визначення з боку криптоаналітика. Водночас базова схема може бути посилена шляхом зміни параметрів КТЗ, зокрема через розширення системи модулів.

Суть запропонованого методу полягає у введенні додаткового модуля системи. Для нього формується окремий залишок. Він може бути заданий довільно або виконувати контрольну функцію. Шифрування виконується за розширеною формулою КТЗ. При цьому виникає питання вибору добутку модулів. Якщо використовувати добуток лише початкової системи модулів, додатковий залишок не повністю впливає на результат і не завжди може виконувати контрольну функцію. Натомість використання добутку всіх модулів, включаючи додатковий, розширює діапазон можливих значень шифротексту та збільшує простір ключів.

Практичне значення такого підходу полягає в тому, що збільшення кількості модулів у СЗК ускладнює структуру криптографічного перетворення. Криптоаналітик має враховувати більшу кількість можливих комбінацій модулів, залишків та проміжних параметрів КТЗ. Крім того, додатковий модуль може використовуватися як механізм контролю цілісності повідомлення після розшифрування. Це особливо важливо для систем, у яких потрібно поєднати захист інформації з виявленням помилок передавання або обробки даних.

Отже, метод шифрування на основі збільшення кількості модулів у СЗК є ефективним способом підвищення криптографічної стійкості та розширення простору ключів. Подальші дослідження доцільно спрямувати на оптимальний вибір додаткових модулів, оцінювання стійкості до криптоаналітичних атак та реалізацію методу в апаратних і гібридних криптографічних системах.

1. 1. Nieles M., Dempsey K., Pillitteri V. *An Introduction to Information Security*. Gaithersburg : NIST, 2017. 101 p..
2. 2. P.V. Ananda Mohan. *Residue number systems: Theory and applications*. Birkhäuser, Basel. 2016. 351 p.

## Штучний інтелект як інструмент підтримки прийняття рішень у системах кібербезпеки

УДК 004.056:004.8

Роман Золотий[1], Ігор Чихіра[2], Віктор Устенко[3]

*Тернопільський національний технічний університет імені Івана Пулюя, [1]zolotyy@gmail.com, [2]ig.vi.chi@gmail.com, Івано-Франківська філія Університету "Україна", [3]ustenkotoda@gmail.com*

Зростання кількості кіберінцидентів і обсягів даних безпеки актуалізує використання штучного інтелекту як інструменту підтримки прийняття рішень у кібербезпеці. На відміну від суто сигнатурних засобів та засобів на основі правил, AI може швидко аналізувати журнали, мережевий трафік, події кінцевих пристроїв, хмарних сервісів та IoT-компонентів. Це важливо з огляду на поширення атак на доступність, програм-вимагачів, загроз даним, соціальної інженерії та експлуатації вразливостей [1].

Метою роботи є обґрунтування моделі використання штучного інтелекту для аналізу подій безпеки, оцінювання ризиків, пріоритезації інцидентів і формування рекомендацій для фахівця. Відповідно до NIST Cybersecurity Framework 2.0 управління кібербезпекою охоплює ідентифікацію активів, захист, виявлення, реагування, відновлення та управління ризиками [2]. AI доцільно розглядати як аналітичний шар цих процесів, а не як заміну експерта.

Наукова новизна підходу полягає в трактуванні AI як допоміжного інтелектуального контуру прийняття рішень, що поєднує технічні події з контекстом критичності активів, історією інцидентів, рівнем ризику та політиками реагування. Відповідно до NIST AI Risk Management Framework, довіра до AI-систем має ґрунтуватися на керованості, надійності, безпечності, прозорості, пояснюваності та підзвітності [3].

Запропонована модель передбачає чотири етапи: збирання й нормалізацію даних із SIEM, IDS/IPS, EDR, мережевих сенсорів і хмарних журналів; AI-аналіз подій із виявленням аномалій та класифікацією сценаріїв атак; оцінювання ризику з урахуванням критичності активу, потенційного впливу й достовірності спрацювання; формування рекомендацій щодо перевірки облікового запису, ізоляції вузла, зміни правил доступу або посилення моніторингу.

Таблиця 1

Функції штучного інтелекту в системі підтримки кібербезпеки

| Функція AI | Призначення | Результат для фахівця |
|---|---|---|
| Виявлення аномалій | пошук нетипової активності в трафіку та журналах | раннє попередження про можливий інцидент |
| Класифікація подій | віднесення подій до типових сценаріїв атак | зменшення кількості ручного аналізу |
| Оцінювання ризику | урахування критичності активу та впливу інциденту | визначення пріоритету реагування |
| Формування рекомендацій | пропозиція дій відповідно до політик безпеки | підтримка прийняття рішення експертом |

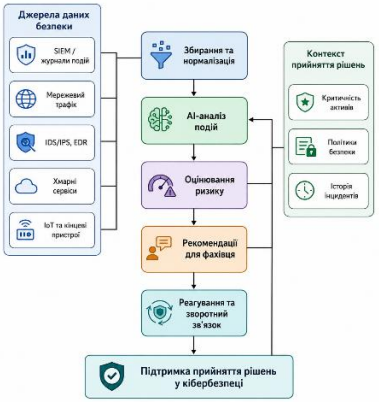


Рис.1. Штучний інтелект у системі підтримки прийняття рішень з кібербезпеки

Цінність підходу полягає у скороченні часу між появою ознак атаки та рішенням щодо реагування. AI-модуль може об'єднати невдалу автентифікацію, нетиповий трафік, звернення до критичного сервера та зміну поведінки користувача в один інцидент із підвищеним пріоритетом. Водночас остаточне рішення має ухвалювати фахівець з урахуванням організаційного контексту. Основними ризиками впровадження AI є залежність від якості навчальних даних, хибнопозитивні або хибнонегативні спрацювання, складність пояснення рішень і вразливість моделей до маніпуляцій. Оскільки ISO/IEC 27005 розглядає управління ризиками як безперервний процес [4], AI-рішення мають супроводжуватися аудитом даних, перевіркою моделей, контролем доступу та журналюванням рекомендацій.

Отже, штучний інтелект є перспективним інструментом підтримки прийняття рішень у кібербезпеці, що підвищує швидкість аналізу, покращує пріоритезацію інцидентів і сприяє обґрунтованому реагуванню. Подальші дослідження доцільно спрямувати на пояснювані AI-моделі для SOC-середовищ, оцінювання довіри до автоматизованих рекомендацій і захист AI-модулів від цілеспрямованих атак.

1. Kaur R., Gabrijelcic D., Klobucar T. Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion. 2023. Vol. 97. Article 101804.
2. Rjoub G. et al. A survey on explainable artificial intelligence for cybersecurity. IEEE Transactions on Network and Service Management. 2023. Vol. 20(4). P. 5115-5140.
3. Capuano N., Fenza G., Loia V., Stanzione C. Explainable artificial intelligence in cybersecurity: A survey. IEEE Access. 2022. Vol. 10. P. 93575-93600.
4. Sarker I.H. et al. Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data. 2020. Vol. 7. Article 41.

## Analysis of modern methods for detecting phishing domains and links

UDK 004.056.5:004.738.5

Ivan Azarov[1], Anna Korchenko[2],
Illia Azarov[3], Kyrylo Davydenko[4]

*State University of Communication and Informational Technologies,*
*[1]azarovphone@gmail.com,*
*NTU Dnipro Polytechnic, [2]annakor@ukr.net, [4]kirilldavy@gmail.com,*
*Kyiv Aviation Institute, [3]azarovforce@gmail.com*

Phishing remains one of the most common cyberattack vectors, utilizing social engineering and technical masking techniques to steal confidential data.

With the emergence of automated tools, attackers have gained the ability to mass-generate deceptive URLs and clone legitimate web resources, which reduces the effectiveness of traditional security measures.

The use of comprehensive approaches to analyzing domains and links is critical for countering phishing attacks, particularly zero-day attacks [1].