5. Rozetka Tech Blog. (2021). *Як ми використовуємо рекомендовані системи для персоналізації.* Отримано з https://rozetka.tech

6. Wang, R. Y., Kung, L. A., & Byrd, T. A. (2018). Beyond a technical perspective: Understanding big data capabilities in health care. *Information Systems Management*, 35(2), 89–102. https://doi.org/10.1080/10580530.2018.1440739

7. ПриватБанк. (2022). *Річний звіт ПриватБанку за 2021 рік.* Отримано з https://privatbank.ua

8. Dignum, V. (2018). Ethics in artificial intelligence: introduction to the special issue. *Ethics and Information Technology*, 20(1), 1–3.

9. Kyivstar Big Data Lab. (2020). *Кейс: як кластеризація допомогла зменшити відтік абонентів.* Отримано з https://bigdatalab.kyivstar.ua

10. ILO. (2021). *Modernizing employment services in Ukraine using AI tools*. International Labour Organization. Отримано з https://www.ilo.org

Янковська К.С.,
к.е.н, доцент,
Сиротюк Г.В.,
к.е.н., доцент,
Львівський національний університет ветеринарної медицини
та біотехнологій ім. С.З. Ґжицького

СМАРТ-АНАЛІТИКА ЯК ІНСТРУМЕНТ ПРЕВЕНТИВНОЇ КІБЕРБЕЗПЕКИ У БІЗНЕС-СЕРЕДОВИЩІ

Сучасне бізнес-середовище характеризується стрімкою цифровізацією, зростанням обсягу даних та активним впровадженням інформаційно-комунікаційних технологій у всі сфери діяльності підприємств. Разом із технологічним розвитком зростають і загрози кібербезпеці: кібератаки стають дедалі складнішими, цілеспрямованими та масштабнішими. Згідно зі звітами провідних компаній у сфері інформаційної безпеки, більшість підприємств щороку зазнає тих чи інших форм атак – від фішингу та шкідливого програмного забезпечення до складних атак типу APT (Advanced Persistent Threat) [2, 3].

У зв’язку з цим актуальним є перехід до превентивної моделі кіберзахисту, яка передбачає виявлення загроз до моменту їх реалізації. Одним з найбільш перспективних інструментів у цьому контексті виступає смарт-аналітика – інтелектуальний підхід до аналізу великих обсягів даних із використанням штучного інтелекту та машинного навчання [4].

Смарт-аналітика (англ. Smart Analytics) – це сукупність методів аналізу даних, яка поєднує в собі технології штучного інтелекту, машинного навчання, аналізу великих даних (Big Data) та автоматизованої обробки інформації. Її особливістю є здатність не лише збирати та обробляти дані, але й робити висновки, виявляти закономірності, прогнозувати події та реагувати на виявлені аномалії [1].

У контексті кібербезпеки смарт-аналітика відіграє важливу роль у забезпеченні ефективного моніторингу та захисту інформаційних систем. Вона дає змогу аналізувати лог-файли, мережевий трафік і події безпеки в реальному часі, що дозволяє оперативно реагувати на потенційні загрози. Завдяки технологіям аналітики поведінки користувачів (User Behavior Analytics – UBA) можливо виявляти відхилення від типових дій, що може свідчити про зловмисну активність або компрометацію облікового запису. Смарт-аналітика також допомагає ідентифікувати кібератаки на ранніх стадіях, наприклад, сканування портів, численні невдалі спроби автентифікації чи підозріле завантаження файлів.

Окрім того, система може автоматично формувати сповіщення та запускати заздалегідь визначені сценарії реагування, що значно підвищує швидкість і ефективність протидії інцидентам безпеки. На відміну від традиційного аналітичного підходу, який базується на ретроспективному аналізі, смарт-аналітика дозволяє здійснювати динамічний, превентивний моніторинг у реальному часі.

Превентивна кібербезпека – це підхід до захисту інформаційних систем, який ґрунтується на активному виявленні ризиків і запобіганні інцидентам до того, як вони стануть загрозами. У цій моделі акцент зміщується з реагування на події до їх передбачення та блокування.

Смарт-аналітика реалізує цей підхід через:

1. побудову моделей «нормальної» поведінки систем і користувачів;
2. виявлення аномалій на основі статистичних методів і нейромереж;
3. автоматичну класифікацію подій за рівнем критичності;
4. формування політик динамічного реагування.

Смарт-аналітичні інструменти в сфері кібербезпеки зазвичай інтегруються в Security Information and Event Management (SIEM) системи, Security Orchestration, Automation and Response (SOAR) платформи, а також хмарні рішення.

Популярні технології включають [3, 4]. :

1. Алгоритми машинного навчання: кластеризація (k-means), класифікація (Random Forest, XGBoost), виявлення аномалій (Isolation Forest, Autoencoder).
2. Хмарні аналітичні платформи: Microsoft Sentinel, AWS Security Hub, Google Chronicle.
3. Інструменти відкритого коду: ELK Stack (Elasticsearch, Logstash, Kibana), Wazuh, Apache Spark + MLlib.
4. Промислові рішення: IBM QRadar, Splunk, Palo Alto Cortex XSOAR.

Для успішного впровадження смарт-аналітики в сфері кібербезпеки необхідно забезпечити низку ключових умов. Перш за все, важливо мати доступ до великого обсягу якісних даних, як структурованих (наприклад, журнали подій, таблиці баз даних), так і неструктурованих (електронні листи, текстові файли, мережевий трафік). Ці дані є основою для ефективного аналізу та виявлення загроз. Також критично важливо мати налагоджену систему логування подій, яка забезпечуватиме повноту, актуальність і цілісність зібраної інформації. Ще одним необхідним компонентом є висока обчислювальна потужність, яка дозволить обробляти великі масиви даних у реальному часі та забезпечити швидке виконання складних аналітичних алгоритмів. Без цих технічних і організаційних передумов впровадження смарт-аналітики буде неефективним або навіть неможливим.

Виклики та перспективи впровадження у бізнесі. Попри очевидну ефективність смарт-аналітики, її впровадження у бізнес-практику супроводжується рядом проблем:

1. Вартість впровадження: рішення потребують інвестицій у інфраструктуру, ліцензії та фахівців.
2. Нестача кадрів: кваліфіковані аналітики та інженери даних є дефіцитними на ринку праці.
3. Питання конфіденційності: обробка персональних даних потребує дотримання нормативних актів (GDPR, Закон України «Про захист персональних даних»), ризик помилкових спрацювань (false positives) або пропущених загроз (false negatives).

Проте, тенденції розвитку є позитивними: зростає кількість хмарних сервісів «як послуга», вдосконалюються алгоритми ШІ, з’являються стандартизовані фреймворки інтеграції кібербезпеки в бізнес-процеси.

Отже, смарт-аналітика – це не лише модний тренд, а стратегічно важливий інструмент формування сучасної моделі кіберзахисту. Вона дозволяє підприємствам виявляти загрози на ранніх стадіях, автоматизувати моніторинг і реагування, а також підвищувати загальну кіберстійкість. У контексті українського бізнесу, впровадження таких рішень може стати ключовим фактором підвищення конкурентоспроможності та забезпечення стабільності в умовах гібридних загроз і воєнних кіберкампаній. У майбутньому доцільно розвивати національні смарт-платформи безпеки, адаптовані до локальних умов, з підтримкою української мови, законодавства та ринку праці.

Список використаних джерел

1. Кустов, В., & Коваленко, М. (2024). Інформаційне забезпечення управління процесами на біржах в умовах цифровізації. *Modeling the development of the economic systems*, (2), 47–57. https://doi.org/10.31891/mdes/2024-12-7.

2. ENISA. *ENISA threat landscape 2023*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

3. IBM Security. *IBM X-Force threat intelligence index 2024*. https://www.ibm.com/reports/threat-intelligence

4. Wang, H., Yang, Y., & Yang, W. (2018). Big data management and analytics: A survey. IEEE Transactions on Knowledge and Data Engineering, 30(6), 1000-1019. https://doi.org/10.1109/TKDE.2018.2800984.

Ярич І.Я.,
методист, викладач,
Державний навчальний заклад «Вище професійне училище №34 м.Стрий»

КІБЕРБЕЗПЕКОВА СТРАТЕГІЯ ПІДПРИЄМСТВА В УМОВАХ ВОЄННОГО ЧАСУ ТА ПОВОЄННОГО ВІДНОВЛЕННЯ УКРАЇНИ

У контексті воєнної агресії росії проти України та масштабного переходу на цифрові інфраструктури, питання кібербезпеки набуло особливої актуальності. Підприємства стають мішенню кібератак, що мають на меті дестабілізацію, викрадення даних, знищення інфраструктури. У післявоєнний період, коли почнеться активне економічне відновлення, ризики залишатимуться високими. Ефективне забезпечення кібербезпеки на підприємствах потребує комплексного вирішення та вимагає скоординованих дій на національному, регіональному і міжнародному рівнях [3].

Ключовими аспектами кібезбезпеки підприємств є захист критичної інфраструктури, резервне копіювання і відновлення даних, навчання персоналу, упровадження сучасних технологій захисту, співпраця з державними і міжнародними організаціями. Повоєнне відновлення України потребуватиме комплексного підходу до кібербезпеки, щоб забезпечити стабільність економіки та захистити підприємства від нових викликів [2].

Заходами кібербезпеки, які можуть бути застосовані підприємствами для захисту своїх даних та мінімізації ризиків кібератак є:

- фішинг-атаки та їх запобігання: навчання персоналу розпізнаванню фішингових листів та підозрілих посилань, що допоможе уникнути витоку конфіденційної інформації;