Міністерство освіти і науки України
Сумський державний університет
Навчально-науковий інститут бізнесу, економіки та менеджменту
Кафедра економічної кібернетики

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

Матеріали
II наукової онлайн-конференції

(Суми, 02 липня 2024)

Суми
Сумський державний університет
2024

004.056.5:336(082)
В43

Головний редактор
доц., к.е.н., ***Койбічук Віталія***, завідувачка кафедри економічної кібернетики, Сумський державний університет
.

Затверджено Вченою Радою Сумського державного університету (протокол № 1, 29.08.2024)

S62 Виклики кібербезпеки індустрії фінансових послуг: Матеріали наукової онлайн-конференції, Суми, 02 липня 2024. Збірник матеріалів тез наукової онлайн-конференції / за загальною редакцією доц. Койбічук В.В. – Суми : Сумський державний університет, 2024. – 72 с.

Матеріали наукової онлайн-конференції "Виклики кібербезпеки індустрії фінансових послуг" присвячені пошуку системного вирішення проблем у сфері протидії кібеззагрозам у сфері фінансових послуг, підвищенню рівня кіберзахисту об'єктів критичної інфраструктури.

Видання розраховане на науковців, викладачів, студентів вищих навчальних закладів, аспірантів, докторантів та інших зацікавлених осіб.

004.056.5:336(082)

ЗМІСТ

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

ШТУЧНИЙ ІНТЕЛЕКТ У БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ: ЕФЕКТИВНІ СТРАТЕГІЇ ТА ІНСТРУМЕНТИ

ARTIFICIAL INTELLIGENCE IN COMBATING CYBERCRIME: EFFECTIVE STRATEGIES AND TOOLS

Еліна Шрамко, студентка
Сумський державний університет, Україна

Науковий керівник:
Вікторія Боженко, к.е.н., доцентка
Сумський державний університет, Україна

У сучасному цифровому світі кібербезпека стає все більш важливою складовою захисту інформації та технологічних систем. З розвитком технологій кількість та складність кіберзлочинів стрімко зростає, ставлячи під загрозу як приватних користувачів, так і великі організації. Традиційні методи захисту стають недостатніми для боротьби з новітніми загрозами, що потребує впровадження передових технологій, таких як штучний інтелект (ШІ).

Актуальність теми обумовлена тим, що штучний інтелект здатний значно підвищити ефективність систем кібербезпеки завдяки своїй здатності до швидкого аналізу великих обсягів даних, виявлення аномалій у реальному часі та адаптації до нових загроз. Використання штучного інтелекту у боротьбі з кіберзлочинністю відкриває нові горизонти у захисті даних та інформаційних систем, дозволяючи створювати більш надійні та ефективні стратегії захисту.

Інтеграція штучного інтелекту у існуючі системи кібербезпеки є першим кроком до підвищення їх ефективності та їх адаптивності до нових загроз. Цей процес розпочинається з оцінки поточних систем для виявлення їхніх слабких місць. Після цього обираються відповідні інструменти ШІ, такі як Splunk, Darktrace, ELK Stack або Cisco Stealthwatch, залежно від потреб організації. Інструменти інтегруються з існуючими системами, налаштовується збір даних і встановлюються зв'язки між різними системами. Далі моделі штучного інтелекту тренуються на історичних даних, щоб навчитися виявляти загрози. Після впровадження системи постійно моніторяться і коригуються для забезпечення їхньої максимальної ефективності. Це дозволяє досягти точного виявлення загроз та швидкого реагування на інциденти, значно підвищуючи рівень кібербезпеки (Holovchak, Holovchak, & Skrypnyk, 2024).

Інтеграція штучного інтелекту в існуючі системи кібербезпеки приносить численні переваги. Вона значно підвищує точність виявлення загроз завдяки здатності штучного інтелекту аналізувати великі обсяги даних і виявляти аномалії, які можуть залишатися непоміченими традиційними методами. Крім того, автоматизація процесів за допомогою штучного інтелекту дозволяє миттєво реагувати на інциденти без затримок, пов'язаних з ручною обробкою. Ще однією перевагою є адаптивність до нових загроз: штучного інтелекту постійно навчається і оновлює свої моделі на основі нових даних, що дозволяє ефективно боротися з новими типами атак. Це робить системи кібербезпеки більш гнучкими і здатними швидко адаптуватися до змін у загрозах (Holovchak et al, 2024).

Втім, інтеграція штучного інтелекту у системи кібербезпеки також стикається з певними викликами. Процеси тренування та застосування моделей штучного інтелекту потребують значних обчислювальних потужностей, що може бути дороговартісним для організацій. Крім того, для ефективного навчання моделей необхідні великі обсяги високоякісних даних, що може бути складно забезпечити. Також інтеграція та підтримка систем ШІ вимагають наявності кваліфікованих фахівців у галузі даних і кібербезпеки, яких не завжди легко знайти. Таким чином, незважаючи на свої численні переваги, інтеграція штучного інтелекту потребує значних ресурсів і добре продуманих підходів для подолання (Holovchak et al, 2024).

Таблиця 1. Опис популярних інструментів з ШІ для інтеграції в системи кібербезпеки (Holovchak et al, 2024).

Інструмент	Особливості	Підтримка ШІ	Типи даних
Splunk	Потужна платформа для збору, аналізу та візуалізації даних	Так	Логи, мережеві дані
Darktrace	Виявлення загроз на основі поведінкових моделей	Так	Мережевий трафік
ELK Stack	Набір інструментів для збору, обробки та візуалізації логів	Так	Логи
Cisco Stealthwatch	Використання аналітики великих даних для виявлення загроз	Так	Мережевий трафік

Автоматизація процесів безпеки є одним із ключових аспектів інтеграції ШІ в системи кібербезпеки. Використання автоматизованих інструментів і технологій на основі ШІ дозволяє значно підвищити ефективність

реагування на загрози та забезпечити проактивний підхід до захисту інформаційних систем (Holovchak et al, 2024).

Основні аспекти автоматизації процесів безпеки:

1. Автоматизація дозволяє здійснювати моніторинг мережевого трафіку та логів у реальному часі. Інструменти на основі ШІ можуть аналізувати великі обсяги даних та виявляти аномалії миттєво, що дозволяє швидко реагувати на потенційні загрози. Це значно зменшує час від виявлення до реагування, мінімізуючи можливі збитки.

2. Завдяки автоматизації, системи безпеки можуть автоматично вживати заходів для усунення загроз. Це включає ізоляцію скомпрометованих систем, блокування підозрілих IP-адрес, застосування патчів та оновлень, а також інформування відповідних фахівців про інциденти. Такі дії можуть бути виконані без втручання людини, що знижує навантаження на IT-персонал.

3. Системи на основі ШІ можуть використовувати прогностичні моделі для виявлення потенційних загроз до їх виникнення. Це дозволяє організаціям бути на крок попереду зловмисників, впроваджуючи заходи безпеки заздалегідь.

4. Однією з проблем традиційних систем безпеки є велика кількість хибнопозитивних спрацювань, що може призводити до зайвих витрат часу та ресурсів. Автоматизація з використанням ШІ дозволяє значно знизити цей показник завдяки точнішому аналізу даних та більш ефективному виявленню реальних загроз (Holovchak et al, 2024).

Прогнозування загроз за допомогою штучного інтелекту є важливою стратегією у сфері кібербезпеки, яка дозволяє організаціям проактивно вживати заходів для захисту своїх інформаційних систем. штучного інтелекту аналізує великі обсяги історичних даних про кіберзагрози, включаючи інформацію про попередні атаки, методи зловмисників та їх поведінкові патерни. Це дозволяє виявляти закономірності та тренди, які можуть вказувати на ймовірність майбутніх атак (Kaur, Gabrijelčič, & Klobučar, 2023).

Основні інструменти для прогнозування загроз використовують алгоритми машинного та глибокого навчання, які навчаються на великій кількості даних, щоб виявляти складні патерни та аномалії. Прогностичні моделі інтегруються з існуючими системами кібербезпеки для постійного моніторингу та аналізу нових даних. На основі прогнозів, системи безпеки можуть автоматично вживати заходів для запобігання атакам, включаючи зміну конфігурацій, оновлення програмного забезпечення, блокування підозрілих IP-адрес або обмеження доступу до критичних ресурсів. Прогнозування загроз дозволяє знизити ризик успішних атак та економити ресурси, зменшуючи кількість інцидентів, які потребують реагування, що

допомагає мінімізувати втрати від кіберзлочинів (Kaur, Gabrijelčič, & Klobučar, 2023).

Виявлення аномалій є одним з найважливіших завдань у сфері кібербезпеки. Штучний інтелект пропонує нові можливості для аналізу великих обсягів даних та ідентифікації нетипової поведінки, що може свідчити про наявність загрози. Розглянемо основні методи та інструменти, що використовуються для виявлення аномалій:

1. Статистичні методи – методи, що базуються на аналізі розподілу даних і виявляють аномалії, порівнюючи поточні дані з попередньо визначеними статистичними моделями. Вони ефективні для виявлення відомих типів аномалій, але можуть бути менш ефективними для нових чи складних загроз.
2. Алгоритми машинного навчання (ML) використовують історичні дані для тренування моделей, здатних виявляти аномалії у нових даних. Найпоширенішими є методи класифікації, кластеризації та нейронні мережі. Вони забезпечують високу точність, але потребують значних обчислювальних ресурсів та попередньої обробки даних.
3. Методи на основі правил – методи, що базуються на встановленні правил або порогових значень, які визначають, чи є подія аномальною. Вони прості у реалізації, але менш гнучкі у порівнянні з іншими методами (Karpyuk & Vengersky, 2021).

Процес виявлення аномалій за допомогою штучного інтелекту починається зі збору великих обсягів даних, таких як мережевий трафік і логи системних подій, які потім очищуються, заповнюються відсутні значення та нормалізуються. Далі, на основі історичних даних, тренуються моделі, зокрема нейронні мережі та методи кластеризації, для вивчення нормальної поведінки системи і виявлення аномалій. Застосовані до нових даних моделі ідентифікують нетипову поведінку та маркують підозрілі події. Останнім етапом є детальний аналіз виявлених аномалій експертами для визначення рівня загрози та вжиття відповідних заходів, таких як ізоляція скомпрометованих систем або блокування доступу (Karpyuk & Vengersky, 2021).

Практичні кейси використання ШІ демонструють його значні переваги та потенціал. Наприклад, компанія Google активно застосовує алгоритми машинного навчання для виявлення та блокування фішингових електронних листів. Це дозволяє ефективно фільтрувати понад 99.9% шкідливих повідомлень, знижуючи ризик компрометації користувачів. Важливість такого підходу підкреслюється в дослідженні, де показано, що машинне навчання є ефективним інструментом для виявлення фішингових атак (Rashid et al., 2020).

Інший приклад – використання прогностичної аналітики для запобігання кібератакам. IBM Watson for Cyber Security аналізує величезні обсяги даних і прогнозує потенційні загрози до їхнього виникнення. Використовуючи природну мову та глибоке навчання, Watson виявляє аномалії та аналізує поведінкові патерни зловмисників. Це дослідження підтверджує, що прогностична аналітика може бути ефективним інструментом для забезпечення кібербезпеки (Freeman & Chio, 2018).

Отже, застосування штучного інтелекту у кібербезпеці значно підвищує ефективність захисту інформаційних систем. ШІ дозволяє швидко аналізувати великі обсяги даних, виявляти аномалії у реальному часі та адаптуватися до нових загроз. Інтеграція штучного інтелекту у існуючі системи кібербезпеки, таких як Splunk, Darktrace, ELK Stack і Cisco Stealthwatch, забезпечує більш надійний та ефективний захист.

Список використаних джерел

1. Holovchak, Y. V., Holovchak, H. V., & Skrypnyk, S. V. (2024). Integration of smart technologies and artificial intelligence in accounting: Key aspects of the digital revolution. Journal "Investments: Practice and Experience", (6), 38-44. https://doi.org/10.32702/2306-6814.2024.6.38

2. Karpyuk, P., & Vengersky, P. (2021). Using machine learning to detect anomalies in cybersecurity to reduce false positives in the daily work of the cyber threat response center. Application Mathematics and Informatics. https://doi.org/10.30970/vam.2021.29.11339

3. Freeman, D., & Chio, C. (2018). Machine Learning and Security: Protecting Systems with Data and Algorithms. O'Reilly Media.

4. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 101804. https://doi.org/10.1016/j.inffus.2023.101804

5. Rashid, J., et al. (2020). Phishing detection using machine learning technique. 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, 3-5 November 2020. https://doi.org/10.1109/smart-tech49988.2020.00026