УДК 004.056

В. О. Демченко
Л. О. Майданевич

ПОРІВНЯЛЬНИЙ АНАЛІЗ МОДЕЛЕЙ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ В УКРАЇНІ ТА ЄС

Вінницький національний технічний університет

Анотація

В досліджені проаналізовано важливість чіткого планування та розподілу ролей у процесі реагування на кіберінциденти. Основну увагу присвячено ознайомленню ієрархії взаємодії між суб'єктами кіберзахисту, що дозволяє уникнути безладу та неузгодженість в кризових ситуаціях. В роботі детально розглянути та порівняно два документи: Постанову КМУ №1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози» та Директиву Європейського парламенту і ради (ЄС) 2022/2555 (NIS2).

Ключові слова: кібербезпека, кіберзахист, об'єкти критичної інфраструктури, реагування на інциденти, кіберінциденти, NIS2, суб'єкти.

Abstract

This study analyses the importance of clear planning and the allocation of roles in the process of responding to cyber incidents. The main focus is on outlining the hierarchy of interaction between cyber defence entities, which helps to avoid chaos and a lack of coordination in crisis situations. The paper examines and compares two documents in detail: Resolution No. 1533 of the Cabinet of Ministers of Ukraine 'Certain Issues Concerning the Response to Cyber Incidents, Cyber Attacks and Cyber Threats' and Directive 2022/2555 of the European Parliament and of the Council (EU) (NIS2).

Key words: cybersecurity, cyber defence, critical infrastructure, incident response, cyber incidents, NIS2, entities.

Вступ

У сучасних реаліях кіберпростір перетворився на повноцінне місце, де відбуваються різного типу протистояння. Для України питання кібербезпеки набуває особливої уваги, ніж для будь-якої країни Європи. За даними звіту Microsoft Digital Defense Report 2025 Україна увійшла до п'яти країн світу та трійки країн Європи за кількістю спрямованих на неї кібератак [1]. Дані позиції підтверджуються статистикою, оскільки у порівнянні з періодом до повномасштабного вторгнення цифрова агресія зросла в рази. Так, зокрема у 2021 році було зафіксовано 1400 кібератак [2], а за підрахунками фахівців CERT-UA за 2025 рік виявлено майже 6000 кібератак на державну та критичну інфраструктуру [3]. Атаки на Київстар [4] та Укрзалізницю [5], які відбулися 12 грудня 2023 та 23 березня 2025 відповідно, довели, що успішний захист систем залежить не лише від технологій, а від швидкості та ефективності координації суб'єктів реагування на ці інциденти.

Результати дослідження

Протидія сучасним кіберзагрозам неможлива без чіткої нормативно-правової бази, яка визначатиме ієрархію та обов'язки кожного учасника процесу. Тому, оскільки в сучасних умовах швидкість реакції є ключовим фактором виживання об'єктів критичної інфраструктури, то органи влади розробили чіткий національний план реагування на кіберінциденти, кібератаки та кіберзагрози, який закріплений у Постанові КМУ №1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози» [6]. Цей документ представляє собою єдиний стандарт для усіх без винятку об'єктів критичної інфраструктури в Україні. Він дозволяє уникнути хаосу та ситуацій, коли різні сектори діють неузгоджено чи ігнорують загрози в надії на їх самоусунення.

Національний план реагування на кіберінциденти, кібератаки та кіберзагрози визначає чітку послідовність етапів реагування, яка передбачає повне усунення загрози: від підготовки та виявлення до стримування, усунення наслідків та аналізу ефективності встановлених заходів.

Ефективність виконання цих етапів забезпечується чітким розподілом ролей між суб'єктами реагування. На локальному рівні основна роль належить власникам та їхнім підрозділам кіберзахисту, які власними силами реагують на інциденти у своїх внутрішніх системах і мають створювати внутрішні команди реагування (CSIRT). На наступному рівні знаходяться галузеві та регіональні команди CSIRT, які координують захист у межах конкретних секторів та за потреби залучають приватних експертів. Найвищим (державним) рівнем є CERT-UA, які забезпечують технічну підтримку та допомогу за відсутності галузевих/регіональних команд та СБУ, що відповідають за реагування у сфері державної безпеки.

Взаємодія між цими суб'єктами здійснюється через сувору ієрархію інформування. У разі виявлення кіберінциденту на об'єкті критичної інфраструктури, власник структури повинен протягом однієї години повідомити про це свій галузевий чи регіональний CSIRT, а у разі їх відсутності напряму – CERT-UA та СБУ. Надалі ці установи аналізують кібератаки, забезпечують координацію дії та передають інформації до Національного координаційного центру. Для оцінки небезпеки використовується шкала критичності: від рівня 0 (білий – некритичний) до рівня 5 (чорний – надзвичайний). Важливою особливістю є право на екстрене втручання, який стається, якщо рівень критичності загрози високий (рівень 3-5), то державні команди мають право починати порятунок системи самостійно, не чекаючи офіційних паперів та узгоджень.

На європейському рівні ключовим документом, який передбачає план дій та розподіл ролей є Директива Європейського парламенту і ради (ЄС) 2022/2555 (NIS2) [7]. Вона визначає стандарти стійкості для всього ЄС, фокусуючись на гармонізації дій різних країн. NIS2, на відмінну від українського плану, класифікує організації за секторами та типами суб'єктів – основні та важливі.

Дана модель забезпечує ефективну багаторівневу ієрархію управління та звітування. На початковому рівні керівні органи суб'єктів несуть персональну відповідальність за затвердження заходів із управління ризиками та контролюють їх виконання. У випадку, якщо виявляють інцидент суб'єкт повинен звітувати перед національною командою реагування (CSIRT) або компетентним органом. При чому CSIRT не лише приймає та опрацьовує звіти, а зобов'язаний надати відповідь на технічні поради суб'єкту протягом 24 годин. Якщо стається масштабний інцидент, який має вплив на інші країни ЄС, то CSIRT, компетентний орган чи єдиний контактний пункт передає цю інформацію державам-членам, ENISA та EU-CyCLONe.

NIS2 передбачає систему звітування, яка містить три етапи. Першим кроком є надання попередження про інцидент протягом 24 годин після виявлення, що дозволяє відповідним органам оцінити загрозу поширення атаки. Другий етап передбачає повного повідомлення про інцидент протягом 72 годин, зо містить у собі детальна оцінка масштабу та наслідків. Останній етап надання фінального звіту протягом 1 місяця, який містить аналіз причини інциденту та вжиті заходи для запобігання повторної ситуації. Також NIS2 передбачає систему нагляду та суворі санкції у разі не виконання суб'єктами та організацією пунктів цього документу.

Висновки

Проведений аналіз Постанови КМУ №1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози» та Директиви Європейського парламенту і ради (ЄС) 2022/2555 демонструє, що дані документи є критично важливими для побудови ефективних систем реагування на кіберінциденти та вирішує проблему усунення хаосу та неузгодженості у діях різних установ під час кризових ситуацій. Кожен з них пропонує свій унікальний інструментарій, адаптований до конкретних викликів безпекового середовища.

Постанова №1533 фокусується на оперативності та технічному реагуванні. Вона забезпечує найшвидшу локалізацію загроз через жорстку ієрархію інформування та право держави на екстрене втручання, що є важливим для захисту інфраструктури в умовах війни.

Директива ЄС NIS2 зосереджується на стратегічній стійкості та відповідальності. Цей підхід спонукає суб'єктів самостійно дбати про безпеку через систему контролю, персональної

відповідальності, регулярні перевірки та суворих фінансових санкцій, ці аспекти формують довготривалу культуру захисту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Україна посіла третє місце в Європі та п'яте у світі серед країн, що найчастіше зазнають кібератак – Microsoft – Forbes.ua. *Forbes.ua*. URL: https://forbes.ua/news/ukraina-potrapila-do-pyatirki-krain-za-kiberatakami-u-sviti-microsoft-17102025-33427 (дата звернення: 17.04.2026).
2. Кількість кібератак на рік на критичну інфраструктуру України зросла з 800 до 4500: СБУ назвала організаторів. *Мінфін - все про фінанси: новини, курси валют, банки*. URL: https://minfin.com.ua/ua/2024/05/07/126427603/ (дата звернення: 17.04.2026).
3. Сахно А. Україна опрацювала 6000 кібератак за рік і стала глобальним хабом кібербезпеки – Delo.ua. *Останні новини України та світу онлайн – delo.ua*. URL: https://delo.ua/news/ukrayina-opracyuvala-6000-kiberatak-za-rik-i-stala-globalnim-xabom-kiberbezpeki-460666/ (дата звернення: 17.04.2026).
4. Koval O. Якою була атака хакерів на «Київстар» та як відновлювалась компанія. *Dou*. 19.03.2024. URL: https://dou.ua/lenta/news/kyivstar-cyber-attack-restoration/ (дата звернення: 17.04.2026).
5. Ukrinform. Кібератака на Укрзалізницю: у Держспецзв'язку кажуть, що були використані тактики спецслужб РФ. *Укрінформ - актуальні новини України та світу*. URL: https://www.ukrinform.ua/rubric-society/3977123-kiberataka-na-ukrzaliznicu-u-derzspeczvazku-kazut-so-buli-vikoristani-taktiki-specsluzb-rf.html (дата звернення: 17.04.2026).
6. Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози : Постанова Каб. Міністрів України від 26.11.2025 № 1533. URL: https://zakon.rada.gov.ua/laws/show/1533-2025-п#Text (дата звернення: 17.04.2026).
7. Директива Європейського Парламенту і Ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2). Офіційний вісник Європейського Союзу від 27.12.2022 року, /L333/, стор. 80. URL: https://zakon.rada.gov.ua/laws/card/9a3_001-22 (дата звернення: 17.04.2026).

Демченко Вероніка Олександрівна – студентка групи 1БКС-23Б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: vdemchenkoo.ol@gmail.com

Майданевич Леонід Олександрович – канд. філос. наук, доцент кафедри захисту інформації факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, адвокат (Рада адвокатів Вінницької області), м. Вінниця, email: lmaidanevych@gmail.com

Demchenko Veronika – student of group 1BKS-23b, Faculty of Information Technologies of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: vdemchenkoo.ol@gmail.com

Maidanevych Leonid – PhD in Philosophical Sciences, Associated Professor, Department of Information Security, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Lawyer, Vinnytsia Bar Council, Vinnytsia, e-mail: lmaidanevych@gmail.com