ПРОБЛЕМИ Й ПЕРСПЕКТИВИ ОПТИМАЛЬНОГО ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Голубєв С.О., Пасько Р.Д.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна
E-mail: serhii.holubiev@nure.ua
ruslan.pasko@nure.ua

Abstract

The problems of protecting critical information infrastructure in Ukraine, its regulatory and legal framework, and threats that endanger the smooth operation of infrastructure objects are considered.

Гарантування й підтримання інформаційної безпеки України — одна з ключових функцій держави й важлива складова національної безпеки, від якої значно залежить рівень захищеності державного суверенітету й територіальної цілісності. З огляду на те, що кіберпростір має унікальні можливості для перебудови сучасного світового порядку, не тільки технологічно розвинені держави й союзи здатні впливати на глобальний розвиток, економіку й соціально-політичний устрій, але й невеликі держави спроможні суттєво змінювати світобудову. Це змушує їх залучати значні ресурси для розроблення методів протидії кібернетичним розвідкам, проведенню атак і саботажів на об'єктах критичної інформаційної інфраструктури, а також шукати інноваційні шляхи й методи використання кіберпростору у веденні сучасної інформаційної війни.

В умовах повномасштабної війни ризики для інфраструктури суттєво зростають, адже рівень її захищеності безпосередньо впливає на безпеку держави й стабільність її функціонування. Діяльність державних органів у сфері забезпечення інформаційної безпеки зосереджена на двох напрямах: по-перше, на підтримці сталого розвитку інформаційного простору України з метою досягнення такого рівня його стійкості, який дозволяє ефективно протидіяти зовнішнім і внутрішнім загрозам; по-друге, на створенні й забезпеченні функціонування системи захисту інформаційного простору від потенційних ризиків. Ці напрями діяльності визначені указом Президента «Про рішення Ради національної безпеки і оборони України від 15.10.2021 року «Про Стратегію інформаційної безпеки»» [4].

Україна стала першою державою з часів проведення операції «Олімпійські ігри», яка вимушено вступила в повноцінну кібервійну проти потужного й розвиненого противника, і зіткнулася з викликами, які не мали аналогів у світовій історії: правовими, технічними, людськими.

По-перше, нормативно-правова база все ще відстає від темпів розвитку й упровадження інформаційних технологій, а тому держава не своєчасно реагує на нові типи загроз у кіберпросторі. Наприклад, атакам на енергетичні компанії «Укренерго» у 2015 році було надано чіткий правовий опис лише після ухвалення Закону України «Про критичну інфраструктуру» (1882-IX від 16.11.2021), який набув чинності 15.12.2021 [3]. Ситуація поступово почала змінюватися лише під час повномасштабної війни. У 2025 році було прийнято Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» [2], що визначив засади створення національної системи реагування на кіберінциденти, удосконалив механізми обміну інформацією про кіберзагрози й передбачив запровадження штатних посад фахівців із кібербезпеки в органах державної влади й на об'єктах критичної інформаційної інфраструктури. Крім того, постановою Кабінету Міністрів України від 28 березня 2025 року № 447 «Про внесення змін щодо кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури» [1] було

впроваджено низку обов'язкових запобіжних заходів: управління ризиками, постійний моніторинг і аудит інформаційної безпеки, розроблення планів реагування на кібератаки та вдосконалення системи кіберзахисту на рівні державних установ.

Стає цілком очевидним, що для оперативного й ефективного реагування на подібні проблеми критично необхідно не лише оновлювати законодавство, а й розробити гнучку систему його подальшого вдосконалення з залученням фахівців у сфері кібербезпеки.

По-друге, із початком повномасштабної українсько-російської війни наша держава змушена відповідати на новий виклик — виявилося, що кількість фахівців з кібербезпеки в державних органах та силових відомствах недостатня для ефективної протидії різнорівневим і частим загрозам. Це спричинило набір до спеціальних служб цивільних фахівців, що дало лише тимчасовий позитивний ефект, адже специфіка роботи фахівців із кібербезпеки потребує значно ширших компетентностей, ніж дозволяє цивільна вища освіта. На новоприбулих працівників покладалося багато завдань, які мають колегіально розв'язувати такі служби як Держспецзв'язку, Служба безпеки України й Головне управління розвідки, а не цивільні співробітники з браком теоретичних знань і практичного досвіду. Для розв'язання цієї проблеми доцільно розширити набір абітурієнтів до вищих державних закладів силових відомств, а також оновити й оптимізувати освітні програми цих закладів відповідно до сучасних викликів у сфері кібербезпеки.

Висновки

Гарантування й підтримання інформаційної безпеки є однією з ключових функцій держави й неодмінна складова національної безпеки України. В умовах гібридної та повномасштабної війни значно зростає рівень ризиків для об'єктів критичної інформаційної інфраструктури, що вимагає підтримки сталого розвитку інформаційного простору України з метою досягнення такого рівня, який міг би протидіяти зовнішнім і внутрішнім загрозам. Важливим завданням є створення та вдосконалення системи захисту інформаційного простору, а також підвищення рівня теоретичної та практичної підготовки фахівців у сфері кібербезпеки й захисту інформації.

Література

1. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27 берез. 2025 р. № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text (дата звернення: 10.11.2025).

2. Про внесення змін щодо кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури до деяких постанов Кабінету Міністрів України : Постанова Кабінету Міністрів України від 28 берез. 2025 р. № 447. URL: https://zakon.rada.gov.ua/laws/show/447-2025-п#Text (дата звернення: 08.11.2025).

3. Про критичну інфраструктуру : Закон України від 16 листоп. 2021 р. № 1882-IX : станом на 21 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 10.11.2025).

4. Про Стратегію інформаційної безпеки : Рішення Ради нац. безпеки і оборони України від 15 жовт. 2021 р. : станом на 30 груд. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/n0080525-21#Text (дата звернення: 11.11.2025).