КОМПЛЕКСНИЙ КІБЕРЗАХИСТ ПРОГРАМНИХ СИСТЕМ ЦИВІЛЬНОГО ЗАХИСТУ

[1]Венгрин Василина Василівна, студентка
[2]Маслова Наталія Олександрівна, к.т.н., доц.
[3]Балацька Валерія Сергіївна, д-р філ. (PhD)
Львівський державний університет безпеки життєдіяльності
[1]vengryn@ldubgd.edu.ua, [2]masgpp2@gmail.com, [3]v.balatska@ldubgd.edu.ua

Цифровізація систем цивільного захисту та ДСНС супроводжується активним впровадженням автоматизованих програмних систем управління, моніторингу та реагування на надзвичайні ситуації. Такі системи забезпечують координацію підрозділів, диспетчеризацію викликів, оброблення геопросторових даних та інтеграцію з державними інформаційними ресурсами. Водночас інтеграційна взаємодія через API та телекомунікаційні канали збільшує поверхню атаки та підвищує ризики кіберінцидентів.

Метою роботи є аналіз особливостей кіберзахисту програмних систем цивільного захисту та обґрунтування комплексного підходу до підвищення їх кіберстійкості на основі мережевого моніторингу, централізованого аналізу подій безпеки та контролю цілісності програмного забезпечення.

Програмні системи цивільного захисту доцільно розглядати як розподілені кіберфізичні комплекси, у яких взаємодіють інформаційні, телекомунікаційні та сенсорні підсистеми. Порушення функціонування хоча б одного компонента може призвести до каскадного ефекту та зниження ефективності реагування під час надзвичайних ситуацій. Особливо критичними є порушення функціонування диспетчерських та комунікаційних сервісів у режимі реального часу. На відміну від класичних моделей ІБ, для систем цивільного захисту ключовим критерієм є доступність, тому оцінювання кіберзахищеності має враховувати безперервність функціонування, мережевий моніторинг та захист програмних компонентів.

Аналіз сучасних кіберзагроз дозволяє виділити найбільш критичні типи атак: DDoS-атаки на сервери диспетчеризації, ransomware-атаки, компрометацію облікових записів, атаки на API та web-інтерфейси, а також атаки типу supply-chain на програмні компоненти. У зв'язку з цим актуальним є впровадження ризик-орієнтованого комплексного підходу до кіберзахисту, який поєднує мережевий моніторинг, централізований аналіз подій безпеки та контроль цілісності службового програмного забезпечення й критичних програмних компонентів.

Особливістю програмних систем цивільного захисту є необхідність функціонування в умовах підвищених навантажень, пошкодження телекомунікаційної інфраструктури та обмеженого часу реагування. У зв'язку з цим кіберзахист таких систем повинен забезпечувати не лише виявлення атак, але й підтримку безперервності функціонування критичних сервісів у режимі реального часу.

Важливим елементом кіберзахисту є також контроль цілісності програмного забезпечення автоматизованих систем управління, серверних

компонентів та диспетчерських сервісів. Несанкціонована модифікація службових програмних модулів може призвести до порушення процесів координації підрозділів, втрати оперативної інформації та зниження ефективності реагування на надзвичайні ситуації.

Для забезпечення мережевого захисту можуть використовуватися системи Snort та Suricata, що реалізують функції IDS/IPS і дозволяють виявляти атаки у режимі реального часу. Інструмент Zeek забезпечує глибокий аналіз мережевих подій та накопичення журналів безпеки, а Wireshark застосовується для детального дослідження мережевого трафіку та діагностики аномалій. Основні інструменти, що можуть застосовуватися для забезпечення кіберзахисту програмних систем цивільного захисту, наведено у табл. 1.

Таблиця 1 – Інструменти кіберзахисту програмних систем цивільного захисту

Інструмент	Основне призначення	Рівень застосування
Snort	Виявлення та блокування мережевих атак	Мережевий
Suricata	IDS/IPS та аналіз мережевого трафіку	Мережевий
Zeek	Аналіз мережевих подій та журналювання	NSM/SOC
Wireshark	Аналіз пакетів та діагностика	Локальний
Security Onion	Централізований моніторинг SOC	Комплексний
Wazuh / Sysmon	Контроль цілісності та процесів	Хостовий
YARA / Ghidra	Аналіз та виявлення шкідливого ПЗ	Аналіз ПЗ

Важливим напрямом є також захист програмного забезпечення автоматизованих систем управління та серверних компонентів. Для цього можуть використовуватися засоби контролю цілісності, моніторингу процесів і первинного аналізу програмного забезпечення: Wazuh, Sysmon, YARA, Process Monitor та Ghidra. Їх застосування дозволяє здійснювати контроль хеш-значень, аналіз поведінки процесів, перевірку цифрових підписів та виявлення модифікованих програмних компонентів. Запропонований підхід поєднує механізми network security та application security у межах єдиної моделі кіберстійкості систем цивільного захисту. Запропонований підхід орієнтований на підвищення стійкості критичних сервісів ДСНС в умовах кіберінцидентів та порушення телекомунікаційної інфраструктури.

У роботі використано ризик-орієнтований підхід до оцінювання кіберзахищеності програмних систем цивільного захисту на основі інтегрального показника:

$$K = w_1A + w_2I + w_3C + w_4R + w_5T,$$

де w_i – вагові коефіцієнти, які обираються залежно від критичності системи; а базовими критеріями оцінювання моделі обрано: A – рівень доступності; I – рівень цілісності; C – рівень конфіденційності; R – стійкість до відмов; T – оперативність реагування.

Для систем диспетчеризації доцільним є встановлення співвідношення: $w_1 > w_2 > w_3$, що відображає пріоритет доступності над конфіденційністю.

Рівень ризику визначається як:

$$Risk = P \times Imp,$$

де P – ймовірність реалізації загрози; Imp – величина наслідків.

Результати демонстраційного оцінювання показали, що впровадження сегментації мереж, багатофакторної аутентифікації та централізованого моніторингу дозволяє зменшити рівень ризику з 0,62 до 0,38, тобто на 38,7 % (рис.1).

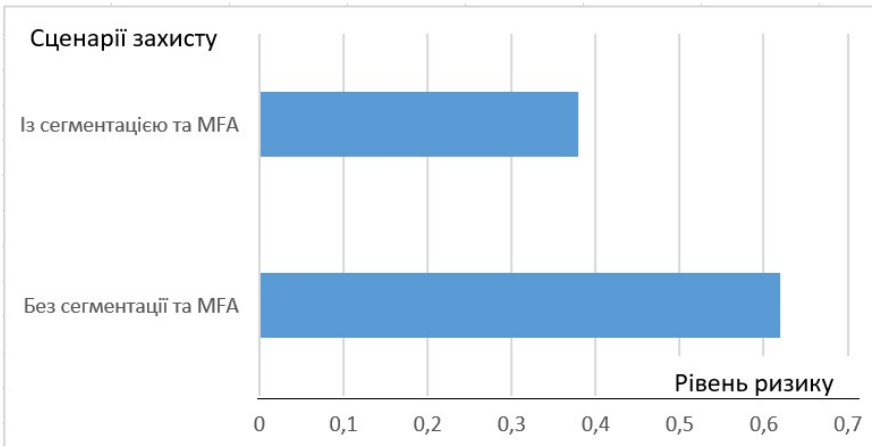

Рисунок 1 – Вплив механізмів захисту на рівень ризику

Отримані результати свідчать про ефективність комплексного поєднання IDS/IPS, SIEM/SOC та засобів захисту програмного забезпечення для підвищення кіберстійкості систем цивільного захисту.

Запропонований підхід може бути використаний для оцінювання рівня захищеності програмних систем ДСНС, ранжування об'єктів критичної інфраструктури та обґрунтування пріоритетів модернізації механізмів кіберзахисту об'єктів критичної інформаційної інфраструктури цивільного захисту та підвищення їх кіберстійкості.

ЛІТЕРАТУРА

1. ISO 22320:2018. Security and resilience – Emergency management – Guidelines for incident management. Geneva : International Organization for Standardization, 2018.

2. Інтеграція баз даних вразливостей у СУІБ – шлях до підвищення кіберстійкості критичних систем / В. І. Ящук та ін. *Resilient Systems: Secure Digital Technologies and Critical Infrastructure* : Proceedings of the 1st International Scientific and Practical Conference. 2025. С. 60–65. DOI: 10.32447/20784643.31.2025.13.

3. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). Gaithersburg : National Institute of Standards and Technology, 2007. 127 p.

4. Bejtlich R. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. San Francisco : No Starch Press, 2013. 376 p.

5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : International Organization for Standardization, 2022.