

можуть впливати на ціну; обмеження чутливих ознак і проксі-змінних; реальна можливість відмови від персоналізації; аудит алгоритмічної системи на системні перекоси, особливо у сферах базових потреб (Future of Privacy Forum, 2026).

Отже, головна проблема полягає не в різних цінах, а в інформаційній перевазі цифрової платформи над споживачем. Якщо персоналізоване ціноутворення прозоре, контрольоване й перевірене на дискримінаційні наслідки, воно може бути інструментом гнучкого управління попитом. Якщо ж воно приховує використання персональних даних для оцінки готовності людини платити більше, така практика стає механізмом непрозорого вилучення додаткової вигоди.

Список використаних джерел

1. California Department of Justice. (2026, January 27). On Data Privacy Day, Attorney General Bonta focuses on surveillance pricing, compliance with California Consumer Privacy Act. <https://oag.ca.gov/news/press-releases/data-privacy-day-attorney-general-bonta-focuses-surveillance-pricing-compliance>
2. European Commission. (2024, March 7). Tinder commits to provide consumers with clear information about personalised prices. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1344
3. . European Parliament and Council of the European Union. (2019). Directive (EU) 2019/2161 as regards the better enforcement and modernisation of Union consumer protection rules. <https://www.legislation.gov.uk/eudr/2019/2161/data.xht?view=snippet&wrap=true>
4. Federal Trade Commission. (2025, January 17). FTC surveillance pricing study indicates wide range of personal data used to set individualized consumer prices. <https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer>
5. Future of Privacy Forum. (2026). The price is right: Responsible uses of personal data in pricing. <https://fpf.org/blog/the-price-is-right-responsible-uses-of-personal-data-in-pricing/>
6. Governor of Maryland. (2026, April 28). Governor Moore signs legislation to protect Marylanders' pocketbooks in grocery stores, safeguard voting rights, and strengthen foster care oversight. <https://governor.maryland.gov/news/press-releases/governor-moore-signs-legislation-protect-marylanders-pocketbooks-grocery-stores-safeguard-voting>
7. Groundwork Collaborative, Consumer Reports, & More Perfect Union. (2025). Same cart, different price: Instacart's price experiments cost families at checkout. <https://groundwork-collaborative.org/work/instacart/>
8. New York State Office of the Attorney General. (2026, January 8). Attorney General James demands answers from Instacart about algorithmic pricing. <https://ag.ny.gov/press-release/2026/attorney-general-james-demands-answers-instacart-about-algorithmic-pricing>

Камінський О.Є.,
д.е.н., професор,

Лютий О. О.,
здобувач першого (бакалаврського) рівня вищої освіти,
Київський національний економічний університет імені Вадима Гетьмана

СМАРТ-АНАЛІТИКА І ПРОАКТИВНИЙ КІБЕРЗАХИСТ КРИТИЧНИХ БІЗНЕС-ПРОЦЕСІВ

Сучасний етап розвитку цифрової економіки характеризується активним впровадженням інформаційних технологій у всі сфери бізнесу. Традиційні методи кіберзахисту, які базуються переважно на реактивному реагуванні на інциденти, поступово втрачають ефективність через високу швидкість розвитку кіберзагроз. Сучасні атаки характеризуються адаптивністю, автоматизацією та використанням елементів штучного інтелекту. Це потребує переходу до

проактивних моделей кібербезпеки, здатних прогнозувати потенційні загрози та запобігати їх реалізації ще до моменту виникнення інциденту.

Смарт-аналітика є комплексом методів обробки та інтерпретації даних, що забезпечують автоматичне виявлення аномалій, оцінювання ризиків та підтримку процесів управління. На відміну від класичних аналітичних систем, смарт-аналітика використовує елементи штучного інтелекту, нейронних мереж та предиктивного моделювання.

У сфері кібербезпеки смарт-аналітика дозволяє здійснювати:

- моніторинг мережевої активності у режимі реального часу;
- виявлення нетипової поведінки користувачів;
- прогнозування потенційних атак;
- автоматизований аналіз кіберінцидентів;
- оцінювання рівня кіберризиків бізнес-процесів.

Відповідно до підходу NIST Cybersecurity Framework 2.0 [1], сучасна кібербезпека має розглядатися як безперервний процес ідентифікації, оцінювання, пріоритизації та комунікації кіберризиків на рівні всієї організації. Це особливо важливо з огляду на актуальний ландшафт загроз, адже у звіті ENISA Threat Landscape 2024 [2] серед провідних ризиків виділено загрози доступності, DDoS-атаки, ransomware та атаки на дані, що безпосередньо впливають на стабільність цифрових бізнес-процесів. Практичну цінність використання штучного інтелекту, автоматизації та аналітичних інструментів у кіберзахисті підтверджують і результати IBM [3], згідно з якими застосування AI та автоматизації у сфері безпеки може суттєво зменшувати фінансові втрати від витоків даних.

Проактивний кіберзахист базується на принципі попередження загроз, а не лише реагування на вже здійснені атаки. Основною метою такого підходу є мінімізація ймовірності реалізації кіберризиків та забезпечення стійкості критичних бізнес-процесів. Узагальнення основних напрямів використання смарт-аналітики у проактивному кіберзахисті критичних бізнес-процесів подано в табл. 1.

Таблиця 1

**Напрями застосування смарт-аналітики
у проактивному кіберзахисті критичних бізнес-процесів**

Напрямок застосування	Дані для аналізу	Аналітичні методи	Очікуваний результат для бізнесу
Моніторинг мережевої активності	журнали подій, мережевий трафік, запити до серверів	виявлення аномалій, кластеризація, аналіз часових рядів	раннє виявлення підозрілої активності та зменшення часу реагування
Поведінкова аналітика користувачів	історія входів, дії користувачів, зміни прав доступу	побудова профілів нормальної поведінки, машинне навчання	виявлення компрометації облікових записів або інсайдерських загроз
Оцінювання кіберризиків бізнес-процесів	дані про вразливості, критичність активів, частоту інцидентів	ризик-скоринг, предиктивна аналітика, експертні моделі	пріоритизація захисту найбільш важливих бізнес-процесів
Прогнозування кібератак	історичні інциденти, дані Threat Intelligence, індикатори компрометації	нейронні мережі, класифікаційні моделі, кореляційний аналіз	попередження потенційних атак до їх реалізації
Автоматизоване реагування	сигнали SIEM/SOAR, події безпеки, рівень критичності інциденту	системи підтримки прийняття рішень, правила реагування, AI-аналіз	скорочення втрат, швидка ізоляція загроз, забезпечення безперервності бізнесу
Цифрові двійники інфраструктури	моделі інформаційних систем, сценарії атак, конфігурації захисту	імітаційне моделювання, сценарний аналіз	тестування захисту без ризику для реальної інфраструктури

Критичними бізнес-процесами є процеси, порушення яких може призвести до значних фінансових втрат, репутаційних ризиків або зупинки діяльності підприємства. До них належать фінансові операції, логістичні системи, управління базами даних, хмарна інфраструктура та системи електронної комерції.

Сучасні проактивні системи кіберзахисту використовують:

- інтелектуальні системи виявлення вторгнень;
- поведінкову аналітику користувачів;
- автоматизоване управління кіберризиками;
- технології цифрових двійників;
- адаптивні алгоритми реагування на інциденти.

Одним із перспективних напрямів є використання цифрових двійників інформаційної інфраструктури підприємства. Такі моделі дозволяють моделювати можливі сценарії атак, оцінювати вразливості систем та тестувати механізми захисту без впливу на реальні бізнес-процеси. Крім того, важливе значення має концепція Zero Trust, відповідно до якої жоден користувач або пристрій не вважається апіорі безпечним. Це забезпечує багаторівневий контроль доступу та постійний моніторинг активності у корпоративній мережі.

Розвиток штучного інтелекту створює нові можливості для побудови адаптивних систем кібербезпеки. AI-технології дозволяють аналізувати складні взаємозв'язки між подіями, автоматично класифікувати загрози та формувати оптимальні сценарії реагування. Інтелектуальні системи підтримки прийняття рішень можуть використовуватися для:

- оптимізації управління кіберризиками;
- автоматичного розподілу ресурсів захисту;
- оцінювання рівня критичності інцидентів;
- прогнозування наслідків кібератак.

Перспективним є також застосування нейромережових моделей для виявлення складних багатоступеневих атак, які важко ідентифікувати традиційними методами. Завдяки здатності до самонавчання AI-системи можуть підвищувати точність аналізу та адаптуватися до нових типів загроз.

Висновки. Отже, цифрова трансформація бізнесу потребує впровадження нових підходів до забезпечення кібербезпеки критичних бізнес-процесів. Використання смарт-аналітики, штучного інтелекту та адаптивних систем захисту дозволяє перейти від реактивних моделей безпеки до проактивного управління кіберризиками. Сучасні системи кіберзахисту повинні забезпечувати безперервний моніторинг інформаційного середовища, прогнозування потенційних загроз та автоматичне реагування на інциденти. Подальші дослідження доцільно спрямувати на розробку гібридних моделей проактивного кіберзахисту із використанням AI-аналітики, квантово-орієнтованих алгоритмів та систем підтримки прийняття рішень в умовах невизначеності.

Список використаних джерел

1. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
2. European Union Agency for Cybersecurity. (2024). *ENISA Threat Landscape 2024*. Publications Office of the European Union. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
3. IBM. (2024). *Cost of data breaches: The business case for security AI and automation*. IBM Think. <https://www.ibm.com/think/insights/cost-of-data-breaches-business-case-for-security-ai-automation>