

УДК 658.8

ІНТЕГРАЦІЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРОМИСЛОВІСТІ: СУЧАСНІ ТЕНДЕНЦІЇ ЗАХОДІВ БЕЗПЕКИ

Курепін В.М., к.е.н., доц.
Миколаївський національний аграрний університет
м. Миколаїв, Україна, kypins@ukr.net

Анотація. У світі промислове виробництво зазнає значних змін, зумовлені стрімким розвитком інформаційних технологій, зокрема в галузі безпеки. Впровадження ІТ-рішень у різні сфери виробничої діяльності відкриває нові можливості для підвищення ефективності, оптимізації процесів та покращення якості своєї продукції. Ми розглянемо актуальні напрямки впровадження інформаційних технологій у промисловому секторі та проаналізуємо пов'язані з цим ризики для інформаційної та технічної безпеки. Окреслимо основні виклики, що виникають під час цифрової трансформації промислових процесів, а також запропоновано заходи для зміцнення безпеки критичної інфраструктури.

Ключові слова: кіберзагроза, захист інформації, штучний інтелект, потенційні ризики, технології

На тлі стрімкого впровадження штучного інтелекту та цифровізації організацій у різних сферах глобальний ландшафт кіберзагроз продовжує змінюватися. Інтеграція ІТ збільшує ризик кіберзагроз. Промислові системи часто стають мішенню хакерів, зокрема у вигляді системних атак [1, с. 169], шкідливого програмного забезпечення, фішингу та шифрувальників. Злам критичних систем може призвести до зупинки виробництва, втрати даних, фінансових збитків і навіть загрози життю працівників.

Багато підприємств використовують застарілі ІТ-рішення або не мають належної системи захисту. Відсутність регулярних оновлень програмного забезпечення, слабка сегментація мереж та відкриті канали доступу створюють додаткові вразливості.

Такі зміни вимагають кваліфікованих фахівців [2, с. 66]. Але реалії сьогодення показують тенденцію дефіциту кваліфікованих фахівців у цій сфері. Навчання персоналу є критично важливим заходом. Об'єкти господарювання повинні регулярно проводити тренінги, моделювати кіберінциденти, підвищувати цифрову грамотність працівників усіх рівнів. Особливої уваги потребують оператори автоматизованих систем та ІТ-відділів.

Аналітики-дослідники, що спеціалізуються на ринках інформаційних технологій окреслили шість ключових трендів у сфері кібербезпеки, які вплинуть на розвиток галузі. Розглянемо їх:

1. Генеративний штучний інтелект. Традиційно зусилля щодо забезпечення безпеки зосереджені насамперед на захисті структурованої інформації, такої як бази даних. Однак розвиток генеративного штучного інтелекту призводить до трансформації цього підходу та усунення фокусу на захист неструктурованих даних – тексту, зображень та відеоматеріалів. На цьому фоні багато об'єктів господарювання повністю переглянули свої

інвестиційні стратегії в галузі штучного інтелекту, що значно впливає на процес навчання великих мовних моделей.

У перспективі, впровадження генеративного штучного інтелекту дозволить мінімізувати кількість інцидентів безпеки з вини співробітників. Крім того, генеративний штучний інтелект значно підвищить ефективність моніторингу ІТ-інфраструктури з метою виявлення підозрілої активності. Оскільки генеративний штучний інтелект дає можливість перекладати результати аналізу природною мовою, співробітники з меншими технічними навичками можуть працювати більш продуктивно. Це може змінити підхід підприємств до найму та навчання фахівців у відповідній сфері [3, с. 225]. Штучний інтелект допомагає виявляти потенційні ризики: невідомі пристрої та хмарні програми, застарілі операційні системи або незахищені конфіденційні дані. Генеративний штучний інтелект може отримати інформацію з кількох джерел для створення простих для розуміння звітів, якими фахівці з безпеки можуть швидко поділитися з іншими співробітниками в організації.

2. Управління ідентифікаційними даними машин. Зростання застосування генеративного штучного інтелекту, хмарних сервісів, призвело до широкого використання облікових записів та ідентифікаційних даних машин, таких як різні фізичні пристрої та робочі навантаження. Для їх захисту застосовують спеціальні ключі, цифрові сертифікати тощо [4, с. 143]. У такій ситуації керівники об'єктів господарювання змушені розробляти стратегії щодо впровадження надійної ідентифікації та керування доступом до машин для захисту від кібератак.

3. Зміна підходу до використання штучного інтелекту. Об'єкти господарювання стикаються зі змішаним ефектом від реалізації проєктів у галузі штучного інтелекту, що змушує їх переглядати пріоритети. На цьому тлі підприємства, організації фокусують зусилля на вужчих варіантах використання штучного інтелекту, які дають вимірний результат і швидше виправдовують інвестиції.

4. Оптимізація технологій кібербезпеки. Великі та малі підприємства використовують у середньому більш як 45 інструментів кібербезпеки (статистика) [5, с. 147]. За наявності біля п'яти тисяч постачальників у сфері інформаційної безпеки керівники об'єктів господарювання стикаються з оптимізацією наборів програмного забезпечення для створення більш ефективних платформ захисту.

5. Програми безпечної поведінки та культури інформаційної безпеки. Фахівці-дослідники зазначають, що все більше керівників об'єктів господарювання усвідомлюють важливість безпекових заходів щодо зниження ризиків кібербезпеки. Некоректні дії співробітників можуть призводити до серйозних інформаційно-безпекових-інцидентів [6, с. 6]. У результаті спостерігається стратегічний зсув у бік впровадження безпеки в організаційну культуру, як структурних підрозділів, так і об'єкту господарювання в цілому.

6. Боротьба з вигорянням у сфері кібербезпеки. Інформаційно-безпекові - фахівці можуть стикатися з тривалим стресом на робочому місці, що пов'язано з ландшафтом загроз, що постійно змінюється, новими нормативно-правовими

вимогами, обмеженими повноваженнями і недостатніми ресурсами. Це призводить до зниження працездатності, погіршення якості, помилок і зазвичай закінчується відходом із компанії.

Отже, успішні приклади інтеграції та автоматизації у промисловому виробництві свідчать про те, що сучасні ІТ-технології відіграють ключову роль у підвищенні ефективності виробництва, покращенні якості продукції та оптимізації бізнес-процесів, якісно вирішують безпекові проблеми. ІТ-технології дозволяють об'єктам господарювання збільшити продуктивність, оптимізувати управління виробництвом, забезпечити безпеку даних виробничих процесів. У майбутньому промисловість неминуче ще більше зануриться у цифровий світ та відкриє для себе нові горизонти.

Список літератури

1. Іваненко В.С. Інструментальні методи конкурентного аналізу підприємств аграрного профілю // Проблеми та перспективи розвитку економіки України: погляд молоді : матеріали XIV Всеукраїнської науково-практичної конференції, м. Черкаси, 20 квітня 2022 р. Черкаси : ЧДБК, 2022. С. 167-170. URL: <https://dspace.mnau.edu.ua/jspui/handle/123456789/11430>.
2. Курепін В. М. Іваненко В. С. Застосування цифрових технологій у сільському господарстві для досягнення цілей сталого розвитку. Modern Economics. 2024. № 47(2024). С. 62-69. DOI: [https://doi.org/10.31521/modecon.V47\(2024\)-09](https://doi.org/10.31521/modecon.V47(2024)-09).
3. Іваненко В. С., Курепін В. М. Подолання кризових явищ у аграрній сфері за допомогою технології доповненої реальності // Урожайність та якість продукції рослинництва за сучасних технологій вирощування : матеріали міжнар. наук.-практ. інтернет-конф., присв. 90-річчю з дня народження професора Г. П. Жемели (м. Полтава, 30 верес. 2023 р.). Полтава : ПДАУ, 2023. С. 224-226. URL: <https://dspace.mnau.edu.ua/jspui/handle/123456789/15512>.
4. Іваненко В. С. Інновації у сфері безпеки: захист різних сфер діяльності місцевих громад. Розвиток територіальних громад: правові, економічні та соціальні аспекти : матеріали IV міжнар. наук.-практ. конф., (м. Миколаїв, 9 грудня 2024 р. Миколаїв : МНАУ, 2024. С. 141-144. URL: <https://dspace.mnau.edu.ua/jspui/handle/123456789/20102>.
5. Лотарева Д. В. Сучасні інформаційні технології у системі управління. Екологічні та соціальні аспекти розвитку економіки в умовах євроінтеграції : матеріали X Всеукраїнської науково-практичної конференції (м. Миколаїв, 23-25 жовтня 2024 р.). Миколаїв : МНАУ, 2024. С. 146-148. URL: <https://dspace.mnau.edu.ua/jspui/handle/123456789/18921>.
6. Кузнецова В. А. Сучасні підходи, стратегія та тактика до управління ризиками на підприємстві. OSHAgro – 2024 : матеріали III Міжнародної науково-практичної конференції (м. Київ, 30 вересня 2024 року). Київ : МОН України, Національний університет біоресурсів і природокористування України, Науково-виробничий журнал «Охорона праці», Європейське співтовариство з охорони, 2024. С. 5-7. URL: <https://dspace.mnau.edu.ua/jspui/handle/123456789/18903>.