and increased the level of complexity of user interfaces. The article noted that with the increase in information with which the user interacts in the web application, the number of users with their own peculiarities of information perception and requirements for comfort and intuitiveness of interfaces also increased.

Web applications use a combination of server-side and client-side scripting to perform user tasks. The use of frameworks and libraries for programming the client part of the web application was analyzed, in particular, such as: Reactjs, Create React App, Babel, Webpack. Server-side programming is supported, in particular, by Node.js (for example, when developing online chat, websites for streaming video). The main reasons for the spread of web applications are considered, in particular: attracting consumers, cross-platform, use of centralized data, ensuring the security of confidential information, ease of maintenance, dynamic expansion and updating, availability and support of customers (users of the web application). The main provisions and tools for the development of modern web applications are presented. Modern software tools for developing web applications and modeling user interfaces are considered.

The classification of modern web applications was considered, which, in particular, included: document-oriented websites, interactive web applications, transactional web applications, workflow-based web applications (web services), shared web applications, portal-oriented web applications, universal web applications, knowledge-based web applications , traditional web applications, rich web applications that have dynamic content, contain a large amount of information, are easy to integrate, and progressive web applications.

As a result of the analysis of web applications and their creation technologies, it was determined that they should offer consistent high-quality performance regardless of screen size, pixel density and the device used to access the application. In addition, when the user introduces touch interaction and responsive design into the development process, convenience can be obtained, which is important because web application owners try to achieve user satisfaction and the so-called "visibility" of the web application's capabilities is the highest.

***Keywords**: web application, website, web page, HTML, CSS, JavaScript, framework, client-server technology, user interface, user interface modeling.*

УДК 004.056(477) doi.org/10.33298/2226-8553.2023.2.38.35

Богом'я В.І.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРАТАК

Кібербезпека є актуальною в Україні, так як сучасний світ все більше залежить від технологій та інформаційних систем. Це створює нові можливості для зростаючої загрози кібербезпеки в Україні.

Актуальність теми в контексті зростаючої загрози кібербезпеки в Україні означає необхідність вивчення даної теми у зв'язку із зростанням загрози кібербезпеки в Україні. Це може бути пов'язане зі збільшенням кількості та складності кібератак, які спрямовані проти українських організацій, владних структур чи громадян.

Сучасний стан кіберзаходів та важливість ефективних заходів для захисту від кібератаків вказує на поточний рівень заходів, які приймаються для кіберзахисту в Україні, і визначає

важливість розробки та впровадження ефективних заходів для захисту від кібератаків. Це може включати вдосконалення технічних систем, вдосконалення стратегій кібербезпеки та впровадження новітніх технологій, таких як штучний інтелект та машинне навчання, для підвищення рівня захисту від кіберзагроз.

Аналіз поточних досліджень та розроблення в галузі застосування штучного інтелекту для кібербезпеки визначив такі напрями: алгоритми виявлення аномалії, прогнозування кібератак, автоматизовані системи реагування.

Перегляд успішного використання машинного навчання для кіберзагроз дозволів визначити такі напрями: визначення загрози в реальному часі, аналіз великих обсягів даних, інтеграція з іншими технологіями, система навчання на власних помилках.

Цей аналіз дозволяє застосувати сучасний стан досліджень у галузі та переваги та обмеження використання штучного інтелекту та машинного навчання для захисту від кібератаків.

Виявлення та запобігання кібератак є важливим науковим завданням, яке потребує дослідження та вирішення. Застосування штучного інтелекту та машинного навчання є одним з основних методів вирішення цього завдання. Врахування особливостей системи та використання оптимальних методів захисту є важливими факторами для успішного розв'язання цього наукового завдання.

Тому метою статті є визначення особливостей використання штучного інтелекту та машинного навчання для виявлення та запобігання кібератак.

Ключові слова: *кібербезпека, системи штучного інтелекту, машинне навчання, рекомендації, кіберзагрози, алгоритми, виявлення аномалій*

Постановка проблеми

Кібербезпека є актуальною в Україні, так як сучасний світ все більше залежить від технологій та інформаційних систем [1–3]. Це створює нові можливості для зростаючої загрози кібербезпеки в Україні.

Актуальність теми в контексті зростаючої загрози кібербезпеки в Україні означає необхідність вивчення даної теми у зв'язку із зростанням загрози кібербезпеки в Україні. Це може бути пов'язане зі збільшенням кількості та складності кібератак, які спрямовані проти українських організацій, владних структур чи громадян.

Сучасний стан кіберзаходів та важливість ефективних заходів для захисту від кібератаків вказує на поточний рівень заходів, які приймаються для кіберзахисту в Україні, і визначає важливість розробки та впровадження ефективних заходів для захисту від кібератаків. Це може включати вдосконалення технічних систем, вдосконалення стратегій кібербезпеки та впровадження новітніх технологій, таких як штучний інтелект та машинне навчання, для підвищення рівня захисту від кіберзагроз [4].

Застосування методів в кібербезпеці. Розглянемо види задач, які можна розв’язувати методами штучного інтелекту [5–8]: регресія (або прогноз) - завдання прогнозування наступного значення на основі попередніх знань; класифікація - завдання розділення явищ на різні категорії. Еталони що відповідають класам, відомі; кластеризація - класи невідомі, групування за схожістю; правила пошуку асоціацій (або рекомендацій) - завдання рекомендувати щось на основі попереднього досвіду; зменшення розмірності - узагальнення, завдання пошуку інших і найбільш важливих ознак у ряді зразків; генеративні моделі - завдання створення чогось на основі попередніх знань про розподіл.

Класи машинного навчання [4–8, 15]: **Supervised learning** (навчання з учителем) – умова – розмічені дані, із вказівкою наприклад, шкідливий файл чи ні. правильна конструкція чи ні. На основі розмічених даних приймається рішення про нові дані. **Ensemble learning** - розширення

supervised learning, змішення простих моделей для одержання більш ефективної складної. **Навчання без учителя** – підхід, який використовується коли нема розмічених даних, і модель повинна розмітити їх самостійно, засновуючись на певних властивостях. Призначається для пошуку аномалій, менш точний ніж контрольовані підходи. **Навчання з підкріпленням** (reinforced learning) – підхід, орієнтований на зворотний зв'язок від середовища, коли поведінка моделі має реагувати на зміни середовища. **Active learning** – підклас навчання із підкріпленням, коли «учитель» допомагає виправляти поведінку на додачу до зміни середовища [5–8, 15].

Аналіз останніх досліджень і публікацій. Аналіз поточних досліджень та розроблення в галузі застосування штучного інтелекту для кібербезпеки візначів такі напрями [5–9]:

1. Алгоритми виявлення аномалії.
2. Прогнозування кібератак.
3. Автоматизовані системи реагування.

Перегляд успішного використання машинного навчання для кіберзагроз дозволів визначити такі напрями [4–9]:

1. Визначення загрози в реальному часі.
2. Аналіз великих обсягів даних.
3. Інтеграція з іншими технологіями.
4. Система навчання на власних помилках.

Цей аналіз дозволяє застосувати сучасний стан досліджень у галузі та переваги та обмеження використання штучного інтелекту та машинного навчання для захисту від кіберзагроз.

Мета статті. Виявлення та запобігання кібератак є важливим науковим завданням, яке потребує дослідження та вирішення. Застосування штучного інтелекту та машинного навчання є одним з основних методів вирішення цього завдання. Врахування особливостей системи та використання оптимальних методів захисту є важливими факторами для успішного розв'язання цього наукового завдання [10, 16].

Тому метою статті є визначення особливостей використання штучного інтелекту та машинного навчання для виявлення та запобігання кібератак.

Виклад основного матеріалу дослідження. Аналіз поточних досліджень та розроблень в галузі застосування штучного інтелекту для кібербезпеки визначив такі напрями [1-3, 5-10, 15].

Алгоритми виявлення аномалії. Дослідження використання алгоритмів машинного навчання для виявлення аномальної активності в комп'ютерних системах та оцінка ефективності методів навчання без учителя для виявлення невідомих кіберзагроз.

Прогнозування кібератак. Розгляд застосування штучного інтелекту для прогнозування можливих кібератак на основі аналізу попередніх зразків та здобуття інформації про нові загрози, оцінка точності та швидкості таких систем передбачення.

Автоматизовані системи реагування. Аналіз розробок у галузі створення автоматизованих систем, які використовують штучний інтелект для реагування на кібератаки та визначення переваг та обмеження таких систем у реальному часі.

Перегляд успішного використання машинного навчання для кіберзагроз дозволів визначити такі напрями:

Визначення загрози в реальному часі. Розгляд повідомлення, де системи машинного навчання успішно виявляли кіберзагрози в реальному часі, забезпечуючи швидке реагування на якісь загрози.

Аналіз великих обсягів даних. Перегляд проектів, де машинне навчання успішно використовувалося для аналізу та відсіювання великих обсягів даних, щоб визначити кібератаки та підвищити ефективність дій.

Інтеграція з іншими технологіями. Аналіз успішної інтеграції системи машинного навчання з іншими технологіями (наприклад, блокчейн, криптографія) для підвищення рівня кібербезпеки.

Система навчання на власних помилках. Оцінка методів навчання систем на власних помилках для постійного вдосконалення їхньої здатності виявляють нові типи кіберзагроз.

Цей аналіз дозволяє застосувати сучасний стан досліджень у галузі та переваги та обмеження використання штучного інтелекту та машинного навчання для захисту від кіберзагроз.

Також результати цього аналізу допоможуть визначити основні проблеми та слабкі місця сучасного стану кібербезпеки в Україні, а також розробити напрямки подальшого вдосконалення системи кіберзахисту в країні.

Статистика кіберзагроз – провести аналіз офіційної статистики щодо кількості та типів кібератаків в Україні за останні роки та оцінити тенденції у розвитку кіберзагроз та їхніх характеристик.

Приклади кібератак – провести розгляд конкретних кібератак на українські організації, включаючи урядові структури, підприємства та інші сектори та проаналізувати методи, які використовуються у кібератаках, та їхніх можливих наслідків.

Оцінка основних викликів – визначити ключові фактори, які збільшують уразливість українських систем до кіберзагроз та проаналізувати фактори, такі як недостатні ресурси, низький рівень кіберосвіти.

Слабкі місця у системах кіберзахисту – проаналізувати системи кіберзахисту в різних секторах, включаючи критичну інфраструктуру, фінансовий сектор та державні органи та визначення найбільш вразливих точок та показників, де страждають слабкі місця у системах кіберзахисту.

Позначення важливих тенденцій – виявлення ключових тенденцій у розвитку кіберзагрози та методів їхньої боротьби та оцінка впливу новітніх технологій, таких як штучний інтелект, на зміну ландшафту кібербезпеки в Україні.

Системи штучного інтелекту можуть допомогти у кібербезпеці України, виявляючи та аналізуючи потенційні загрози, виявлення аномальної активності в мережі, а також удосконалення систем виявлення вторгнень. Вони можуть вдосконалювати аналіз великого обсягу даних, швидше розпізнавати вразливості та реагувати на нові види кібератак за допомогою вже відомих методів [11–16].

Так, наприклад:

Машинне навчання – системи можуть навчатися звичайному патерну поведінки мережі та виявляти аномальну активність, що може свідчити про атаку.

Прогнозування загроз – аналіз великих даних, штучний інтелект може обробляти великі обсяги даних для виявлення тенденцій та попередження про можливі кіберзагрози.

Виявлення вразливостей – сканування за допомогою інтелектуальних агентів, використання агентів, які автоматично сканують систему на предмет вразливостей та слабких місць.

Аналіз поведінки – використання систем, які аналізують поведінку користувачів та системи для виявлення невідповідностей та потенційних загроз.

Автоматизована відповідь на інциденти – використання систем, які автоматично реагують на кібератаки, блокуючи атаку та відновлюючи нормальну роботу системи.

Виявлення аномалій.

Ці методи дозволяють ефективніше виявляти, аналізувати та реагувати на кіберзагрози, забезпечуючи вищий рівень кібербезпеки для України.

Слід відмитити, що виявлення аномалій за допомогою машинного навчання може використовувати різноманітні методи. Один із популярних підходів - це навчання моделі на

"нормальному" поведінці системи та виявлення аномальних змін. Ось кілька конкретних прикладів [9–15]:

Метод одного класу – навчання моделі лише на "нормальних" даних, а потім використання цієї моделі для виявлення будь-якої аномальної активності. Наприклад, автентифікація користувача на основі його звичайного патерну входження.

Метод здоров'я системи – аналіз здоров'я системи, такий як використання різних метрик продуктивності. Виявлення аномальних відхилень від звичайних значень може свідчити про можливий вторгнення або проблеми з безпекою.

Метод кластеризації – розділення даних на кластери та виявлення екземплярів, які не належать жодному з кластерів. Аномалії можуть бути представлені як окремі кластери або як окремі точки.

Використання нейронних мереж – використання рекурентних нейронних мереж для моделювання звичайних послідовностей дій та виявлення аномалій в нових даних.

Ці підходи дозволяють системам машинного навчання навчатися на основі стандартного патерну поведінки та виявляти аномалії, які можуть вказувати на потенційні кіберзагрози [2, 17].

Як виглядає типова схема або алгоритм для виявлення аномалій за допомогою машинного навчання (див. рис.1):

Збір даних – збирання "нормальних" даних, що представляють звичайне функціонування системи або мережі.

Навчання моделі – використання цих даних для навчання моделі машинного навчання. Може використовуватися метод одного класу, кластеризація або інші техніки.

Валідація моделі – тестування моделі на даних, які не використовувалися під час навчання, для перевірки ефективності та точності виявлення аномалій.

Визначення порогу – встановлення порогу, за яким визначається, коли певна активність вважається аномалією. Це може бути на основі відхилення від звичайного патерну або інших параметрів.

Виявлення аномалій в реальному часі – застосування моделі до нових даних в реальному часі для виявлення аномалій або ненормальної активності.

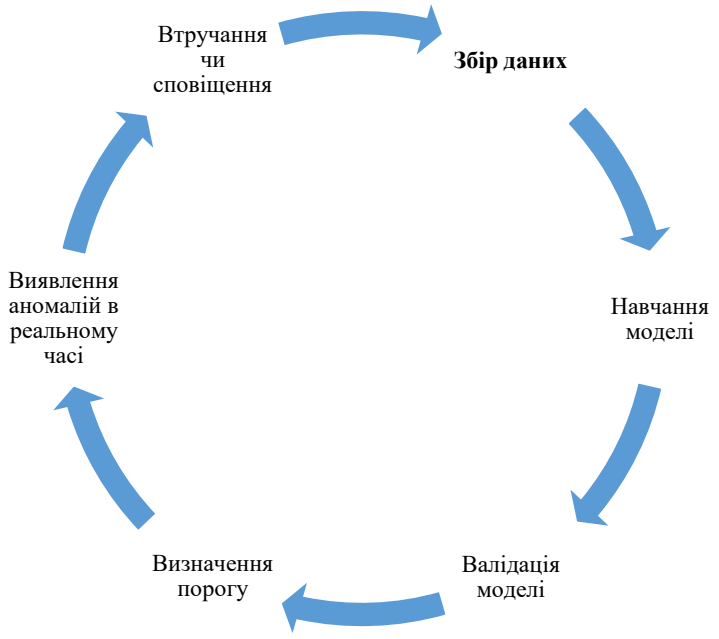

Рисунок 1 – Типова схема для виявлення аномалій за допомогою машинного навчання

Втручання чи сповіщення – визначення механізмів втручання або сповіщення, які активуються в разі виявлення аномалій, щоб вчасно реагувати на потенційні загрози.

Оновлення моделі – регулярне оновлення моделі з урахуванням нових даних та змін у патерні поведінки системи.

Ця схема може варіюватися в залежності від конкретного використання та типу даних, але вона відображає загальний процес виявлення аномалій за допомогою машинного навчання в кібербезпеці.

Висновки й перспективи подальших досліджень. Покращення рівня кіберзахисту в Україні може включати в себе ряд заходів та рекомендацій, спрямованих на вирішення виявлених викликів та усунення слабких місць. Наприклад:

1. Зміцнення інформаційно-комунікаційної інфраструктури (ІКТ).

Рекомендація: Забезпечення безпеки критичних інфраструктур, зокрема систем енергетики, транспорту та інших важливих галузей.

Дії: Проведення аудиту та аналізу існуючих ІКТ-систем, впровадження сучасних систем виявлення та захисту, застосування стандартів кіберзахисту.

2. Підвищення обізнаності та навичок.

Рекомендація: Розвиток кадрового потенціалу та підвищення обізнаності про кіберзагрози серед персоналу.

Дії: Організація тренінгів, семінарів та навчання з питань кібербезпеки для урядових служб, підприємств та громадян.

3. Регулярні аудити та тестування на вразливості.

Рекомендація: Проведення регулярних аудитів та тестувань на вразливості для виявлення слабких місць у системах.

Дії: Залучення експертів для проведення аудитів, використання автоматизованих інструментів для тестування вразливостей.

4. Створення національної стратегії кібербезпеки.

Рекомендація: Розроблення та впровадження національної стратегії з кібербезпеки, яка враховує сучасні тенденції та виклики.

Дії: Залучення експертів, представників громадянського суспільства та бізнесу до процесу розробки стратегії, визначення конкретних заходів та відповідальних структур.

5. Розвиток міжнародного співробітництва.

Рекомендація: Активна участь в міжнародних ініціативах та обмін інформацією про кіберзагрози з іншими країнами та організаціями.

Дії: Підписання та виконання міжнародних угод про кібербезпеку, створення каналів обміну інформацією та співпраці з іншими країнами.

Ці рекомендації можуть служити вихідною точкою для розробки комплексного плану з покращення кіберзахисту в Україні, враховуючи специфічні виклики та потреби країни.

ЛІТЕРАТУРА

1. Абрахам, А., Камарудін, С., і Чай, С. Т. (2020). Опитування щодо використання штучного інтелекту в кібербезпеці. Комп’ютери та безпека, 88, 101628 с.

2. Caviglione, L., Coccoli, M., Lops, C., & Nocerino, R.(2019). Застосування машинного навчання до кібербезпеки: вичерпний огляд. Прикладні науки, 9(10), 2038 с.

3. Poonia, P., Sharma, S.K., & Kumar, A. (2020). Система виявлення вторгнень на основі машинного навчання: комплексне дослідження. Journal of Ambient Intelligence and Humanized Computing, 11(9), С. 3963-3983.

4. Чжан, Х., Хуан, Х., і Чжан, Ю. (2019). Дослідження прогресу штучного інтелекту в кібербезпеці. Міжнародний журнал систем обчислювального інтелекту, 12 (1), С. 316-326.

5. Чжан Ю., Чен В., Ян Дж. та Сю В. (2019). Машинне навчання в кібербезпеці. IEEE Access, 7, С.108700- 108707

6. S. Varshney et al, Review of various Artificial Intelligence Techniques and its applications, 2019. IOP Conf. Ser.: Mater. Sci. Eng. 594 012023, DOI: 10.1088/1757-899X/594/1/012023.

7. G. Belani, The Use of Artificial Intelligence in Cybersecurity: A Review URL: https://www.computer.org/publications/tech-news/trends/the-use-ofartificial-intelligence-in-cybersecurity.

8. S. Ray, 7 Regression Techniques you should know! URL: https://www.analyticsvidhya.com/blog/2015/08/comprehensive-guideregression/

9. "AI and cybersecurity: The future of cyber defence" [Електронний ресурс]. Режим доступу до ресурсу: https://www.forbes.com/sites/andrewrossow/2021

10. "The role of AI in cybersecurity" by John Boitnot " [Електронний ресурс]. Режим доступу до ресурсу: https:// venturebeat. com /2018/03/31/the-role-ofai- in-cybersecurity/

11. Ду, М., Лі, Ф., Чжен, Г., і Срікумар, В. (2019). DeepLog: виявлення та діагностика аномалій із системних журналів за допомогою глибокого навчання. ACM Transactions on Privacy and Security (TOPS), 22(4), 1-27. https: // doi. org/ 10.1145 /3338501

12. Бланко, Е., Атлідакіс, В., Фонсека, Р. (2020). Drain3: гнучкий і ефективний фреймворк аналізу журналів. Матеріали конференції USENIX 2020 року з оперативного машинного навчання (OpML 20). https:/ /www.usenix.org/ conference/opml20/ presentation/blanco

13. "How AI is transforming cybersecurity" by Gary Eastwood, " [Електронний ресурс]. Режим доступу до ресурсу: https: / / www. Information - age. com/how-ai-is-transforming-cybersecurity-123478294/

14. Кларк, Дж., Джейкоб, Дж. (2018). ШІ та кібербезпека: загрози та рішення. Журнал кібербезпеки, 4(1), С. 1-14.

15. Методи штучного інтелекту в кібербезпеці [Електронний ресурс]: навч. посіб. для здобувачів спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: І.В. Стьопочкіна, О.М. Новіков. – Київ : КПІ ім. Ігоря Сікорського, 2022 – 82 с.

16. Богом'я В.І., Кочегаров В.С. Кібербезпека в хмарних сервісах за допомогою застосування криптографічних методів. Водний транспорт. № 1 (37). 2023. 239–246 с. doi.org/10.33298/2226-8553.2023.1.37.27

17. Gonfalonieri, How to Build A Data Set For Your Machine Learning Project, 2019. URL: https://towardsdatascience.com/how-to-build-a-dataset-for-your-machine-learning-project-5b3b871881ac

REFERENCE

1. Abraham, A., Kamarudin, S., & Chai, S. T. (2020). A survey on the use of artificial intelligence in cyber security. Computers and security, 88, 101628 p.

2. Caviglione, L., Coccoli, M., Lops, C., & Nocerino, R. (2019). Applications of Machine Learning to Cyber Security: A Comprehensive Review. Applied Sciences, 9(10), 2038 p.

3. Poonia, P., Sharma, S.K., & Kumar, A. (2020). Intrusion detection system based on machine learning: a comprehensive study. Journal of Ambient Intelligence and Humanized Computing, 11(9), pp. 3963-3983.

4. Zhang, H., Huang, X., & Zhang, Y. (2019). Exploring the Advances of Artificial Intelligence in Cyber Security. International Journal of Computational Intelligence Systems, 12 (1), pp. 316-326.

5. Zhang, Y., Chen, W., Yang, J., and Xu, W. (2019). Machine learning in cyber security. IEEE Access, 7, pp. 108700-108707

6. S. Varshney et al, Review of various Artificial Intelligence Techniques and its applications, 2019. IOP Conf. Ser.: Mater. Sci. Eng. 594 012023, DOI: 10.1088/1757-899X/594/1/012023.

7. G. Belani, The Use of Artificial Intelligence in Cybersecurity: A Review URL: https://www.computer.org/publications/tech-news/trends/the-use-ofartificial-intelligence-in-cybersecurity.

8. S. Ray, 7 Regression Techniques you should know! URL: https://www.analyticsvidhya.com/blog/2015/08/comprehensive-guideregression/

9. "AI and cybersecurity: The future of cyber defense" [Electronic resource]. Mode of access to the resource: https://www.forbes.com/sites/andrewrossow/2021

10. "The role of AI in cybersecurity" by John Boitnot " [Electronic resource]. Mode of access to the resource: https:// venturebeat. com /2018/03/31/the-role-ofai- in-cybersecurity/

11. Du, M., Li, F., Zheng, H., & Sreekumar, V. (2019). DeepLog: Detecting and diagnosing anomalies from system logs using deep learning. ACM Transactions on Privacy and Security (TOPS), 22(4), 1-27. https: // doi. org/ 10.1145 /3338501

12. Blanco, E., Atlidakis, V., Fonseca, R. (2020). Drain3: A flexible and efficient log analysis framework. Proceedings of the 2020 USENIX Conference on Operational Machine Learning (OpML 20). https:/ /www.usenix.org/ conference/opml20/ presentation/blanco

13. "How AI is transforming cybersecurity" by Gary Eastwood, " [Electronic resource]. Mode of access to the resource: https: / / www. Information - age. com/how-ai-is-transforming-cybersecurity-123478294/

14. Clark, J., Jacob, J. (2018). AI and Cyber Security: Threats and Solutions. Journal of Cybersecurity, 4(1), pp. 1-14.

15. Methods of artificial intelligence in cyber security [Electronic resource]: training. manual for applicants of special 125 "Cyberbezpeka" / KPI named after Igor Sikorskyi; comp.: I.V. Styopochkina, O.M. Novikov. – Kyiv: KPI named after Igor Sikorskyi, 2022 - 82 p.

16. Bogomya V.I., Kochegarov V.S. Cyber security in cloud services using cryptographic methods. Water transport. No. 1 (37). 2023. pp. 239–246. doi.org/10.33298/2226-8553.2023.1.37.27

17. Gonfalonieri, How to Build A Data Set For Your Machine Learning Project, 2019. URL: https://towardsdatascience.com/how-to-build-a-dataset-for-your-machine-learning-project-5b3b871881ac

Bohomia V.I.

The Use of Artificial Intelligence and Machine Learning for Cyber Attack Detection and Prevention: Features and Recommendations

Cybersecurity is a crucial issue in Ukraine, given the increasing reliance on technology and information systems in the modern world. This dependence creates new opportunities for the growing threat of cybersecurity in Ukraine.

The relevance of the topic, in the context of the rising cybersecurity threat in Ukraine, signifies the necessity to study this issue due to the increasing frequency and complexity of cyber attacks targeting Ukrainian organizations, governmental structures, and citizens.

The current state of cybersecurity measures and the importance of effective actions against cyber attacks indicate the current level of efforts taken for cybersecurity in Ukraine. It emphasizes the importance of developing and implementing effective measures to protect against cyber threats. This may include improving technical systems, enhancing cybersecurity strategies, and adopting advanced technologies such as artificial intelligence and machine learning to elevate the level of protection against cyber threats.

The analysis of current research and developments in the application of artificial intelligence for cybersecurity has identified several directions: anomaly detection algorithms, prediction of cyber attacks, and automated response systems.

A review of successful applications of machine learning for cyber threats has identified directions such as real-time threat detection, big data analysis, integration with other technologies, and a self-learning system.

This analysis allows for the application of current research in the field, considering the advantages and limitations of using artificial intelligence and machine learning for protection against cyber attacks.

The detection and prevention of cyber attacks are crucial scientific tasks that require research and resolution. The application of artificial intelligence and machine learning is one of the primary methods to address this task successfully. Taking into account the system's peculiarities and utilizing optimal protection methods are vital factors for the successful resolution of this scientific task.

Therefore, the aim of this article is to identify the features of using artificial intelligence and machine learning for the detection and prevention of cyber attacks.

Keywords: *cybersecurity, artificial intelligence systems, machine learning, recommendations, cyber threats, algorithms, anomaly detection.*