Дорохіна Ю.А.

Таврійський національний університет ім. В.І. Вернадського, професор кафедри кримінально-правових дисциплін Навчально-наукового гуманітарного інституту, д.ю.н., доцент

Dorokhina Yu.A.

Taurian National University V.I. Vernadsky, Professor of the Department of Criminal-Legal Disciplines of Educational and scientific humanitarian institute, D.Sc., associate professor

РОЗВИТОК СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

Гарантування безпеки та стійкості національної критичної інфраструктури є приорітетним напрямом безпекової політики України, оскільки критична інфраструктура забезпечує життєвоважливі для населення, суспільства та держави опції, без яких неможливо безпечне існування та забезпечення належного рівня національної безпеки.

Критична інформаційна інфраструктура розглядається як основний компонент у критичній інфраструктурі багатьох держав, що знаходить відображення у відповідних підходах до визначення цього поняття. Головні причини критичності інформаційної складової інфраструктури випливають зі стрімкого поширення інформаційних технологій у всіх сферах нашого життя та, відповідно, до зросту уразливостей і потенційних загроз різного характеру. Очевидно, що за таких умов забезпечення безпеки кібертехнологій у критичних інфраструктурах (інфраструктурах державного управління, фінансового, банківського, транспортного, енергетичного, ресурсного, комунального та продуктового забезпечення) сучасного суспільства стає одним з головних питань.

Попри очевидну необхідність у розвитку системи захисту критичної інформаційної інфраструктури, доцільно вказати, що низка первинних (першочергових) питань до сьогодні стоять на порядку денному. До таких питань доцільно віднести й проблему відсутності поняття «критична інформаційна інфраструктура» у законодавстві як України, так і багатьох держав. Проте така ситуація пояснюється тим, що інформаційна складова входить до обсягу поняття інфраструктури взагалі (тобто критичної інфраструктури) і не виокремлюється як певна ланка. Перевагою концеп-

туального підходу, основаного на понятті – «критична інфраструктура», є можливість системного вирішення питання захисту критично важливих для життєдіяльності держави, безпеки її громадян та довкілля систем і об'єктів та створення можливостей для більш ефективного управління ризиками на глобальному, регіональному та національному рівнях.

На сучасному етапі розвиток системи захисту критичної інформаційної інфраструктури на національному рівні забезпечується поступовими кроками Уряду нашої держави щодо розробки оптимальної державної системи захисту критичної інфраструктури України. Так, Уряд прийняв Концепцію створення державної системи захисту критичної інфраструктури нашої держави (далі – Концепція), яка була розроблена Мінекономрозвитку разом з Національним інститутом стратегічних досліджень та Службою безпеки України. Нагадаємо, що 6 грудня 2017 р. розпорядженням № 1009-р Кабінет Міністрів України згадану Концепцію було схвалено.

Концепція є основою для створення державної системи захисту об'єктів критичної інфраструктури, порушення роботи яких може завдати шкоди національним інтересам України. У ній наведено визначення усіх ключових понять та запропоновано механізм взаємодії державних органів. В Уряді переконані, що створення такої системи захисту дозволить забезпечити стійкість до загроз усіх видів. Тобто Концепція закладає якісно новий рівень державного управління у цій сфері та передбачає сучасні підходи до управління безпековими ризиками, оптимізоване використання наявних ресурсів, гнучкість та швидкість реагування на інциденти та кризи.

До об'єктів критичної інфраструктури віднесено підприємства та установи, які є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв. Термін «критична інфраструктура» вживається у такому значенні – об'єкти, системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності населення, суспільства, соціально-економічного розвитку, обороноздатності держави та забезпечення національної безпеки.

Наступним кроком у створенні системи захисту критичної інфраструктури (у тому ж числі інформаціної) є розробка та розгляд законопроекту «Про критичну інфраструктуру та її захист», який має визначити

держоргани, відповідальні за забезпечення здійснення заходів відносно пріоритетних секторів критичної інфраструктури, у тому числі сектору телекомунікації і зв'язку.

Важливим також є активізація міжнародного співробітництва у сфері захисту критичної інфраструктури, на що поряд із посиленням спроможності національних урядів забезпечувати захист критичної інфраструктури, звертає увагу резолюція Ради безпеки ООН щодо захисту критичної інфраструктури від терористичних атак № 2341 від 13 лютого 2017 р..

Вбачається, що в сучасних умовах на перший план щодо розбудови якісної системи захисту критичної інформаційної інфраструктури для нашої держави виходить забезпечення безпеки в інформаційній сфері, тобто кібербезпеки. У зв'язку з цим 5 жовтня 2017 р. Верховна Рада України ухвалила Закон «Про основні засади забезпечення кібербезпеки України», який вступить у силу через шість місяців з дня його опублікування. Згаданий Закон є новаторським документом, оскільки закріплює на законодавчому рівні багато важливих визначень: кіберзагроза, кібершпіонаж, кіберзлочинність, кібератака, а також визначає необхідність впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки і кіберзахисту.

Законом передбачено, що до об'єктів критичної інфраструктури можуть бути віднесені підприємства й установи, які: ведуть діяльність і надають послуги в галузях хімічної промисловості, енергетики, транспорту, ІКТ, банківському та фінансовому секторі, електронних комунікацій; надають послуги у сфері життєзабезпечення населення; є комунальними, аварійними і рятувальними службами; включені до переліку підприємств, що мають стратегічне значення для економіки.

Цей нормативно-правовий акт відкриває нові можливості для впорядкування ситуації в інформаційній сфері. Незважаючи на тривалі дискусії і побоювання певних експертів щодо можливості появи надмірного контролю від держави в кіберсфері, цей Закон дає змогу в перспективі перевести розвиток вітчизняного інформаційного простору на якісно новий рівень [1].

Завдання захисту критичної інфраструктури зміщують фокус уваги на попередження кризових ситуацій, пов'язаних із її функціонуванням. У зв'язку з цим слід підкреслити, що до існуючих систем протидії абсолютно правильно додано й нову систему боротьби із кіберзагрозами, яка формується на виконання Стратегії кібербезпеки України. Таким чином, саме попередження кризових ситуацій має стати ключовою складовою у побудові системи заходів щодо протидії кіберзагрозами, оскільки у

сучасному суспільстві практично всі інфраструктури, які забезпечують його життєдіяльність, використовують інформаційні технології (кібертехнології), які в свою чергу відіграють критичну роль практично в будь-якій інфраструктурі.

Доцільно відмітити, що захист критичної інформаційної інфраструктури − це не просто оновлення термінів в чинному законодавстві, це впровадження нового підходу. Основними його складниками є створення безпекового партнерства між всіма зацікавленими сторонами, організація комплексної оцінки загроз такої інфраструктурі та їх впливу на рівень національної безпеки в окремих її складових, створення механізму моніторингу та попередження кризових ситуацій, що пов'язані із функціонуванням кіберпростору.

1. *Рудь І. Закон про кібербезпеку: основні положення, оцінки експертів та розвиток вітчизняного інформаційного простору [Електронний ресурс] / І. Рудь // Україна: події, факти, коментарі. – 2017. – № 19. – С. 42–48. – Режим доступу: http://nbuviap.gov.ua/images/ukraine/2017/ukr19.pdf.*

Дорохіна Ю.А. Розвиток системи захисту критичної інформаційної інфраструктури в Україні

Гарантування безпеки та стійкості національної критичної інфраструктури є приорітетним напрямом безпекової політики України, оскільки критична інфраструктура забезпечує життєвоважливі для населення, суспільства та держави опції, без яких неможливо безпечне існування та забезпечення належного рівня національної безпеки.

Критична інформаційна інфраструктура розглядається як основний компонент у критичній інфраструктурі багатьох держав, що знаходить відображення у відповідних підходах до визначення цього поняття. Головні причини критичності інформаційної складової інфраструктури випливають зі стрімкого поширення інформаційних технологій у всіх сферах нашого життя та, відповідно, до зросту уразливостей і потенційних загроз різного характеру.

Захист критичної інформаційної інфраструктури − це не просто оновлення термінів в чинному законодавстві, це впровадження нового підходу. Основними його складниками є створення безпекового партнерства між всіма зацікавленими сторонами, організація комплексної оцінки загроз такої інфраструктурі та їх впливу на рівень національної безпеки в окремих її складових, створення механізму моніторингу та попередження кризових ситуацій, що пов'язані із функціонуванням кіберпростору.

Ключові слова: критична інфраструктура, система захисту критичної інфраструктури

Dorokhina Y.A. Development of critical informational infrastructure protection system in Ukraine

The guarantee of the security and stability of the national critical infrastructure is a priority direction of the security policy of Ukraine, since critical infrastructure provides vital options for the population, the society and the state, without which it is impossible to secure the existence and ensure an adequate level of national security.

Critical information infrastructure is considered as the main component of the critical infrastructure of many countries, which is reflected in the relevant approaches to defining this concept. The main reasons for the criticality of the information component of the infrastructure stem from the rapid spread of information technology in all spheres of our lives and, accordingly, the growth of vulnerabilities and potential threats of various nature.

Protecting critical information infrastructure is not just an update of the terms in the current legislation, it is the introduction of a new approach. Its main components are the creation of a security partnership between all stakeholders, the organization of a comprehensive assessment of the threats to such infrastructure and their impact on the level of national security in its separate components, the creation of a mechanism for monitoring and preventing crises associated with the functioning of cyberspace.

Key words: critical infrastructure, critical infrastructure protection system