

і правового регулювання. Український бізнес має можливість адаптувати європейські практики (GDPR, етичні кодекси, технічні рішення), при цьому дбаючи про прозорість, добровільність збору даних і захист цифрових прав працівників. Баланс між ефективністю та етикою стане визначальним фактором довіри до HR-систем майбутнього.

Список використаних джерел

1. Загальний регламент про захист даних (GDPR). Офіційний переклад українською мовою. <https://kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf>
2. Thakral, P., Srivastava, P., Dash, S., Jasimuddin, S., & Zhang, Z. (2023). Trends in the thematic landscape of HR analytics research: a structural topic modeling approach. *Management Decision*. <https://doi.org/10.1108/md-01-2023-0080>.
3. Wirges, F., & Neyer, A. (2022). Towards a process-oriented understanding of HR analytics: implementation and application. *Review of Managerial Science*, 1 - 32. <https://doi.org/10.1007/s11846-022-00574-0>.

Джалладова І.А.,
д. ф.-м. н., професор,
Камінський О.Є.,
д. е. н., доцент,
Гребельний А. Б.,
здобувач третього (наукового) рівня вищої освіти,
КНЕУ імені Вадима Гетьмана

ШТУЧНИЙ ІНТЕЛЕКТ У ВИЯВЛЕННІ СОЦІОТЕХНІЧНИХ ЗАГРОЗ КІБЕРБЕЗПЕКИ БІЗНЕСУ

Швидкий прогрес у галузі штучного інтелекту (ШІ) створює як можливості, так і загрози, які обіцяють стати трансформаційними та руйнівними для сфери кібербезпеки. Сучасні підходи до забезпечення безпеки та захисту користувачів обмежені. До поширених методів таких атак належать фішинг, маніпулятивна комунікація та зловмисні дії з боку внутрішніх суб'єктів. Розвиток генеративного штучного інтелекту змінює кібербезпеку, оскільки він одночасно застосовується як для створення шкідливого контенту, так і для підвищення

ефективності захисту за допомогою методів аналізу аномалій і прогнозування ризиків.

У 2024 році 94% світових компаній зазнали фішингових атак, при цьому 73% таких порушень безпеки були пов'язані з фішингом та соціальною інженерією [1]. У 2024 році вже 40% фішингових листів були згенеровані за допомогою штучного інтелекту. Також, в тому ж році, 79% кіберінцидентів не використовували традиційне шкідливе програмне забезпечення, а були засновані на соціотехнічних методах, посилені штучним інтелектом [2].

Таким чином, дослідження впливу штучного інтелекту на соціотехнічну безпеку є актуальним як з наукового, так і з прикладного погляду, оскільки дозволяє створити основу для формування нового покоління інтегрованих систем кіберзахисту в умовах цифрової економіки. Так, у роботі [3] досліджуються соціотехнічні виклики, пов'язані з впровадженням штучного інтелекту у системи кібербезпеки, зокрема ризик маніпуляцій, обману користувачів та прихованих галюцинацій мовних моделей. Автори наголошують на потребі запровадження етичного законодавства та створення пояснюваних систем на базі моделей ШІ. В дослідженні [4] наведено застосування великих мовних моделей (LLM), зокрема моделі GPT, для ідентифікації кіберзагроз та аномалій мережевого трафіку.

Соціотехнічний підхід до кібербезпеки визнає взаємозалежність між технологічними системами та соціальними (людськими, організаційними) процесами. Завдяки вивченню та застосуванню соціотехнічного підходу, який підкреслює важливість та цінність партисипативних практик, ми можемо створити нові способи концептуалізації викликів штучного інтелекту в контексті кібербезпеки. З поширенням технологій штучного інтелекту (ШІ) цей підхід зазнає якісних змін — від класичної взаємодії людина-комп'ютер до симбіозу людина-ШІ. Згідно з дослідженням, ефективна кібербезпека потребує врахування трьох рівнів: мікро рівень - індивідуальні дії користувачів та пристроїв, мезо рівень - взаємодія між організаціями та ланцюгами постачання, макро рівень- національні та міжнародні політики та стандарти. Аналіз, який

наведено в табл.1. показує, що під впливом технологій штучного інтелекту системи кібербезпеки змінюються:

Таблиця 1

**Основні трансформації систем кібербезпеки
під впливом технологій штучного інтелекту**

Складова	Традиційна система	Впровадження технологій ШІ
Центр ухвалення рішень	Людина як основний оператор і аналітик	Автономні або напівавтономні ШІ-системи самостійно приймають рішення
Взаємодія людина–технологія	Використання інструментів, людина задає логіку	ШІ самостійно навчається, прогнозує та пропонує дії людині
Управління ризиками	Залежить від обізнаності персоналу	Виявлення загроз до їх реалізації за допомогою прогнозування
Роль користувача	Активна участь у всіх процесах	Наглядова/коригувальна роль, фокус зміщється на довіру до рішень ШІ
Прозорість	Людина розуміє логіку дій системи	Необхідно пояснюєння рішень (впровадження спеціальних систем)
Безпека	Залежна від людських помилок або зловживань	Є можливість самостійного виявлення маніпулятивних моделей поведінки

Тобто, ми можемо визначити ключові зміни в кібербезпеці бізнесу:

1. Сучасні технології штучного інтелекту дозволяють здійснювати комплексний аналіз не лише технічних параметрів, але й характеристик поведінки користувачів, що відкриває можливості для виявлення аномалій та шкідливої активності в корпоративних мережах. Також застосування адаптивних моделей штучного інтелекту забезпечить індивідуальне налаштування захисних механізмів відповідно до особливостей поведінки працівників, що сприятиме виявленню нетипових дій персоналу та мінімізації внутрішніх загроз.

2. Використання генеративних моделей суттєво ускладнює ідентифікацію фішингових атак. У зв'язку з цим виникає необхідність розробки нових підходів до протидії цим загрозам, які враховують, як технологічний, так і психологічний аспекти маніпуляцій.

3. Автономність штучного інтелекту як фактор ризику. Зростаюча інтеграція автономних агентів ШІ у процеси виявлення та реагування на кіберінциденти супроводжується ризиком втрати контролю людини над прийняттям рішень. Непрозорість алгоритмічної логіки моделей ШІ та

складність її інтерпретації можуть призводити до критичних помилок у системах безпеки.

Таким чином, для адаптації систем кіберзахисту в сучасних умовах є необхідним розвиток та інституційна інтеграція систем пояснювального штучного інтелекту, тобто включення систем пояснюваного штучного інтелекту у процеси аудиту, сертифікації та ієрархії відповідальності системи безпеки.

Пропонуємо вдосконалену структуру системи кіберзахисту бізнесу, яку наведено на рис.1.

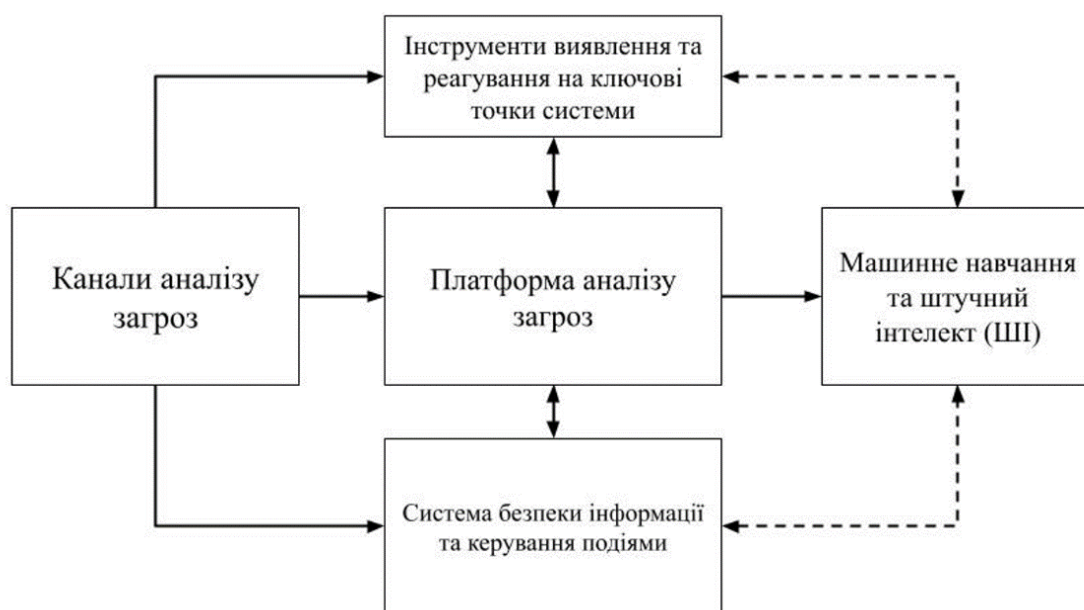


Рис.1. Структурна схема системи кіберзахисту на основі технологій штучного інтелекту.

Запропонована структурна схема включає наступні модулі:

1. Платформа аналізу загроз, яка збирає дані про загрози з всіх джерел інформації підприємства і передає їх для аналізу модулю штучного інтелекту.

2. Модуль системи захисту інформації та керування подіями, який збирає і аналізує дані щодо поведінки працівників з усієї організації, виявляючи потенційні загрози.

3. Модуль машинного навчання та штучного інтелекту, який використовується для аналізу даних та виявлення закономірностей і аномалій поведінки користувачів та трафіку комп'ютерних мереж.

4. Модуль виявлення та реагування на ключові точки, який відстежує стан ключових точок системи (сервери, маршрутизатори) на наявність ознак шкідливої діяльності та надає інформацію про потенційні загрози.

5. Канали аналізу загроз - безперервний потік даних у режимі реального часу, який збирає інформацію, пов'язану з кіберризиками або загрозами, навчаючи систему новим загрозам.

Важливим також є вдосконалення методів соціотехнічного аудиту, тобто регулярна оцінка взаємодії між людьми, алгоритмами, інтерфейсами та ризиками соціального впливу. Кібератаки, зумовлені штучним інтелектом, мають глибокий хвильовий ефект, впливаючи на економічні структури, політичний ландшафт та соціальні норми. Тому є необхідним інтегрувати в дискусії щодо кібербезпеки людиноцентричні та нетехнічні аспекти, що вимагає переходу від традиційно техноцентричної парадигми до більш інклюзивного та міждисциплінарного підходу.

Висновок. Соціотехнічний підхід в епоху штучного інтелекту змінюється від моделі «людина керує машиною» до співжиття з інтелектуальною системою, яка самостійно аналізує, адаптується, прогнозує й іноді приймає критичні рішення. Це потребує нових інструментів прозорості, підзвітності, довіри та етичного контролю — основ нової епохи «соціотехнічної безпеки з штучним інтелектом». Всі ці аспекти призведуть до появи концепції «Кібергігієна 2.0» — нового рівня підготовки користувачів, які будуть не лише знати базові правила кібербезпеки, але і розуміти можливості ШІ та його вразливості.

Список використаних джерел

1. Secureframe. (2024). Social engineering statistics and trends to watch in 2024. Retrieved from <https://secureframe.com/blog/social-engineering-statistics>
2. Digital Watch Observatory. (2024). Cyber threats in 2024 shift to AI-driven attacks and cloud exploits, says CrowdStrike. Retrieved from <https://dig.watch/updates/cyber-threats-in-2024-shift-to-ai-driven-attacks-and-cloud-exploits-says-crowdstrike>

3. Taddeo, M., & Floridi, L. (2023) The ethics of artificial intelligence in cybersecurity: A social-technical perspective. *Journal of Cybersecurity*, 9(1), 1–15. <https://doi.org/10.1093/cybsec/tyad004>

4. Ruzickova, M., Dzhalladova, I., Kaminsky, O., Bartash, O., & Pavlov, A. (2023). AI and LLM models to analyze and identify cybersecurity incidents. CEUR Workshop Proceedings, 3746, 115–123. <https://ceur-ws.org/Vol-3746/paper11.pdf>

Калганова В.І.,
старший викладач,
Барташ О.В.,
асистент,
КНЕУ імені Вадима Гетьмана

ІНФОРМАЦІЙНА ЕТИКА ЯК ІНСТРУМЕНТ ПРОТИДІЇ КОРУПЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

У сучасному цифровому середовищі соціальні мережі стали потужним каналом не тільки для комунікації, а й для поширення маніпуляцій, фейкових новин і корупційних схем. Ці платформи використовуються для впливу на громадську думку, мобілізації електорату, дестабілізації ситуації, фінансових зловживань. Тому зростає потреба у формуванні інформаційної культури з акцентом на етичні норми поведінки в цифровому просторі. Інформаційна етика, як складова інформаційної культури, виступає одним із найважливіших чинників стримування подібних загроз [5].

Інформаційна етика — це система моральних принципів, що регулює процес створення, поширення та споживання інформації в Інтернеті. Її ключовими складовими є достовірність, відповідальність, приватність, прозорість намірів та поважне спілкування [5]. Дотримання цих принципів знижує ризик участі в інформаційних маніпуляціях та сприяє прозорості цифрового простору.

Окреме значення має протидія фейковим новинам, які, за даними дослідження МІТ, поширюються у Twitter на 70% швидше, ніж достовірна інформація [2]. Їх часто супроводжують емоційні заголовки, навмисне