розвиток цих систем пов'язаний із поглибленням інтеграції штучного інтелекту, розширенням використання великих даних та вдосконаленням методів аналізу складних мережевих структур кіберзагроз.

Список використаних джерел:

1. Schmitt, M. *Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection*. arXiv preprint arXiv:2401.01342, 2025. URL: https://arxiv.org/abs/2401.01342

2. Mishra, S., Alfahidah, R. A., Alharbi, F. *BERT-spaCy hybrid NLP and blockchain-enhanced adaptive CTI for IOC extraction and threat prediction*. Scientific Reports, 16, 8147 (2026). DOI: https://doi.org/10.1038/s41598-025-34505-2

КІБЕРБЕЗПЕКА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ: НОВІ ТЕХНОЛОГІЧНІ ВИКЛИКИ

Моргунова Тетяна Іванівна
к.т.н., доцент, доцент кафедри
кримінального аналізу та інформаційних технологій
Одеського державного університету внутрішніх справ
Шипрінський Нікіта Олегович
здобувач першого (бакалаврського)
рівня вищої освіти спеціальності 081 «Право»
Одеського державного університету внутрішніх справ

Сучасний етап розвитку економіки характеризується глибокою цифровою трансформацією, яка охоплює практично всі сфери діяльності підприємств, організацій та державних інституцій.

Цифрова трансформація відбувається, коли організації впроваджують цифрові технології у всі свої операції [1].

Інтенсивне впровадження цифрових технологій сьогодні вже не виглядає як щось нове або виняткове, швидше як звична частина розвитку підприємств, хоча ще кілька років тому це сприймалося інакше. Хмарні сервіси, аналітика великих даних, рішення на основі штучного інтелекту, різні пристрої Інтернету речей поступово вбудовуються у повсякденну діяльність і дають

відчутний ефект, особливо коли мова йде про оптимізацію процесів або скорочення витрат. Разом із цим виникає інша сторона питання, яку іноді недооцінюють, – збільшення кількості кіберзагроз, причому не тільки кількісно, а й за складністю. Через це вже складно говорити про кібербезпеку як про окрему функцію, швидше це стає частиною загальної логіки управління, хоча не всі підприємства до цього готові.

Якщо дивитися на практику, то стає помітно, що кібербезпека поступово виходить за межі технічних підрозділів. У багатьох випадках вона вже впливає на стратегічні рішення, навіть якщо це прямо не визнається. Будь-який збій в інформаційній системі, або навіть незначний витік даних, може створити проблеми, які важко швидко компенсувати. Особливо це відчувається у компаніях, що працюють на зовнішніх ринках, де додається ще й фактор різних вимог і правил, інколи досить суперечливих. До речі, іноді саме регуляторні обмеження створюють більше труднощів, ніж самі технічні ризики.

Останнім часом змінюється і характер самих кіберзагроз. Якщо раніше це були переважно поодинокі спроби втручання, то зараз частіше йдеться про складніші сценарії, де поєднуються різні підходи. Наприклад, атаки типу «ransomware» або «фішинг» вже стали майже буденністю, але при цьому вони постійно змінюються і адаптуються.

«Ransomware» – це тип шкідливої програми, який злочинці встановлюють на комп'ютерах користувачів. Програми, які вимагають викуп, надають злочинцям можливість віддалено заблокувати комп'ютер [2].

«Фішингові» атаки мають на меті викрасти або пошкодити конфіденційну інформацію, примушуючи людей обманом розкрити свої персональні дані, зокрема паролі й номери кредитних карток [3].

Додаються ще й ризики, пов’язані з постачальниками програмного забезпечення, що іноді випадає з уваги. Усе це накладається на збільшення кількості пристроїв у мережі, і межі цієї мережі вже не так просто окреслити, як це було раніше.

Окремо варто згадати про хмарні технології, які, з одного боку, дійсно спрощують багато процесів. Підприємства отримують доступ до ресурсів без значних інвестицій у власну інфраструктуру,

але при цьому виникає певна залежність від зовнішніх провайдерів. Не завжди зрозуміло, де проходить межа відповідальності, і це інколи створює додаткові ризики. Часто буває так, що рішення впроваджують швидше, ніж встигають продумати їх захист, і потім доводиться виправляти ситуацію вже в процесі роботи.

Ситуація з Інтернетом речей виглядає ще складнішою. Різні сенсори, контролери, допоміжні пристрої активно використовуються у виробництві та логістиці, і це дійсно підвищує ефективність. Але одночасно з'являється багато точок потенційного доступу, і далеко не всі вони достатньо захищені. Іноді один слабкий елемент може вплинути на всю систему, що вже неодноразово підтверджувалося на практиці. У невеликих компаніях це питання взагалі часто відкладається на потім, поки не виникає реальна проблема.

Ще один момент, який останнім часом активно обговорюється, – використання штучного інтелекту. Його застосовують і для захисту, і для атак, що виглядає дещо парадоксально. Алгоритми допомагають швидше виявляти відхилення або підозрілі дії, але водночас можуть використовуватись для створення складніших схем впливу. Наприклад, генерація текстів для «фішингових» повідомлень або спроби обійти системи «автентифікації». У цьому сенсі розвиток технологій не завжди однозначно покращує ситуацію, інколи навпаки ускладнює її.

У цьому контексті доцільно систематизувати ключові технологічні виклики кібербезпеки в умовах цифрової трансформації. З цією метою в табл. 1 узагальнено основні напрями загроз та їх практичні прояви.

Таблиця 1

Основні технологічні виклики кібербезпеки в умовах цифрової трансформації

Напрям цифровізації	Основні кіберзагрози	Практичні прояви	Наслідки для підприємства
Хмарні технології	Несанкціонований доступ, витік даних	Злам облікових записів, помилки конфігурації	Фінансові втрати, порушення конфіденційності
Інтернет речей	Вразливість пристроїв, відсутність оновлень	Захоплення контролю над пристроями	Збої в операційній діяльності

Великі дані	Несанкціонована обробка інформації	Маніпуляції з аналітичними результатами	Прийняття помилкових управлінських рішень
Штучний інтелект	Зловживання алгоритмами	Генерація фальшивого контенту, обхід захисту	Репутаційні втрати
Ланцюги постачання	Атаки через сторонніх постачальників	Інфікування програмного забезпечення	Масове поширення загроз

Якщо узагальнити наведені положення, то кібербезпека в умовах цифрових змін уже складно сприймається як окремий напрям роботи, вона швидше розчиняється в загальній системі управління підприємством. Тут переплітаються технічні рішення, організаційні підходи і навіть управлінські звички, які склалися раніше і не завжди швидко змінюються. Окремо варто згадати про персонал, бо саме на цьому рівні часто виникають слабкі місця. Практика показує, що значна кількість інцидентів пов'язана не стільки зі складними атаками, скільки з банальною необережністю або недостатнім розумінням ризиків. І це не завжди легко виправити лише інструкціями чи формальними навчаннями.

У реальній діяльності підприємств поступово приживається ризик-орієнтований підхід, хоча він не завжди впроваджується послідовно. Ідентифікація ризиків, їх оцінка, визначення пріоритетів – усе це виглядає логічно, але на практиці часто залежить від доступних ресурсів і навіть від особистого бачення керівництва. При цьому важливо, щоб цей процес не зводився до одноразових дій, адже кіберзагрози змінюються досить швидко, інколи навіть швидше, ніж очікується. Виходить, що система управління ризиками повинна бути постійно в русі, хоча забезпечити таку безперервність вдається не всім.

Щодо міжнародних стандартів, то їх значення важко заперечити, особливо для підприємств, які працюють із закордонними партнерами. Вони задають певні орієнтири і створюють відчуття впорядкованості у підходах до захисту інформації. Водночас пряме перенесення стандартів у практику не завжди дає очікуваний результат, оскільки доводиться враховувати локальні умови, вимоги законодавства і навіть специфіку галузі. Іноді цей процес

виглядає дещо формальним, коли головною метою стає відповідність документам, а не реальне підвищення рівня безпеки.

Якщо говорити про подальший розвиток систем кібербезпеки, то можна виділити кілька напрямів, які зазвичай згадуються, хоча вони не завжди реалізуються в повному обсязі. Насамперед це інтеграція питань безпеки у стратегічне управління, що виглядає очевидним, але потребує певної перебудови підходів. Далі – розвиток систем моніторингу, які дозволяють реагувати на інциденти швидше, ніж це було раніше. Також важливим залишається питання підготовки персоналу, причому не лише вузьких спеціалістів, а й звичайних працівників. І, звичайно, використання сучасних технологій, включаючи штучний інтелект, хоча тут теж не все однозначно, бо разом із новими можливостями з'являються і додаткові ризики, про які іноді згадують уже після впровадження.

Підсумовуючи, слід зазначити, що цифрова трансформація створює не лише нові можливості, але й суттєві ризики, пов'язані з кібербезпекою. Ефективне протидіяння цим ризикам можливе лише за умови комплексного підходу, який поєднує технічні рішення, організаційні заходи та стратегічне бачення розвитку підприємства. У сучасних умовах кібербезпека стає невід'ємною складовою конкурентоспроможності та стійкості підприємств, особливо тих, що функціонують у міжнародному середовищі.

Список використаних джерел:

1. Що таке цифрова трансформація? *SAP*: офіційний веб-сайт компанії SAP. 2023. 27 груд. 2023 р. URL: https:/ /www.sap.com/ukraine /resources/what-is-digital-transfor ma tion

2. Ransomware. *Вікіпедія*: вільна онлайн-енциклопедія. URL: https://uk.wikipedia.org/wiki/Ransomware (дата звернення: 18.04.2026).

3. Що таке фішинг? *Microsoft*: офіційний веб-сайт компанії Microsoft. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-phishing (дата звернення: 18.04.2026).