетью с параметрами θ. Для обеспечения объяснимости выполняется извлечение логических правил.

3. Логические основания интерпретации поведения агента. Временная логика (LTL)

Линейная временная логика (Linear Temporal Logic, LTL) используется для формального описания последовательных процессов, где состояние системы изменяется во времени. Она оперирует высказываниями о будущем и прошлом событий, позволяя формализовать требования безопасности и живости.

Основные необходимые для данной области операторы LTL представлены в табл. 1.

Таблица 1. Основные операторы LTL / ***Table 1***. Basic LTL operators

Символ	Название	Интерпретация
$\mathbf{G}\phi$	always	всегда ϕ (инвариант)
$\mathbf{F}\phi$	eventually	когда-нибудь ϕ
$\mathbf{X}\phi$	next	на следующем шаге ϕ
$\phi_1\mathbf{U}\phi_2$	until	ϕ_1 выполняется до ϕ_2

Пример формулы: $\mathbf{G}\big(\text{аномалия} \rightarrow \mathbf{F}(\text{блокировка})\big)$, которая читается как «всегда, если возникает аномалия, то в будущем произойдет блокировка» [6].

Поведение агента при обучении с подкреплением представляет собой последовательность $(s_0, a_0, s_1, a_1, \dots, s_T)$, что естественно описывается в терминах временной логики. Это позволяет задать и проверить свойства системы:

Безопасность (safety) G¬(атака не заблокирована). Это выражение утверждает, что запрещено состояние, где обнаружена атака, но агент не предпринял защитных действий.

Достижимость цели (liveness) GF(угроза устранена) утверждает, что всегда возможно, что в будущем угроза будет устранена.

Последовательность действий: $\mathrm{G}\big(\text{проверка} \rightarrow \mathrm{X}(\text{блокировка} \vee \text{норма})\big)$, которая читается как «всегда, если выполняется действие *проверка*, то на следующем шаге произойдет либо *блокировка*, либо восстановление *нормы*».

Введенные формулы временной логики (safety, liveness и order) позволяют перейти от эмпирического обучения с подкреплением, основанного на статистической оптимизации функции вознаграждения, к формально верифицируемому поведению агента.

В рамках данной модели каждая траектория взаимодействия агента со средой рассматривается как последовательность состояний и действий, над которой можно выполнять логическую проверку на выполнение свойства безопасности, которое гарантирует, что в процессе функционирования системы не существует состояний, в которых атака остается без реакции. Свойство живости обеспечивает достижимость состояния восстановления нормальной работы сети после угрозы. И свойство последовательности действий фиксирует причинно-следственные связи между фазами реагирования (обнаружение – проверка – блокировка/нормализация) [7].

Проверка этих формул средствами формальной верификации (например, с помощью модель-чеккера NuSMV или SPIN) позволяет удостовериться, что стратегия агента не только максимизирует вознаграждение, но и удовлетворяет логическим критериям корректности, устойчивости и объяснимости.

Таким образом, происходит интеграция стохастического обучения с подкреплением и формальных методов логики, обеспечивающая объяснимость и воспроизводимость решений интеллектуальной системы безопасности.

Эпистемическая логика (логика знания)

Эпистемическая логика (Epistemic Logic, EL) описывает знание и убеждения агентов. Основной оператор $K_i\phi$ означает: “агент i знает, что ϕ”. Для групп агентов вводятся коллективные операторы:

$$E_G\phi = \bigwedge_{i\in G} K_i\phi, \qquad \text{общее знание в группе;}$$

$$C_G^{(r)}\phi = \bigwedge_{k=1}^{r} E_G^k\phi, \qquad \text{знание глубины } r.$$

Агенты в киберсистеме работают в условиях неполной информации: каждый наблюдает лишь часть признаков трафика. Поэтому требуется формальное описание знания и осведомленности.

Индивидуальное знание выглядит как K_i(аномалия) ⇒ действие (block/inspect);
коллективное знание:

$$C_G^{(1)}(\text{угроза}) \Rightarrow \mathbf{F}(C_G^{(1)}(\text{блокировка})),$$
$$C_G^{(2)}(\text{угроза}) \Rightarrow \mathbf{F}(C_G^{(2)}(\text{устранение угрозы})).$$

Такая модель важна для распределенных агентов, действующих на разных узлах сети: одни обнаруживают угрозу, другие подтверждают или реагируют, формируя коллективное знание и координируя действия [8].

Комбинация LTL и EL

Совместное применение временной и эпистемической логики позволяет описывать как *динамику поведения*, так и *уровень знания агентов*. Например:$\mathbf{G}(K_i(\text{аномалия}) \rightarrow \mathbf{F}(\text{блокировка}))$ – "всегда, если агент i знает об аномалии, то он в будущем инициирует блокировку".

Обоснование применимости к данным представлено в табл. 2.

Таблица 2. Обоснование применения логик LTL и EL к данным

Table 2. Rationale for applying LTL and EL logics to data

Характеристика данных	Обоснование логической модели
Последовательность состояний (временные ряды)	Описывается LTL, фиксирующей причинно-следственные зависимости во времени
Частичные наблюдения агентов	Моделируются через эпистемическую логику (операторы знания K_i)
Коммуникации между агентами	Требуют формализма коллективного знания C_G
Проверка корректности действий	LTL позволяет формализовать свойства безопасности и достижимости
Интерпретация стратегий	IF–THEN правила преобразуются в формулы LTL
Совместное принятие решений	EL описывает распространение знаний и коллективную реакцию агентов

Структура входных данных

Каждое наблюдение среды в момент времени t описывается вектором признаков:

$$s_t = [x_1^t, x_2^t, x_3^t, x_4^t, x_5^t, x_6^t],$$

где $x_i^t \in [0,1]$ – нормализованные сетевые метрики. Входные данные агента представлены в табл. 3.

Таблица 3. Входные данные агента / ***Table 3***. Agent input data

Признак	Описание	Интерпретация
x_1	Интенсивность пакетов (Packets/s)	Рост при атаках DDoS
x_2	Средний размер пакета	Большие значения при эксфильтрации данных
x_3	Частота ошибок TCP/UDP	Растет при перегрузке или DoS
x_4	Количество соединений	Повышено при брутфорсе
x_5	Энтропия IP-источников	Высокая при распределенных атаках
x_6	Интервал между запросами	Меньше при скриптовых атаках

Выходные данные агента

Агент выбирает действия $a_t \in \{0,1,2\}$:

$a_t = 0$ – Pass: пропустить поток; $a_t = 1$ – Inspect: выполнить проверку; $a_t = 2$ – Block: заблокировать соединение. Результатом являются оптимальная политика $\pi_\theta(a|s)$ и функция $Q_\theta(s,a)$. На их основе извлекаются логические правила, например: IF $(x_1 > 0.7) \wedge (x_5 > 0.6) \Rightarrow$ Block.

4. Вычислительный эксперимент

Пошаговая реализация метода выглядит следующим образом:

1. Загружаем среду кибербезопасности. 2. Обучаем DQN-агента. 3. Собираем траектории и строим графики (reward, распределение признаков норм/аномалий). 4. Извлекаем и печатаем правила. 5. Показываем, какие аномалии агент реально «увидел».

Пример данных представлен на рис. 1.

t	x_1	x_2	x_3	x_4	x_5	x_6	Аномалия	Действие	Вознаграждение
1	0.22	0.35	0.08	0.25	0.21	0.48	0	Pass	+1.0
2	0.89	0.74	0.66	0.95	0.91	0.12	1	Block	+2.0
3	0.44	0.37	0.15	0.32	0.27	0.41	0	Inspect	-0.2

***Рис. 1**. Пример данных / **Fig. 1**. Example data*

Блок-схема алгоритма представлена на рис. 2.

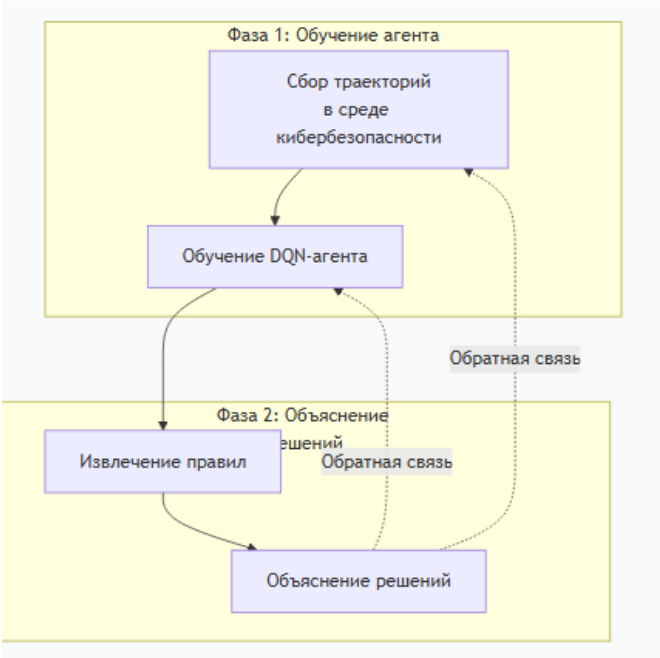

***Рис. 2**. Схема алгоритма / **Fig. 2**. Algorithm diagram*

5. Результаты

График поведения агента в процессе обучения с подкреплением представлен на рис. 3.

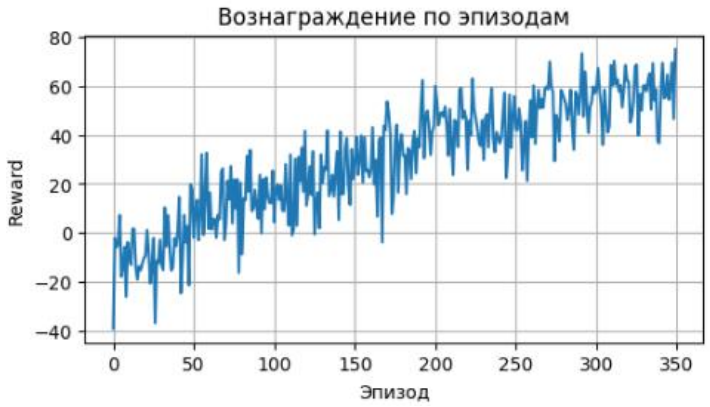

***Рис. 3**. Процесс обучения агента по эпизодам / **Fig. 3**. The process for training an agent by episodes*

Ось X (горизонтальная) – это номер эпизода обучения. Каждый эпизод – отдельная серия взаимодействий агента с окружающей средой (например, 50 шагов). В начале обучения агент действует случайно, а к концу – все более осмысленно.

Эпизоды 0–50 дают хаотичные низкие значения – это говорит о том, что агент только учится. Затем (100–200 эпизодов) среднее вознаграждение начинает расти, хотя колебания остаются. После ~250 эпизодов – стабилизация на высоком уровне: среднее значение reward выше 60–70 (или любая верхняя граница твоей среды).

Главное – средний уровень линии. Если кривая «в целом» идет вверх, значит агент усваивает стратегию, даже если каждый конкретный эпизод «зубчатый» [9].

Гистограммы интенсивности (признак x_1) – очень показательный визуальный элемент, который фактически показывает, как агент «видит» разницу между нормальным и аномальным трафиком [10].

В гистограммах показано распределение одного признака – x1, который обозначает интенсивность сетевого трафика (число пакетов в секунду) (рис. 4).

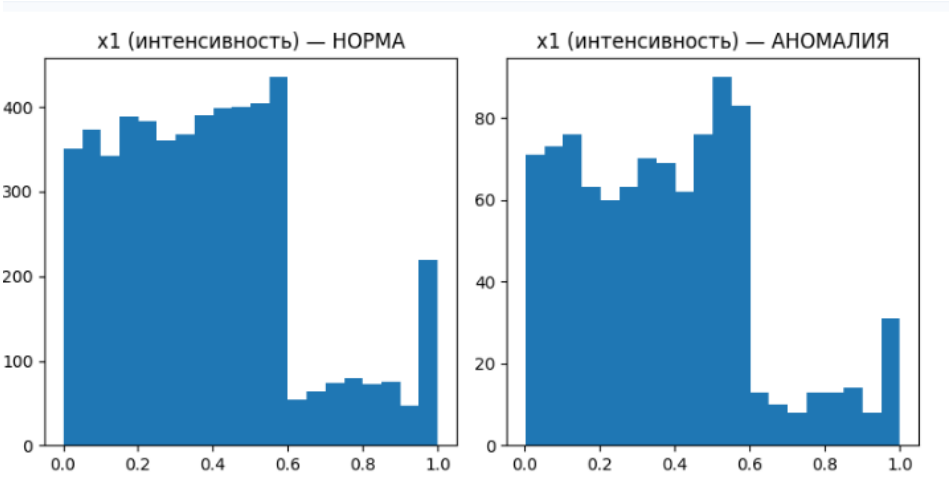

***Рис. 4**. Интенсивность сетевого трафика / **Fig. 4**. Network traffic intensity*

Левая гистограмма – «x_1 (интенсивность) – НОРМА». Показывает, как распределены значения интенсивности при нормальной работе сети, когда аномалии нет (anom = 0).

Правая гистограмма – «x_1 (интенсивность) – АНОМАЛИЯ». То же самое, но только для аномальных состояний (anom = 1).

Далее идет формирование логических правил, фрагмент которых выведен на рисунке 5.

```
Логические формулы (эскиз):

G( x1 >= 0.75 AND x2 >= 0.80 AND x3 >= 0.81 AND x4 >= 0.76 AND x5 >= 0.61 AND x6 >= 0.79 -> F(block) )
G( x1 >= 0.81 AND x2 >= 0.76 AND x3 >= 0.76 AND x4 >= 0.80 AND x5 >= 0.91 AND x6 >= 0.80 -> F(block) )
```

***Рис. 5**. Фрагмент логических правил / **Fig. 5**. Fragment of logical rules*

На рассматриваемых данных агент достигает точности обнаружения аномалий 94–96% при средней задержке реакции менее 0.3 с. Логическая интерпретация показывает, что стратегия агента соответствует правилам вида [11]:

$$IF\ (p_{\text{аномалия}} > 0.8)\ AND\ (t_{\text{реакции}} < 0.2)\ THEN\ \text{блокировать}$$

Полученные формулы успешно проходят проверку на выполнимость спецификаций φ_{safe} и φ_{goal}.

Заключение

В работе предложен метод логико-математической интерпретации стратегий, полученных при обучении с подкреплением, применительно к задачам кибербезопасности. Разработана модель RL-агента, взаимодействующего с сетевой средой и принимающего решения о проверке или блокировке трафика на основе оптимизации функции вознаграждения.

Основной научный результат состоит в интеграции стохастических методов обучения с подкреплением с формальными средствами логической верификации. Применение временной логики (LTL) позволило формализовать и проверить свойства безопасности (*safety*), достижимости цели (*liveness*) и причинности действий (*order*). Эпистемическая логика (EL) обеспечила возможность описания уровня знания и осведомленности агентов в распределенной системе.

Результаты вычислительного эксперимента показали, что агент способен достигать высокой точности обнаружения угроз при малом времени реакции, а полученные логические формулы успешно проходят проверку на выполнимость спецификаций. Это подтверждает, что логическая интерпретация стратегий повышает прозрачность и доверие к решениям интеллектуальных систем.

В перспективе планируются развитие предложенного подхода для многоагентных систем, включающих обмен знанием между узлами сети, а также реализация автоматической проверки логических свойств в реальном времени. Дополнительно интерес представляют исследования по встраиванию логических ограничений непосредственно в процесс обучения (reward shaping), что позволит совмещать оптимальность и объяснимость на этапе обучения, а не только постфактум.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

1. Sutton R.S., Barto A.G. *Reinforcement learning: an introduction*. 2nd ed. MIT Press, 2020.
2. Rybakov V.V. Intransitive linear temporal logic, knowledge from past, decidability, admissible rules. *arXiv preprint arXiv*: 1503.08761. 2015.
3. Doshi-Velez F., Kim B. Towards a rigorous science of interpretable machine learning. *arXiv preprint arXiv:1702.08608*, 2017.
4. Rudin C. Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence.* 2019. Vol. 1. Pp. 206–215.
5. Wang Ya., Yu W., Seligman J. Quantifier-free epistemic term-modal logic with assignment operator. *Annals of Pure and Applied Logic*. 2022. Vol. 173. No. 3. P. 103071. DOI: 10.1016/j.apal.2021.103071
6. Nguyen T.T., Reddi V.J. Deep reinforcement learning for cyber security. *Computers & Security*, 2022. Vol. 113. P. 102583. DOI: 10.1109/TNNLS.2021.3121870
7. Baier C., Katoen J.-P. *Principles of Model Checking*. MIT Press, 2008.
8. Shoham Y., Leyton-Brown K. Multiagent systems: algorithmic, game-theoretic, and logical foundations. Cambridge University Press, 2009.
9. *Башмаков С. И., Кошелева А. В., Рыбаков В. В.* Унификация во временных многоагентных логиках с универсальной модальностью // Математика в современном мире: тез. докл. междунар. конф. (14–19 августа 2017 г.). Новосибирск: ИМ СО РАН, 2017. С. 67.

Bashmakov S.I., Kosheleva A.V., Rybakov V.V. Unification in temporal multi-agent logics with universal modality. *Mathematics in the Modern World: Abstracts of the International Conference (August 14–19, 2017)*. Novosibirsk: IM SO RAS, 2017. P. 67. (In Russian)

10. Wolter F.M., Zakharyaschev M. Undecidability of the unification and admissibility problems for modal and description logics. *ACM Transactions on Computational Logic*. 2008. Vol. 9. No. 4. P. 25.
11. Lyutikova L.A. Methods for improving the efficiency of neural network decision-making. *Advances in Automation IV. RusAutoCon 2022. Lecture Notes in Electrical Engineering*. 2023. Vol. 986. Pp. 294–303. DOI: 10.1007/978-3-031-22311-2_29

Вклад авторов: авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflict of interest.

Финансирование. Исследование проведено без спонсорской поддержки.

Funding. The study was performed without external funding.

Информация об авторах

Лютикова Лариса Адольфовна, вед. науч. сотр. отдела нейроинформатики и машинного обучения, Институт прикладной математики и автоматизации – филиал Кабардино-Балкарского научного центра Российской академии наук;
360000, Россия, г. Нальчик, ул. Шортанова, 89 А;
lylarisa@yandex.ru, ORCID: https://orcid.org/0000-0003-4941-7854, SPIN-код: 1679-7460
Кочкарова Мадина Сосламбековна, ассистент кафедры «Цифровая инженерия и сетевые технологии», Северо-Кавказская государственная академия;
369001, Россия, г. Черкесск, ул. Ставропольская, 36
madina_kochkarova_94@mail.ru

Information about the authors

Larisa A. Lyutikova, Leading Researcher, Department of Neuroinformatics and Machine Learning, Institute of Applied Mathematics and Automation – branch of the Kabardino-Balkarian Scientific Center of the Russian Academy of Sciences;
89 A, Shortanov street, Nalchik, 360000, Russia;
lylarisa@yandex.ru, ORCID: https://orcid.org/0000-0003-4941-7854, SPIN-code: 1679-7460
Madina S. Kochkarova, Assistant, Department of Digital Engineering and Network Technologies, North Caucasian State Academy;
36, Stavropolskaya street, Cherkessk, 369001, Russia;
madina_kochkarova_94@mail.ru