

АГРАРНИЙ СЕКТОР І КІБЕРБЕЗПЕКА ЦИФРОВОЇ ЕКОНОМІКИ: СУЧАСНІ ВИКЛИКИ

Цифровізація економіки сприяє активному впровадженню інформаційних технологій у різні сфери господарської діяльності, зокрема в аграрний сектор. Сучасне сільське господарство дедалі більше використовує цифрові рішення, зокрема системи точного землеробства (precision farming), GPS-навігацію, безпілотні літальні апарати, датчики моніторингу стану ґрунтів і врожаю, автоматизовані системи управління технікою та цифрові платформи для торгівлі аграрною продукцією. Такі технології підвищують продуктивність аграрного виробництва, оптимізують використання ресурсів та сприяють підвищенню конкурентоспроможності підприємств.

Водночас використання сучасних агротехнологій створює нові кіберризики. Безпілотні літальні апарати, IoT-сенсори моніторингу ґрунтів і кліматичних умов, а також «розумна» сільськогосподарська техніка, підключена до мережі Інтернет, можуть бути вразливими до несанкціонованого доступу або кібератак. Порушення роботи таких систем може призвести до втрати даних про врожайність, некоректного управління технікою або збоїв у технологічних процесах, що негативно впливає на ефективність аграрного виробництва. Таким чином, сучасний аграрний сектор поступово перетворюється на складну кіберфізичну систему, у якій тісно поєднуються цифрові технології, виробничі процеси та інформаційна інфраструктура.

Одним із найбільш відчутних наслідків кіберзлочинності є значні фінансові втрати. За даними дослідження IBM Global Average Data Breach, середня вартість витоку даних у світі постійно зростає: у 2020 році вона становила 3,9 млн доларів США, у 2021 році — 4,2 млн доларів, а у 2022 році — 4,4 млн доларів [1]. Зростання витрат пов'язане з ускладненням кіберзагроз, збільшенням кількості атак та необхідністю відновлення інформаційних систем після інцидентів.

Фінансові збитки від кібератак можуть проявлятися у різних формах. Передусім це витрати на відновлення інформаційних систем, модернізацію програмного забезпечення та посилення систем кіберзахисту. Показовим прикладом є масштабна кібератака NotPetya у 2017 році, яка завдала світовій економіці збитків приблизно на 10 млрд доларів США та спричинила значні втрати для низки міжнародних компаній [2].

В умовах цифровізації аграрного сектору кіберінциденти можуть мати серйозні фінансові наслідки й для учасників ринку аграрної продукції. Нині аграрні підприємства активно використовують електронні фінансові системи та онлайн-платформи для реалізації продукції, що підвищує ризики фінансового шахрайства та викрадення комерційної інформації.

Важливим економічним наслідком кіберінцидентів є також зниження доходів підприємств у результаті тимчасового припинення діяльності або зменшення ділової активності. У глобальній практиці відомі численні випадки, коли кібератаки призводили до значних економічних втрат для компаній. Наприклад, у 2013 році компанія Target зазнала збитків у розмірі 162 млн доларів США через витік даних кредитних карток клієнтів, а у 2017 році кібератака на компанію Equifax призвела до втрат приблизно у 1,4 млрд доларів США.

Окрім фінансових втрат, кіберзлочинність спричиняє серйозні репутаційні ризики. Втрата довіри клієнтів і партнерів може мати довгострокові економічні наслідки. За даними дослідження Ponemon Institute, близько 62% споживачів припиняють співпрацю з компанією після витоку їхніх персональних даних. Для аграрних підприємств, які дедалі активніше використовують цифрові платформи торгівлі та електронні сервіси, такі наслідки можуть призводити до втрати ринків збуту та зниження конкурентоспроможності.

Особливу загрозу становлять кібератаки на об'єкти критичної інфраструктури. Наприклад, кібератака на трубопровід Colonial Pipeline у США у 2021 році спричинила перебої у постачанні пального, що вплинуло на транспортні та виробничі процеси. Подібні інциденти відбувалися і в Україні, зокрема кібератака на енергетичну інфраструктуру у 2015 році, що призвела до

масштабних відключень електроенергії. Такі події демонструють вразливість економічних систем до кіберзагроз, що може негативно впливати і на стабільність аграрного виробництва.

У зв'язку з цим інвестиції у кібербезпеку стають важливою умовою розвитку цифрової економіки. Світовий ринок кібербезпеки демонструє стабільне зростання: його обсяг оцінюється приблизно у 186 млрд доларів США та, за прогнозами, може досягти понад 271 млрд доларів до 2029 року. В Україні також спостерігається позитивна динаміка розвитку ринку кібербезпеки: у 2024 році його обсяг становив близько 138 млн доларів США [3].

Таким чином, забезпечення кібербезпеки є важливим чинником сталого розвитку аграрного сектору в умовах цифровізації економіки. Для мінімізації кіберризиків необхідно впроваджувати сучасні технології захисту інформації, розвивати системи кібермоніторингу, підвищувати рівень кіберграмотності працівників аграрних підприємств, а також удосконалювати нормативно-правову базу та міжнародну співпрацю у сфері протидії кіберзлочинності.

Список літератури:

1. Global average total cost of a data breach in 2022 growth up to \$4.4 mn.
URL: <https://beinsure.com/news/global-average-data-breach-2022> (дата звернення: 10.03.2026).
2. Історія вірусу NotPetya: чи варто остерігатися подібних кібератак в майбутньому? URL: <https://www.imena.ua/blog/notpetya-cyberattack> (дата звернення: 10.03.2026).
3. Statista. URL: <https://www.statista.com/statistics/> (дата звернення: 10.03.2026).

Підготовлено ГО «Інститут екологічної економіки та цифрового аграрного розвитку»

© 2026 Всі права захищені.

Дозволяється використання матеріалів за умови обов'язкового посилання на джерело.