УДК 342.41 + 342.511.5 Вестник УрФО № 1(47) / 2023, с. 59–68

Бухарев Д. А., Соколов А.Н., Рагозин А.Н.

DOI: 10.14529/secur230106

ПРИМЕНЕНИЕ ИЕРАРХИЧЕСКОГО КЛАСТЕРНОГО АНАЛИЗА ДЛЯ КЛАСТЕРИЗАЦИИ ДАННЫХ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ АСУ ТП, ПОДВЕРГАЮЩИХСЯ ВОЗДЕЙСТВИЮ КИБЕРАТАК [1]

Техническое развитие промышленных средств автоматизации и увеличение уровня интеграции промышленных и корпоративных сетей приводит к увеличению рисков проведения успешных кибератак. Реализация таких кибератак может подразумевать получение доступа к управлению важными промышленными установками, что влечет за собой риск остановки производства или создания аварийной ситуации. Практическое обеспечение информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП) требует своевременного обнаружения кибератак, как известного, так и неизвестного типа. Эти кибератаки можно выделить в виде аномалий в динамических процессах, регулярно регистрируемых при работе АСУ ТП. В контексте решения задачи обнаружения атак на информационные системы АСУ ТП, кластерный анализ применяется как один из методов, реализующих обнаружение аномалий. Исследуется применение иерархического кластерного анализа для кластеризации данных информационных процессов АСУ ТП, подвергающихся воздействию различным кибератак, решается задача выбора уровня иерархии кластеров, соответствующий минимальному набору кластеров, агрегирующих раздельно нормальные и аномальные данные. Показано, что метод Уорда реализует наилучшее разделение на кластеры. Следующим этапом исследования предполагается решение задачи классификации сформированного минимального набора кластеров, то есть определения какой кластер является нормальным, какой кластер является аномальным.

Ключевые слова: *Автоматизированная система управления технологическим процессом, кибератака, классификация кибератак, иерархическая кластеризация, обнаружение аномалий.*

[1] Исследование поддержано грантом Российского научного фонда (проект № 22-71-10095).

APPLICATION OF HIERARCHICAL CLUSTER ANALYSIS FOR CLUSTERING THE DATA OF ICS INFORMATION PROCESSES AFFECTED BY CYBERATTACKS

The technical development of industrial automation tools and an increase in the level of integration of industrial and corporate networks leads to an increase in the risks of successful cyberattacks. The implementation of such cyberattacks may involve gaining access to the control of important industrial installations, which entails the risk of stopping production or creating an emergency. The practical provision of information security for industrial control systems (ICS) requires the timely detection of cyberattacks, both known and unknown. These cyber-attacks can be identified as anomalies in dynamic processes that are regularly recorded during the operation of ICS. In the context of solving the problem of detecting attacks on ICS information systems, cluster analysis is used as one of the methods that implement anomaly detection. The application of hierarchical cluster analysis for clustering data of ICS information processes exposed to various cyberattacks is studied, the problem of choosing the level of the cluster hierarchy corresponding to the minimum set of clusters aggregating separately normal and abnormal data is solved. It is shown that Ward's method implements the best division into clusters. The next stage of the study involves solving the problem of classifying the formed minimum set of clusters, that is, determining which cluster is normal and which cluster is abnormal.

Keywords: *Industrial control systems, cyberattack, cyberattack classification, hierarchical clustering, anomaly detection.*

Современные автоматизированные системы управления технологическими процессами (АСУ ТП) организованы в сеть, соединяющую множество контрольно-измерительной аппаратуры, программируемых логических контроллеров, станций оператора, SCADA систем и другого сетевого оборудования. Такая обширная сеть позволяет эффективно управлять производством и реагировать на различные ситуации, возникающие в ходе функционирования производства. Однако, инциденты информационной безопасности промышленной сети передачи данных могут привести к выводу из строя дорогостоящего оборудования, а также стать причиной экологической катастрофы. Злоумышленники, также могут проводить несанкционированный доступ к защищенной информации о технологическом производстве. Актуальной является задача обнаружения атак как известного, так и не известного типов, а также реализация возможности классификации воздействующих различных типов атак

Системы обнаружения атак (СОА), основанные на методах обнаружения аномалий, показывают высокие показатели эффективности обнаружения атак, как известного, так и не известного типов. Одним из методов интеллектуального анализа данных, который может быть применен для решения задачи обнаружения атак, а также их последующей классификации, является кластерный анализ. Предполагается, что нормальные данные, соответствующие штатному режиму работы системы, образуют большие плотные кластеры, или плотные скопления небольших нормальных кластеров, а аномальные данные, соответствующие аномальному режиму работы системы, распределяются в более маленькие и разрозненные аномальные кластеры, силь-

но удаленных от выделенных кластеров нормального поведения исследуемой системы.

В исследовании проведен анализ возможности использования агломеративной иерархической кластеризации для целей построения системы кластеров, соответствующих нормальным и аномальным состояниям исследуемой системы. В результате анализа наблюдаемого набора данных исследуемой системы, формируется иерархическая система кластеров, отображаемая в виде дендрограммы. Самый нижний уровень дендрограммы соответствует исходному (начальному) набору данных, самый верхний уровень дендрограммы, соответствует одному кластеру, включающего в себя все исходные начальные данные. Промежуточные уровни иерархии кластеров, отображаемой в виде дендрограммы, соответствуют системе кластеров, агрегирующих нормальные и аномальные исходные данные с соответствующим уровнем обобщения. Очевидно, существует максимальный уровень иерархической кластеризации исходных данных, отображаемой в виде дендрограммы, соответствующий минимальному количеству кластеров, агрегирующих раздельно (без перекрытия) нормальные и аномальные исходные данные. При этом, в формируемом минимальном наборе кластеров, одна часть кластеров соответствует только нормальным исходным данным (нормальные кластеры), другая часть кластеров соответствует только аномальным исходным данным (аномальные кластеры). Соответствующее отображение на дендрограмме выделенного минимального набора нормальных и аномальных кластеров содержит информацию для идентификации вида кластеров, то есть, идентификации отдельно нормальных кластеров и идентификации отдельно аномальных кластеров. Идентификация видов кластеров соответствует решению задачи двух классовой классификации кластеров, то есть разделения кластеров на нормальные и аномальные кластеры.

Построение системы обнаружения аномалий в наблюдаемых данных технической системы, возникающих вследствие воздействия кибератак, предполагает построение иерархии кластеров исходных данных, далее, предполагается выбор уровня иерархии кластеров, соответствующий минимальному набору кластеров, агрегирующих раздельно нормальные и аномальные данные, далее предполагается решение задачи классификации сформированного минимального набора кластеров, то есть определения какой кластер является нормальным, какой кластер является аномальным.

В проведённом исследовании рассматриваются первые два этапа: построение иерархии кластеров исходных данных, затем, рассматриваются выбор оптимального уровня иерархии кластеров, соответствующий минимальному набору кластеров, агрегирующих раздельно нормальные и аномальные данные.

Метод кластерного анализа заключается в выделении таких характеристик из сетевого трафика или записей состояния АСУ ТП, которые позволят разбить классифицируемые объекты на группы, соответствующие нормальному функционированию системы или сети. Все остальные экземпляры, которые не попадают в построенные области, классифицируются как аномальные [1]. В каждом конкретном методе кластерного анализа используется своя метрика, которая позволяет оценивать принадлежность наблюдаемого вектора параметров процессов системы одному из кластеров или выход за границы сформированных кластеров.

Современные тенденции предполагают объединение индустриальных и корпоративных сетей, поскольку это, с одной стороны, позволяет уменьшать затраты бизнеса и делать эксплуатацию индустриальных объектов более удобной, но с другой увеличивает риски проведения успешных кибератак. Это связано с необходимостью открытия удаленного доступа для контроля и анализа технологического процесса на предприятии. Такой доступ позволяет не находиться непосредственно на предприятии, но также дает злоумышленнику возможность получить доступ к промышленному оборудованию внутри промышленной сети. Кластерный анализ позволяет производить одновременную обработку разнородных данных, наблюдаемых как в контрольных точках корпоративных сетей, также данных, наблюдаемых с сенсоров или актуаторов АСУ ТП промышленных систем.

На основании анализа векторов обучающей выборки производится построение кластеров, описывающих нормальное поведение системы (в виде совокупности кластеров), после чего выполняет поиск аномалий – кластеров состояний, сильно удаленных от выделенных кластеров нормального поведения системы, то есть кластеров, соответству-

ющих аномальным состояниям системы, возникающих в следствии воздействия атак. Также, кластерный анализ позволяет формировать систему кластеров, соответствующих различным типам воздействующих атак, то есть проводить непрерывное обучение СОА в процессе текущей работы.

Обзор методов кластерного анализа приведён в работе [2]. Обзор иерархических методов кластерного анализа приведён в работе [3]. Применение методов кластерного анализа для обнаружения аномалий на основе анализа выбросов в данных рассмотрено в работах [4–7]. Обнаружение аномалий в данных с использованием кластерного анализа при делении выбросов на локальные и глобальные, рассмотрено в работах [8, 9].

Для определения оптимальных параметров агломеративной иерархической кластеризации в первую очередь требуется определиться с метрикой, на основании которой будет происходить сравнение. При получении готовой разбивки на кластеры данных, у которых есть метки аномальности, мы можем разделить их на 2 группы – содержащие аномальные данные и содержащие нормальные данные. Разделение на группы происходит на основании наличия в кластере хотя бы одной аномальной точки. После получения размеченных кластеров можно рассчитать следующие значения: N_a – общее количество аномальных кластеров; N_{an} – количество аномальных кластеров, содержащих нормальные данные; N_{aa} – количество аномальных кластеров, не содержащих нормальные данные. По этим значениям рассчитываются следующие метрические параметры (метрики):

$$R_{an} = \frac{N_{an}}{N_a} \quad (1)$$

– доля аномальных кластеров, содержащих нормальные данные;

$$R_{aa} = \frac{N_{aa}}{N_a} \quad (2)$$

– доля аномальных кластеров, не содержащих нормальные данные.

Метрики (1), (2) можно использовать для определения качества кластеризации, а также для определения оптимального уровня иерархии кластеров. Основной метрикой, которая использовалась в рамках данного исследования, является метрика R_{aa}, которая показывает, на сколько точно распределены данные по кластерам, содержащие аномальные данные. Для получения наиболее информативного анализа параметров кластеризации производится серия экспериментов, в которой рассчитывается кривая значений R_{aa} в зависимости от увеличения числа разбиения на кластеры (диапазон от 1 до 1000). Получив группу кривых, можно определить оптимальное значение параметра кластеризации и оптимальный уровень иерархии кластеров.

Для определения оптимального уровня иерархии кластеров с использованием метрики R_{aa} необходимо получить точку перегиба для кривой R_{aa}, которая будет являться базовым уровнем. Для получения точки перегиба можно применить интерполяционный полином, на основе которого вычисляется вторая производная.

В будущих работах также планируется исследовать возможность проведения классификации кластеров, полученных в результате работы иерархической кластеризации. Полученные кластеры должны подаваться на некоторый классификатор, который будет создавать две группы – аномальную и нормальную. Корректное разделение классификатором набора кластеров будет означать точное выделение аномальных точек в наборе данных. После получения таких групп возможно внедрение процесса постоянного анализа поступающих данных для выделения аномалий в режиме реального времени.

В качестве набора данных для проведения исследования при помощи методов иерархического кластерного анализа использовался набор данных Secure Water Treatment (SWaT) [10]. Набор данных генерируется моделью, имитирующую реальное водоочистное сооружение. Моделируемое водоочистное сооружение содержит промышленное оборудование, в котором присутствует несколько программируемых логических контроллера, SCADA система, а также сетевое оборудование промышленного образца. Структурная схема макета водоочистного сооружения представлена на рис. 1.

Набор данных, используемый в работе, состоит из 14996 записей, каждая из которой описывает состояние 77 датчиков или механизмов водоочистного сооружения в конкретный момент времени. В формируемом моделью SWaT наборе данных были сформированы и промаркированы шесть кибератак на информационную инфраструктуру водоочистного сооружения, в ходе которых производилось несанкционированное изменение параметров системы, отражающей работу во-

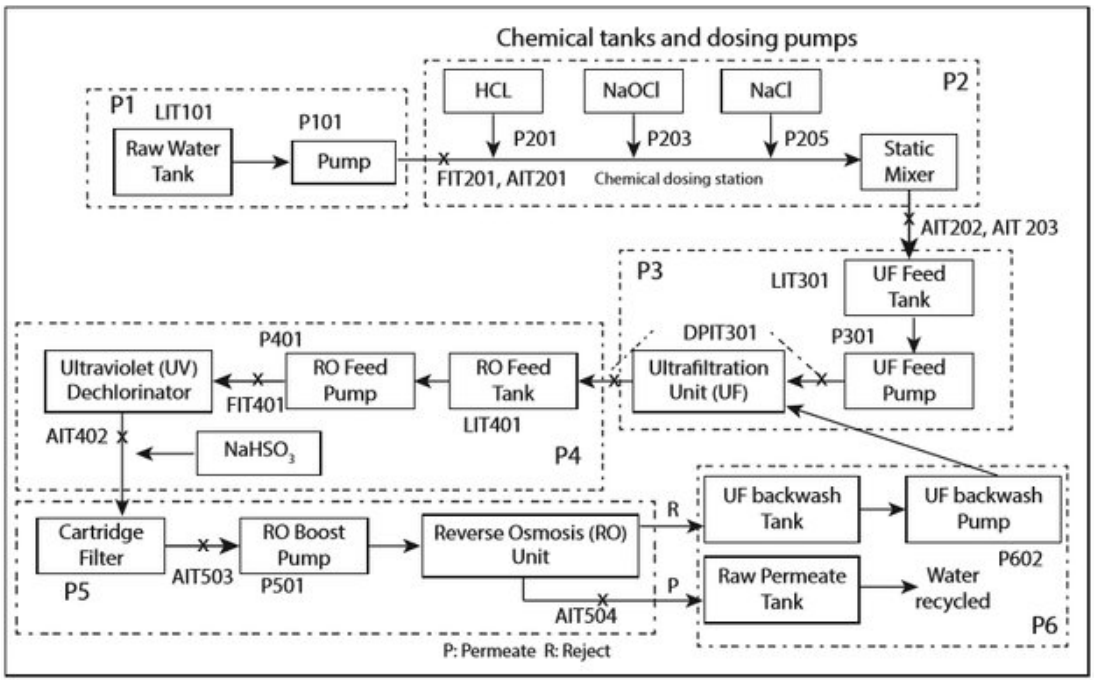

Рис. 1. Структурная схема макета SWaT [10]

Рис. 2. Распределение атак на систему с течением времени (атаки обозначены красными столбцами)

доочистного сооружения. Расположение этих атак на наборе данных изображено на рис. 2. Доля точек данных, в которых производились атаки по отношению к общему количеству точек данных – 14%.

Для обработки данных модели SWaT в исследовании использован агломеративный метод иерархического кластерного анализа. В качестве метрики расстояния в применяемом методе кластеризации была использована евклидова метрика, при этом, в качестве метода связи кластеров использовался метод полной связи кластеров.

В ходе вычислительного эксперимента исследовались различные методы разбиения на кластеры с использованием иерархической кластеризации. Применялись методы разбиения: Уорда, средней связи, центроидный, полной связи, одиночной связи. В качестве метрики расстояния использовалась ев-

клидова метрика. Результаты эксперимента отражены в табл. 1 и рис. 3, 4.

В таблице 1 приведены численные значения R_{aa} для рассмотренных методов при числе разбиении на кластеры в 500 и 1000 кластеров. По результатам эксперимента видно, что метод Уорда является наилучшим методом разбиения в обоих случаях, т.к. метрика R_{aa} обладает наиболее высоким значением. Это означает, что при кластеризации с использованием метода Уорда получались наиболее «чистые» аномальные кластеры, без примесей нормальных данных.

На рис. 4 изображен график второй про-

Таблица 1

Значения R_{aa} различных методов разделения на кластеры при использовании евклидовой метрики

Кол-во кластеров при разбиении	Метод	R_{aa}
500	Уорда	0,8657
1000	Уорда	0,9433
500	Средней связи	0,7719
1000	Средней связи	0,8909
500	Центроидный	0,7705
1000	Центроидный	0,8948
500	Полной связи	0,8376
1000	Полной связи	0,9162
500	Одиночной связи	0,5704
1000	Одиночной связи	0,7767

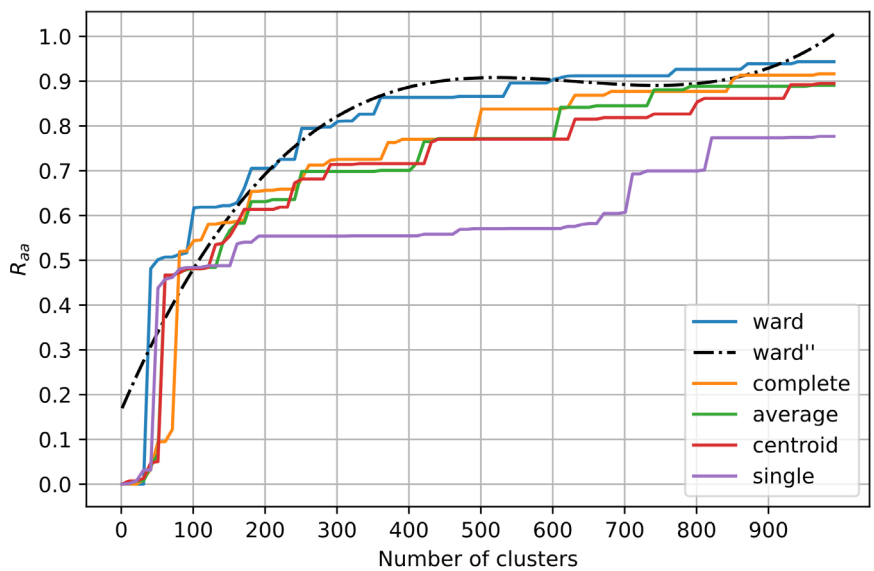

Рис. 3. График кривых R_{aa} различных методов разделения на кластеры при использовании евклидовой метрики

изводной для кривой R_{aa}. На графике можно увидеть, что кривая имеет точку перегиба в районе от 500 до 600 кластеров – 520 кластеров. Эта точка является оптимальным уровнем иерархии кластеров, при котором возможно достичь достаточно точного разбиения на аномальные и нормальные кластеры.

Для увеличения точности кластеризации возможно дополнять исходные данные историческими точками. В данном эксперименте показано, как изменяется точность кластеризации при добавлении 1, 2 и 3 предыдущих точек. Результаты эксперимента отражены в табл. 2 и рис. 5.

В таблице 3 приведены численные значения R_{aa} для рассмотренных отсчетов при числе разбиении на кластеры в 500 и 1000 кластеров. Также для сравнения представлены результаты, когда дополнительные данные не использовались. В таблице 3 видно, что до-

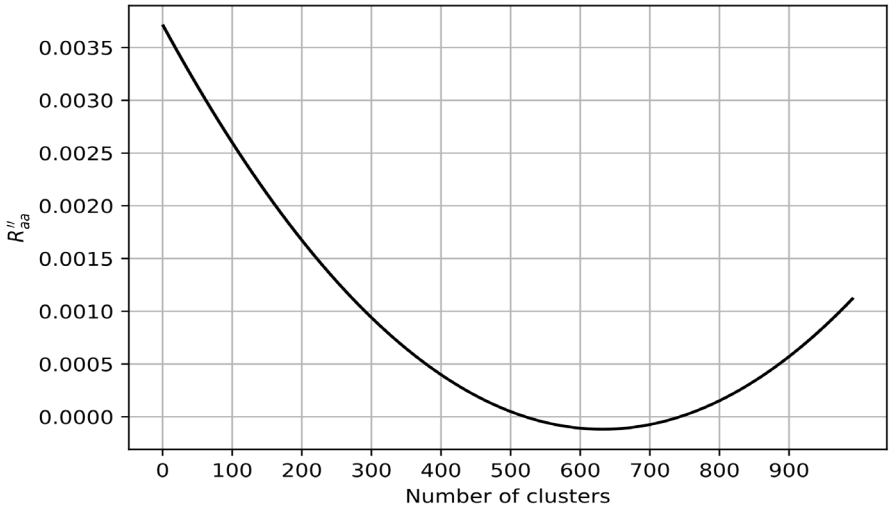

Рис. 4. График второй производной для кривой R_{aa} (метод Уорда)

Таблица 2

Значения R_{aa} при различном количестве исторических данных при анализе

Кол-во кластеров при разбиении	Кол-во отсчетов	R_{aa}
500	0	0,8657
1000	0	0,9433
500	1	0.88
1000	1	0.9347
500	2	0.8576
1000	2	0.93
500	3	0.8823
1000	3	0.9309

бавление исторических данных не дает весомого прироста в точности. В случае, когда добавляется 3 точки исторических данных при 500 кластерах, мы видим прирост в 0,0116. При анализе на большем количестве кластеров при разбиении точность снижается. На рис. 5 также можно заметить, что добавление исторических данных визуально не позволяет явно понять, что дополнительные отсчеты добавляют точности кластеризации.

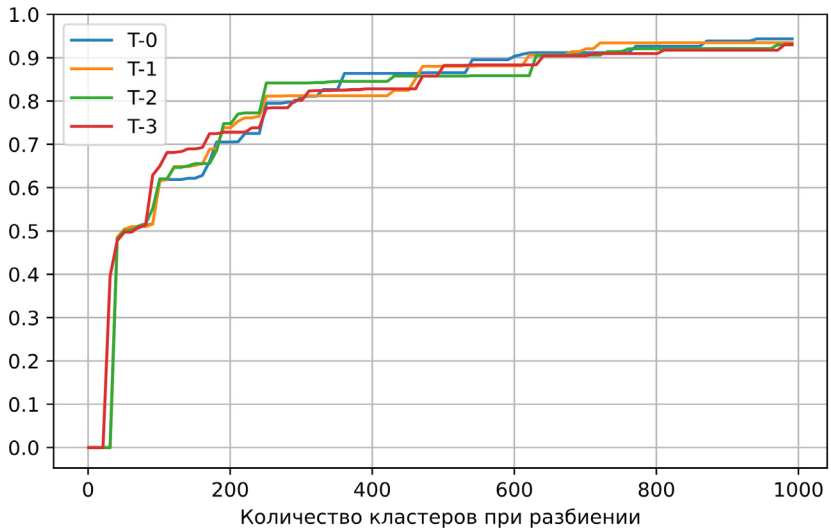

Рис. 5. График кривых R_{aa} при различном количестве исторических данных (евклидова метрика, метод Уорда)

При отнесении кластера к аномальным изначально использовалось предположение о том, что при наличии в кластере хотя бы одной аномальной точки этот кластер считался аномальным. Изменение такого критерия (принятие кластера аномальным при допустимом большем количестве аномальных точек внутри кластера) позволит нам уменьшить уровень разбиения на кластеры. В рамках этого эксперимента сравнивалось 6 различных критериев отнесения кластера к аномальным: < 1 точки, < 2, < 3, < 5, < 10, < 20. Результаты эксперимента отражены на рис. 6.

По рисунку 6 видно, что изменение критерия в большую сторону позволяет снизить количество кластеров при разбиении на нормальные и аномальные кластеры и получить более низкий уровень иерархической кластеризации для определения минимального количества кластеров, но при этом снижается качество разбивки на кластеры анализируемых данных наблюдаемых процессов, за счёт увеличения метрики R_{aa}.

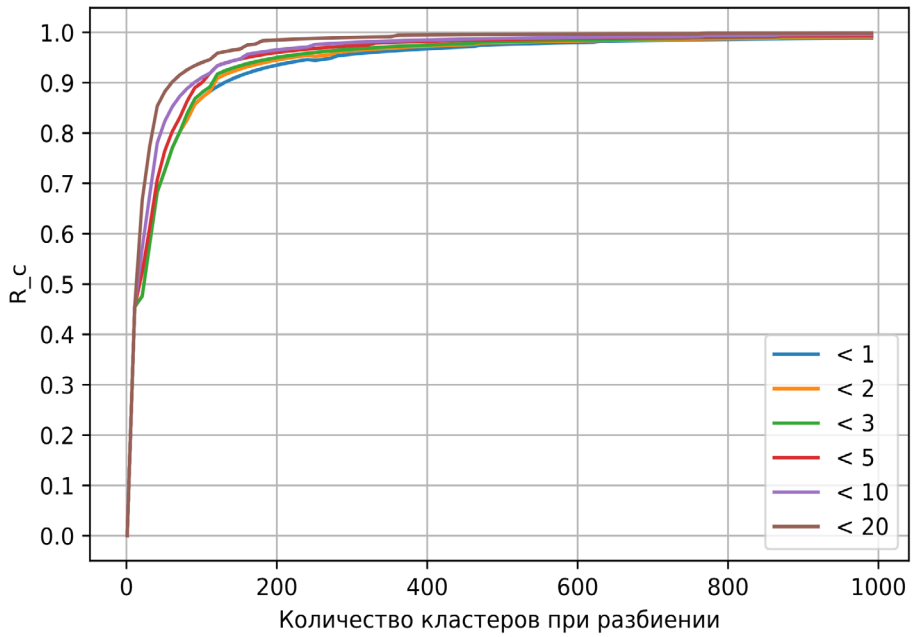

Рис. 6. График кривых Raa при различных критериях принятия кластера как аномального (евклидова метрика, метод Уорда)

Проведено исследование метода агломеративной иерархической кластеризации для определения минимального количества кластеров данных информационных процессов АСУ ТП, подвергающихся воздействию кибератак.

Показана возможность использования метода агломеративной иерархической кластеризации для целей построения системы не перекрывающихся кластеров, соответствующих раздельно нормальным и аномальным состояниям исследуемой системы.

Разработаны и исследованы критерии для определения максимального уровня иерархической кластеризации исходных данных, отображаемой в виде дендрограммы, соответствующий минимальному количеству кластеров, агрегирующих раздельно (без перекрытия) нормальные и аномальные исходные данные информационных процессов АСУ ТП, подвергающихся воздействию кибератак.

Показана эффективность определения оптимального уровня иерархической кластеризации на основе вычисления метрики R_{aa}, которая отражает степень качества (чистоты) кластеризации. Показано, что метод Уорда агломеративной иерархической кластеризации является наилучшим для решения задачи определения аномалий в информационных процессах АСУ ТП, подвергающихся воздействию кибератак.

Соответствующее отображение на дендрограмме определённого минимального набора не перекрывающихся нормальных и аномальных кластеров содержит информацию для дальнейшей идентификации вида кластеров, то есть разделения кластеров на нормальные и аномальные кластеры, без

предварительной разметки исходных данных, что делает возможным в ходе дальнейших исследований и разработок реализовать систему обнаружения аномалий в наблюдаемых динамических потоках данных АСУ ТП, подвергающихся воздействию кибератак.

Литература

1. Волкова В. Н. Основы теории систем и системного анализа: учебник / В. Н. Волкова, А. А. Денисов. – СПб: Изд-во СПбГТУ, 1999. – 512 с.

2. Флейшман Б. С. Основы системологии / Б. С. Флейшман. – М.: Радио и связь. 1982. – 368 с.

3. Тырсин А. Н. О математическом моделировании сложных организационных систем / А. Н. Тырсин // Организация и управление эффективностью и производительностью производственных и социальных систем: Матер. межд. научно-практ. конф. – Новочеркасск: ЮРГТУ (НПИ), 2005. – С. 49–50.

4. Биргер И. А. Техническая диагностика / И. А. Биргер. – М.: Наука, 1978. – 239 с.

5. Debar H., Dacier M., Wespi A. Towards a taxonomy of intrusion-detection systems // Computer Networks. 1999. vol. 31. Issue 8. P. 805–822.

6. Браницкий А. А., Котенко И. В., Анализ и классификация методов обнаружения сетевых атак // Тр. СПИИРАН, 2016, выпуск 45, 207–244 DOI: https://doi.org/10.15622/sp.45.13 [A. A. Branitskiy, I. V. Kotenko, Analiz i klassifikatsiya metodov obnaruzheniya setevykh atak, Tr. SPIIRAN, 2016, vypusk 45, 207–244 DOI: https://doi.org/10.15622/sp.45.13].

7. Herve Debar, Monique Becker, and Didier Siboni, "A neural network omponent for an intrusion detection system." // Proceedings of the 1992 IEEE Computer Sociecty Symposium on Research in Security and Privacy, pages 240–250, Oakland, CA, USA, May 1992.

8. Rasool Jalili, Fatemeh Imani-Mehr, Morteza Amini, Hamid Reza Shahriari, "Detection of Distributed Denial of Service Attacks Using Statistical Pre- Processor and Unsupervised Neural Networks." // Lecture notes in computer science, 2005.

9. Смелянский Р.Л., Качалин А.И. "Применения нейросетей для обнаружения аномального поведения объектов в компьютерных сетях"./ Факультет Вычислительной Математики и Кибернетики, МГУ им. М. В. Ломоносова, Москва, 2004.

10. Neural network and artificial immune systems for malware and network intrusion detection / V. Golovko [et al.] // Studies in computational intelligence. – Heidelberg, 2010. – Vol. 263: Advances in machine learning II. – P. 485–513.

11. Muna, A. H., Moustafa, N., & Sitnikova, E. (2018). Identification of malicious activities in industrial internet of things based on deep learning models. Journal of Information Security and Applications, 41, 1–11.

12. Sung Jin Kim, Woo Yeon Jo, Taeshik Shon. APAD: Autoencoder-based Payload Anomaly Detection for industrial IoE. December 2019 Applied Soft Computing 88:106017. DOI: 10.1016/j.asoc.2019.106017.

13. Baldi P. Autoencoders, unsupervised learning, and deep architectures //Proceedings of ICML workshop on unsupervised and transfer learning. – 2012. – С. 37–49.

14. Schmidhuber J. Deep learning in neural networks: An overview //Neural networks. – 2015. – Т. 61. – С. 85–117.

15. Goodfellow I. et al. Generative adversarial nets //Advances in neural information processing systems. – 2014. – С. 2672–2680.

16. Madry A. et al. Towards deep learning models resistant to adversarial attacks //arXiv preprint arXiv:1706.06083. – 2017.

17. Donahue J., Krähenbühl P., Darrell T. Adversarial feature learning //arXiv preprint arXiv:1605.09782. – 2016.

References

1. Volkova V.N. Osnovy teorii sistem i sistemnogo analiza / V.N. Volkova, A.A. Denisov. – SPb: Izd-vo SPbGTU, 1999. – 512 s.

2. Fleyshman B.S. Osnovy sistemologii / B.S. Fleyshman. – M.: Radio i svyaz'. 1982. – 368 s.

3. Tyrsin A.N. O matematicheskom modelirovanii slozhnykh organizatsionnykh sistem // Organizatsiya i upravlenie effektivnost'yu i proizvoditel'nost'yu proizvodstvennykh i sotsial'nykh sistem: Mater. mezhd. nauchno-prakt. konf. – Novocherkassk: YuRGTU (NPI), 2005. – S. 49 – 50.

4. Birger I.A. Tekhnicheskaya diagnostika. – M.: Nauka, 1978. – 239 s.

5. Debar H., Dacier M., Wespi A. Towards a taxonomy of intrusion-detection systems // Computer Networks. 1999. vol. 31. Issue 8. P. 805–822.

6. Branitskiy A.A., Kotenko I.V. Analiz i klassifikatsiya metodov obnaruzheniya setevykh atak. – Trudy SPIIRAN. – 2016. – Vyp. 45 – S. 207 – 244.

7. Herve Debar, Monique Becker, and Didier Siboni, "A neural network omponent for an intrusion detection system." // Proceedings of the 1992 IEEE Computer Sociecty Symposium on Research in Security and Privacy, pages 240–250, Oakland, CA, USA, May 1992.

8. Rasool Jalili, Fatemeh Imani-Mehr, Morteza Amini, Hamid Reza Shahriari, "Detection of Distributed Denial of Service Attacks Using Statistical Pre- Processor and Unsupervised Neural Networks." // Lecture notes in computer science, 2005.

9. Smelyanskiy R.L., Kachalin A.I. Primeneniya neyrosetey dlya obnaruzheniya anomal'nogo povedeniya ob"ektov v komp'yuternykh setyakh //Fakul'tet Vychislitel'noy Matematiki i Kibernetiki, MGU im. M. V. Lomonosova, Moskva, 2004.

10. Neural network and artificial immune systems for malware and network intrusion detection / V. Golovko [et al.] // Studies in computational intelligence. – Heidelberg, 2010. – Vol. 263: Advances in machine learning II. – P. 485–513.

11. Muna, A. H., Moustafa, N., & Sitnikova, E. (2018). Identification of malicious activities in industrial internet of things based on deep learning models. Journal of Information Security and Applications, 41, 1–11.

12. Sung Jin Kim, Woo Yeon Jo, Taeshik Shon. APAD: Autoencoder-based Payload Anomaly Detection for industrial IoE. December 2019 Applied Soft Computing 88:106017. DOI: 10.1016/j.asoc.2019.106017.

13. Baldi P. Autoencoders, unsupervised learning, and deep architectures //Proceedings of ICML workshop on unsupervised and transfer learning. – 2012. – С. 37–49.

14. Schmidhuber J. Deep learning in neural networks: An overview //Neural networks. – 2015. – Т. 61. – С. 85–117.

15. Goodfellow I. et al. Generative adversarial nets //Advances in neural information processing systems. – 2014. – С. 2672–2680.

16. Madry A. et al. Towards deep learning models resistant to adversarial attacks //arXiv preprint arXiv:1706.06083. – 2017.

17. Donahue J., Krähenbühl P., Darrell T. Adversarial feature learning //arXiv preprint arXiv:1605.09782. – 2016.

БУХАРЕВ Дмитрий Александрович, аспирант кафедры защиты информации, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: bukharevdmitrii@gmail.com

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sokolovan@susu.ru

РАГОЗИН Андрей Николаевич, кандидат технических наук, доцент кафедры защиты информации, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: ragozinan@susu.ru

BUKHAREV Dmitriy Aleksandrovich, Post-graduate student of the Department of Information Security, South Ural State University (national research university). Russia, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: bukharevdmitrii@gmail.com

SOKOLOV Alexander Nikolaevich, Ph.D., Associate professor, Head of the Department of Information Security, South Ural State University (national research university). Russia, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: sokolovan@susu.ru

RAGOZIN Andrey Nikolaevich, Ph.D., Associate Professor of the Department of Information Security, South Ural State University (national research university). Russia, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: ragozinan@susu.ru