УДК 004.056:621.391

Свиридов Григорій Ігорович,

студент магістратури;
Харківський національний університет радіоелектроніки, Харків, Україна

Заболотний Володимир Ілліч,

Професор кафедри безпеки інформаційних технологій, к.т.н., доцент;
Харківський національний університет радіоелектроніки, Харків, Україна

ГАРМОНІЗАЦІЯ ЗАХОДІВ КОМПЛЕКСІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ТА ЗАХИСТУ ВІД ТЕХНІЧНИХ РОЗВІДОК З РИЗИКО-ОРІЄНТОВАНИМИ ПІДХОДАМИ КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

Анотація. Досліджено проблему необхідності об’єднання заходів комплексу технічного захисту інформації, заходів захисту від технічних розвідок та новітньої ризико-орієнтованої моделі кібербезпеки, що впроваджується в Україні. Показано, що

в умовах воєнного стану статичне застосування комплексу технічного захисту інформації не забезпечує своєчасного реагування на динамічні загрози від технічних розвідок та загрози кібератак, а ризико-орієнтований підхід поки що залишається слабко інтегрованим із традиційними заходами технічного захисту інформації та захисту від технічних розвідок. Запропоновано підхід до гармонізації, що поєднує інженерно-технічні заходи комплексу технічного захисту інформації та заходи захисту від технічних розвідок із безперервним циклом оцінювання ризиків кібербезпеки. Показано на доцільність адаптації нормативно-методичного забезпечення до умов воєнного часу.

Abstract. This study examines the need to integrate the services of the technical information protection system, measures to protect against technical reconnaissance, and the latest risk-based cybersecurity model currently being implemented in Ukraine. It has been demonstrated that, under martial law, the static application of the technical information protection system does not ensure a timely response to dynamic threats from technical reconnaissance and cyber-attacks, whilst the risk-based approach remains poorly integrated with traditional measures of technical information protection and protection against technical reconnaissance. An approach to harmonisation is proposed, combining the engineering and technical measures of the technical information protection system and measures to protect against technical intelligence with a continuous cycle of cybersecurity risk assessment. The paper demonstrates the advisability of adapting regulatory and methodological frameworks to wartime conditions.

Ключові слова: воєнний стан, гармонізація, залишковий ризик, заходи захисту від технічних розвідок, канали витоку інформації, кібербезпека, комплекси технічного захисту інформації, легендування, моніторинг ефективності заходів, об’єкт інформаційної діяльності, оцінювання ризиків, План кіберзахисту, профілі безпеки, ризико-орієнтований підхід.

Вступ. Сучасний стан кібербезпеки України визначається безпрецедентним рівнем загроз, зумовленим повномасштабною збройною агресією. Аналітичні огляди засвідчують зростання кількості та складності кібератак на державні й критично важливі об’єкти [1]. Ці атаки тісно поєднуються з активним веденням технічних розвідок (ТР) з боку противника. Водночас вітчизняна система захисту інформації потребує перегляду класичних детермінованих моделей і перебуває на етапі трансформації. Традиційні комплекси технічного захисту інформації (КТЗІ) та заходи захисту від технічних розвідок (ЗвТР), регламентовані Законом України «Про захист інформації в інформаційно-комунікаційних системах» [2], орієнтовані на статичний периметр та фіксовані нормативні вимоги. Проте загрози воєнного часу (фізичне руйнування інфраструктури, міграція

сервісів у хмарні середовища, застосування противником засобів радіоелектронної розвідки) потребують впровадження динамічних систем управління безпекою. Наказ Держспецзв'язку № 402 [3] затвердив Методику оцінювання ризиків кібербезпеки, закріпивши перехід до ризико-орієнтованого підходу.

Проблема полягає в тому, що заходи КТЗІ та ЗвТР, які традиційно базуються на нормативно-технічних вимогах і моделі порушника, функціонують відносно автономно від новітніх процесів управління ризиками кібербезпеки [4]. Вітчизняний ризико-орієнтований підхід, що передбачає безперервний цикл ідентифікації, оцінювання та обробки ризиків кібербезпеки [3; 5], поки що не став органічною складовою планування інженерно-технічних заходів. В умовах воєнного стану ця роз'єднаність створює розриви в захисті, особливо на об'єктах критичної інфраструктури, де фізичні та кіберзагрози тісно переплітаються [1; 4].

Актуальним науково-практичним завданням є гармонізація інженерно-технічних заходів КТЗІ/ЗвТР із новими кібербезпековими підходами для оптимізації ресурсів об'єктів інформаційної діяльності. *Основна ідея дослідження* полягає в урахуванні параметрів інженерно-технічного захисту КТЗІ/ЗвТР під час оцінювання ризиків кібербезпеки. *Метою дослідження* є розробка пропозицій щодо гармонізації інженерно-технічних заходів КТЗІ та ЗвТР із ризико-орієнтованими підходами до забезпечення кібербезпеки для підвищення стійкості систем захисту інформації в умовах воєнного стану.

Основна частина роботи. Аналіз нормативно-методичної бази та наукових публікацій засвідчує, що традиційна модель захисту інформаційно-телекомунікаційної системи (ІТКС) виявилася надто статичною та нормативно орієнтованою [2; 4]. Її процедури проєктування, сертифікації та атестації часто не відповідають темпам розвитку цифрових

сервісів і динаміці кіберзагроз воєнного часу [1]. Ризико-орієнтований підхід, навпаки, передбачає відхід від суто атестаційної логіки до постійного циклу оцінки ризиків кібербезпеки, моніторингу кіберзагроз та вдосконалення контрзаходів [3; 5]. Однак заходи КТЗІ та ЗвТР – інженерний захист приміщень, виявлення та блокування технічних каналів витоку інформації, ЗвТР об'єктів критичної інфраструктури – залишаються переважно поза межами цього циклу, реалізуючись як відносно сталий комплекс організаційно-технічних рішень [5].

Водночас воєнний стан суттєво змінює профіль кіберзагроз. Зростає технічна складність кібератак, спостерігається конвергенція квантових технологій та штучного інтелекту, що створює нові виклики для кіберзахисту [1; 6]. За таких умов розрив між статичними заходами КТЗІ/ЗвТР і динамічним ризико-орієнтованим підходом стає критичним: система технічного захисту може відповідати формальним вимогам, але не враховувати актуальні вектори кібератак, зокрема ті, що поєднують кібернетичні та фізичні впливи [4; 5].

Такий підхід до гармонізації базується на трьох взаємопов'язаних принципах.

1) Інтеграція моделі кіберзагроз і порушника КТЗІ/ЗвТР у процес оцінювання ризиків кібербезпеки: модель порушника та модель кіберзагроз, які традиційно розробляються для потреб технічного захисту, мають стати вхідними даними для ризико-орієнтованого аналізу, а не існувати паралельно з ним [3; 5]. Це дозволяє враховувати специфічні технічні канали витоку та фізичні способи несанкціонованого доступу в загальній матриці ризиків кібербезпеки.

2) Включення заходів КТЗІ та ЗвТР до профілів безпеки та Плану кіберзахисту: відповідно до вітчизняного підходу, що впроваджується на заміну комплексної системи захисту інформації, заходи з кіберзахисту мають формуватися на основі профілів безпеки та включатися до Плану

кіберзахисту [3; 4]. Доцільно, щоб цей План містив не лише програмно-апаратні та організаційні кіберзаходи, а й інженерно-технічні рішення КТЗІ/ЗвТР. Це забезпечить цілісність захисту та унеможливить ситуацію, коли заходи технічного захисту залишаються поза межами ризико-орієнтованого управління.

3) Запровадження безперервного моніторингу ефективності заходів КТЗІ/ЗвТР у циклі управління ризиками кібербезпеки: оцінювання залишкового ризику після впровадження інженерно-технічних заходів має проводитися регулярно, а не лише під час атестації [3; 5]. Це особливо важливо в умовах воєнного стану, коли фізична інфраструктура зазнає руйнувань, а склад і інтенсивність кіберзагроз змінюються швидше, ніж традиційні процедури переатестації [1; 4].

В практиці захисту, також згадується необхідність легендування об’єктів і робіт. З цього витікає включення до загальної концепції захисту відповідних заходів.

Практична реалізація запропонованої гармонізації потребує відповідного методичного інструментарію. Зокрема, доцільним є використання інтегральних показників захищеності, які поєднують криптографічні, організаційні, технічні та експлуатаційні параметри [5; 6]. Для умов воєнного часу такими параметрами, окрім традиційних, мають стати стійкість до фізичних впливів, швидкість відновлення після кіберінцидентів та адаптивність до змін моделі кіберзагроз [1; 4].

Висновки. Проведене дослідження дозволяє дійти висновку, що гармонізація заходів КТЗІ та ЗвТР із ризико-орієнтованими підходами до забезпечення кібербезпеки є необхідною умовою підвищення ефективності систем захисту інформації в умовах воєнного стану. Запропоновано підхід до гармонізації, що передбачає інтеграцію моделі кіберзагроз і порушника заходів КТЗІ/ЗвТР у процес оцінювання ризиків кібербезпеки, включення

інженерно-технічних заходів до профілів безпеки та Плану кіберзахисту, а також запровадження безперервного моніторингу залишкового ризику [3; 4; 5]. Практична значущість отриманих результатів полягає у можливості їх використання під час формування Планів кіберзахисту органами державної влади та на об’єктах критичної інфраструктури [1; 4]. Подальші дослідження доцільно спрямувати на розроблення методики кількісного оцінювання внеску заходів КТЗІ/ЗвТР у зниження ризиків кібербезпеки та на адаптацію інтегральних показників захищеності до умов воєнного часу [5; 6].

Список використаних джерел

1. Кібер-дайджест МОЗ України: аналітика кіберзагроз, алгоритми захисту та актуальні вимоги державних регуляторів (ДССЗІ, НКЦК, CERT-UA). 2026. URL: https://www.nuozu.edu.ua/zagruzka3/CyberDigest_07_04_26N.pdf (дата звернення: 14.10.2026).
2. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР, поточна редакція від 20.04.2025. URL: https://zakon.rada.gov.ua (дата звернення: 10.10.2026).
3. Про затвердження Методики оцінювання ризиків кібербезпеки : Наказ Держспецзв’язку від 02.06.2026 № 402. Зареєстровано в Міністерстві юстиції України 18.06.2026 р. за № 880/46274. URL: https://zakon.rada.gov.ua/ (дата звернення: 13.09.2026).
4. Ризик-орієнтоване управління безпекою в державних інформаційних системах: перехід від КСЗІ до адаптивної архітектури. Cybersecurity: Education, Science, Technique. 2025. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/download/975/805/3199 (дата звернення: 14.10.2026).
5. Рубан І.В., Тютюник В.В., Заболотний В.І., Тютюник О.О. Оцінка вразливості об’єктів кіберзахисту на основі ризико-орієнтованого підходу. *Безпека інформації*. 2020. Том 26, № 3. С. 145–155. DOI: http://dx.doi.org/10.18372/2225-5036.26.14947 (дата звернення: 24.09.2026).
6. Мельник Р.П., Мельник О.Г. Методика оцінки криптостійкості та захищеності інформаційно-комунікаційних систем в умовах сучасних кіберзагроз. Технічні науки. 2025. URL: https://tech.vernadskyjournals.in.ua/journals/2025/6_2025/part_2/33.pdf.