Инженерный вестник Дона, №12 (2024)
ivdon.ru/ru/magazine/archive/n12y2024/9670

Предобработка данных табличной структуры для решения задач многозначной классификации компьютерных атак

Д.И. Раковский, И.Д. Александров
Московский технический университет связи и информатики

Аннотация: Рассматривается разработка и применение методов предварительной обработки табличных данных для решения задач многозначной классификации компьютерных атак. Объектом исследования является набор данных, содержащий многозначные записи, собранный при помощи разработанного авторами программно-аппаратного комплекса. Проведен анализ атрибутов набора данных, в ходе которого были выявлены 28 атрибутов, имеющих наибольшую информационную важность при их использовании для классификации алгоритмами машинного обучения. Обоснована целесообразность использования автокодировщиков в области информационной безопасности, в задачах, связанных с наборами данных, обладающих свойством многозначности целевых атрибутов. Практическая значимость: предварительная обработка данных может быть использована для повышения точности обнаружения и классификации многозначных компьютерных атак.

Ключевые слова: информационная безопасность, компьютерные атаки, multi-label, multi-label classification, многозначная классификация, анализ набора данных, сбор экспериментальных данных, многозначные данные, сетевые атаки, информационная безопасность.

Введение

Обеспечение информационной безопасности компьютерных сетей является комплексной задачей, которая решается с помощью различных подходов. Одним из разделов обеспечения информационной безопасности (далее ИБ) в компьютерных сетях является разработка систем обнаружения вторжений, позволяющих обнаруживать компьютерные атаки (далее КА) в сетевом трафике. С ростом объемов межсетевого взаимодействия и комплексности сетей, увеличивается количество угроз и вероятных векторов атаки на компьютерные сети [1, 2]. Злоумышленниками предпринимаются новые способы деструктивного воздействия на сеть, в том числе, и при помощи проведения комбинированных КА – одновременной атаки на один или несколько узлов компьютерных сетей.

Возможность обнаружения таких атак может быть достигнута за счет применения методов многозначной классификации алгоритмами и методами машинного обучения [3, 4].

Актуальность работы обусловлена современным состоянием компьютерных сетей, особенностями реализации на них комбинированных КА, а также сбора с них диагностической информации. Вследствие роста таких атак, важно иметь возможность отслеживать их одновременную реализацию на компьютерную сеть при создании систем обнаружения вторжений.

Целью работы является анализ и предобработка данных, полученных в ходе проведения имитационного моделирования КА на компьютерных сетях в условиях многозначности целевых атрибутов (классовых меток), маркирующих тип КА.

Актуальность задачи многозначной классификации в области ИБ

Под многозначностью целевых атрибутов будем понимать одновременное соответствие нескольких классовых меток одному объекту.

Многозначные данные могут быть обнаружены и в классических наборах, связанных с областью ИБ. Малое количество наборов данных, собранных в целях апробации алгоритмов многозначной классификации КА, находящихся в открытом доступе, актуализируют разработку и реализацию программно-аппаратного комплекса (ПАК) (см. [5,6]) для сбора телеметрии и имитационного моделирования многозначных КА. Как показано в работе [7], зафиксирован синергетический эффект [8] от учета многозначности классовых меток, проявляющийся в повышении точности классификации по таким метрикам, как *ROC AUC (от англ. Area Under Curve), F-мера (от англ. F-score).*

Известны «классические» базы данных, широко используемые для разработки систем обнаружения вторжений, в которых проявляется многозначность целевых атрибутов [9]. Данный факт, как правило, не учитывается как авторами наборов данных, так и разработчиками систем обнаружения вторжений. Выявление многозначности классовых меток может

выполняться при помощи поиска полных дубликатов по атрибутному пространству, за исключением целевых атрибутов.

Приведем алгоритм «поиск дубликатов», состоящий из 4-х шагов. На первом шаге целевые атрибуты преобразуются в бинарное представление. На втором шаге в исходной двухмерной таблице атрибутов производится поиск дубликатов с игнорированием целевых атрибутов (столбца с классовыми метками). Третий шаг – группировка обнаруженных дубликатов методом «полного совпадения всех значений», игнорируя целевые атрибуты. Четвертый шаг – выполнение операции «логическое ИЛИ» по целевым атрибутам в каждой группе дубликатов.

Как только все дубликаты будут обнаружены, необходимо проанализировать целевой атрибут. Если одинаковым записям будут соответствовать разные классовые метки – то значит набор данных обладает свойством многозначности классовых меток.

Таблица № 1

Результаты эксперимента поиска дубликатов для определения доли многозначных записей в наборах данных, связанных с ИБ

Наименование авторского набора данных	**(I)**	**(II)**	**(III)**	**(IV)**	**(V)**
SR-BH 2020	24	14	1	1,2	1,3
UNSW-NB15	45	10	16	18	37
Kitsune *	115	10	0	0	$4 \cdot 10^{-4}$%
NF-UQ-NIDS **	46	21	$5 \cdot 10^{-3}$	42	86

Проведено сравнение наборов данных, связанных с ИБ, находящихся в свободном доступе. Результаты анализа сведены в таблице 1. Проведено два эксперимента: сокращение размерности не проводилось (данные исследовались «как есть»); сокращение размерности проводилось до 10 и 5 наиболее значимых атрибутов. Целью эксперимента являлось исследование изменения доли многозначных записей при уменьшении размерности атрибутного пространства. Актуальность эксперимента обусловлена

распространенностью выполнения указанной операции исследователями данных для экономии вычислительных мощностей и удаления малозначимых атрибутов.

Обозначения, приводимые в таблице: (I) – Кол-во атрибутов в наборе данных, ед.; (II) – Количество уникальных классовых меток, ед.; (III) – Процент многозначных записей (без сокращения размерности); (IV) – Процент многозначных записей (10 наиболее информативных атрибутов); (V) – Процент многозначных записей (5 наиболее информативных атрибутов).

Проблема многозначности целевых атрибутов особенно актуальна в задачах обучения с учителем; данная проблема наиболее часто встречается при преобразовании данных. Потеря информации, возникающая в ходе применения однозначных классификаторов, может являться критичной при решении задач информационной безопасности.

Описание эксперимента и структура собранных данных

Топология T исследуемой компьютерной сети можно представить в виде двух множеств:

$$T = \left\{VH_i; i = \overline{1,I}\right\} \cup \left\{AH_j; j = \overline{1,J}\right\} \cup DAS \cup Router\ , \quad (1.1)$$

где: VH_i – i-й атакуемый хост; AH_j – j-й хост далее – атакующий хост; DAS – сервер агрегации данных; $Router$ – маршрутизатор сети. Предполагается проведение контролируемой компьютерной атаки на VH_i с атакующих хостов.

Введем в рассмотрение перечень контролируемых КА AL:

$$AL = \left\{attack_k; k = \overline{1,K}\right\}. \quad (1.2)$$

Каждая КА описывается рядом статичных $attack_k$ и варьируемых $vattack_k$ параметров - $AoI_k : attack_k \cup vattack_k$. Параметры $attack_k : \left\langle params_{l_k} \right\rangle; pl_k = \overline{1,PL_k}$ являются общими для каждой реализации КА. Общее число параметров атаки PL_k варьируется в зависимости от специфики КА [10, 11].

Графическое представление структуры ПАК представлено на рисунке 1. На рисунке зеленым цветом выделены атакуемые хосты; синим цветом – атакующие. Сервер *DAS* выделен красным цветом; ниже приводится детализация содержимого базы данных. В правом нижнем углу схемы приводится иллюстрация варьируемых параметров контролируемых компьютерных атак, которые возможно задавать при помощи ПАК.

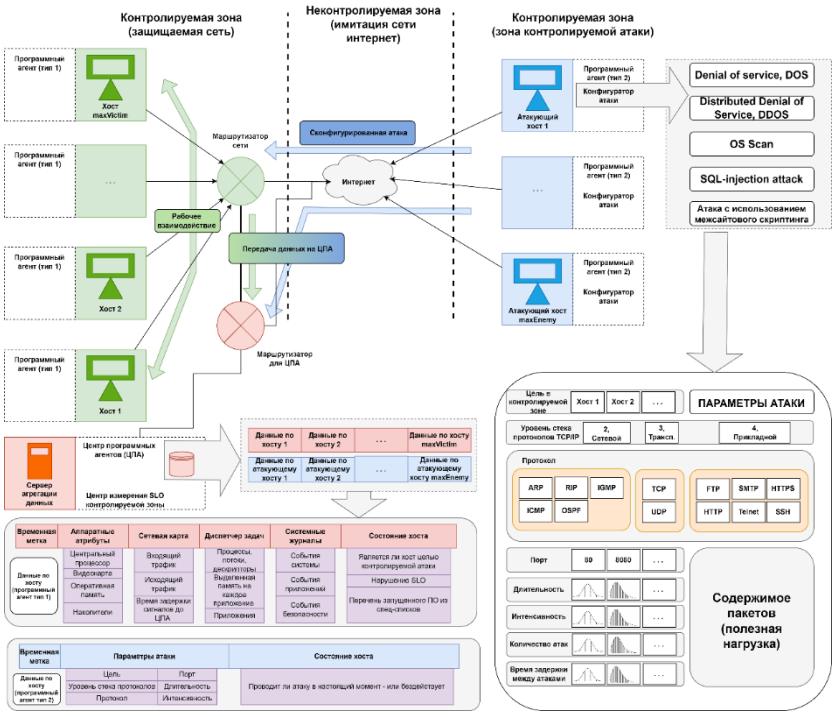

Рис. 1. – Графическое представление структуры ПАК

Анализ *многозначности* собираемых данных продемонстрируем на примере визуализации расписания контролируемых компьютерных атак. Визуализация представляет собой 24-часовую сетку с часовым интервалом (0:00–23:00). Каждый час может содержать одну или несколько контролируемых компьютерных атак шести различных типов. Цветовая кодировка указывает на наличие (светло-серый) или отсутствие (белый) атак в конкретный час. Каждый атакующий хост способен осуществлять атаки одного или нескольких типов с различными параметрами. Расписание контролируемых компьютерных атак было разработано таким образом,

чтобы обеспечить одновременное выполнение атак различных типов, что позволило учесть многомерность данных.

Примерами интервалов времени, когда наблюдаются многозначные КА, являются: 22.04.2024; 0:00 – 2:00 (Атака №1 и №4); 22.04.2024; 2:00 – 5:00 (Атака №1, №2 и №4); 22.04.2024; 7:00 – 8:00 (Атака №1, №2, №3); иные.

Таблица № 2

Фрагмент расписания КА

ХОСТ		$АН_1$		$АН_2$			$АН_3$		$АН_4$			$АН_5$		
Тип атаки		1	2	3	4	5	6	7	8	9	10	11	12	13
Дата	Время, ч													
25.04.2024	12:00													
	13:00													
	14:00													
	15:00													
	16:00													
	17:00													
	18:00													
	19:00													
	20:00													
	21:00													
	22:00													
	23:00													

Одновременное воздействие на целевой хост VH_i нескольких КА с различными параметрами, как описано выше, может приводить к синергетическому эффекту, вызывающему критические последствия [12]. Это проявляется в одновременном «наложении» реализаций атак.

В случае если несколько типов атак проводятся одновременно, то можно утверждать, что собранные наборы данных обладают свойством многозначности. Это явление делает анализ набора данных обычными методами неполноценным и требует другого подхода. Многие методы анализа данных не способны учитывать наличие нескольких классовых меток одновременно, из-за чего использование их в наборах данных с наличием свойства многозначности может привести к некорректным результатам.

Представленное свойство многозначности данных наблюдается в реальных компьютерных сетях [13].

Результатом работы ПАК является сформированная многозначная база данных КА, предназначенная для исследования специфического явления – многозначности классовых меток, маркирующих КА.

Анализ собранных данных

Как было упомянуто ранее, анализ телеметрических данных и результатов имитационного моделирования КА затруднен ограниченным количеством доступных наборов данных, что препятствует всестороннему изучению многозначности классовых меток. В целях нивелирования при помощи ПАК был собран набор данных в целях исследования свойства многозначности в данных.

Набор данных состоит из 263.388 записей и 118 атрибутов. Данные собирались с сетевой карты и сенсоров механических комплектующих хостов. Его уникальность заключается в представлении одновременно осуществляемых КА как одной записи, а не отдельных событий, что позволяет рассматривать такие атаки как отдельный тип — многозначные КА. Подробная статистика о собранном наборе данных представлена на рисунках 2 – 5.

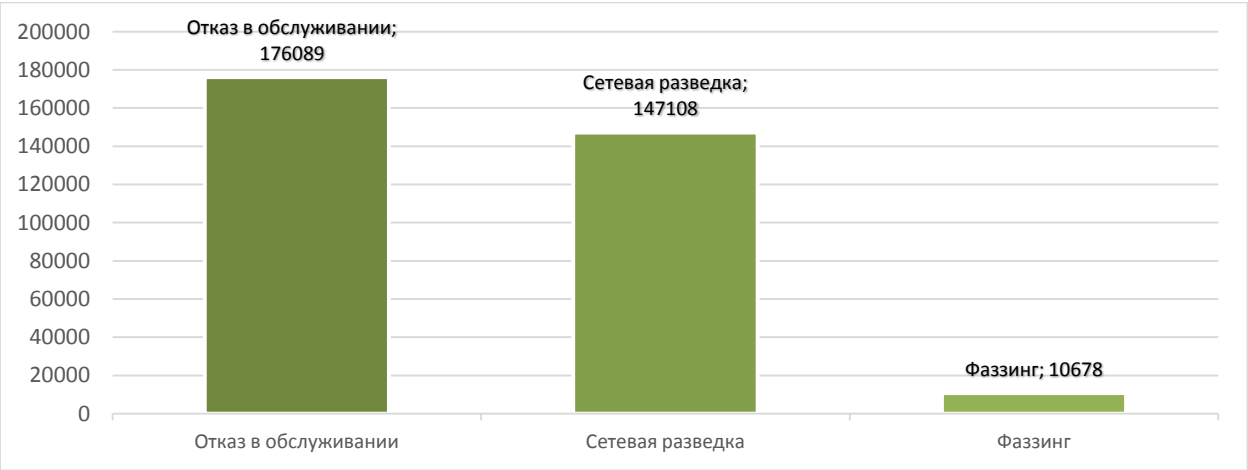

Рис. 3. – Распределение КА каждого типа

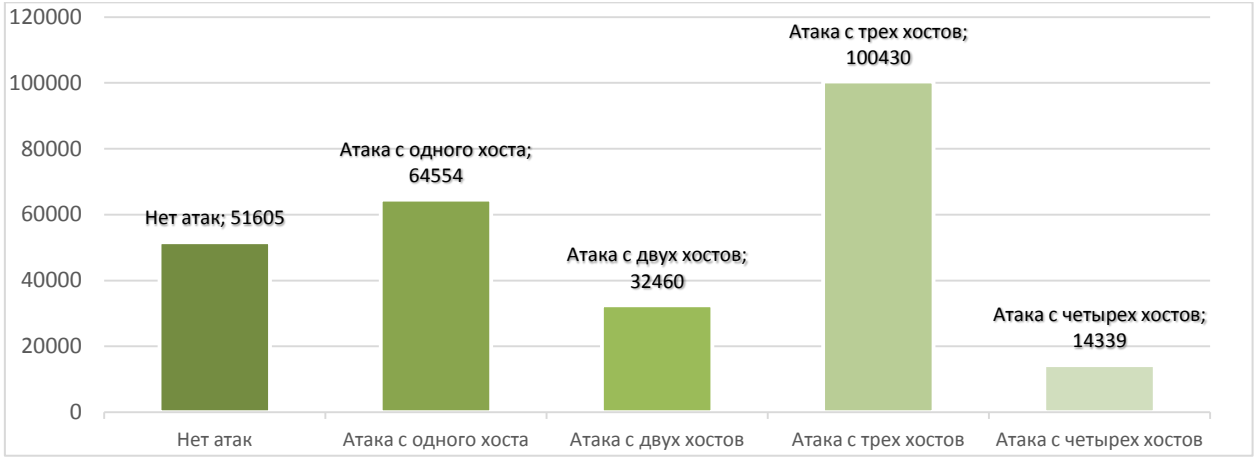

Рис. 4. – Распределение классовых меток по одновременно задействованным хостам при реализации КА

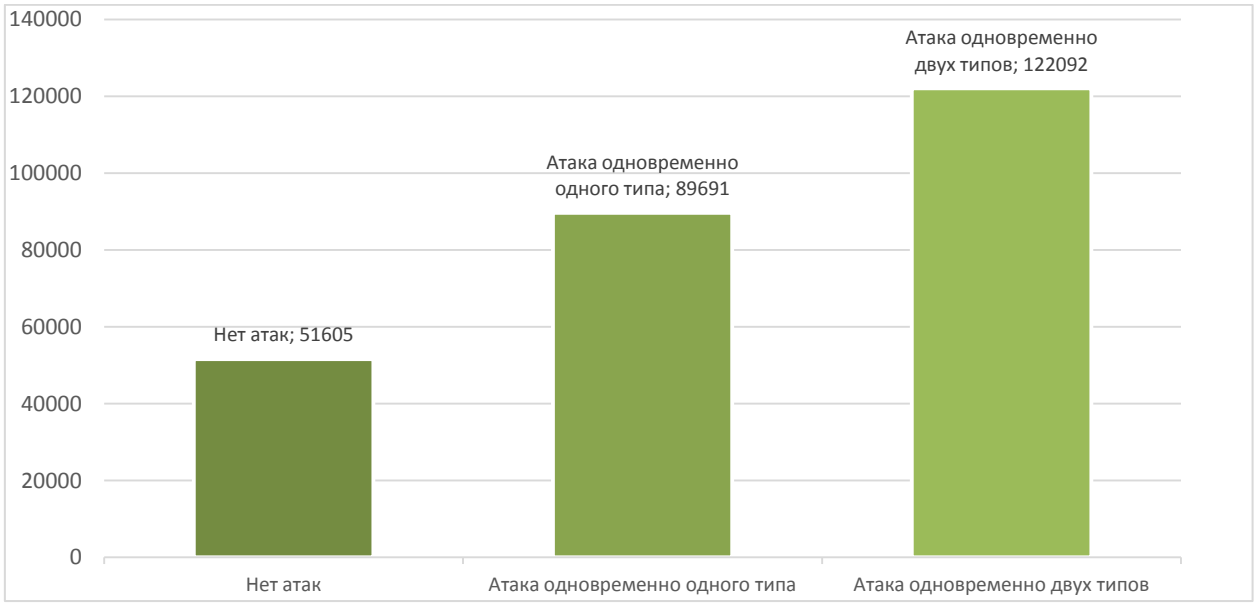

Рис. 5. – Распределение классовых меток по одновременно совершаемым типам КА

Как видно из рисунка 2 с атакующего хоста $АН_1$ было проведено – 26% всех КА, с хоста $АН_2$ – 24% КА, $АН_3$ – 10% КА, $АН_4$ – 21% КА, $АН_5$ – 19% КА. При этом большая доля КА приходится на атаки типа «отказ в обслуживании» 53%, дальше идет тип «сетевая разведка» 44%, тип «фаззинг» 3%, статистика в виде графика представлена на рисунке 3. Также доля КА двух разных типов совершенных одновременно на атакуемый хост составляет 46%, а одного типа 34% (рис. 5), при это наиболее всего атак совершалось с трех хостов одновременно (рис. 4). Так как данных,

собранных о атаках типа «фаззинг» мало (рис. 3), то она не будет рассматриваться.

Для оценки каждого атрибута собранной базы данных применялось несколько методов. Для начала были убраны все атрибуты с одним уникальным значением – это атрибуты номер 5, 12, 13, 57, 60, 61, 62, 63, 65, 66, 67. После этого происходит оценка информационной важности каждого атрибута — это мера, которая оценивает вклад каждого атрибута в предсказательную способность модели машинного обучения.

На рисунках 6 – 7 представлены гистограммы информационной важности 30 наиболее значимых атрибутов всех, рассмотренных выше КА.

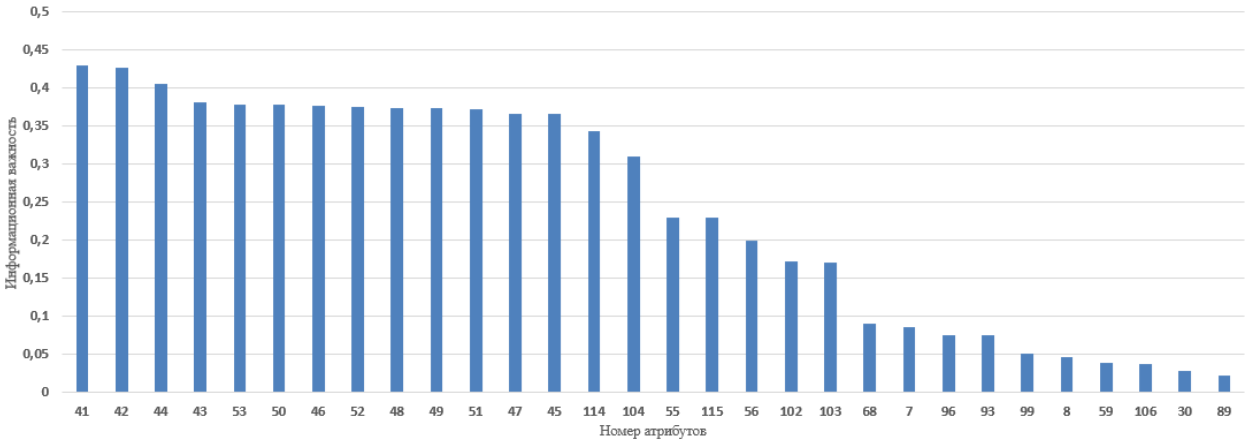

Рис. 6. – Распределение информационной важности 30 наиболее важных атрибутов атак типа «отказ в обслуживании»

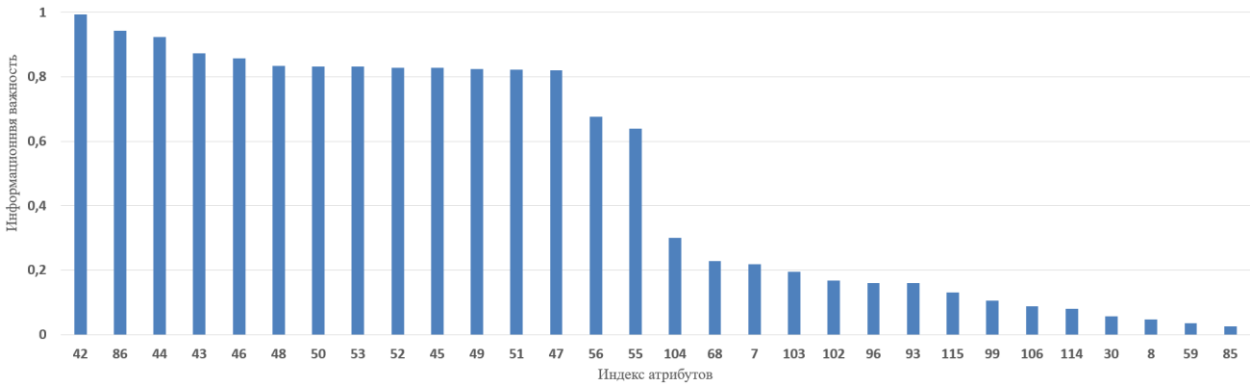

Рис. 7. – Распределение информационной важности 30 наиболее важных атрибутов атак типа «сетевая разведка»

Исследование информационной важности атрибутов собранного набора данных методом chi^2 (рис. 6 – 7) позволило выяснить на примере атак типа «отказ в обслуживании» и «сетевая разведка», что каждая КА имеет собственное распределение информационной важности атрибутов. Атрибуты, которые присутствуют во всех 30 наиболее важных атрибутов для анализируемых КА, представлены в табл. 3. Тем самым, самую большую информационную важность имеют атрибуты, которые содержат в себе информацию о сетевых пакетах, памяти, информацию с видеокарты, событиях *Windows XML EventLog*. Корреляционная диаграмма, представленная в виде тепловой матрицы тридцати наиболее важных атрибутов, представлена на рисунке 8.

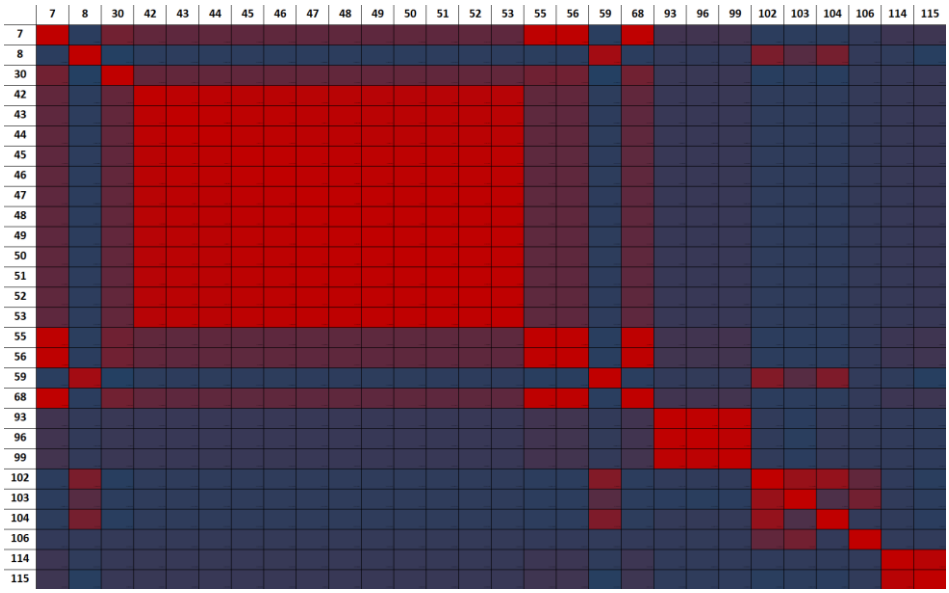

Рис. 8. – Тепловая матрица всех описанных атрибутов, входящих в 30 наиболее важных атрибутов

В табл. 3 представлено описание 28 оставшихся атрибутов. Наибольшую корреляцию имеют атрибуты с 41 по 53, это связано с тем, что они означают частоту каждого из ядер процессора. Атрибуты 82, 83 и 84 коррелируют друг с другом, так как отвечают за температуру первого и второго жесткого диска. Однако, так как на атакуемом хосте использовался только один жесткий диск, значения этих трех атрибутов равны. Атрибуты с

90 по 93 коррелируют друг с другом, потому что они хранят в себе данных о TLS (от англ. *Transport Layer Security*), а именно: количество уникальных типов содержимого записей TLS, количество уникальных типов длины записей TLS, количество уникальных длин данных приложений TLS. Атрибуты с 108 по 113 имеют корреляцию, так как хранят в себе данные о взаимодействии пользователя с различными сайтами, при этом наибольшую корреляцию имеют атрибуты с 108 по 110, из-за того, что они хранят в себе данные обработки HTTP (от англ. *Hyper Text Transfer Protocol*) запросов.

Таблица № 3

Описание атрибутов

Индекс	Атрибут базы данных	Краткое описание
7	Memoryusage	Уровень использования памяти GPU в процентах
8	Coreclock	Частота ядра GPU в мегагерцах (MHz)
30	CPU3usage	Уровень загрузки 3 ядра процессора (CPU) в процентах
42	CPU2clock	Частота 2 ядра процессора (CPU) в мегагерцах (MHz)
43	CPU3clock	Частота 3 ядра процессора (CPU) в мегагерцах (MHz)
44	CPU4clock	Частота 4 ядра процессора (CPU) в мегагерцах (MHz)
45	CPU5clock	Частота 5 ядра процессора (CPU) в мегагерцах (MHz)
46	CPU6clock	Частота 6 ядра процессора (CPU) в мегагерцах (MHz)
47	CPU7clock	Частота 7 ядра процессора (CPU) в мегагерцах (MHz)
48	CPU8clock	Частота 8 ядра процессора (CPU) в мегагерцах (MHz)
49	CPU9clock	Частота 9 ядра процессора (CPU) в мегагерцах (MHz)
50	CPU10clock	Частота 10 ядра процессора (CPU) в мегагерцах (MHz)
51	CPU11clock	Частота 11 ядра процессора (CPU) в мегагерцах (MHz)
52	CPU12clock	Частота 12 ядра процессора (CPU) в мегагерцах (MHz)
53	CPUclock	Средняя частота процессора (CPU) в мегагерцах (MHz)
55	RAMusage	Уровень использования оперативной памяти (RAM) в процентах
56	Commitcharge	Объем зарезервированной памяти в системе
59	GPUengine1usage	Уровень загрузки 2 графического движка GPU в процентах
68	GPUdedicatedmemoryusage	Уровень использования выделенной памяти GPU в процентах
93	tcp_sessions_per_time	Количество TCP-сессий за единицу времени
96	tcp_unique_ports_src_per_time	Количество уникальных исходных TCP-портов за единицу времени
99	tcp_unique_ports_dst_per_time	Количество уникальных целевых TCP-портов за единицу времени
102	avg_length_all_pack_per_time	Средняя длина всех пакетов за единицу времени
103	avg_length_tcp_pack_per_time	Средняя длина TCP-пакетов за единицу времени
104	avg_length_udp_pack_per_time	Средняя длина UDP-пакетов за единицу времени
106	avg_length_tls_per_time	Средняя длина TLS-пакетов за единицу времени
114	evnxContent_L	Содержимое события EVNX
115	evnxFull_Content_L	Полное содержимое события EVNX

На рисунке 9 представлена тепловая матрица между КА, запускаемыми с определенного IP адреса, и атрибутов. На данной тепловой матрице видно, что у каждой КА собственная корреляция с атрибутами.

Рис. 9. – Тепловая матрица КА, запускаемыми с определенного IP адреса, и атрибутов

Как изображено на рисунке 9, каждая КА имеет собственную корреляцию с атрибутами. Корреляция с атрибутами разная даже у атак одного типа. Это связано с тем, что каждая КА имеет собственные настройки параметров. Данное свойство может являться одним из маркеров многозначности классовых меток в наборах данных.

Помимо анализа линейных зависимостей, между атрибутным пространством набора данных и классовыми метками необходимо выявлять и нелинейные связи. Нелинейные связи могут быть обнаружены разными способами, одним из которых является анализ ошибки восстановления атрибутов до и после подачи в нелинейный фильтр (цифровые и аналоговые фильтры; искусственные нейронные сети, в том числе и автокодировщики [14]).

Визуализируем процесс использования искусственных нейронных сетей на базе автокодировщиков для обнаружения многозначных КА. На рисунке 10 представлено в графическом виде расписание КА, фрагмент которого приведен в табл. 2, за период с 14:00 25.04.2024 по 18.00 26.04.2024. Наличие КА отображено в виде прямоугольников, нанесенных на временную ось. Многозначные КА показаны в виде «наслоения» прямоугольников друг на друга; в целях визуализации разные КА маркированы разным цветом.

Поверх на график синей линией нанесена ошибка восстановления исходных значений набора данных после прохождения данных через автокодировщик, восстанавливающий нормальный трафик. Для наглядности приведена ошибка восстановления одного атрибута.

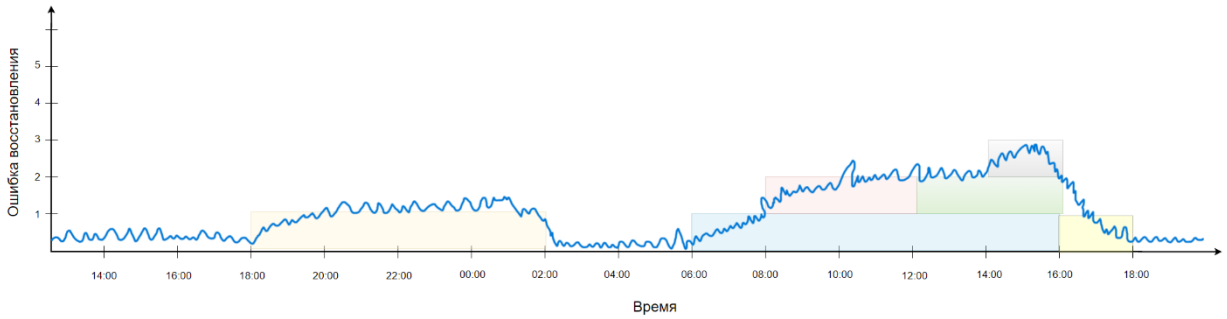

Рис. 10. – Расписание КА, представленное в графическом виде

Как видно из визуализации, ошибка восстановления увеличивается при воздействии КА на компьютерные сети вследствие изменения статистических свойств трафика. С ростом количества одновременно воздействующих КА на компьютерные сети ожидается рост ошибки восстановления, поскольку статистические свойства трафика с многозначными КА еще сильнее отличаются от свойств нормального трафика.

Выводы

Учет свойства многозначности целевых атрибутов в наборах данных при решении задачи классификации позволит снизить долю ошибок первого и второго рода, связанных с неверной классификацией многозначных записей в данных.

В соответствии с целью работы, проведен анализ набора данных, собранного во время моделирования КА на хосты при помощи ПАК. Данные представляют из себя набор записей, в которых хранится информация о сетевой и физической активности на хостах во время КА. Анализ набора данных выявил уникальные распределения информационной важности атрибутов для разных типов атак, таких как «отказ в обслуживании» и «сетевая разведка».

Проведена предобработка данных, после которой осталось 28 атрибутов с самой высокой информационной важностью среди атрибутов атак типа «отказ в обслуживании» и атак типа «сетевая разведка». Так как в

наборе данных, представленном в исследовании, наблюдается многозначность классовых меток, его обработка и анализ традиционными методами машинного обучения может привести к потере важной информации и снижению точности прогнозов, что критично в области информационной безопасности. Традиционные однозначные методы не всегда способны корректно учитывать наличие нескольких классовых меток для одного и того же наблюдения, что ограничивает их применение в таких задачах.

Для выявления и анализа специфического свойства многозначности целевых атрибутов использовать искусственные нейронные сети с архитектурой автокодировщиков.

Литература

1. Vulfin A.M. Detection of network attacks in a heterogeneous industrial network based on machine learning // Programming and Computer Software. 2023. V. 49. № 4. pp. 333-345.

2. Usoh M., Asuquo Ph., Ozuomba S., Stephen B., Inyang U. A hybrid machine learning model for detecting cybersecurity threats in IoT applications // International Journal of Information Technology (Singapore). 2023. V. 15. № 6. pp. 3359-3370.

3. Молодцов Д.А., Осин А.В. Новый метод применения многозначных закономерностей. Нечеткие системы и мягкие вычисления, 2020, т. 15, № 2, с. 83-95.

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

5. Шелухин О.И., Раковский Д.И., Александров И.Д., Боков А.Д. Имитационное моделирование многозначных компьютерных атак // I-methods. 2023. Т. 15. № 4.

6. Раковский Д.И., Александров И.Д., Боков А.Д., Шелухин О.И. Разработка стенда для сбора телеметрии и имитационного моделирования многозначных компьютерных атак // В сборнике: Безопасные информационные технологии. Материалы XII Международной научно-технической конференции, посвященной 25-летию кафедры ИУ8. Москва, 2024. С. 102-107.

7. Шелухин О.И., Раковский Д.И Многозначная классификация компьютерных атак с использованием искусственных нейронных сетей с множественным выходом // Труды учебных заведений связи. Т. 9. № 4. С. 95–111.

8. Покусов В.В. Синергетические Эффекты Взаимодействия Модулей Системы Обеспечения Информационной Безопасности // Информатизация И Связь. № 3. С. 61–67

9. Cheung K.Y., Lee S.M.S. High-dimensional local polynomial regression with variable selection and dimension reduction // Stat Comput. 2024. V. 34, № 1. P. 1c. DOI: 10.1007/s11222-023-10308-1.

10. Suman A., Kumar C., Suman P. ADVANCE ROUTING STRATEGY FOR VANETS // International Journal of Internet Protocol Technology. 2021. V. 14. № 4. pp. 205-218.

11. Common Attack Pattern Enumeration and Classification // A Community Resource for Identifying and Understanding Attacks URL: capec.mitre.org/index.html (дата обращения: 11.10.2024).

12. Шелухин О.И., Раковский Д.И. Обнаружение компьютерных атак на основе многозначных закономерностей // Материалы 33-й всероссийской научно-технической конференции «Методы и технические средства обеспечения безопасности информации». СПб.: Необит, 2024. С. 36-38.

13. Riera T.S., Higuera J.-R.B., Higuera J.B., Herraiz J.-J.M., Montalvo J.-A.S. A new multi-label dataset for Web attacks CAPEC classification using machine learning techniques // Computers & Security. 2022. V. 120. P. 102788c.

14. Cakir M.Y., Sirin Ya. Enhanced autoencoder-based fraud detection: a novel approach with noise factor encoding and SMOTE // Knowledge and Information Systems. 2024. V. 66. № 1. P. 635-652.

References

1. Vulfin A.M. Programming and Computer Software. 2023. V. 49. № 4. pp. 333-345.

2. Usoh M., Asuquo Ph., Ozuomba S., Stephen B., Inyang U. International Journal of Information Technology (Singapore). 2023. V. 15. № 6. pp. 3359-3370.

3. Molodtsov D.A., Osin A.V. Nechetkie sistemy i myagkie vychisleniya. 2020. V. 15. № 2. pp. 83-95.

4. Rakovskiy D.I. Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli. 2023. V. 15. № 1. pp. 48-56.

5. Sheluhin O.I., Rakovskiy D.I., Aleksandrov I.D., Bokov A.D. I-methods. 2023. V. 15. № 4. pp. 1 – 15.

6. Rakovskiy D.I., Aleksandrov I.D., Bokov A.D., Sheluhin O.I., Bezopasnye informatsionnye tekhnologii. Materialy KhII Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii, posvyashchennoy 25-letiyu kafedry IU8. Moskva, 2024, pp. 102-107.

7. Sheluhin O.I., Rakovskiy D.I. Trudy uchebnykh zavedeniy svyazi. V. 9. № 4. pp. 95–111.

8. Pokusov V.V. Informatizatsiya I Svyaz'. № 3. pp. 61–6.

9. Cheung K.Y., Lee S.M.S. Stat Comput. 2024. V. 34, № 1. P. 1.

10. Suman A., Kumar C., Suman P. International Journal of Internet Protocol Technology. 2021. V. 14. № 4. pp. 205-218.

11. A Community Resource for Identifying and Understanding Attacks URL: capec.mitre.org/index.html (accessed: 11.10.2024).

12. Sheluhin O.I., Rakovskiy D.I Materialy 33-y vserossiyskoy nauchno-tekhnicheskoy konferentsii «Metody i tekhnicheskie sredstva obespecheniya bezopasnosti informatsii» (Proceedings of the 33rd All-Russian Scientific and Technical Conference "Methods and Technical Means of Ensuring Information Security"). Sankt-Peterburg, 2024, pp. 36-38.

13. Riera T.S., Higuera J.-R.B., Higuera J.B., Herraiz J.-J.M., Montalvo J.-A.S. Computers & Security. 2022. V. 120. P. 102788c.

14. Cakir M.Y., Sirin Ya. Knowledge and Information Systems. 2024. V. 66. № 1. pp. 635-652.

Дата поступления: 4.11.2024

Дата публикации: 5.12.2024