Инженерный вестник Дона, №11 (2025)
ivdon.ru/ru/magazine/archive/n11y2025/10511

Модель представления взвешенных многозначных зависимостей для обнаружения редких аномальных событий в задачах информационной безопасности

Д.И. Раковский

Московский технический университет связи и информатики, г. Москва

Аннотация: Предложена новая модель функционирования компьютерной сети, учитывающая взвешенные многозначные зависимости, для выявления редких аномальных событий в компьютерной сети. Модель учитывает ранее не встречавшиеся в исходных данных многозначные зависимости, позволяя «превентивно» оценивать их потенциальное деструктивное воздействие на сеть. Предложен алгоритм расчета потенциального урона от реализации многозначной зависимости. Предложенная модель применима для анализа редких событий широкого профиля информационной безопасности и разработки новых методов и алгоритмов защиты информации на основе многозначных закономерностей.
Ключевые слова: многозначная классификация, многозначная зависимость, атрибутное пространство, компьютерные атаки, информационная безопасность, классификация сетевого трафика, обнаружение атак, информативность атрибутов, модель, редкие аномальные события, аномальные события.

Введение

Исследование распределенных во времени, многоступенчатых инцидентов информационной безопасности, становится всё более актуальным. Современные компьютерные атаки, проводимые на распределенные компьютерные сети (системы), чаще всего выходят за рамки одного типа, и сочетают в себе элементы сетевой разведки; закрепления; эксплуатации уязвимостей; воздействия на все свойства циркулирующей в сети информации [1].

Более того, всё актуальнее становятся атаки, направленные одновременно на разные элементы распределенных сетей. Проблема многозначных, многовекторных компьютерных атак в настоящее время также актуальна.

Согласно техническому отчету компании Cloudflare (см. «*DDoS threat report for 2024 Q1*»), в 2024 году наблюдалась атака типа «массовый отказ в

обслуживании» на глобальную телекоммуникационную инфраструктуру одновременно по ряду протоколов: UDP/ICMP-флуд; TCP-атаки; атаки типа «HTTP/2 Rapid Reset» и др.

Последствия от реализации таких «многозначных» атак могут приводить к катастрофическим последствиям для функционирования компьютерных сетей. Катастрофические последствия могут наступать как при реализации атаки, так и в рамках инцидентов, чьей причиной мог стать одновременный выход из строя нескольких критически важных узлов компьютерной сети или системы.

Под узлами понимается как отдельный хост (если рассматривается уровень локальной сети), так и телекоммуникационное оборудование или же – при рассмотрении проблемы на уровне системы – отдельные компоненты хоста. Как правило, подобные инциденты крайне редки – но крайне деструктивны [2]. Помимо кратковременных (относительно времени наблюдения) аномальных инцидентов, необходимо учитывать деградацию поддерживающей инфраструктуры компьютерной сети.

В научной периодике подобные события получили название «черные лебеди» [3] или «редкие аномальные события» [4]. В настоящее время актуальны исследования, направленные на разработку новых методов машинного обучения, учитывающих сложную структуру таких инцидентов. Одним из перспективных направлений является многозначное обучение (от англ. *multi-label learning*), бурно развивающееся с 10-х годов XXI века [5, 6], в том числе и в сфере информационной безопасности [7, 8].

Для выявления редких аномальных событий в информационной безопасности целесообразно использовать аппарат многозначной классификации [9].

В настоящее время проблемное поле, связанное с влиянием многозначных зависимостей на результаты принятия решений в области

информационной безопасности, в том числе и в рамках обнаружения редких аномальных событий, разработано слабо и представлено разрозненными публикациями с неустойчивой терминологией [10].

В ранее проведенных исследованиях [11] для описания поведения компьютерной сети использовалась модель на основании метода представления многозначных данных *Binary Relevance* [12]. Однако такие модели без дополнений не учитывают взаимосвязи между классовыми метками, входящими в состав многозначной зависимости, что затрудняет выявление редких аномальных событий в информационной безопасности [13, 14].

Целью работы является разработка модели представления многозначных зависимостей, отражающей в своей структуре частотные.

Существующая табличная модель представления поведения компьютерной сети, учитывающая многозначные зависимости

Данные о поведении компьютерной сети могут быть представлены в виде модели, объединяющей две таблицы: атрибутов размером Λ (столбцов) N (строк) $\boldsymbol{A}$, и таблицы целевых атрибутов (классовых меток) размером Ξ (столбцов) N (строк) $\boldsymbol{L}$ [15]:

$$\boldsymbol{D}_{NM} = \left\{ \left(\boldsymbol{A}(n,\ ), \boldsymbol{L}(n,\ ) \right); \boldsymbol{A} = \left(a_{n\lambda} \right), \boldsymbol{L} = \left(l_{n\xi} \right), \lambda = \overline{1,\Lambda}, \xi = \overline{1,\Xi}, n = \overline{1,N}, M = \Lambda + \Xi \right\}, \quad (1)$$

где $\boldsymbol{A}(n,\ ) = (a_{n1}, a_{n2}, \ldots, a_{n\Lambda})$ - n-ный вектор-строка матрицы атрибутов экспериментальных данных $\boldsymbol{A}$, состоящая из Λ столбцов; $\boldsymbol{L}(n,\ ) = (l_{n1}, l_{n2}, \ldots, l_{n\Xi})$ - n-ый вектор-строка матрицы целевых атрибутов (классовых меток) экспериментальных данных $\boldsymbol{L}$, состоящая из Ξ столбцов; N – количество записей экспериментальных данных.

Рассмотрим отличие модели (1) от классического представления данных табличной структуры. В таблице 1 приведено «классическое» табличное однозначное представление процесса функционирования компьютерной сети, маркированное одним целевым атрибутом, $L(n,\ ) = l_n$. Как правило, такие структуры часто применяются при разработке систем принятия решений в области информационной безопасности [16]. В таблице 2 приведен фрагмент набора данных UNSW-NB15 [17], представленный в однозначном представлении.

Таблица № 1

Однозначное представление процесса функционирования компьютерной сети

n	***A(n,) – n*-ный вектор-строка матрицы атрибутов экспериментальных данных *A*, состоящая из *Λ* столбцов.**						***Целевой атрибут*, $L(n,\ ) = l_n$**
	a_{n1}	a_{n2}	…	$a_{n\lambda}$	…	$a_{n\Lambda}$	l
1	a_{11}	a_{12}	…	$a_{1\lambda}$	…	$a_{1\Lambda}$	l_1
2	a_{21}	a_{22}	…	$a_{2\lambda}$	…	$a_{2\Lambda}$	l_2
3	a_{31}	a_{32}	…	$a_{3\lambda}$	…	$a_{3\Lambda}$	l_3
…	…	…	…	…	…	…	…
N-1	$a_{N-1\ 1}$	$a_{N-1\ 2}$	…	$a_{N-1\ \lambda}$	…	$a_{N-1\ \Lambda}$	l_{N-1}
N	$a_{N\ 1}$	$a_{N\ 2}$	…	$a_{N\ \lambda}$	…	$a_{N\ \Lambda}$	l_N

Таблица № 2

Фрагмент набора данных UNSW-NB15, представленный в однозначном представлении

№	**srip**	**proto**	**state**	**dur**	**…**	**stime**	**Целевой атрибут, $L(n,\ ) = l_n$**
1	*175.45.176.2*	*ospf*	*INT*	*0.518061*	…	*1421927596*	Exploits
2	*175.45.176.2*	*ospf*	*INT*	*0.518061*	…	*1421927596*	Exploits
3	*175.45.176.2*	*ospf*	*INT*	*0.518061*	…	*1421927596*	Reconnaissance
4	*175.45.176.2*	*ospf*	*INT*	*0.518061*	…	*1421927596*	Fuzzers
5	*175.45.176.2*	*ospf*	*INT*	*0.518061*	…	*1421927596*	Exploits
6	*175.45.176.2*	*ospf*	*INT*	*0.518061*	…	*1421927596*	Exploits
7	*175.45.176.2*	*ospf*	*INT*	*0.518061*	…	*1421927596*	Reconnaissance
8	*175.45.176.2*	*ospf*	*INT*	*0.518061*	…	*1421927596*	Fuzzers

Как видно из представленного фрагмента в таблице 2, в наборе данных зафиксировано 8 одинаковых по атрибутному пространству записей, имеющих различную маркировку. К примеру, запись №1 маркирована классовой меткой «Exploits», а запись №3 - классовой меткой «Reconnaissance».

В таблице 3 приведена визуализация модели многозначного табличного представления компьютерной сети (1), учитывающая многозначные зависимости.

Таблица №3

Многозначное представление процесса функционирования компьютерной сети (иллюстративный пример)

n	**Вектор значений атрибутного пространства,** $A(n,\ ) = (a_{n1}, a_{n2}, \dots, a_{n\Lambda})$	**Вектор значений целевых атрибутов,** $L(n,\ ) = (l_{n1}, l_{n2}, \dots, l_{n\Xi})$					
		l_1	l_2	l_3	l_4	l_5	…
1	*A(1,)*	1	0	0	0	0	…
2	*A(2,)*	0	1	0	0	0	…
3	*A(3,)*	0	1	1	1	0	…
4	*A(4,)*	0	1	1	0	0	…
5	*A(5,)*	1	0	0	0	0	…

Преобразуем иллюстративный пример из табл. 2 согласно модели (1). Преобразованный фрагмент набора данных UNSW-NB15, представленный в многозначном представлении, приведен в табл. 4 Как показал ее анализ, преобразование к многозначному представлению таблицы без дополнительных этапов обработки данных не позволяет выявить многозначные зависимости, «скрытые» в однозначных наборах данных (в таблице 4 пропущенные классовые метки выделены цветом). К тому же, затруднительно подсчитать частотные характеристики однозначных и многозначных зависимостей.

Таблица № 4

Фрагмент набора данных UNSW-NB15, представленный согласно (1)

№	srip	proto	state	dur	…	stime	Целевой атрибут, $L_{example}(n,\ ) = (l_{n1}, l_{n2}, l_{n3})$		
							$l_{Exploits}$	$l_{2\ reconnaissance}$	$l_{3\ Fuzzers}$
1	*175.45.176.2*	*ospf*	*INT*	*0.518061*	…	*1421927596*	1	0	0
2	*175.45.176.2*	*ospf*	*INT*	*0.518061*	…	*1421927596*	1	0	0
3	*175.45.176.2*	*ospf*	*INT*	*0.518061*	…	*1421927596*	0	1	0
4	*175.45.176.2*	*ospf*	*INT*	*0.518061*	…	*1421927596*	1	0	1
5	*175.45.176.2*	*ospf*	*INT*	*0.518061*	…	*1421927596*	1	0	0
6	*175.45.176.2*	*ospf*	*INT*	*0.518061*	…	*1421927596*	1	0	0
7	*175.45.176.2*	*ospf*	*INT*	*0.518061*	…	*1421927596*	0	1	0
8	*175.45.176.2*	*ospf*	*INT*	*0.518061*	…	*1421927596*	0	0	1

Модификация существующей модели многозначного табличного представления функционирования компьютерной сети

В работе [18] предложено определять дубликаты строк при помощи алгоритма «Поиск полных дубликатов».

Алгоритм «Поиск полных дубликатов»:

1. *Целевые атрибуты преобразуются в бинарное представление.*
2. *В исходной двухмерной таблице атрибутов производится поиск дубликатов, игнорируя целевые атрибуты.*
3. *Обнаруженные дубликаты группируются методом «полного совпадения всех значений», игнорируя целевые атрибуты.*
4. *Проводится операция «логическое ИЛИ» по целевым атрибутам в каждой группе дубликатов.*

Алгоритма «Поиск полных дубликатов» может быть усовершенствован. Например, путём применения мягкого хеширования в целях поиска схожих векторов-строк в атрибутном пространства или

проведения «огрубления» части атрибутов исходного пространства данных при помощи мягких множеств [19].

Остается нерешенной задача формирования частотной статистики по многозначным целевым атрибутам. Основные критерии для формирования статистики определяются использованием модифицированной модели в задаче обнаружения редких аномальных событий.

Поскольку модель применяется, в первую очередь, для описания функционирования компьютерных систем и сетей, подвергаемых компьютерным атакам, то под редким аномальным событием будем понимать сочетание компьютерных атак (классовых меток), приводящее к максимальному ущербу сети / системе. Для перехода от качественной оценки в количественную предлагается подход, увязывающий наименования известных типов компьютерных атак и базы данных, содержащих описание атак и численную оценку их деструктивности (к примеру – MITRE ATT&CK [20]). В случае отсутствия возможности получения таких оценок, проводится экспертная оценка, например, методом анализа иерархий [21].

Выделим из модели (1) все уникальные компьютерные атаки и сформируем вектор оценок их деструктивного воздействия на КС:

$$Damage = \left(q_\xi\right), \xi = \overline{1,\Xi}, \tag{2}$$

где q_ξ – численное значение ущерба, наносимого атакой определенного типа компьютерной системе, определенное *экспертно*. Размерность вектора оценок деструктивного воздействия на КС *Damage* соответствует размерности пространства целевых атрибутов модели (1). Диапазон изменения оценок деструктивного воздействия $0 < q < Q$ варьируется от 0 (атака не актуальна / ущерб отсутствует) до Q – максимального численного значения ущерба.

Выделим из набора данных, представленного моделью (1), информацию о частотном распределении каждой зависимости. Поскольку

пространство целевых атрибутов состоит из бинарных векторов, размерность которых определяется Ξ, существует 2^{Ξ} вариантов комбинаций классовых меток. Формализуем частотную статистику как функцию *f*, отображающую каждую возможную комбинацию меток $\boldsymbol{L}(n,)\in\{0,1\}^{\Xi}$ в частоту её появления в наборе данных, ограниченном N записями:

$$f\left(\hat{\boldsymbol{L}}(n,)\right)=\sum_{n=1}^{N}\mathbf{1}_{\boldsymbol{L}(n,)==\hat{\boldsymbol{L}}(n,)}, \tag{3}$$

где $\hat{\boldsymbol{L}}(n,)$ - многозначная зависимость, для которой необходимо подсчитать количество раз, которое она встречалась в **L**; $\mathbf{1}_{\boldsymbol{L}(n,)==\hat{\boldsymbol{L}}(n,)}$ - индикаторная функция, возвращающая «1» при соблюдении условия $\boldsymbol{L}(n,)==\hat{\boldsymbol{L}}(n,)$, «0» - при несоблюдении.

Всего существует 2^{Ξ} вариантов комбинаций классовых меток. Они образуют множество:

$$SumLib=\left\{f\left(\hat{\boldsymbol{L}}(n,)\right)\middle|\hat{\boldsymbol{L}}(n,)\in\{0,1\}^{\Xi}\right\}. \tag{4}$$

Для получения статистики нормируем (3) и объединим это в библиотеку частотных распределений аналогично (4):

$$FreqLib=\left\{\frac{1}{N}f\left(\hat{\boldsymbol{L}}(n,)\right)\middle|\hat{\boldsymbol{L}}(n,)\in\{0,1\}^{\Xi}\right\}. \tag{5}$$

Таким образом, каждой возможной комбинации классовых меток из множества $\boldsymbol{L}(n,)\in\{0,1\}^{\Xi}$ соответствует своя частота.

Объединим информацию о деструктивном воздействии компьютерных атак (2) с полученной библиотекой частотных распределений (5). Учтем возникновение редких аномальных событий, которые могут встретиться лишь в будущем.

Предлагается следующая формула вычисления потенциального урона компьютерной сети, наносимого многозначной зависимостью:

$$Pdam\left(\hat{\boldsymbol{L}}(n,)\right)=\frac{Damage\hat{\boldsymbol{L}}(n,)}{\left(\frac{1}{N}f\left(\hat{\boldsymbol{L}}(n,)\right)+\mathrm{B}\right)}, \quad (6)$$

где $Damage\hat{\boldsymbol{L}}(n,)$ - скалярное произведение вектора оценок деструктивного воздействия на сеть (2) *Damage* и многозначной зависимости; $\frac{1}{N}f\left(\hat{\boldsymbol{L}}(n,)\right)$ - частота многозначной зависимости (см. (5)); $\mathrm{B}=\frac{1}{\beta Q\Xi}$ - дополнительный коэффициент, вводимый для предотвращения неопределенности, возникающий при отсутствии частоты $\left(\frac{1}{N}f\left(\hat{\boldsymbol{L}}(n,)\right)=0\right)$ по многозначной зависимости, в котором: β - коэффициент устаревания, выбираемый эмпирически и регулирующий степень «предвзятости» к еще не встреченным многозначным зависимостям; Q – максимальное численное значение ущерба; Ξ – размерность пространства целевых атрибутов (1).

Раскроем смысл (6). Чем больше компьютерных атак, задействованных одновременно, включено в многозначную зависимость – тем больше произведение $Damage\hat{\boldsymbol{L}}(n,)$ - соответственно, значение итогового потенциального урона увеличивается. Чем больше произведение трех коэффициентов в знаменателе $\mathrm{B}=\frac{1}{\beta Q\Xi}$, тем меньше будет результирующее значение коэффициента. Следовательно, уменьшается общий знаменатель и, соответственно, значение урона также увеличивается. К уменьшению потенциального урона приводит малое абсолютное значение деструктивного воздействия на сеть атак, включенных в многозначную зависимость.

Проведем оценку всех многозначных зависимостей $\vartheta\in\{0,1\}^{\Xi}$ с использованием формулы (6). Оценку выполним как для известных и встреченных ранее многозначных зависимостей ($\vartheta\in\boldsymbol{L}$), так и для всех отсутствующих в «исторических данных» потенциально возможных зависимостей. Полученный вектор-столбец назовем взвешенными оценками

деструктивного воздействия многозначных зависимостей на компьютерную сеть:

$$\Psi = \left(Pdam\left(\vartheta_i\right)\right), i = \overline{1, \left|\{0,1\}^{\Xi}\right|}. \quad (7)$$

Получим итоговую модель функционирования компьютерной сети, учитывающую взвешенную оценку деструктивного воздействия многозначных зависимостей:

$$\boldsymbol{D}_{NM} = \left\{\left(\boldsymbol{A}(n,\ ), \boldsymbol{L}(n,\ )\right), \Psi\right\}; \boldsymbol{A} = \left(a_{n\lambda}\right), \boldsymbol{L} = \left(l_{n\xi}\right), \lambda = \overline{1,\Lambda}, \xi = \overline{1,\Xi}, n = \overline{1,N}, M = \Lambda + \Xi. \quad (8)$$

Данная модель может быть использована для анализа информации о функционировании компьютерной сети в целях выявления редких аномальных событий.

Приведем краткий алгоритм получения данных согласно модели (8):

1. Преобразовать исходные данные к табличному представлению (1);
2. Обнаружить дубликаты записей;
3. Сформировать частотную статистику по каждой комбинации классовых меток в многозначных зависимостях согласно (5);
4. Вычислить взвешенные оценки деструктивного воздействия для всех возможных многозначных зависимостей согласно (7);
5. Дополнить исходную таблицу (2) вектором-столбцом взвешенными оценками деструктивного воздействия многозначных зависимостей Ψ (7), получив итоговую модель (8);

Недостатками предлагаемой модели является потенциальная трудоемкость в определении метода подсчета деструктивного воздействия многозначной зависимости на компьютерную сеть (2).

Выводы

Предложена новая модель функционирования компьютерной сети, учитывающая взвешенные многозначные зависимости, для выявления редких аномальных событий в компьютерной системе / сети. Модель учитывает

ранее не встречаемые в исходных данных многозначные зависимости, позволяя «превентивно» оценивать их деструктивное воздействие на сеть. В зависимости от поставленной цели и условий функционирования компьютерной сети, варьируя параметры β, Q, Ξ, возможна «тонкая» настройка параметров учета многозначных зависимостей в модели.

Потенциальный урон от реализации многозначной зависимости (6) применим для анализа редких событий широкого профиля информационной безопасности. На основании предложенной модели (8) возможна разработка новых алгоритмов и методов алгоритмов обнаружения и прогнозирования редких аномальных событий.

Публикация выполнена в рамках гранта на реализацию отраслевой научно-педагогической школы МТУСИ "Современные технологии исследования аномалий в информационной безопасности" по проекту "Обнаружение и прогнозирование редких аномальных событий для обеспечения информационной безопасности" (Пр. 93-х от 25.04.2025).

Литература

1. Kotenko I., Gaifulina D., Zelichenok I. Systematic Literature Review of Security Event Correlation Methods // IEEE Access. 2022. №. 10. С. 43387–43420.

2. Шелухин О.И., Осин А.В., Костин Д.В. Диагностика «здоровья» компьютерной сети на основе секвенциального анализа последовательностных паттернов // T-Comm: Телекоммуникации и транспорт. 2020. № 2. С. 9–16.

3. Жабин А.П., Волкодавова Е.В., Кандрашина (Жабина) Е.А. Управление предпринимательскими рисками, или “Черный лебедь" Covid-19

как тест на антихрупкость // Вестник Самарского государственного экономического университета. 2020. № 3. С. 38–45.

4. Шелухин О.И., Раковский Д.И. Выбор метрических атрибутов редких аномальных событий компьютерной системы методами интеллектуального анализа данных // T-Comm: Телекоммуникации и транспорт. 2021. № 6. С. 40–47.

5. Li Y., Wang K., Tan L., Min F. Label-specific disentanglement and correlation-guided fusion for multi-label classification // Knowledge and Information Systems. 2025. № 6. С. 4991–5017.

6. Shajee Mohan B. S., Mohan S.S. Distance metric learning techniques for the performance improvement of ML-kNN and Ranking-SVM-based multi-label pattern classification // ASEAN Journal on Science and Technology for Development. 2025. № 1. С. 163 – 174.

7. Балыбердин, А. В. Крылов Г. О. Повышение точности выявления аномалий для систем обнаружения вторжения с помощью ансамблевого обучения // Безопасность информационных технологий. 2025. № 1. С. 153-171.

8. Мяличева, А. А., Фатхулин Т.Д. Анализ методов машинного обучения для прогнозирования дефектов в исходном коде // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2024. № 2. С. 16-19.

9. Молодцов Д.А. Мягкая динамическая экстраполяция многозначных зависимостей // Нечеткие системы и мягкие вычисления. 2019. № 1. С. 5–18.

10. Добрышин М.М. Модель разнородных компьютерных атак, проводимых одновременно на узел компьютерной сети связи // Телекоммуникации. 2019. № 12. С. 31–35.

11. Шелухин О.И., Раковский Д.И. Обнаружение компьютерных атак на основе многозначных закономерностей // Методы и технические средства обеспечения безопасности информации. 2024. № 33. С. 36–38.

12. Zhang M.-L., Li Y.-K., Liu X.-Y., Geng X. Binary relevance for multi-label learning: an overview // Frontiers of Computer Science. 2018. № 2. С. 191–202.

13. Рыбаков С.Ю. Методы защиты IoT от атак нулевого дня // Инженерный Вестник Дона. 2025. № 3. URL: ivdon.ru/ru/magazine/archive/n3y2025/9944.

14. Осин А.В., Хализев К.А. Прогнозирование редких событий на основе анализа графлетов взаимодействия в социальных сетях // Инженерный вестник Дона. 2025. № 4. URL: ivdon.ru/ru/magazine/archive/n4y2025/9986.

15. Раковский Д.И. Влияние проблемы многозначности меток классов системных журналов на защищенность компьютерных сетей // Наукоемкие технологии в космических исследованиях Земли. 2023. № 1. С. 48–56.

16. Хализев, К. А. Построение пространства атрибутов для оценки поведенческих аномалий при взаимодействии пользователей с CRM-системой // Инженерный вестник Дона. 2025. № 6. URL: ivdon.ru/ru/magazine/archive/n6y2025/10135

17. Иванникова В.П., Шелухин О.И. Бинарная классификация компьютерных атак на примере базы данных UNSW-NB15 // Телекоммуникации и информационные технологии. 2020. № 1. С. 10–18.

18. Раковский Д.И., Александров И.Д. Предобработка данных табличной структуры для решения задач многозначной классификации компьютерных атак // Инженерный Вестник Дона. 2024. № 12. URL: ivdon.ru/ru/magazine/archive/n12y2024/9670.

19. Молодцов Д.А., Осин А.В. Новый метод применения многозначных закономерностей // Нечеткие системы и мягкие вычисления. 2020. № 2. С. 83–95.

20. Гетьман А.И., Горюнов М.Н., Мацкевич А.Г., Рыболовлев Д.А. Методика сбора обучающего набора данных для модели обнаружения компьютерных атак // Труды института системного программирования РАН. 2021. № 5. С. 83–104.

21. Стригунов, В. В. Выбор средства защиты информации методами многокритериального анализа решений PROMETHEE // Информатика и системы управления. 2024. № 4. С. 48-55.

References

1. Kotenko I., Gaifulina D., Zelichenok I. IEEE Access. 2022. №. 10. pp. 43387–43420.

2. Sheluhin O.I., Osin A.V., Kostin D.V. T-Comm. 2020. № 2. pp. 9–16.

3. Zhabin A.P., Volkodavova E.V., Kandrashina (Zhabina) E.A. Vestnik Samarskogo gosudarstvennogo ekonomicheskogo universiteta. 2020. № 3. pp. 38–45.

4. Sheluhin O.I., Rakovskiy D.I. T-Comm. 2021. № 6. pp. 40–47.

5. Li Y., Wang K., Tan L., Min F. Knowledge and Information Systems. 2025. № 6. pp. 4991–5017.

6. Shajee Mohan B. S., Mohan S.S. ASEAN Journal on Science and Technology for Development. 2025. № 1. pp. 163 – 174.

7. Balyberdin, A. V. Krylov G. O. Bezopasnost' informatsionnykh tekhnologiy. 2025. № 1. pp. 153-171.

8. Myalicheva, A. A., Fatkhulin T.D. Trudy Severo-Kavkazskogo filiala Moskovskogo tekhnicheskogo universiteta svyazi i informatiki. 2024. № 2. pp. 16-19.

9. Molodtsov D.A. Nechetkie sistemy i myagkie vychisleniya. 2019. № 1. pp. 5–18.

10. Dobryshin M.M. Telekommunikatsii. 2019. № 12. pp. 31–35.

11. Sheluhin O.I., Rakovskiy D.I. Metody i tekhnicheskie sredstva obespecheniya bezopasnosti informatsii. 2024. № 33. pp. 36–38.

12. Zhang M.-L., Li Y.-K., Liu X.-Y., Geng X. Frontiers of Computer Science. 2018. № 2. pp. 191–202.

13. Rybakov S.Yu. Inzhenernyj vestnik Dona, 2025. № 3. URL: ivdon.ru/ru/magazine/archive/n3y2025/9944.

14. Osin A.V., Khalizev K.A. Inzhenernyj vestnik Dona, 2025. № 4. URL: ivdon.ru/ru/magazine/archive/n4y2025/9986.

15. Rakovskiy D.I. H&ES. 2023. № 1. pp. 48–56.

16. Khalizev K.A. Inzhenernyj vestnik Dona. 2025. № 6. URL: ivdon.ru/ru/magazine/archive/n6y2025/10135

17. Ivannikova V.P., Shelukhin O.I. Telekommunikatsii i informatsionnye tekhnologii. 2020. № 1. pp. 10–18.

18. Rakovskiy D.I. Aleksandrov I.D. Inzhenernyj vestnik Dona, 2024. № 12. URL: ivdon.ru/ru/magazine/archive/n12y2024/9670.

19. Molodtsov D.A., Osin A.V. Nechetkie sistemy i myagkie vychisleniya. 2020. № 2. pp. 83–95.

20. Get'man A.I., Goryunov M.N., Matskevich A.G., Rybolovlev D.A. Trudy instituta sistemnogo programmirovaniya RAN. 2021. № 5. pp. 83–104.

21. Strigunov, V. V. Informatika i sistemy upravleniya. 2024. № 4. pp. 48-55.

Дата поступления: 12.09.2025

Дата публикации: 26.10.2025