МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.23670/IRJ.2023.133.112

ВЫЯВЛЕНИЕ УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Научная статья

Силантьев И.О.[1, *], Аникин И.В.[2]
[1] ORCID : 0009-0007-9145-1876;
[1, 2] Казанский национальный исследовательский технический университет им. А.Н. Туполева, Казань, Российская Федерация

* Корреспондирующий автор (i.silantev[at]icloud.com)

Аннотация

Целью работы стал аналитический обзор различных технических подходов для решения задач выявления утечек конфиденциальной информации, позволяющих создать более защищенную информационную среду. Обозначены некоторые проблемы защиты конфиденциальной информации с использованием современных средств обеспечения безопасности и представлены возможные направления их решения.

В данной работе рассматриваются такие технические решения, как DLP, UEBA, SIEM системы. Проводится анализ использования методов машинного обучения и алгоритмов искусственного интеллекта, а также описывается проблема, с которой сталкивается большинство проектов, использующие методы машинного обучения.

Предлагаются способы решения проблем методов машинного обучения в решении задач выявления утечек конфиденциальной информации.

Ключевые слова: информационная безопасность, утечки конфиденциальной информации, DLP, UEBA, SIEM, методы машинного обучения, алгоритмы искусственного интеллекта.

IDENTIFICATION OF LEAKS OF CONFIDENTIAL INFORMATION IN INFORMATION SYSTEMS

Research article

Silantev I.O.[1, *], Anikin I.V.[2]
[1] ORCID : 0009-0007-9145-1876;
[1, 2] Kazan National Research Technical University named after A.N. Tupolev, Kazan, Russian Federation

* Corresponding author (i.silantev[at]icloud.com)

Abstract

The aim of the work was to analyse various technical approaches for solving the problems of detecting confidential information leaks, allowing to create a more secure information environment. Some problems of confidential information protection using modern security tools are outlined and possible directions of their solution are presented.

This article discusses technical solutions such as DLP, UEBA, and SIEM systems. It analyses the use of machine learning methods and artificial intelligence algorithms and describes the problem faced by most projects using machine learning methods.

The ways of solving the problems of machine learning methods in dealing with the problems of detecting leaks of confidential information are proposed.

Keywords: information security, confidential information leaks, DLP, UEBA, SIEM, machine learning methods, artificial intelligence algorithms.

Введение

Возможные утечки конфиденциальной информации, обрабатываемой в информационных системах, являются актуальной проблемой в настоящее время, несмотря на активное развитие систем защиты информации, направленных на противодействие этому.

Под утечкой конфиденциальной информации понимается такое негативное событие, при котором информация, содержащая ценные сведения, без согласия владельца становится доступной лицу или группе лиц, не имеющих разрешения на доступ к этой информации.

Методы и принципы исследования

Согласно данным аналитического центра InfoWatch [23], всего в базу утечек за 2022г. было внесено 6856 случаев преднамеренной и случайной компрометации конфиденциальных данных в госсекторе и коммерческих организациях по всему миру, что в свою очередь 3,57 раза больше, чем за 2021 год (см. рис. 1).

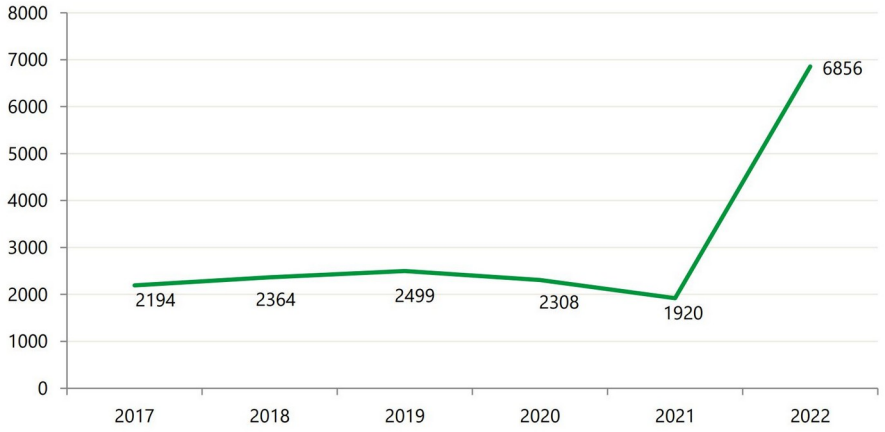

Рисунок 1 - Число зарегистрированных утечек информации, Мир за 2017-2022
DOI: https://doi.org/10.23670/IRJ.2023.133.112.1

Согласно исследованию [1] в 2022 году в открытый доступ попало свыше 2 млрд записей, содержащих конфиденциальную информацию. Пользовательских данных 300 млн записей, из которых 16% – около 48 млн строк – содержали пароли. Большую часть данных (64%) скомпрометировали вследствие атак на крупный бизнес.

Аналитиками из InfoWatch тоже был зафиксирован тренд смещения причин утечек конфиденциальной информации от внутренних нарушителей, в сторону внешних нарушителей. Отдельно стоит отметить рекордный рост доли утечек, в которых на момент публикации факта утечки данных не были известны причины, тип нарушителя и методы совершения компрометации данных (см. рис. 2).

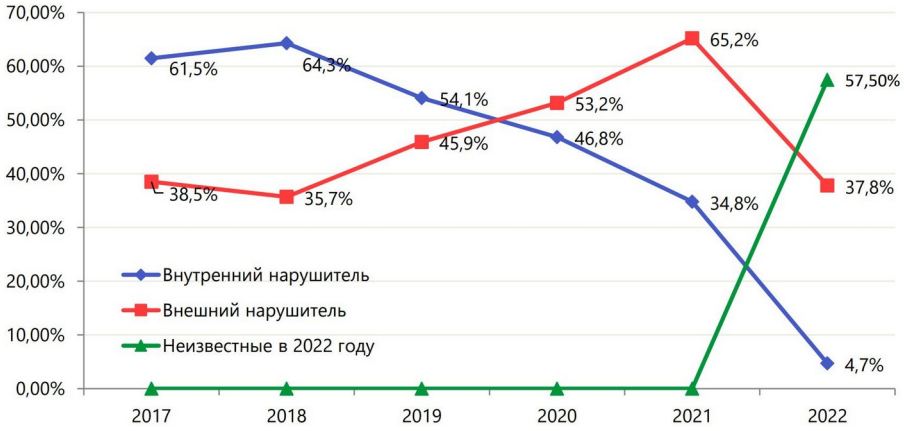

Рисунок 2 - Распределение утечек информации по вектору воздействия (внешний/внутренний): Мир, 2017–2022 гг.
DOI: https://doi.org/10.23670/IRJ.2023.133.112.2

Как правило, причины утечек могут быть различными: кибератаки, ошибки в системах безопасности или действия внутренних сотрудников. Независимо от причин утечки информации, последствия этого могут быть катастрофическими. Утечки конфиденциальной информации приводят к потере конкурентного преимущества, нарушению репутации и утрате доверия клиентов и/или партнеров, штрафам, судебным разбирательствам, что в итоге приводит к финансовым потерям.

С целью минимизации последствий от утечек конфиденциальной информации применяются различные методы и средства защиты информации: организационно-правовые и технические. Наиболее полно эти методы приводятся в работе [2], в данной работе нас будут интересовать только технические меры защиты информации.

Основные результаты

Одним из основных технических средств, используемых для борьбы с утечкой конфиденциальной информации, являются системы выявления таких утечек (Data Leakage Prevention – DLP). Данный класс средств предназначен для выявления и блокирования попыток несанкционированной передачи данных за пределы корпоративной сети [3]. Большинство DLP систем используют лингвистические методы выявления утечек информации. Среди основных их недостатков можно выделить следующие:

- проблема классификации и категорирования конфиденциальной информации;
- отсутствие возможности прогнозирования негативного сценария для принятия своевременных действий для недопущения утечки конфиденциальной информации, как следствие реагирование на утечки происходит постфактум;
- ограничение в создании сложных корреляций, как следствие неспособность противодействовать методам обхода систем контроля утечек конфиденциальной информации со стороны высококвалифицированных нарушителей;

- отсутствие возможности противодействия внешним нарушителям.

В организациях обрабатывается большое количество различной информации. Проблема классификации и категорирования конфиденциальной информации связана с трудоёмкостью процесса определения полного и точного перечня конфиденциальной информации в конкретной организации. Для решения данной проблемы организациями используются автоматизированные системы маркирования конфиденциальной информации, которые помогают организовать процесс создания документов таким образом, что пользователь информационной системы, который создает электронный файл, на этапе сохранения ее определил ее уровень конфиденциальности самостоятельно. В результате определения уровня конфиденциальности в электронном файле проставляется графический объект, обозначающий уровень конфиденциальности, и добавляется невидимый для пользователя набор символов, позволяющие DLP системе в момент передачи документа определить критичность нарушения. Данный подход значительно позволяет упростить задачу категорирования информации, но он не защищает от преднамеренного занижения уровня конфиденциальности документа с чувствительной информацией.

Для борьбы с проблемой совершения преднамеренных нарушений пользователями информационной системы правил информационной безопасности, организациями применяются системы выявления аномального поведения пользователя (UEBA) [4]. Среди основных недостатков применения технологий поведенческого анализа выделяют:

- наличие ошибок первого и второго рода, т.е. событие может детектироваться системой обнаружения как угроза (угрозой не являясь) или, наоборот, аномальная активность может быть воспринята как легитимная;
- отсутствие в прозрачности в принятии решения о выявлении аномалии самой моделью;
- необходимость постоянной корректировки профиля поведения пользователей;
- низкая эффективность противодействия против отложенных сложных атак и угроз злоупотреблений со стороны инсайдеров, в том числе и против внешнего нарушителя.

Высокую актуальность в организациях в настоящее время приобретает создание ситуационных центров мониторинга событий информационной безопасности (Security Operations Center – SOC). Основной целью таких центров является своевременное выявление и предотвращение инцидентов, связанных с внешними нарушителями. В основе SOC используется система анализа событий информационной безопасности (Security Information and Event Management – SIEM), которая агрегирует события информационной безопасности от различных источников (межсетевые экраны, антивирусы, системы противодействия сетевым вторжениям, DLP системы, UEBA системы и т.д.) и на основании правил корреляций выявляет подозрительные события в информационных системах. Основной парадигмой в работе SOC является выявление несанкционированных действий злоумышленника на объектах информатизации до момента совершения им негативного события, в том числе компрометации конфиденциальной информации. Проблема данного подхода заключается в том, что в центре внимания сотрудников ситуационного центра находятся информационное объекты и события их возможной компрометации, а не события компрометации конфиденциальной информации. В итоге при недостаточном полном наборе правил корреляций в организациях происходят события утечки конфиденциальной информации до момента выявления компрометации информационного объекта, который эту информацию обрабатывал.

Особую актуальность проблеме утечек информации придает тот факт, что в большинстве случаев конфиденциальность, как свойство информации, крайне сложно, а порой невозможно, восстановить. Например, если пользовательские логины и пароли в информационных системах можно сменить с использованием средств автоматизации за короткий временной период, то информация, содержащая персональные данные, секреты производства или секретные сведения государства, не теряют свою актуальность и ценность на протяжении долгого времени с момента их компрометации. В связи с этим, в задачах выявления утечек конфиденциальной информации необходимо применять проактивные меры, включающие в себя этапы корректного категорирования информации, выявления предпосылок для утечек конфиденциальной информации (изменения в поведении пользователя информационной системы, контексте пользователя, появлении уязвимостей публичных приложений), прогнозирования совершения несанкционированных действий и применения оперативных действий для недопущения негативного события. Для решения ряда из перечисленных задач могут быть использованы методы машинного обучения, которые дополняют корреляционную логику SIEM систем.

Обсуждение

В последнее время известно о широком использовании следующих подходов при решении задач выявления утечек конфиденциальной информации с использованием методов машинного обучения:

- анализ потока данных: алгоритмы машинного обучения применяются для анализа потока данных, например, сетевого трафика или журналов системных событий и позволяют обнаруживать аномальные паттерны и поведения, которые могут свидетельствовать о возможной утечке конфиденциальной информации [5], [6], [7];
- анализ поведения пользователей: алгоритмы машинного обучения и искусственного интеллекта используются для анализа поведения пользователей в системе, с целью определения, какие действия могут свидетельствовать о возможной утечке конфиденциальной информации [8], [9], [10];
- моделирование угроз: алгоритмы машинного обучения позволяют моделировать различные угрозы и определять, какие данные могут быть наиболее уязвимыми. Это позволяет компаниям и организациям принимать предупредительные меры и улучшать свои системы безопасности [11], [12], [13];
- анализ содержания данных: алгоритмы машинного обучения помогают производить анализ содержания данных, например, текстовых документов или электронных писем, для обнаружения утечек конфиденциальной информации [14], [15], [16];
- анализ социальных сетей: алгоритмы машинного обучения могут использоваться для анализа социальных сетей и других источников информации [17], [18];

- мониторинг устройств: алгоритмы машинного обучения успешно применяют для мониторинга устройств, например, мобильных устройств и ноутбуков, что позволяет обнаруживать утечки конфиденциальной информации [19], [20];

Одним из основных недостатков применения методов машинного обучения при решении задач выявления утечек конфиденциальной информации является неустойчивость применяемых алгоритмов. Данная проблема описана в работе [21]. Неустойчивость алгоритмов возникает, когда на этапе обучения были достигнуты требуемые показатели работы (включая тестовую и валидационную выборку), а на этапе практической эксплуатации требуемые показатели не достигаются. Согласно результатам работы [22] процент неудачных проектов в области машинного обучения равен 87%. Применительно к противодействию утечкам конфиденциальной информации, это происходит по следующим причинам:

- отсутствие репрезентативных наборов данных для обучения разрабатываемых алгоритмов;
- репрезентативный набор данных для одной организации, может полностью отличаться от репрезентативного набора другой организации, что затрудняет распространение применения успешных разработок с использованием машинного обучения;
- различающиеся наборы источников данных, т.е. в различных организациях могут быть использованы различные SIEM, DLP системы, что затрудняет разработку универсальных алгоритмов.

Следует отметить, что для противодействия утечкам конфиденциальной информации необходимо ориентироваться в первую очередь не на создание принципиально новых алгоритмов машинного обучения, а на создании универсальной методологии использования существующих алгоритмов применительно к различным источникам данных. В рамках такой методологии необходима:

- разработка единого подхода к представлению данных о событиях информационной безопасности для последующего применения методов машинного обучения;
- создание универсального подхода к применению методов машинного обучения, решающего проблему неустойчивости;
- реализация датацентрического подхода, ставящего конфиденциальную информацию в основу дальнейшего анализа.

Заключение

Несмотря на развитие современных методов анализа информации, для специалистов по информационной безопасности остается актуальной проблема выявления утечек конфиденциальной информации. Решение этой проблемы ставит амбициозные цели, направленные на дальнейшее совершенствование подходов к использованию методов машинного обучения в данной проблемной области.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Значимые утечки данных в 2022 году [Электронный ресурс] // Аналитический отчёт команды Kaspersky Digital Footprint Intelligence. — 2023. — URL: https://go.kaspersky.com/ru-data-leakage-report-2022. (дата обращения: 16.05.23)

2. Борлакова М.А. Современные методы и средства защиты информации. / М.А. Борлакова // Вестник Академии знаний. — 2023. — 54(1). — с. 68-72.

3. Гречанная А.Ю. DLP-системы и их роль в защите от утечек конфиденциальной информации. / А.Ю. Гречанная, А.Д. Тастенов // Наука и техника Казахстана. — 2015. — №3-4. — с. 23-27.

4. Миронова Н.Г. Об использовании методов предиктивного анализа для защиты информационной инфраструктуры. / Н.Г. Миронова // Национальная ассоциация ученых. — 2021. — №74. — с. 45-47.

5. Li W. Real-Time Data Leakage Detection in Cloud Environment Using Machine Learning Techniques. / W. Li, D. Zhang, L. Zhang // Journal of Parallel and Distributed Computing. — 2019. — 131. — p. 101-112.

6. Zhang H. A Data Stream-Based Method for Detecting Confidential Data Leakage in Cloud Computing. / H. Zhang, G. Liu, B. Luo et al. // IEEE Access. — 2018. — 6. — p. 32808-32819.

7. Zhang Q. Detecting Data Leakage in Cloud Computing: Challenges and Solutions. / Q. Zhang, Y. Li, K. Ren // IEEE Network. — 2018. — 32(2). — p. 96-103.

8. Yu X. Detecting Anomalous User Behavior for Insider Threat Detection in Cloud Computing. / X. Yu, J. Liu, X. Wu // Future Generation Computer Systems. — 2020. — 102. — p. 1147-1159.

9. Nassehzadeh-Tabrizi A. Detecting Insider Threats Using User Behavior Analysis in Information Systems. / A. Nassehzadeh-Tabrizi // Computers & Security. — 2019. — 81. — p. 67-83.

10. Khan M.S. Detecting Insider Threats in Cyber-Physical Systems Using User Behavior Analysis. / M.S. Khan, S. Iqbal // Journal of Network and Computer Applications. — 2019. — 140. — p. 152-162.

11. Almukaynizi M. Detecting Data Exfiltration Using Machine Learning Techniques. / M. Almukaynizi, S. Bokhari, M.S. Malik et al. // Future Generation Computer Systems. — 2019. — 92. — p. 245-259.

12. Papamartzivanos D. Towards a Machine Learning Framework for Insider Threat Modelling. / D. Papamartzivanos, H. Mouratidis // Computers & Security. — 2019. — 82. — p. 350-366.
13. Shahid M. Machine Learning-Based User and Entity Behavior Analysis for Insider Threat Detection. / M. Shahid, S.U. Khan, A.M. Hamza // IEEE Access. — 2018. — 6. — p. 62544-62556.
14. Bahrami A. Content-Based Data Leak Prevention Using Machine Learning Techniques. / A. Bahrami, G.F. Cretu, M. St-Hilaire // IEEE Access. — 2020. — 8. — p. 205897-205910.
15. Fei H. A Machine Learning-Based Approach for Data Leakage Detection in Cloud Computing. / H. Fei, Z. Ma, L. Wei et al. // Journal of Ambient Intelligence and Humanized Computing. — 2020. — 11(12). — p. 5699-5711.
16. Karygiannis T. Machine Learning-Based Detection of Data Exfiltration over DNS. / T. Karygiannis, T. Phillips, R. Kuhn // Computers & Security. — 2019. — 85. — p. 28-45.
17. Li Y. Social Network Analysis for Information Leakage Detection Using Machine Learning Techniques. / Y. Li, D. Zhao, L. Guo et al. // Journal of Ambient Intelligence and Humanized Computing. — 2020. — 11(12). — p. 5673-5684.
18. Mishra S. Detecting Insider Threats in Social Media Using Machine Learning Techniques. / S. Mishra, P. Tiwari // Journal of Ambient Intelligence and Humanized Computing. — 2019. — 10(9). — p. 3607-3617.
19. Lee K. A Machine Learning-Based Approach for Device Monitoring and Anomaly Detection in IoT Environments. / K. Lee, T. Kwon, J. Kim // Computers & Security. — 2020. — 92. — p. 101717.
20. Ahn G.J. MINDS: A Framework for IoT Device Monitoring and Security Event Prediction. / G.J. Ahn, H. Hu, H. Chen et al. // IEEE Internet of Things Journal. — 2018. — 6(4). — p. 6977-6986.
21. Nigam A. Anomaly Detection in IoT Systems Using Machine Learning and Fuzzy Logic. / A. Nigam, S. Kundu // Journal of Ambient Intelligence and Humanized Computing. — 2019. — 10(2). — p. 715-731.
22. Намиот D.E. О причинах неудач проектов машинного обучения. / D.E. Намиот, E.A. Ильюшин // International Journal of Open Information Technologies. — 2023. — 11(1).
23. Утечки информации ограниченного доступа в мире 2022 г. [Электронный ресурс] // ЭАЦ ГК InfoWatch. — 2023. — URL: https://www.infowatch.ru/analytics/analitika/utechki-informatsii-ogranichennogo-dostupa-v-mire-2022-g . (дата обращения: 16.05.23)

Список литературы на английском языке / References in English

1. Znachimy'e utechki danny'x v 2022 godu [Significant data breaches in 2022] [Electronic source] // Analytical report of the Kaspersky Digital Footprint Intelligence team. — 2023. — URL: https://go.kaspersky.com/ru-data-leakage-report-2022. (accessed: 16.05.23) [in Russian]
2. Borlakova M.A. Sovremenny'e metody' i sredstva zashhity' informacii [Modern Methods and Means of Information Protection]. / M.A. Borlakova // Vestnik Akademii znanij [Bulletin of the Academy of Knowledge]. — 2023. — 54(1). — p. 68-72. [in Russian]
3. Grechannaya A.Yu. DLP-sistemy' i ix rol' v zashhite ot utechek konfidencial'noj informacii [DLP Systems and Their Role in Protection against Leaks of Confidential Information]. / A.Yu. Grechannaya, A.D. Tastenov // Nauka i texnika Kazaxstana [Science and Technology of Kazakhstan]. — 2015. — №3-4. — p. 23-27. [in Russian]
4. Mironova N.G. Ob ispol'zovanii metodov prediktivnogo analiza dlya zashhity' informacionnoj infrastruktury' [On the Use of Predictive Analysis Methods to Protect Information Infrastructure]. / N.G. Mironova // Nacional'naya associaciya ucheny'x [National Association of Scientists]. — 2021. — №74. — p. 45-47. [in Russian]
5. Li W. Real-Time Data Leakage Detection in Cloud Environment Using Machine Learning Techniques. / W. Li, D. Zhang, L. Zhang // Journal of Parallel and Distributed Computing. — 2019. — 131. — p. 101-112.
6. Zhang H. A Data Stream-Based Method for Detecting Confidential Data Leakage in Cloud Computing. / H. Zhang, G. Liu, B. Luo et al. // IEEE Access. — 2018. — 6. — p. 32808-32819.
7. Zhang Q. Detecting Data Leakage in Cloud Computing: Challenges and Solutions. / Q. Zhang, Y. Li, K. Ren // IEEE Network. — 2018. — 32(2). — p. 96-103.
8. Yu X. Detecting Anomalous User Behavior for Insider Threat Detection in Cloud Computing. / X. Yu, J. Liu, X. Wu // Future Generation Computer Systems. — 2020. — 102. — p. 1147-1159.
9. Nassehzadeh-Tabrizi A. Detecting Insider Threats Using User Behavior Analysis in Information Systems. / A. Nassehzadeh-Tabrizi // Computers & Security. — 2019. — 81. — p. 67-83.
10. Khan M.S. Detecting Insider Threats in Cyber-Physical Systems Using User Behavior Analysis. / M.S. Khan, S. Iqbal // Journal of Network and Computer Applications. — 2019. — 140. — p. 152-162.
11. Almukaynizi M. Detecting Data Exfiltration Using Machine Learning Techniques. / M. Almukaynizi, S. Bokhari, M.S. Malik et al. // Future Generation Computer Systems. — 2019. — 92. — p. 245-259.
12. Papamartzivanos D. Towards a Machine Learning Framework for Insider Threat Modelling. / D. Papamartzivanos, H. Mouratidis // Computers & Security. — 2019. — 82. — p. 350-366.
13. Shahid M. Machine Learning-Based User and Entity Behavior Analysis for Insider Threat Detection. / M. Shahid, S.U. Khan, A.M. Hamza // IEEE Access. — 2018. — 6. — p. 62544-62556.
14. Bahrami A. Content-Based Data Leak Prevention Using Machine Learning Techniques. / A. Bahrami, G.F. Cretu, M. St-Hilaire // IEEE Access. — 2020. — 8. — p. 205897-205910.
15. Fei H. A Machine Learning-Based Approach for Data Leakage Detection in Cloud Computing. / H. Fei, Z. Ma, L. Wei et al. // Journal of Ambient Intelligence and Humanized Computing. — 2020. — 11(12). — p. 5699-5711.
16. Karygiannis T. Machine Learning-Based Detection of Data Exfiltration over DNS. / T. Karygiannis, T. Phillips, R. Kuhn // Computers & Security. — 2019. — 85. — p. 28-45.
17. Li Y. Social Network Analysis for Information Leakage Detection Using Machine Learning Techniques. / Y. Li, D. Zhao, L. Guo et al. // Journal of Ambient Intelligence and Humanized Computing. — 2020. — 11(12). — p. 5673-5684.

18. Mishra S. Detecting Insider Threats in Social Media Using Machine Learning Techniques. / S. Mishra, P. Tiwari // Journal of Ambient Intelligence and Humanized Computing. — 2019. — 10(9). — p. 3607-3617.

19. Lee K. A Machine Learning-Based Approach for Device Monitoring and Anomaly Detection in IoT Environments. / K. Lee, T. Kwon, J. Kim // Computers & Security. — 2020. — 92. — p. 101717.

20. Ahn G.J. MINDS: A Framework for IoT Device Monitoring and Security Event Prediction. / G.J. Ahn, H. Hu, H. Chen et al. // IEEE Internet of Things Journal. — 2018. — 6(4). — p. 6977-6986.

21. Nigam A. Anomaly Detection in IoT Systems Using Machine Learning and Fuzzy Logic. / A. Nigam, S. Kundu // Journal of Ambient Intelligence and Humanized Computing. — 2019. — 10(2). — p. 715-731.

22. Namiot D.E. O prichinax neudach proektov mashinnogo obucheniya [About the Reasons for the Failure of Machine Learning Projects]. / D.E. Namiot, E.A. Il'yushin // International Journal of Open Information Technologies [International Journal of Open Information Technologies]. — 2023. — 11(1). [in Russian]

23. Utechki informacii ogranichennogo dostupa v mire 2022 g. [Leaks of information of limited access in the world of 2022] [Electronic source] // Expert Analytical Center of Infowatch Group of Companies. — 2023. — URL: https://www.infowatch.ru/analytics/analitika/utechki-informatsii-ogranichennogo-dostupa-v-mire-2022-g . (accessed: 16.05.23) [in Russian]