візуалізацію результатів розпізнавання. Подальше навчання й тестування моделей дадуть змогу оцінити якість роботи системи та визначити можливості її практичного застосування.

Загалом розроблення такої програмної системи є перспективним напрямом автоматизації моніторингу сільськогосподарських угідь. Її практичне використання може спростити аналіз відеоданих, прискорити виявлення заданих об’єктів і створити основу для подальшого розвитку інтелектуальних систем моніторингу територій.

Список використаних джерел

1. Redmon J., Divvala S., Girshick R., Farhadi A. You only look once: unified, real-time object detection. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). 2016. P. 779–788. DOI: https://doi.org/10.1109/CVPR.2016.91.

2. Liu W. et al. SSD: single shot multibox detector. Computer Vision – ECCV 2016. Lecture Notes in Computer Science. Vol. 9905. Cham : Springer, 2016. P. 21–37. DOI: https://doi.org/10.1007/978-3-319-46448-0_2.

3. Ren S., He K., Girshick R., Sun J. Faster R-CNN: towards real-time object detection with region proposal networks. Advances in Neural Information Processing Systems. 2015. Vol. 28. P. 91–99.

4. Kamilaris A., Prenafeta-Boldú F. X. Deep learning in agriculture: a survey. Computers and Electronics in Agriculture. 2018. Vol. 147. P. 70–90. DOI: https://doi.org/10.1016/j.compag.2018.02.016.

5. Zhu P., Wen L., Du D., Bian X., Fan H., Hu Q., Ling H. Detection and tracking meet drones challenge. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2022. Vol. 44, No. 11. P. 7380–7399. DOI: https://doi.org/10.1109/TPAMI.2021.3119563.

УДК 519.21:004.032.26

ЗАСТОСУВАННЯ МЕТОДІВ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ ОЦІНКИ ТА ПІДТРИМКИ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ ЗЕРНОВИХ СХОВИЩ В СУЧАСНИХ УМОВАХ

[1]Віктор Передерій, [2]Євген Борчик

[1]Національний університет кораблебудування ім. адм. Макарова

[2]Миколаївський національний аграрний університет

Миколаїв, Україна

Зернові сховища насьогодні дедалі частіше відносять до об'єктів критичної інфраструктури, тому побудова зрілої системи функціональної стійкості - це питання не лише збереження прибутків бізнесу, а й стабільності всього продовольчого сектору держави.

В період воєнного стану кібер та інформаційна безпека зернових хранилищ (елеваторів) перетворилася з суто корпоративного IT-питання на стратегічний елемент національної та глобальної продовольчої безпеки. Оскільки агросектор є критично важливою галуззю економіки України, сучасні зерносховища стали об'єктами підвищеного інтересу для кібератак і технічного шпигунства з боку ворога [1].

Вимоги до кібер та інформаційної безпеки зернових сховищ (елеваторів) регулюються міжнародним стандартом IEC 62443 (безпека промислової автоматизації), в Україні регулюються законодавством про критичну інфраструктуру (аграрний сектор та продовольство), зокрема Постановою КМУ № 518 (в оновленій редакції № 1470). Оскільки сучасні агропідприємства критично залежать від автоматизованих систем керування технологічними процесами (АСУ ТП/SCADA), систем обліку зерна та логістичних баз даних. В умовах війни ці системи стають пріоритетними цілями для російських хакерів, які намагаються дезорганізувати експорт та знищити інфраструктуру.

Основними загрозами та векторами атак на зернові сховища є:

· програми-вимагачі (Ransomware) - шифрування баз даних обліку або серверів керування елеватором;

· спотворення даних - зміна хакерами даних про якість зерна у системі обліку з метою викрадення продукції чи фінансових махінацій;

· атаки на системи моніторингу (IoT) - фальсифікація даних у програмному забезпеченні;

· DDoS-атаки на логістичні сервіси - блокування доступу до клієнтських кабінетів,

Функціональна стійкість (functional Resilience) - це здатність систем елеватора продовжувати функціонувати або швидко відновлюватися після інцидентів [2, 3.]

Оцінка та підтримка функціональної стійкості зернових сховищ (елеваторів) є критично важливою, оскільки сучасні агропідприємства відносяться до об'єктів критичної інфраструктури (сектор продовольства). Цифровізація елеваторів (АСУ ТП, датчики вологості, автоматизовані системи зважування та обліку зерна) робить їх вразливими до кібератак, які можуть призвести до псування зерна, зупинки логістики або фінансових збитків. [4]

Основними задачами функціональної стійкості (Resilience) є:

· резервування каналів зв'язку - наявність альтернативних і дублюючих каналів інтернет-зв'язку для безперебійного передавання звітів та моніторингу.

· автономність при блекаутах - забезпечення серверних кімнат та диспетчерських пунктів джерелами безперебійного живлення (ДБЖ/UPS) та промисловими генераторами для запобігання втрати даних та збоїв ПЗ при різкому вимкненні світла.

· захист конфіденційних даних - обмеження доступу та шифрування комерційної інформації про обсяги зберігання зерна, логістичні маршрути, укладені контракти та реєстри власників зернових партій.

На сьогодні тема функціональної стійкості елеваторів і в зерносховищах перебуває на стику захисту критичної інфраструктури (ICS/SCADA), інтернету речей (IoT) та продовольчої безпеки. Дослідження за цим напрямом частіше публікуються у міжнародних виданнях, оскільки цифровізація агросектору (Smart Farming) там розпочалася раніше, проте українські вчені також активно вивчають це питання в контексті воєнних загроз та захисту підприємств АПК.

Міжнародні дослідження з кібербезпеки зерносховищ та продовольчих ланцюгів в основному зосереджені на дослідженні вразливостей централізованих систем автоматизованого керування елеваторами, аналізує загрози кібертероризму та пропонують заходи для підвищення стійкості інфраструктури зберігання зерна [5-9].

Українські наукові праці у сфері кіберзахисту АПК в основному фокусується на побудові комплексного кіберзахисту критичної інфраструктури зберігання зерна в умовах воєнного стану [10-12].

Для побудови надійної системи захисту пропонується підхід до оцінювання та підтримки функціональної стійкості зерносховищ (елеваторів) в реальному часі який базується на методах інтелектуальної та інформаційно – когнітивної технології.

У відповідності до нормативних документів та результатів досліджень основними факторами і вразливостями які мають найбільш значний вплив на функціональну стійкість інформаційної інфраструктури зерносховищ є:

1. Фактори інформаційної безпеки: DC - узгодженість даних; AD - доступність даних; DP - конфіденційність даних, DI - цілісність даних.

2. Фактори кібербезпеки: EI - зовнішній вплив; SF- шкідливе програмне забезпечення (Wipers / Ransomware); DS – захищеність даних; ILC – захищеність каналів витоку інформації.

3. Фактори емоційно-когнітивного стану користувачів: (ET) - емоційна напруга, (F) - фізична та емоційна втома, (PR) – продуктивність, (PI) - сприйняття інформації, (RT) - час реакції, (DT) - час прийняття рішень, (C) – концентрація уваги.

До основних типів вразливостей відносяться:

1. Фізичні вразливості $PV = f_1(Pa, Ae, Cd)$: недостатній захист від віддаленої фізичної атаки (Pa); недостатній контроль доступу до обладнання (Ae); несанкціоноване копіювання даних (Cd).

2. Вразливості програмного забезпечення $SV = f_2(Vd, Ve, Aa)$: нразливості валідації введених даних (Vd); нразливості в шифруванні (Ve); нразливості автентифікації та авторизації (Aa).

3. Вразливості технічного захисту інфраструктури $Pt = f_3(Pa, Rc, Cd)$: недостатній захист від віддаленої фізичної атаки (Pa); недостатній контроль віддаленого доступу до обладнання (Rc); несанкціоноване копіювання даних (Cd).

4. Вразливості мережевих засобів $NV = f_4(Np, Ns, Nd)$: використання незахищених мережевих протоколів (Np); недостатня сегментація мережі (Ns); вразливості мережевих пристроїв (Nd.)

Для оцінки та визначення оперативного стану функціональної стійкості інформаційної інфраструктури зерносховища від впливу зазначених факторів розроблена інформаційно-логічна модель представлена на рис. 1.

Особливістю нечітких факторів є неможливість їх безпосереднього виміру і запису в числовому виді. Для цього існують різні тести для оцінки, однак вони вимагають затрат часу і можуть представляти результат з деякою мірою невизначеності. Для рішення вказаних проблемних питань, та кількісної оцінки оперативного стану комплексної безпеки заданого об'єкту критичної інфраструктури ставиться завдання застосування ймовірнісного математичного апарату з використанням Байєсовської мережі довіри (БМД), теорії нечітких множин та інформаційно-когнітивних технологій. На стан комплексної безпеки заданого об'єкту критичної інфраструктури найбільш значний вплив мають фактори інформаційної та кібербезпеки, фактори вразливості та стан людського фактору.

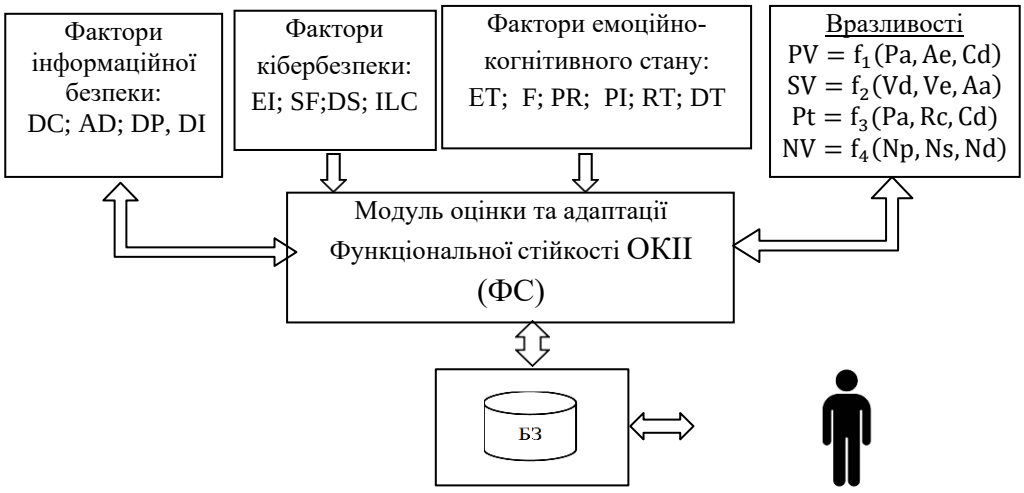


Рис. 1 - Інформаційно-логічна модель оцінки та корекції оперативного стану функціональної стійкості.

На сьогоднішній день однією з найбільш відповідних моделей, призначених для роботи з неповною, неточною і суперечливою інформацією, є БМД, яка заснована на ймовірнісному підході і здатна у максимальному ступені використовувати інформацію, що надходить з виділених джерел для досягнення максимального ефекту.

Баєсові мережі - це графові моделі імовірнісних і прич[illegible]о-наслідкових зв'язків між змінними в статистичному інформаційному моделюванні. У Баєсових мережах, можуть органічно поєднуватися емпіричні частоти, появи різних значень змінних, суб'єктивні оцінки «очікувань» і теоретичні уявлення про математичні ймовірності тих чи інших наслідків з апріорної інформації. Це являється важливою практичною перевагою і відрізняє Баєсові мережі від інших методик інформаційного моделювання.

У відповідності до інформаційно – логічної схеми (рис.1) визначається ступінь впливу зазначених нечітких факторів на заданий об'єкт критичної інфраструктури. Отримані результати представляються у вигляді ймовірностей можливих станів, отриманих методом експертних оцінок.

Для визначення відповідності стану зазначених нечітких факторів комплексної безпеки до категорії критичності ОКІ необхідно створити систему прогнозування значень ймовірностей, в основу якої покладено нечіткий логічний вивод за алгоритмом Мамдані з нечіткою Бази знань, в якій значення вхідних та вихідної змінної задаються експертами нечіткими множинами [13]. Після чого

необхідно побудувати та дослідити БМД оцінки стану функціональної стійкості заданого об’єкту у відповідності до категорії критичності, спрощена структура якої наведена на рисунку 2.

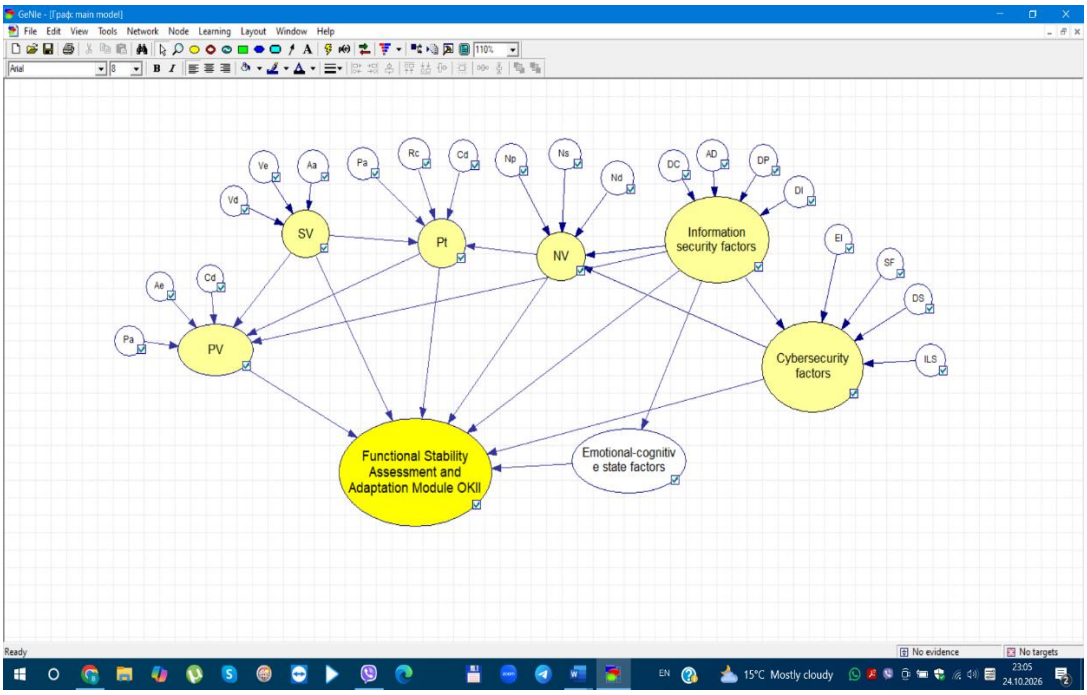


Рис. 2 - БМД оцінки стану функціональної стійкості заданого об’єкту.

Висновки. Для побудови надійної системи захисту запропоновано підхід до оцінювання та підтримки функціональної стійкості зерносховищ (елеваторів) в сучасних умовах який базується на методах інтелектуальної та інформаційно – когнітивної технології.

Визначені основні пріоритетні напрями наукових досліджень у напрямку розробки і впровадженню інформаційних технологій оцінки та підтримки стійкості зерносховищ. Для визначення комплексу показників що впливають на функціональну стійкість та безпеку критичного об’єкту розроблено інформаційно-логічну модель. Побудовано нечітку Байєсовську мережу довіри за допомогою якої на підставі знань експертів, проводиться комплексна оцінка та адаптація ймовірності станів функціональної стійкості зернових сховищ (елеваторів).

Список використаних джерел

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 17.08.2022 р № 2163-VIII. Відомості Верховної Ради. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 25.12.2023 р.)

2. Cyber defence. (30 Jul. 2024). NATO.

3.Perederyi V, Borchik E, Zosimov V and Bulgakova O (2026) Functional stability assessment and adaptation for critical infrastructure facilities. Front. Artif. Intell. 9:1777258. doi: 10.3389/frai.2026.1777258

Link: https://www.nato.int/cps/uk/natohq/topics_78170.htm?selectedLocale=en

4. Суходоля О. (2023). Стійкість критичної інфраструктури ЄС: посилення політики та координації. НІСД, 9 с.

Link: https://niss.gov.ua/sites/default/files/2023-02/az_eu-cip-coordinated_24022023.pdf

5. Jones, R., & Feoktistov, D. (2025). Cybersecurity vulnerabilities in the food supply chain and their impact on food security: A systematic literature review. Global Smart Food Systems, 1(1), 1-27. https://doi.org/10.1108/GSFS-10-2024-0001

6. Jian, Y.; Zhang, Q.; Ge, L.; Jiang, Y. Technical methods of national security supervision: Grain storage security as an example. J. Saf. Sci. Resil. 2023, 41, 61–74. [Google Scholar] [CrossRef] [Scilit]

7. Tushar, S.R.; Alam, M.F.B.; Zaman, S.M.; Garza-Reyes, J.A.; Bari, A.B.M.M.; Karmaker, C.L. Analysis of the factors influencing the stability of stored grains: Implications for agricultural sustainability and food security. Sustain. Oper. Comput. 2023, 4, 40–52. [Google Scholar] [CrossRef] [Scilit]

8. Éverton, L.; Paulo, C.C. Applications of new technologies for monitoring and predicting grains quality stored: Sensors, Internet of Things, and Artificial Intelligence. Measurement 2022, 188, 110609. [Google Scholar] [CrossRef] [Scilit]

9. Said, P.; Pradhan, R. Food grain storage practices: A review. J. Grain Process. Stor. 2014, 11, 1–5. [Google Scholar]

10. Мордовцев, О., Аванесова, Н., & Любушин, Р. (2022). Формування системи інформаційної безпеки у сфері зберігання та розподілу продовольчих та енергетичних ресурсів. Аспекти публічного управління, 10(3), 21–30. https://doi.org/10.15421/152216.

11. Романашенко М. О., Романашенко І. О., Поливана Л. А. Важливість захисту інформації сільськогосподарських підприємств. Вісник студентського наукового товариства. 2021. Вип. 1. С. 13-16.

12. Урсол, О., & Гальчинський, Л. (2022). ОЦІНЮВАННЯ РИЗИКУ КІБЕРЗАГРОЗ ПІДПРИЄМСТВА З МЕТОЮ ВИЗНАЧЕННЯ НЕОБХІДНИХ ВИТРАТ ДЛЯ ПЕВНОГО РІВНЯ КІБРЕЗБЕЗПЕКИ. Collection of Scientific Papers «SCIENTIA», (June 10, 2022; Sydney, Australia), 57–63. Retrieved from https://previous.scientia.report/index.php/archive/article/view/240

13. Perederyi V, Borchik E, Zosimov V and Bulgakova O (2026) Functional stability assessment and adaptation for critical infrastructure facilities. Front. Artif. Intell. 9:1777258. doi: 10.3389/frai.2026.1777258.