and international partners to support the sustainable development of the local agri-food sector. Mechanisms aimed at enhancing the adaptive capacity of communities to external risks and ensuring the economic accessibility of food for all population groups are proposed.

Keywords: food resilience, territorial communities, public governance, socio-economic planning, short supply chains, food reserve.

УДК 004.056:338.439 DOI 10.31521/978-617-7149-94-0-145

КІБЕРБЕЗПЕКА АГРОПРОДОВОЛЬЧИХ ІНФОРМАЦІЙНИХ СИСТЕМ У КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Жебко О.О., аспірант
Миколаївський національний аграрний університет
https://orcid.org/0009-0009-1604-5952

Анотація: Досліджено проблеми кібербезпеки агропродовольчих інформаційних систем в умовах зростання цифровізації аграрного сектора та загострення геополітичних конфліктів. Розглядаються основні кіберзагрози для агропромислового комплексу, зокрема атаки на системи управління виробництвом, бази даних продовольчих запасів та логістичні платформи. Аналізується зв'язок між захищеністю аграрних інформаційних систем і рівнем продовольчої безпеки держави. Обґрунтовується необхідність формування комплексної стратегії кіберзахисту агропродовольчої інфраструктури як складової національної безпеки України.

Ключові слова: кібербезпека, агропродовольчі інформаційні системи, національна безпека, кіберзагрози, продовольча безпека.

Цифрова трансформація агропромислового комплексу України формує принципово нове середовище виробництва, в якому інформаційні системи відіграють ключову роль у забезпеченні безперервності технологічних процесів. Від платформ точного землеробства та автоматизованих елеваторних комплексів до державних реєстрів земельного кадастру і систем моніторингу продовольчих запасів – усі ці ресурси становлять критичну цифрову інфраструктуру, вразливість якої безпосередньо позначається на стані продовольчої безпеки держави. В умовах повномасштабної збройної агресії росії проти України цифровий фронт набув стратегічного значення нарівні з кінетичними операціями.

Масштаби кіберзагроз для агропродовольчого сектора підтверджуються конкретними прикладами. У лютому 2022 року, одночасно з початком вторгнення, угруповання Sandworm здійснило масовану атаку на українські комунікаційні та енергетичні мережі за допомогою шкідливого програмного забезпечення Industroyer2 та CaddyWiper, яке знищувало дані на інфікованих системах [1]. Під удар потрапили й логістичні оператори, що обслуговували агропродовольчі ланцюги постачання. Збої в роботі транспортних

диспетчерських систем призвели до затримок у відвантаженні зернових з портів Миколаєва та Одеси в перші тижні вторгнення, що безпосередньо загострило глобальну продовольчу кризу.

Не менш показовим є інцидент із злочинним угрупованням BlackCat (ALPHV), яке в 2023 році атакувало одного з провідних американських агрохолдингів Crystal Valley Cooperative за допомогою ransomware, зашифрувавши бази даних постачання добрив і насіннєвого матеріалу в розпал посівної кампанії [2]. Схожі атаки у 2021 році зазнала NEW Cooperative – американська фермерська кооперативна мережа, чиї системи управління зберіганням зерна були заблоковані програмою-вимагачем BlackMatter. Зловмисники вимагали 5,9 млн доларів викупу, погрожуючи оприлюднити дані про харчові ланцюги постачання та технологічні вразливості [3]. Ці випадки наочно демонструють, що кіберзлочинці цілеспрямовано обирають аграрний сектор як об'єкт тиску саме в критичні агрономічні періоди.

В українському контексті особливу небезпеку становлять атаки на автоматизовані системи управління технологічними процесами (АСУ ТП) переробних підприємств і елеваторів. На відміну від корпоративних IT-систем, промислові контролери (PLC) та SCADA-системи часто використовують застаріле програмне забезпечення без регулярних оновлень безпеки, не ізольовані від зовнішніх мереж і не передбачають механізмів автентифікації операторів [4]. Згідно зі звітом Держспецзв'язку за 2024 рік, кількість зафіксованих кіберінцидентів на об'єктах критичної інфраструктури – до яких відносяться великі зернові термінали та переробні комбінати – зросла на 62% порівняно з 2021 роком.

Окремим вектором загроз є атаки на державні інформаційні ресурси агропродовольчого призначення. Зокрема, Державний земельний кадастр України неодноразово ставав об'єктом спроб несанкціонованого доступу: у 2022 році зафіксовано спробу знищення бази даних із понад 7 млн записів про права власності на земельні ділянки, що могло паралізувати земельний ринок у критичний момент [5]. Компрометація реєстрів виробників сільськогосподарської продукції та систем виплати аграрних субсидій несе подвійну загрозу: фінансові втрати для сектора та дезорганізація державного управління продовольчим забезпеченням.

Проблема посилюється структурною неготовністю більшості аграрних підприємств до кіберзагроз. Дослідження, проведене Українською аграрною асоціацією у 2025 році, показало, що лише 18% агропідприємств мають затверджені плани реагування на кіберінциденти, а 64% ніколи не проводили аудит інформаційної безпеки [6]. Типова картина середнього господарства – це підключений до інтернету комп'ютер для бухгалтерії та прийому замовлень, корпоративна пошта без двофакторної автентифікації і відсутність резервних копій критичних даних. За таких умов навіть масовий фішинг здатен зупинити роботу підприємства в розпал збирання врожаю.

На міжнародному рівні проблема кібербезпеки агропродовольчих систем активно опрацьовується у форматі ФАО та G7. У 2022 році країни G7 ухвалили «Принципи кіберстійкості харчових і сільськогосподарських систем», що

закликають уряди розробляти галузеві стратегії кіберзахисту та налагоджувати обмін даними про інциденти між операторами критичної агропродовольчої інфраструктури [7]. Україна, як ключовий глобальний постачальник зерна, олії та іншої продукції, має особливі підстави для активної участі в таких ініціативах і імплементації міжнародних стандартів захисту.

З точки зору нормативно-правового регулювання, Закон України «Про основні засади забезпечення кібербезпеки України» (2017) та Стратегія кібербезпеки на 2021–2025 роки визначають загальну архітектуру захисту критичної інфраструктури. Утім, агропродовольчий сектор не виокремлений у самостійний захищений сегмент, тоді як енергетика, банківська система та телекомунікації мають окремі профільні вимоги до кіберзахисту. Це нормативне відставання потребує усунення шляхом доповнення переліку об'єктів критичної інфраструктури великими зерновими терміналами, елеваторами, переробними комплексами та системами державного аграрного моніторингу.

Для підвищення кіберстійкості агропродовольчої інфраструктури пропонується реалізація системи взаємопов'язаних заходів. На інституційному рівні доцільно створити Галузевий центр реагування на кіберінциденти в АПК (AgriCERT) за аналогією з фінансовим CERT-UA, який здійснював би координацію, збір і аналіз даних про загрози в режимі реального часу. На технічному рівні необхідно впровадити обов'язкову сегментацію мереж АСУ ТП від корпоративних та зовнішніх мереж, а також запровадити регулярне незалежне тестування на проникнення (*penetration testing*) для підприємств, що входять до переліку об'єктів критичної інфраструктури. На освітньому рівні слід інтегрувати модулі з кібергігієни та інформаційної безпеки в програми підвищення кваліфікації для агроменеджерів і технологів.

Таким чином, кібербезпека агропродовольчих інформаційних систем є невід'ємним виміром національної безпеки України. Реальні атаки на аграрну інфраструктуру, як вітчизняні, так і зарубіжні, переконливо свідчать: цифровий захист продовольчих ланцюгів є таким самим пріоритетом, як і фізичний захист виробничих об'єктів. Ефективна протидія кіберзагрозам у цій сфері потребує консолідованих зусиль держави, бізнесу, наукової спільноти та міжнародних партнерів, а також оновлення нормативної бази з урахуванням реалій гібридної війни.

Список використаних джерел

1. ESET Research. Industroyer2: Industroyer reloaded. 2022. URL: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (дата звернення: 05.04.2026).

2. U.S. Cybersecurity and Infrastructure Security Agency (CISA). Alert AA21-287A: Ransomware Activity Targeting the Food and Agriculture Sector. 2021. URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a (дата звернення: 07.04.2026).

3. Recorded Future. BlackMatter Ransomware Targets NEW Cooperative. 2021. URL: https://www.recordedfuture.com/ (дата звернення: 07.04.2025).

4. Живило М. О., Петренко С. А. Кіберзагрози для АСУ ТП аграрних підприємств. *Інформаційна безпека*. 2023. № 3. С. 22–30.

5. Держгеокадастр України. Звіт про спроби несанкціонованого доступу до Державного земельного кадастру у 2024 році. URL: https://land.gov.ua/ (дата звернення: 10.04.2026).
6. Українська аграрна асоціація. Дослідження стану кібербезпеки в АПК України. Київ, 2023. 34 с.
7. G7 Agriculture Ministers. Principles of Cyber Resilience for Food and Agriculture Systems. 2022. URL: https://www.g7germany.de/ (дата звернення: 09.04.2026).

Abstract: The problems of cybersecurity of agri-food information systems in the context of the growing digitalization of the agricultural sector and the aggravation of geopolitical conflicts are investigated. The main cyber threats to the agro-industrial complex are considered, in particular attacks on production management systems, food stock databases and logistics platforms. The relationship between the security of agricultural information systems and the level of food security of the state is analyzed. The need to form a comprehensive strategy for cyber protection of agri-food infrastructure as a component of the national security of Ukraine is substantiated.
Keywords: cybersecurity, agri-food information systems, national security, cyber threats, food security, critical infrastructure.

УДК 631.4:355.424:338.43 DOI 10.31521/978-617-7149-94-0-146

HUMAN ORGANIZATIONAL PERFORMANCE ЯК ОСНОВА СТІЙКОСТІ ГРОМАД У СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Іваненко В.С., головний спеціаліст відділу планування та координації дій у надзвичайних ситуаціях
Управління з питань надзвичайних ситуацій та цивільного захисту населення Миколаївської міської ради
Курепін В.М., канд. екон. наук, доцент
Миколаївський національний аграрний університет
https://orcid.org/0000-0003-0006-4090

Анотація: Концепція Human Organizational Performance розглядається як основа підвищення стійкості громад у системі національної безпеки. Акцентовано роль людського чинника, організаційної культури та взаємодії у формуванні здатності громад ефективно реагувати на загрози, адаптуватися до змін та забезпечувати стабільний розвиток.
Ключові слова: Human Organizational Performance, людський фактор, стійкість громад, національна безпека, організаційна ефективність, культура безпеки, управління ризиками.

Ключовим елементом системи національної безпеки в умовах нестабільності та військових загроз є стійкість громад. Це виклики особливого значення. Саме місцеві громади першими реагують на загрози, зберігаючи соціальну стабільність та підтримуючи життєдіяльність населення.

Ефективність реагування на кризові ситуації багато в чому залежить від людського фактору. У цьому контексті визначальним є рівень підготовки, свідомість, відповідальність та взаємодія людей [1, с. 42]. Забезпечити безпеку