УДК 004.056, 004.089 **DOI 10.52167/1609-1817-2024-132-3-319-328**

Д.Ж. Сатыбалдина, Н.К. Бисенбаева, М.Н. Касенова,
Е.Н. Сейткулов✉, С.С. Жузбаев
Евразийский национальный университет имени им. Л.Н.Гумилева, Астана, Казахстан
E-mail: yerzhan.seitkulov@gmail.com

ИСПОЛЬЗОВАНИЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ СОТОВЫХ СЕТЕЙ СВЯЗИ

Аннотация. Настоящее исследование направлено на систематическое изучение методов искусственного интеллекта для выявления угроз сетевой безопасности, выявления сетевых аномалий и классификации. Целью работы является изучение вопросов безопасности и конфиденциальности в сетях сотовой связи, построения систем обнаружения вторжений на основе передовых методов интеллектуального анализа данных, алгоритмов машинного и глубокого обучения. Представлен обзор методов сбора сетевых данных для анализа, анализ подходов по отбору атрибутов (информативных признаков) нормального трафика и данных, соответствующих различным типам атак, описаны доступные базы (датасеты) сетевых атак. В работе приведены результаты литературного обзора существующих подходов детектирования событий кибербезопасности в сетях сотовой связи, а также результаты исследований по разработке интеллектуальной системы обнаружения аномальных сетевых событий, количественные характеристики производительности алгоритмов классификации сетевых атак.

Ключевые слова. Алгоритмы машинного обучения, базы данных сетевых атак, классификация сетевых аномалий, сети сотовой связи, сетевая безопасность, системы обнаружения вторжений.

Введение.

Развитие и внедрение мобильных технологий нового поколения (5G, а также и Beyond 5G, или B5G, как технологии беспроводной связи следующего поколения после 5G) является основой для цифровой трансформации различных областей экономики, государственного управления и общества, предоставляя в сотни раз больше подключенных мобильных устройств, высокую скорость передачи пользовательских данных, увеличение не менее в 1000 раз объема передаваемых данных в территориальном разрезе и снижение задержки до менее 1 миллисекунды [1]. Автономные транспортные средства [2], умные города и интеллектуальные системы управления транспортными потоками [3], цифровые двойники рудников [4] – это некоторые примеры, для которых системы сотовой связи 5G, и циркулируемые в них большие данные уже играют важную роль, повышая эффективность, безопасность и качество жизни людей.

В то же время высокие характеристики производительности сотовых сетей 5G, повышенная сложность (виртуализация сетевых функций и сетевых элементов, динамическая архитектура сети с множеством точек доступа, интеграция с другими сетями), появление новых уязвимостей и новых видов атак, в том числе на основе искусственного интеллекта – все это требует разработки новых или адаптации имеющихся подходов обесечения кибербезопасности в мобильных коммуникаций нового поколения в режиме реального времени [5].

Исследователи и профессионалы в области кибербезопасности в последние десятилетия разрабатывали научные подходы и практические решения, направленные на устранение угроз конфиденциальности, целостности и доступности. Примерами являются системы управления информацией и событиями безопасности (Security Information and

Event Management, SIEM), межсетевые экраны, системы предотвращения вторжений и обнаружения вторжений (Intrusion Prevention System / Intrusion Detection System, IPS/IDS), статические анализаторы исходного кода и sandbox- системы с динамическим анализом подозрительных файлов. Значительный вклад в повышении эффективности данных решений внесли методы искусственного интеллекта [6]. Интеграция алгоритмов машинного обучения с наборами данных от различных источников информации позволяет IDS -системам эффективно выполнять функции мониторинга и анализа аномалий.

С внедрением технологий мобильных коммуникаций нового поколения, рост скорости передачи и объемов информации, проходящих через сети, затрудняют сбор и анализа всех сетевых пакетов, вследствие чего некоторые инструменты анализа трафика не могут функционировать и распознать потенциальные угрозы безопасности. В работе [7] представлены результаты тестирования производительности IDS-систем Snort и Suricata при различных скоростях передачи данных. Было показано, Snort может правильно работать в проводных сетях со скоростью до 1 Гбит/с. Интеграция Snort и методов машинного обучения позволили несколько повысить эффективность IDS-системы в сетях со скоростью передачи до 4 Гбит/с, дальнейшее повышение скорости приводит к повышению значения среднего процента потери до 20% в сетях со скоростью 10 Гбит/с [8].

Таким образом несмотря на то, что методы обнаружения сетевых аномалий постоянно совершенствуются, их эффективность в задачах обеспечения кибербезопасности современных сотовых сетей связи является недостаточной. Внедрение мобильных технологий 5G и B5G требует развития алгоритмов детектирования сетевых аномалий и их классификации без потери точности обнаружения в условиях реального времени.

В связи с этим целью настоящего исследования работы является изучение приложений машинного обучения и искусственного интеллекта для различных вариантов использования в системах детектирования сетевых атак, которые станут возможными в современных и будущих системах мобильной связи. Представлен обзор методов сбора сетевых данных для анализа, анализ подходов по отбору атрибутов (информативных признаков) нормального трафика и данных, соответствующих различным типам атак, описаны доступные базы (датасеты) сетевых атак. В работе приведены результаты литературного обзора существующих подходов детектирования событий кибербезопасности в сетях сотовой связи, а также результаты исследований по разработке интеллектуальной системы обнаружения аномальных сетевых событий, количественные характеристики производительности алгоритмов классификации сетевых атак

Материалы и методы.

На первом этапе исследований было проведено систематическое картографическое исследование (a Systemical Mapping Study, SMS), направленное на анализ существующих методов и технологий в сфере интеллектуальных методов обеспечения сетевой безопасности в целом, и кибербезопасности сотовых сетей связи, в частности. Были использованы методы библиометрического анализа с использованием как встроенных аналитических функций баз данных научного цитирования, так и специализированного инструмента VOSviewer [9] для визуализации ключевой карты и выделения трендов анализа. В качестве источника данных была выбрана онлайн платформа Web of Science Core Collection (далее - WoS).

В таблице 1 представлены основные параметры поиска:

– ключевые термины в строке поиска;

– период поиска ограничен 5-ю последними годами (с 01.01.2019 г. по 01.04.2024 г.);

– поиск ограничен оригинальными статьями и обзорами на английском языке по категориям Computer Science, Engineering.

На первом этапе был выполнен поиск всех статей и обзоров по запросу, отвечающему использованию методов искусственного интеллекта для целей кибербезопасности (найдено 1006 публикаций).

Таблица 1 - Параметры поиска публикаций по тематике исследований в WoS

Номер поисково запроса	Строка поиска (ключевые слова для поиска)	Период публикаций	Тип публикаций	Язык	Категория	Итог поиска (число статей)
1	“machine learning” AND “cyber security”	2019-2024	article OR review OR er	English	Computer Science OR Telecommunications OR Engineering Or Multidisciplinary	1006
2	(“mobile network” OR “cellular communication”) AND “intrusion detection”	2019-2024	article OR review OR	English	Computer Science OR Telecommunications OR Engineering Or Multidisciplinary	980
3	((“mobile network” OR “cellular communication”)AND “intrusion detection”) AND (“machine learning” AND “cyber security”)	2019-2024	article OR review OR	English	Computer Science OR Telecommunications OR Engineering Or Multidisciplinary	285

На втором этапе поиск был ограничен ключевыми словами, соответствующими методам обнаружения сетевых вторжений в сотовых сетях (980 статей). Итоговый список, полученный объединением (And) результатов двух поисков в WoS, содержит 285 документов (таблица 1). Для анализа 285 статей использован программный инструмент VOS Viewer, версии 1.6.20 [20]. С его помощью созданы визуальные карты ключевых слов (рисунок 1) и цитируемых документов (рисунок 2, таблица 2).

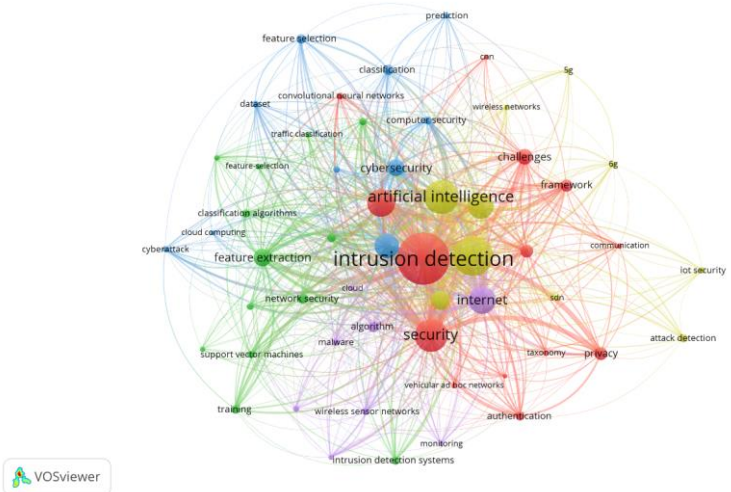

Рисунок 1 - Графическое представление взаимосвязи ключевых слов в публикациях по тематике исследований. На карте представлены ключевые слова, повторившиеся не менее 5 раз

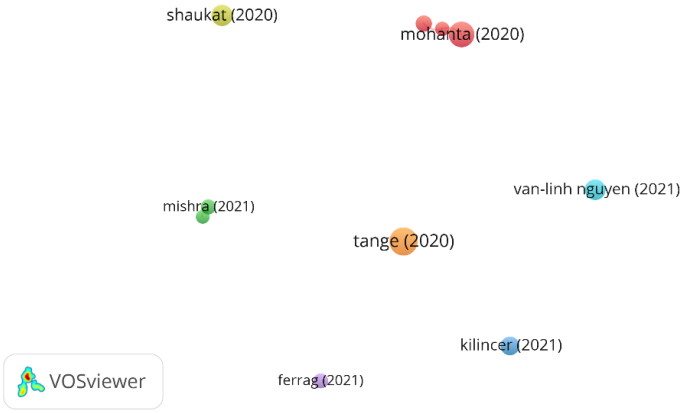

Рисунок 2 - Карта цитирования документов по тематике исследований. На карте представлены документы, имеющие количество цитирования не менее 70

Таблица 2 - Топ 10 публикаций по результатам поиска публикаций по тематике исследований в WoS

№	Выходные данные публикации	Количество цитирований
[10]	Tange K., De Donno M., Fafoutis X. and Dragoni N. A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities // *EEE* Communications Surveys & Tutorials. – 2020. – V. 22. – no. 4.- Pp. 2489-2520.	194
[11]	Mohanta B. K. et al. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology //Internet of Things. – 2020. – V. 11. – P. 100227.	168
[12]	Shaukat K., Luo S., Varadharajan V., Hameed I. A. and Xu M. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade // IEEE Access. – 2020. – V. 8. – Pp. 222310-222354.	135
[13]	Nguyen V. -L., Lin P. -C., Cheng B. -C., Hwang R. -H. and Lin Y. -D. Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges," // IEEE Communications Surveys & Tutorials. – 2021. – V. 23. – no. 4. – Pp. 2384-2428.	129
[14]	Kilincer I. F., Ertam F., Sengur A. Machine learning methods for cyber security intrusion detection: Datasets and comparative study //Computer Networks. – 2021. – V. 188. – P. 107840.	112
[15]	Kumar R. et al. SP2F: A secured privacy-preserving framework for smart agricultural Unmanned Aerial Vehicles //Computer Networks. – 2021. – V. 187. – P. 107819.	93
[16]	Ferrag M. A. and Shu L. The Performance Evaluation of Blockchain-Based Security and Privacy Systems for the Internet of Things: A Tutorial // IEEE Internet of Things Journal. – V. 8. – no. 24. – Pp. 17236-17260.	84
[17]	Mishra N. and Pandya S. Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review // IEEE Access. – 2021. – V. 9. – Pp. 59353-59377.	83
[18]	Kumar P. et al. A Distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT Systems by leveraging Fog computing //Transactions on Emerging Telecommunications Technologies. – 2021. – V. 32. – №. 6. – P. e4112.	77
[19]	Kim A., Park M., Lee D. H. AI-IDS: Application of deep learning to real-time Web intrusion detection //IEEE Access. – 2020. – V. 8. – Pp. 70245-70261.	74

Для карты ключевых слов размер узлов указывает на частоту ключевых слов; толщина линии указывает на силу связи, а цвета обозначают кластеры. Размер узла на карте цитируемых указывает на частоту цитирования автора, а связи между узлами указывают на взаимоотношения между разными авторами. Сила этой связи возрастает с увеличением количества взаимных цитирований. Для сети совместно цитируемых авторов проведен анализ совместно цитируемых авторов, чтобы определить размер влияния различных авторов в области исследования.

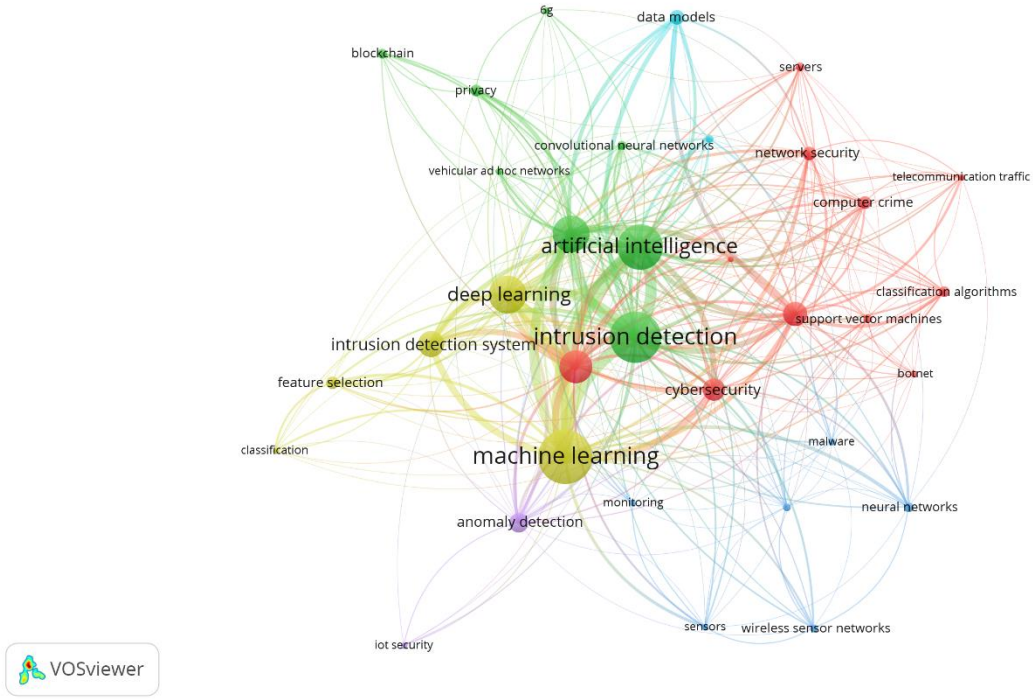

Рисунок 3 - Графическое представление взаимосвязи ключевых слов в публикациях по тематике исследований. На карте представлены ключевые слова из списка терминов, указанных авторами документов, повторившиеся не менее 5 раз

Результаты и обсуждение.

SMS -анализ выявил 1226 ключевых слов, из которых 101 слово встречается не менее пяти раз в заголовках и аннотациях выбранных 285 статей. Все ключевые слова объединены в 5 кластеров. Среди 285 статей количество цитирований более 10 имеют 90 документов, более 70 раз процитированы 10 документов (таблица 2). На карте цитируемых документов отсутствуют связи между кластерами, что указывает на отсутствие взаимных цитирований между авторами данных документов.

Анализ ключевых слов выполнен на основе списков ключевых терминов, указанных авторами при подготовке рукописи статей, а также дополнительных ключевых слов, предоставленных редакциями изданий. На рисунке 3 представлена карта ключевых слов, созданная на основе только ключевых слов, указанных авторами документов.

На основе анализа ключевых слов из аннотации документов по тематике исследований, индексируемых в Web of Science Core Collection, можно сделать следующие выводы:

– для детектирования сетевых аномалий используются как алгоритмы машинного обучения (Decision Trees, Support Vector Machines, Nearest Neighbor Search, Random Forest, Logistic Regression, KNN, Adaptive Boosting), так и технологии глубокого обучения (Convolutional Neural Network, Recurrent Neural Networks, Long Short-term Memory);

– основные виды сетевых атак, детектируемых с использованием методов искусственного интеллекта, являются Botnet, Denial-of-service Attack, Distributed Denial Of Service;

– объектами исследований являются преимущественно системы Интернета вещей, незначительное количество работ посвящено исследованиям интеллектуальных систем детектирования вторжений для сетей сотовой связи [21-23];

– наиболее часто используемыми открытыми наборами данных для обучения и тестирования систем обнаружения сетевых вторжений являются CTU [24], NSL-KDD [25], UNSW-NB15B [26], CSE-CIC IDS-2018 [27], bot-IoT [28].

Источниками данных для создания датасетов для сетевых IDS -систем являются пакеты (парсинг пакетов, анализ полезной нагрузки), потоки (связанные пакеты), log-файлы журнала на основе окон сеанса [6]. В потоковых IDS (рисунок 4) вместо просмотра всех пакетов, проходящих через сетевое соединение, собирается агрегированная информацию о связанных пакетах сетевого трафика в виде потока, к анализу которого применяются методы извлечения признаков и нейронные сети глубокого обучения.

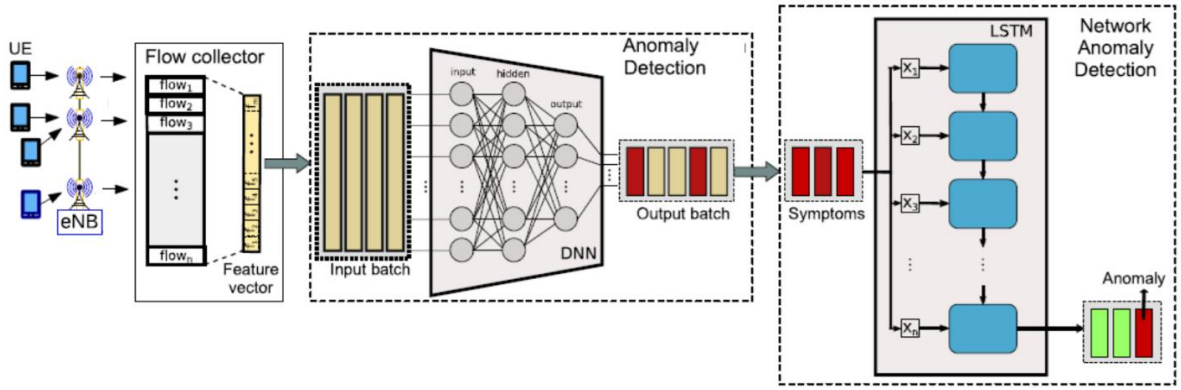

Рисунок 4 - Потоковая IDS -система, адаптированная для сотовых сетей [21]

Каждый поток содержит агрегированную информацию о количестве переданных пакетов и байтов, IP-адреса и порты источника и назначения, временные метки, флаги TCP, сетевые маски и другие параметры.

В ходе эксперимента были собраны обучающие выборки из набора данных CTU [24] для 5 сценариев ботнет атак. На первом этапе для извлечения признаков аномальных и номральных состояний сети использована сверточная нейронная сеть, реализованная в виде Python-приложения для интерактивных вычислений (файл формата ipynb), содержащие исходный код, входные данные, результаты вычислений в числовом и графическом представлении. На втором этапе распознавание сетевых аномалий реализовано с использованием алгоритмов машинного обучения. В таблице 3 представлены оценки производительности использованных алгоритмов классификации для известных ботнет атак из датасета CTU.

Таблица 3 - Метрики точности алгоритмов классификации сетевых атак

Алгоритм	**Accuracy**	**Precision**	**Recall**	**F-score**
Random Forest	0,94	0,94	0,94	0,94
Decision Tree	0,86	0,89	0,86	0,87
Logistic Regression	0,91	0,91	0,91	0,91
Support Vector Machines	0,70	0,84	0,70	0,73

Заключение.

В работе представлены результаты систематического изучения методов и алгоритмов искусственного интеллекта для выявления угроз сетевой безопасности, классификации атак и сетевых аномалий в сетях сотовой связи, адаптации систем обнаружения вторжений, под требования технологий мобильной связи нового поколения. В рамках данного исследования проведено картографическое исследование с использованием методов и инструментов биометрического анализа публикаций за последние 5 лет в Web of Science Core Collection. На основе анализа существующих методов и технологий в сфере интеллектуальных методов обеспечения кибербезопасности сотовых сетей связи выявлены наиболее эффективные алгоритмы машинного обучения и архитектуры глубоких нейронных сетей, используемые для детектирования основных классов кибератак в мобильных коммуникациях, определены наборы открытых данных для обучения и тестирования сетевых IDS -систем, определены ключевые тенденции и направления развития данной области исследований. В экспериментальной части реализованы методы сбора сетевых данных для анализа, проанализированы методы отбора атрибутов (информативных признаков) нормального и аномального трафика, представлены оценки производительности обнаружения и классификации аномальных событий в сетях сотовой связи.

Благодарности. Данная работа выполнена при финансовой поддержке Комитета науки Министерства науки и высшего образования Республики Казахстан (ПЦФ № BR18574045).

ЛИТЕРАТУРА

[1] The 5G-Infrastructure-PPP. Key Performance Indicators (KPI) of new communication networks. Available online: http://5g-ppp.eu/kpis (accessed on 16 March 2024).

[2] Hakak, S., Gadekallu, T. R., Maddikunta, P. K. R., Ramu, S. P., Parimala, M., De Alwis, C., & Liyanage, M. Autonomous Vehicles in 5G and beyond: A Survey // Vehicular Communications. – 2023. – V. 39. – Paper Number. 100551.

[3] Guevara L., Auat Cheein F. The role of 5G technologies: Challenges in smart cities and intelligent transportation systems // Sustainability. – 2020. – V. 12. – №. 16. – Paper Number. 6469.

[4] Chen, L., Hu, X., Wang, G., Cao, D., Li, L., & Wang, F. Y. Parallel mining operating systems: From digital twins to mining intelligence. // 2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI). – IEEE, 2021. – Pp. 469-473.

[5] Ramezanpour K., Jagannath J., Jagannath A. Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective // Computer Networks. – 2023. – V. 221. – Paper Number. 109515.

[6] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. A survey on machine learning techniques for cyber security in the last decade // IEEE access. – 2020. – V. 8. – Pp. 222310-222354.

[7] Richariya V., Singh U. P., Mishra R. Distributed approach of intrusion detection system: Survey // International Journal of Advanced Computer Research. – 2012. – V. 2. – №. 4. – Paper Number 358.

[8] Shah S. A. R., Issac B. Performance comparison of intrusion detection systems and application of machine learning to Snort system // Future Generation Computer Systems. – 2018. – V. 80. – Pp. 157-170.

[9] Van Eck, N.J.; Waltman, L.; Noyons, E.C.M.; Buter, R.K. Automatic term identification for bibliometric mapping // Science. – 2010. – V. 82. – Pp. 581–596.

[10] Tange K., De Donno M., Fafoutis X. and Dragoni N. A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities // *EEE* Communications Surveys & Tutorials. – 2020. – V. 22. – no. 4.- Pp. 2489-2520.

[11] Mohanta B. K. et al. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology //Internet of Things. – 2020. – V. 11. – P. 100227.

[12] Shaukat K., Luo S., Varadharajan V., Hameed I. A. and Xu M. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade // IEEE Access. – 2020. – V. 8. – Pp. 222310-222354.

[13] Nguyen V. -L., Lin P. -C., Cheng B. -C., Hwang R. -H. and Lin Y. -D. Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges," // IEEE Communications Surveys & Tutorials. – 2021. – V. 23. – no. 4. – Pp. 2384-2428.

[14] Kilincer I. F., Ertam F., Sengur A. Machine learning methods for cyber security intrusion detection: Datasets and comparative study //Computer Networks. – 2021. – V. 188. – P. 107840.

[15] Kumar R. et al. SP2F: A secured privacy-preserving framework for smart agricultural Unmanned Aerial Vehicles //Computer Networks. – 2021. – V. 187. – P. 107819.

[16] Ferrag M. A. and Shu L. The Performance Evaluation of Blockchain-Based Security and Privacy Systems for the Internet of Things: A Tutorial // IEEE Internet of Things Journal. – V. 8. – no. 24. – Pp. 17236-17260.

[17] Mishra N. and Pandya S. Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review // IEEE Access. – 2021. – V. 9. – Pp. 59353-59377.

[18] Kumar P. et al. A Distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT Systems by leveraging Fog computing //Transactions on Emerging Telecommunications Technologies. – 2021. – V. 32. – №. 6. – P. e4112.

[19] Kim A., Park M., Lee D. H. AI-IDS: Application of deep learning to real-time Web intrusion detection //IEEE Access. – 2020. – V. 8. – Pp. 70245-70261.

[20] Van Eck, N.; Waltman, L. Manual for VOS Viewer Version 1.6.10, CWTS, Universiteit Leiden, Leiden, Holland, 2019.

[21] Maimó L.F et al. A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks // IEEE Access. – 2018. – V. 6. – Pp. 7700-7712.

[22] Kohli P., Sharma S., Matta P. Intrusion Detection Techniques for Security and Privacy of 6G Applications //2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC). – IEEE, 2023. – Pp. 560-565.

[23] Saeed, M. M., Saeed, R. A., Abdelhaq, M., Alsaqour, R., Hasan, M. K., & Mokhtar, R. A. Anomaly detection in 6G networks using machine learning methods //Electronics. – 2023. – V. 12. – №. 15. – P. 3300.

[24] Garcia S. et al. An empirical comparison of botnet detection methods // Computers & security. – 2014. – V. 45. – Pp. 100-123.

[25] NSL-KDD99 Dataset. 2009. Available online: https://www.unb.ca/cic/datasets/nsl.html (accessed on on 16 March 2024).

[26] Moustafa N., Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set) // 2015 military communications and information systems conference (MilCIS). – IEEE, 2015. – Pp. 1-6.

[27] Sharafaldin I. et al. Toward generating a new intrusion detection dataset and intrusion traffic characterization //ICISSp. – 2018. – V. 1. – Pp. 108-116.

[28] Koroniotis N. et al. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset //Future Generation Computer Systems. – 2019. – V. 100. – Pp. 779-796.

Дина Сатыбалдина, ф.-м.ғ.к., қауымдастырылған профессор, Л.Н.Гумилев атындағы Евразиялық ұлттық университеті, Астана, Қазақстан, satybaldina_dzh@enu.kz

Назерке Бисенбаева, докторант, Л.Н.Гумилев атындағы Евразиялық ұлттық университеті, Астана, Қазақстан, n.kobylandievna@gmail.com

Мерейлим Касенова, докторант, Л.Н.Гумилев атындағы Евразиялық ұлттық университеті, Астана, Қазақстан, mikassen@gmail.com

Ержан Сейткұлов, ф.-м.ғ.к., қауымдастырылған профессор, Л.Н.Гумилев атындағы Евразиялық ұлттық университеті, Астана, Қазақстан, yerzhan.seitkulov@gmail.com

Серік Жүзбаев, ф.-м.ғ.к., қауымдастырылған профессор, Л.Н.Гумилев атындағы Евразиялық ұлттық университеті, Астана, Қазақстан

ҰЯЛЫ БАЙЛАНЫС ЖЕЛІЛЕРІНІҢ КИБЕРҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ҮШІН ЖАСАНДЫ ИНТЕЛЛЕКТ ӘДІСТЕРІН ҚОЛДАНУ

Аңдатпа. Бұл зерттеу желілік қауіпсіздік қатерлерін анықтау, желілік ауытқуларды анықтау және жіктеу үшін жасанды интеллект әдістерін жүйелі түрде зерттеуге бағытталған. Жұмыстың мақсаты-ұялы байланыс желілеріндегі қауіпсіздік пен құпиялылық мәселелерін зерттеу, деректерді өндірудің озық әдістері, машиналық және терең оқыту алгоритмдері негізінде интрузияны анықтау жүйелерін құру. Талдау үшін желілік деректерді жинау әдістеріне шолу, қалыпты трафиктің атрибуттарын (ақпараттық ерекшеліктерін) және әртүрлі шабуыл түрлеріне сәйкес келетін деректерді таңдау тәсілдерін талдау, қол жетімді желілік шабуыл базалары (деректер жиынтығы) сипатталған. Жұмыста ұялы байланыс желілеріндегі киберқауіпсіздік оқиғаларын анықтаудың қолданыстағы тәсілдеріне әдеби шолу нәтижелері, сондай-ақ аномальды желілік оқиғаларды анықтаудың интеллектуалды жүйесін әзірлеу бойынша зерттеулер нәтижелері, желілік шабуылдарды жіктеу алгоритмдерінің өнімділігінің сандық сипаттамалары келтірілген.

Түйінді сөздер. Машиналық оқыту алгоритмдері, желілік шабуыл дерекқорлары, желілік ауытқулардың жіктелуі, ұялы байланыс желілері, желілік қауіпсіздік, кіруді анықтау жүйелері.

Dina Satybaldina, candidate of physical and mathematical sciences, associate professor, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, satybaldina_dzh@enu.kz

Nazerke Bisenbayeva, doctoral student, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, n.kobylandievna@gmail.com

Mereilim Kassenova, doctoral student, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, mikassen@gmail.com

Yerzhan Seitkulov, candidate of physical and mathematical sciences, associate professor, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, yerzhan.seitkulov@gmail.com

Serik Zhuzbayev, candidate of physical and mathematical sciences, associate professor, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

ARTIFICIAL INTELLIGENCE METHODS USING FOR ENSURING THE CYBERSECURITY OF CELLULAR COMMUNICATION NETWORKS

Abstract. The systematic study of artificial intelligence methods to identify threats to network security, identify network anomalies and its classification are considered in present paper. The purpose of the work is to study security and privacy issues in cellular networks,

development of the intrusion detection systems based on advanced data mining methods, machine learning algorithms and deep learning. An overview of methods for collecting network data for analysis is presented. An analysis of approaches for features extraction for normal traffic and attacks is described. Open datasets of network attacks are described. The paper presents the results of a literary review of existing approaches to detecting cybersecurity events in cellular networks, as well as the results of research on the development of an intelligent system for detecting abnormal network events, quantitative performance characteristics of algorithms for classifying network attacks.

Keywords. Machine learning algorithms, datasets of network attacks, classification of network anomalies, cellular networks, network security, intrusion detection systems.

****