Инженерный вестник Дона, №7 (2025)
ivdon.ru/ru/magazine/archive/n7y2025/10218

Оценка размерности атрибутного пространства в условиях многозначной классификации

Д.И. Раковский, И.Д. Александров

Московский технический университет связи и информатики

Аннотация: Рассматриваются особенности оценки размерности атрибутного пространства в контексте многозначной классификации компьютерных атак. Объектом исследования является табличное представление данных, собранное с использованием программно-аппаратного комплекса, предназначенного для имитационного моделирования многозначных компьютерных атак. Исследуется влияние многозначных зависимостей, проявляющихся в одновременной реализации нескольких типов компьютерных атак на компьютерную сеть, на результаты оценки информативности атрибутного пространства и точность классификации на примере алгоритма Random Forest. Практическая значимость работы заключается в повышении точности обнаружения и классификации компьютерных атак за счёт учёта многозначных зависимостей атрибутов.
Ключевые слова: информационная безопасность, машинное обучение, многозначная классификация, многозначная зависимость, сетевой трафик, оценка информативности, энтропия, целевой атрибут, multi-label dependencies, multi-label, multi-label classification, метрики, экспериментальные данные, атрибуты

Введение

Современные компьютерные сети (КС) порождают разнородные и многомерные наборы данных, ассоциированные с элементами, входящими в их состав [1,2]. Данные агрегируют с системных журналов, сетевых карт, системных датчиков, установленных на каждом из хостов; перечня установленных программ или установочных файлов.

Согласно последним исследованиям, современные КС обладают свойством самоорганизации [3], проявляющееся в их способности динамически адаптироваться к изменениям среды, перераспределять ресурсы и оптимизировать свою структуру без прямого вмешательства человека. Одновременно с усложнением структуры самоорганизующихся сетей, усложняются и компьютерные атаки – как по сложности исполнения, так и по задействованным технологиям [4]. Вследствие роста таких атак, важно

иметь возможность отслеживать их одновременную реализацию на компьютерную сеть при создании систем обнаружения [5].

Это, в свою очередь, усложняет их анализ и требует разработки нового научно-методологического аппарата обеспечения защищенности таких сетей [6-8], включая ввод и проработку новых терминов в технической сфере [9]. Это свойство обеспечивается за счёт внедрения распределённых алгоритмов распределения сетевой нагрузки, технологий машинного обучения [10, 11], учитывающих как состояния исследуемой системы, так и внешние воздействия [12, 13]. Отдельно необходимо обратить внимание на интенсивное развитие технологий искусственного интеллекта [14–16].

В настоящее время развивается сфера многозначной классификации в контексте решения задач информационной безопасности. Одной из важных особенностей успешного выполнения многозначной классификации является корректное представление многозначных зависимостей, часто скрытых в наборах данных [4].

Под многозначной зависимостью понимается одновременное соответствие нескольких маркеров *состояний* одному *объекту*. Под *объектом* понимается КС или ее часть, характеризуемая набором значений её атрибутов; а под *состоянием* – характеристика объекта, используемая для решения задачи обеспечения информационной безопасности.

В настоящее время наиболее известными моделями представления многозначных зависимостей являются модели бинарного представления данных (от англ. *Binary relevance*) [17].

Целью работы является исследование влияния многозначных зависимостей при оценке размерности атрибутного пространства в наборах данных на точность многозначной классификации.

Описание проведенного эксперимента

В ранее проводимых исследованиях рассматривалась топология T исследуемой КС в виде двух множеств хостов [18]:

$$T = \left\{VH_i; i = \overline{1,I}\right\} \cup \left\{AH_j; j = \overline{1,J}\right\} \cup DAS \cup Router, \quad (1)$$

где VH_i – i-й атакуемый хост; AH_j – j-й атакующий хост; DAS – сервер агрегации данных; $Router$ – маршрутизатор.

В рамках предыдущих исследований, введен перечень контролируемых компьютерных атак AL, которые атакующие хосты AH_j способны реализовать на атакуемые хосты VH_i:

$$AL = \left\{attack_k; k = \overline{1,K}\right\}. \quad (2)$$

На основании введенной формализации разработан программно-аппаратный комплекс [19] (ПАК) для имитационного моделирования многозначных компьютерных атак.

Собранные при помощи ПАК данные предобрабатывались и приводились к модели табличного представления функционирования сети. Модель представляет собой объединение двух таблиц: атрибутов размером Λ (столбцов) N (строк) $\boldsymbol{A}$, и таблицы целевых атрибутов (классовых меток) размером Ξ (столбцов) N (строк) $\boldsymbol{L}$:

$$\boldsymbol{D}_{NM} = \left\{\left(\boldsymbol{A}(n,\ ), \boldsymbol{L}(n,\ )\right); \boldsymbol{A} = \left(a_{n\lambda}\right), \boldsymbol{L} = \left(l_{n\xi}\right), \lambda = \overline{1,\Lambda}, \xi = \overline{1,\Xi}, n = \overline{1,N}, M = \Lambda + \Xi\right\}, \quad (3)$$

где $\boldsymbol{A}(n,\ ) = (a_{n1}, a_{n2}, \dots, a_{n\Lambda})$ - n-ный вектор-строка матрицы атрибутов экспериментальных данных $\boldsymbol{A}$, состоящая из Λ столбцов. Элемент этой строки, $a_{ni} \in \boldsymbol{A}(n,\ )$, означает метрическое значение λ-го атрибута на n-ой строке экспериментальных данных, например, связанного с загрузкой оперативной памяти хоста; $\boldsymbol{L}(n,\ ) = (l_{n1}, l_{n2}, \dots, l_{n\Xi})$ - n-ый вектор-строка матрицы целевых атрибутов (классовых меток) экспериментальных данных $\boldsymbol{L}$, состоящая из Ξ столбцов; $l_{n\xi} \in \boldsymbol{L}(n,\ ); \xi = \overline{1,\Xi}, n = \overline{1,N},$, означает значение ξ-го целевого атрибута (классовой метки) на n-той строке экспериментальных данных (например, бинарное значение о совершении компьютерной атаки

типа «Отказ в обслуживании» (от англ. *Denial of Service*)); N – количество записей экспериментальных данных; M – совокупное количество столбцов в (3), $M = \Lambda + \Xi$.

Идея модели основана на методе представления многозначных данных *Binary Relevance* и требует тождественности Ξ (столбцов) количеству уникальных компьютерных атак.

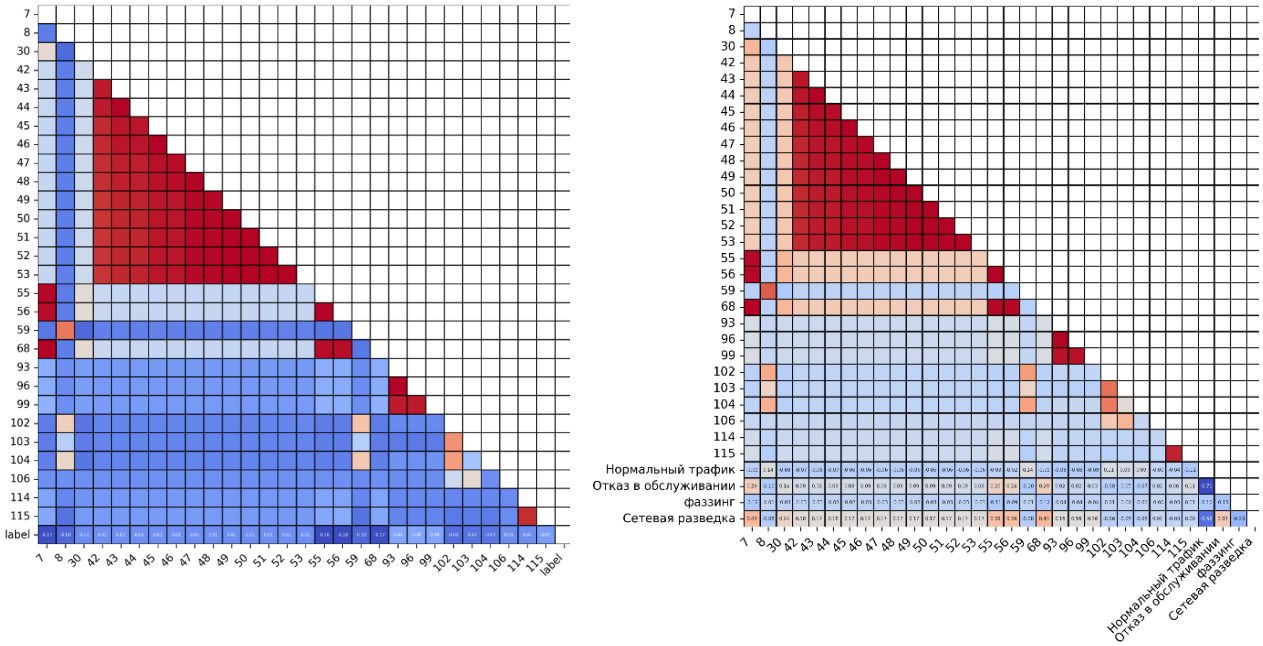
В контексте поставленной цели данные представлялись либо по модели (3), где размерность пространства целевых атрибутов $\Xi > 1$, либо по классической модели представления однозначных данных с одним целевым атрибутом [20,21].

Дальнейшее исследование направлено на оценку влияния модели представления данных (3) на информативность атрибутов в условиях изменяющейся атрибутной размерности.

Результаты оценки информативности атрибутного пространства в условиях многозначной классификации

Проведено исследование влияния многозначных зависимостей на информативность атрибутов набора данных, собранного при помощи программно-аппаратного комплекса [19]. Как известно, информационная значимость атрибутов вычисляется относительно целевого атрибута [22]. В случае однозначного представления данных, целевым атрибутом является столбец с классовыми метками - значимость каждого атрибута вычисляется относительно него. В условиях учёта многозначных зависимостей в моделях, основанных на методе *Binary Relevance*, количество целевых атрибутов увеличивается (см. (3)).

Наглядно эта разница может быть показана на примере сравнения корреляционных диаграмм, построенных для собранных ранее данных с ПАК [19] (см. рис. 1).



а) б)

Рис. 1 – Корреляционная диаграмма для: a) табличного представления данных без учета многозначных зависимостей (посредством бинарного преобразования); b) табличного представления данных, учитывающего многозначные зависимости.

Так, при построении корреляционной диаграммы для однозначного представления табличных данных (рис. 1а), корреляция каждого атрибута оценивается относительно единственного целевого атрибута *label*. В модели, учитывающей многозначные зависимости (рис. 1б), корреляция рассчитывается между каждым атрибутом и каждым целевым атрибутом отдельно, что влияет не только на численные значения оценки корреляции, но и на размерность корреляционной диаграммы.

Разные целевые атрибуты имеют разное численное значение корреляции с атрибутным пространством. Из этого следует, что для

классификации каждого известного типа компьютерных атак (в контексте парадигмы контролируемого обучения [23]), важно собственное «подмножество» атрибутов, наиболее точно характеризующее атаку. Многозначные зависимости же усложняют выделение таких подмножеств, поскольку предполагают одновременную реализацию сразу нескольких компьютерных атак на хост.

В табл. 1 приведены численные значения корреляции между целевыми атрибутами табличного представления данных, учитывающего многозначные зависимости для набора данных, собранного с использованием ПАК.

Таблица № 1

Фрагмент корреляционной диаграммы для набора данных, собранного с использованием ПАК

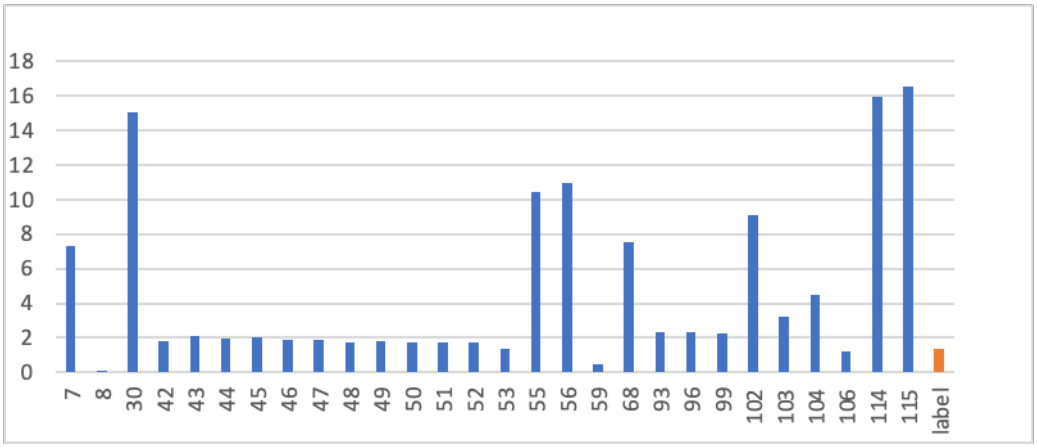
	Штатное функционирование КС	**Отказ в обслуживании**	**фаззинг**	**Сетевая разведка**
Штатное функционирование КС	1	-0,70107	-0,10147	-0,55522
Отказ в обслуживании	-0,70107	1	-0,14721	0,328155
фаззинг	-0,10147	-0,14721	1	-0,23121
Сетевая разведка	-0,55522	0,328155	-0,23121	1

Из фрагмента видно, что целевые атрибуты не являются независимыми, что, потенциально, может быть использовано при исследовании влияния многозначных зависимостей на свойства данных. К примеру, из табл. 1 видно, что целевой атрибут, связанный с состоянием штатного функционирования КС, имеет высокую отрицательную корреляцию со всеми остальными целевыми атрибутами, что соответствует плану проведения эксперимента с использованием ПАК. Атаки типов «отказ в обслуживании» и «сетевая разведка», наоборот, высоко скоррелированны

между собой, что также соотносится с расписанием проведения контролируемых компьютерных атак (см. [19]).

В рамках проведенного эксперимента оценена энтропия по каждому атрибуту, включая целевые, для двух случаев: данные в табличном представлении без учета многозначных зависимостей (рис. 2а) и данные в табличном представлении, учитывающие многозначные зависимости (рис. 2б).

а)



б)

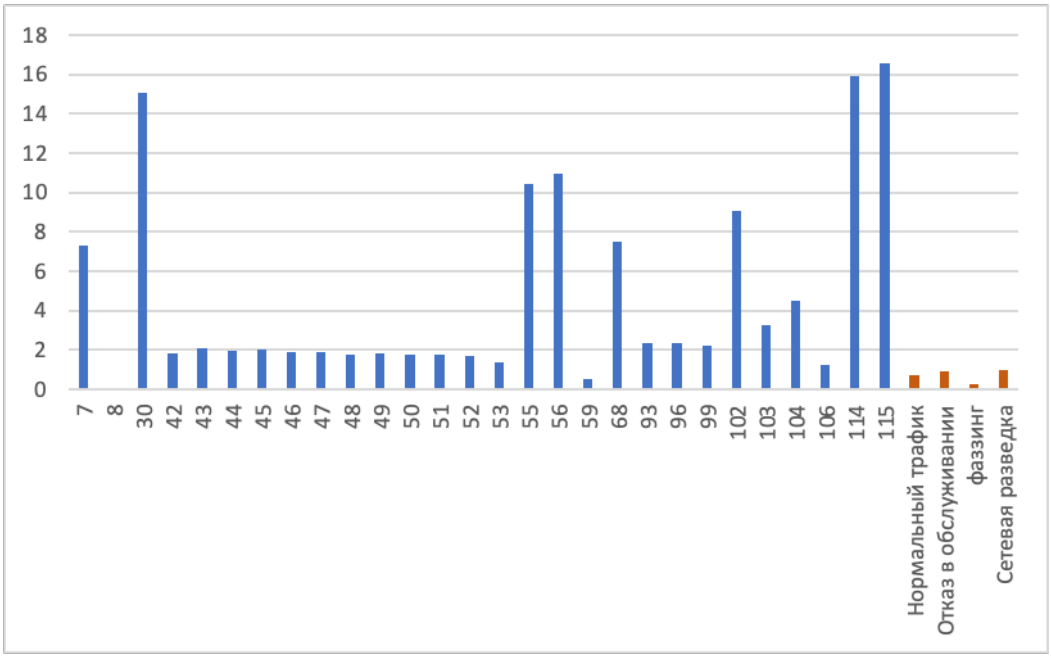


Рис. 2 – Оценка энтропии для: а) табличного представления данных без учета многозначных зависимостей; б) табличного представления данных, учитывающего многозначные зависимости.

Как видно из гистограмм на рис. 2, энтропия не изменяется для атрибутов, связанных с функционированием КС, но различна для целевых атрибутов.

В результате проведенного анализа двух случаев представления данных, выявлено различие энтропии целевых атрибутов (табл. 2). Из таблицы видно, что сумма энтропии по целевым атрибутам в случае многозначного представления данных не равна энтропии единственного целевого атрибута при однозначном представлении данных.

Таблица № 2

Информационная значимость целевых меток в наборах данных.

Классовая метка	**Энтропия (**	**Сумма**
Штатное функционирование КС	0,71	**2,86**
Отказ в обслуживании	0,91	
Фаззинг	0,24	
Сетевая разведка	0,99	
label	1,34	**1,34**

Разница в сумме энтропии по целевым атрибутам в случае многозначного представления данных по сравнению с однозначным представлением более, чем в два раза, сигнализирует о наличии синергического эффекта от реализации отдельных компьютерных атак, образующих многозначную зависимость.

Для оценки влияния многозначных зависимостей на точность классификации, использован алгоритм ансамблевой классификации *Random Forest*. Проведен эксперимент, заключающийся в классификации компьютерных атак в ранее собранном наборе данных в одинаковых условиях. Рассматривалось два случая: набор данных представлен в «классическом» виде с одним целевым атрибутом, многозначные зависимости игнорируются; набор данных представлен в виде модели (3), учитывающей многозначные зависимости.

Для модели, учитывающей многозначные зависимости, использовалась многозначная реализация алгоритма *Random Forest*. Для оценки точности классификаторов выбран набор метрик $\Phi^{it} = \{Accuracy, Precision, Recall, F_1, AUC\}$. Визуализация метрик оценки точности выполнялась посредством построения диаграммы типа «радар».

Результаты классификации представлены на рисунке 3. Рассматривалось четыре возможных результата классификации: «штатное функционирование КС» (рис. 3а), атака типа «отказ в обслуживании» (рис. 3б), атака типа «сетевая разведка» (рис. 3в), атака типа «фаззинг» (рис. 3г). Синим цветом на график нанесены результаты классификации с использованием модели, учитывающей многозначные зависимости. Оранжевым цветом на график нанесены результаты классификации с использованием «классической» однозначной реализации алгоритма *Random Forest*.

Из диаграмм видно, что многозначная реализация алгоритма *Random Forest* успешнее однозначной при классификации компьютерных атак типов «отказ в обслуживании» (на 6%) и «сетевая разведка» (на 13%), что связано с их частой совместной реализацией на атакуемый хост.

Однозначная реализация алгоритма *Random Forest* же успешнее классифицирует состояние штатного функционирования КС (выигрыш до 2%) и атаку типа «фаззинг» (до 3%).

Отметим, что состояние штатного функционирования всегда однозначно, поскольку в ином случае на сеть совершается компьютерная атака. Выигрыш многозначной реализации *Random Forest* обуславливается за счет наличия ошибок первого и второго рода при классификации именно компьютерных атак, т.к. они отчасти многозначные.

Выигрыш в классификации атаки типа «фаззинг» обусловлен существенным классовым дисбалансом и слабой представленностью записей, маркированных данным типом атаки, в данных.

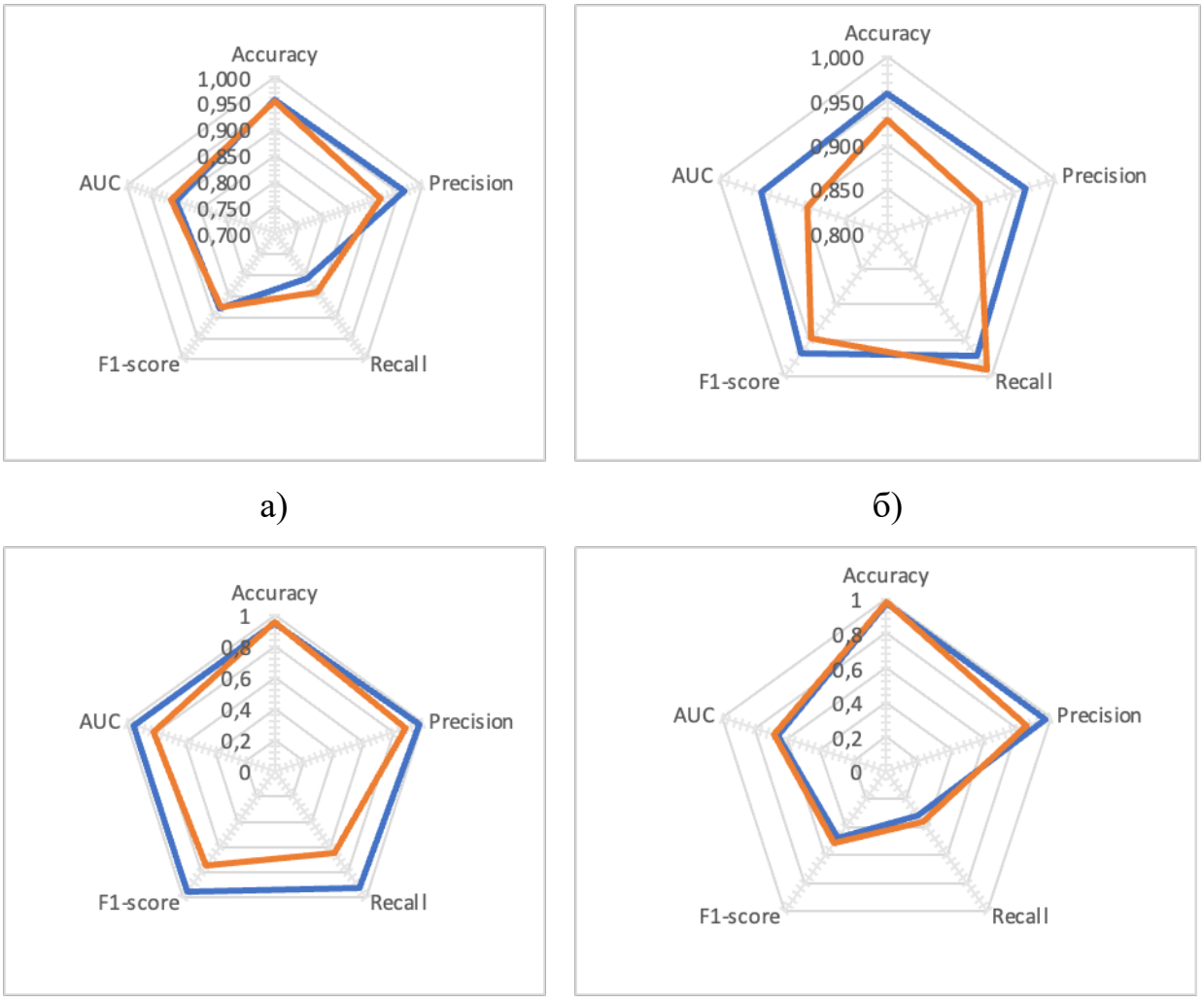


Рис. 3 – Визуализация набора метрик Φ^{it} для: a) штатного функционирования КС; b) для компьютерных атак типа «отказ в обслуживании»; c) для компьютерных атак типа «сетевая разведка»; d) для компьютерных атак типа «фаззинг».

Заключение

Проведена оценка влияния многозначных зависимостей на размерность атрибутивного пространства. Анализ включал построение корреляционных диаграмм с использованием коэффициента Пирсона и энтропии для двух представлений данных.

В данных, учитывающих многозначные зависимости, суммарная энтропия по целевым атрибутам (2.86) более чем вдвое превышает аналогичный показатель для данных с однозначным представлением (1.34). Это свидетельствует о наличии синергетического эффекта, возникающего при одновременном проведении нескольких компьютерных атак.

Для оценки влияния многозначных зависимостей на точность классификации, использован алгоритм ансамблевой классификации *Random Forest*. Проведен эксперимент, заключающийся в классификации компьютерных атак в ранее собранном наборе данных в одинаковых условиях. Рассматривалось два случая: набор данных представлен в «классическом» виде с одним целевым атрибутом, многозначные зависимости игнорируются; набор данных представлен в виде модели, учитывающей многозначные зависимости. Выявлено, что многозначная реализация алгоритма *Random Forest* успешнее однозначной при классификации компьютерных атак типов «отказ в обслуживании» (на 6%) и «сетевая разведка» (на 13%), что связана с их частой совместной реализацией на атакуемый хост. Выигрыш многозначной реализации *Random Forest* обуславливается за счет наличия ошибок первого и второго рода при классификации именно компьютерных атак, т.к. они отчасти многозначные. Выигрыш в классификации атаки типа «фаззинг» обусловлен существенным классовым дисбалансом и слабой представленностью записей, маркированных данным типом атаки, в данных.

Однозначная реализация алгоритма *Random Forest* же успешнее классифицирует состояние штатного функционирования КС (выигрыш до 2%) и атаку типа «фаззинг» (до 3%).

Полученные различия в результатах классификации подтверждают необходимость учета многозначных зависимостей для более точного обнаружения и анализа сложных и комбинированных атак.

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. Полтавцева М.А., Зегжда Д.П. Анализ гетерогенных прецедентов в задачах информационной безопасности // Методы и технические средства обеспечения безопасности информации. 2022. № 31. С. 4–6.

2. Шелухин О.И., Зегжда Д.П., Раковский Д.И., Самарин Н.Н., Александрова (Маховенко) Е.Б. Интеллектуальные технологии информационной безопасности. НТИ «Горячая линия - Телеком», 2023. 384 с.

3. Павленко Е.Ю. Показатели киберустойчивости для самоорганизующихся киберфизических систем // Методы и технические средства обеспечения безопасности информации. 2024. № 33. С. 30–32.

4. Раковский Д.И. Многозначная классификация сетевых атак методами машинного обучения: дисс.. канд. технич. наук. Санкт-Петербург, 2025. 170 с.

5. Зегжда Д.П. и др. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. М.: Научно-техническое издательство «Горячая линия-Телеком». 2023. 560 с.

6. Штеренберг С.И., Севостьянов В.А., Бударный Г.С. Уникальные направления атак на искусственный интеллект и нейронные сети // Вестник

Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2024. № 2. С. 103–112с. DOI: 10.46418/2079-8199_2024_2_19.

7. Шенец Н.Н. Способ защиты данных пользователей мобильных устройств на основе многофакторной аутентификации, визуальной криптографии и стеганографии // Проблемы информационной безопасности. Компьютерные системы. 2023. № 1 (53). С. 26–36с. DOI: 10.48612/jisp/rm3r-3f2m-a1kp.

8. Ageev A., Konstantinov A., Utkin L. ADA-NAF: Semi-Supervised Anomaly Detection Based on the Neural Attention Forest // IA. 2025. Т. 24, № 1. С. 329–357с. DOI: 10.15622/ia.24.1.12.

9. Звежинский С.С., Духан Е.И. Понятия и термины научных исследований в технической сфере // Правовая информатика. 2024. № 4. С. 89–96с. DOI: 10.24412/1994-1404-2024-4-89-96.

10. Леохин Ю.Л., Фатхулин Т.Д., Кожанов М.С. Анализ и исследование применения нейросетевых технологий для генерации программного кода // Вестник Рязанского государственного радиотехнического университета. 2024. № 87. С. 41–53с. DOI: 10.21667/1995-4565-2024-87-41-53.

11. Гусева О.А., Раковский Д.И., Симонян А.Г. Предобработка данных для решения задач классификации методом машинного обучения // Системы синхронизации, формирования и обработки сигналов. 2023. Т. 14, № 2. С. 20–24.

12. Хализев К.А., Осин А.В. Прогнозирование редких событий безопасности с использованием данных социальных сетей // Московский государственный технический университет им. Н.Э. Баумана (национальный исследовательский университет). 2024. С. 205–206.

13. Осин А.В., Мурашко Ю.В., Суворов В.И. Поведенческие характеристики взаимодействия с сенсорным экраном для идентификации пользователей мобильных устройств // Инженерный Вестник Дона. 2024. № 12 (120) URL: ivdon.ru/ru/magazine/archive/n12y2024/9687.

14. Котенко И.В., Дун Х. Обнаружение атак в интернете вещей на основе многозадачного обучения и гибридных методов сэмплирования // Вопросы кибербезопасности. 2024. Т. 60, № 2. С. 10–21с. DOI: 10.21681/2311-3456-2024-2-10-21.

15. Емец Л.В., Большаков А.С. Обнаружение фишингового сайта методами машинного обучения // Телекоммуникации И Информационные Технологии. 2023. Т. 10, № 1. С. 36–43.

16. Шелухин О.И., Рыбаков С.Ю., Ванюшина А.В. Оценка характеристик мультифрактального спектра фрактальной размерности сетевого трафика и компьютерных атак в IoT // Труды Учебных Заведений Связи. 2024. Т. 10, № 3. С. 104–115с. DOI: 10.31854/1813-324X-2024-10-3-104-115.

17. Sheluhin O.I., Rakovskiy D.I. Multi-Label learning in computer networks // 2023 Systems of signals generating and processing in the field of on board communications. Moscow, Russian Federation: IEEE, 2023. С. 1–5с. DOI: 10.1109/IEEECONF56737.2023.10092157.

18. Раковский Д.И., Александров И.Д. Разработка экспериментального стенда для моделирования сетевых атак на компьютерную систему в контролируемых условиях // Сборник трудов научно-технической конференции «Управление и безопасность информации в киберфизических системах». М.: МТУСИ. 2023. С. 111–117.

19. Шелухин О.И., Раковский Д.И. Разработка программно-аппаратного комплекса моделирования многозначных компьютерных атак //

Вопросы кибербезопасности. 2024. № 4 (62). С. 116–130с. DOI: 10.21681/2311-3456-2024-4-116-130.

20. 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.

21. Шелухин О.И., Раковский Д.И. Обнаружение компьютерных атак на основе многозначных зависимостей // Материалы Всероссийской научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 2024. Т. 33, № 1. С. 36–38.

22. Murphy K.P. Probabilistic machine learning: an introduction. Cambridge, Massachusetts: The MIT Press, 2022. 826 с.

23. Schmidhuber J. Deep learning in neural networks: An overview // Neural Networks. 2015. Т. 61. С. 85–117с. DOI: 10.1016/j.neunet.2014.09.003.

References

1. Poltavtseva M.A., Zegzhda D.P. Metody i tekhnicheskie sredstva obespecheniya bezopasnosti informatsii. 2022. № 31. pp. 4–6.

2. Shelukhin O.I., Zegzhda D.P., Rakovskiy D.I., Samarin N.N., Aleksandrova (Makhovenko) E.B. Intellektualnye tekhnologii informatsionnoy bezopasnosti [Intelligent Information Security Technologies]. NTI «Goryachaya liniya - Telekom», 2023. 384 p.

3. Pavlenko E.Y. Metody I Tekhnicheskie sredstva obespecheniya bezopasnosti informatsii. 2024. № 33. pp. 30–32.

4. Rakovskiy D.I. Mnogoznachnaya klassifikatsiya setevykh atak metodami mashinnogo obucheniya: diss. kand. tekhn. nauk [Multi-valued classification of network attacks by machine learning methods: PhD diss.]. St. Peterburg, 2025. 170 p.

5. Zegzhda D.P. et al. Kiberbezopasnost' tsifrovoy industrii. Teoriya i praktika funktsional'noy ustoychivosti k kiberatakam [Cybersecurity of the digital industry. Theory and practice of functional resistance to cyber attacks]. M.: Nauchno-tekhnicheskoe izdatelstvo «Goryachaya liniya-Telekom», 560 p.

6. Shterenberg S.I., Sevostyanov V.A., Budarnyy G.S. Vestnik sankt-peterburgskogo gosudarstvennogo universiteta tekhnologii i dizayna. Seriya 1: Estestvennye i tekhnicheskie nauki. 2024. № 2. pp. 103–112.

7. Shenets N.N. Problemy informatsionnoy bezopasnosti. Komp'yuternye sistemy. 2023. № 1 (53). pp. 26–36. DOI: 10.48612/jisp/rm3r-3f2m-a1kp.

8. Ageev A., Konstantinov A., Utkin L. ADA-NAF: Semi-supervised anomaly detection based on the neural attention forest. IA. 2025. Vol. 24, № 1. pp. 329–357. DOI: 10.15622/ia.24.1.12.

9. Zvezhinskiy S.S., Dukhan E.I. Pravovaya informatika. 2024. № 4. pp. 89–96. DOI: 10.24412/1994-1404-2024-4-89-96.

10. Leokhin Yu.L., Fatkhulin T.D., Kozhanov M.S. Vestnik ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta. 2024. № 87. pp. 41–53. DOI: 10.21667/1995-4565-2024-87-41-53.

11. Guseva O.A., Rakovskiy D.I., Simonyan A.G. Sistemy sinkhronizatsii, formirovaniya i obrabotki signalov. 2023. Vol. 14, № 2. pp. 20–24.

12. Khalizev K.A., Osin A.V. Moskovskiy gosudarstvennyy tekhnicheskiy universitet im. N.E. Baumana (natsional'nyy issledovatel'skiy universitet). 2024. pp. 205–206.

13. Osin A.V., Murashko Yu.V., Suvorov V.I. Inzhenernyj Vestnik Dona, 2024, № 12. URL: ivdon.ru/ru/magazine/archive/n12y2024/9687.

14. Kotenko I.V., Dun H. Voprosy kiberbezopasnosti. 2024. Vol. 60, № 2. pp. 10–21. DOI: 10.21681/2311-3456-2024-2-10-21.

15. Emets L.V., Bolshakov A.S. Telekommunikatsii I Informatsionnye Tekhnologii. 2023. Vol. 10, № 1. pp. 36–43.

16. Sheluhin O.I., Rybakov S.Yu., Vanyushina A.V. Trudy Uchebnykh Zavedeniy Svyazi. 2024. Vol. 10. № 3. pp. 104–115. DOI: 10.31854/1813-324X-2024-10-3-104-115.

17. Sheluhin O.I., Rakovskiy D.I. Multi-label learning in computer networks. 2023 systems of signals generating and processing in the field of on board communications. Moscow, Russian Federation: IEEE, 2023. pp. 1–5. DOI: 10.1109/IEEECONF56737.2023.10092157.

18. Rakovskiy D.I., Aleksandrov I.D. Sbornik trudov nauchno-tekhnicheskoy konferentsii «Upravlenie i bezopasnost' informatsii v kiberfizicheskikh sistemakh». M.: MTUCI. 2023. pp. 111–117.

19. Sheluhin O.I., Rakovskiy D.I. Voprosy kiberbezopasnosti. 2024. № 4 (62). pp. 116–130. DOI: 10.21681/2311-3456-2024-4-116-130.

20. Rakovskiy D.I., Aleksandrov I.D. Inzhenernyj Vestnik Dona, 2024, № 12 (120) URL: ivdon.ru/ru/magazine/archive/n12y2024/9670.

21. Sheluhin O.I., Rakovskiy D.I. Materialy Vserossiyskoy nauchno-tekhnicheskoy konferentsii «Metody i tekhnicheskie sredstva obespecheniya bezopasnosti informatsii». 2024. Vol. 33, № 1. pp. 36–38.

22. Murphy K.P. Probabilistic machine learning: an introduction. Cambridge, Massachusetts: The MIT Press, 2022. 826 p.

23. Schmidhuber J. Deep learning in neural networks: An overview. Neural Networks. 2015. Vol. 61. pp. 85–117. DOI: 10.1016/j.neunet.2014.09.003.

Дата поступления: 6.05.2025

Дата публикации: 25.06.2025