Державна наукова установа
«Інститут інформації, безпеки і права
Національної академії правових наук України»

Олександр ДОВГАНЬ
Тарас ТКАЧУК

КІБЕРРИЗИКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ВІД АНАЛІЗУ ЗАГРОЗ ДО ВПРОВАДЖЕННЯ РІШЕНЬ

Науково-практичний посібник

Київ-Одеса
Фенікс
2024

УДК 005.308+335/339
Д 27

Рекомендовано до друку вченою радою Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України» (протокол № 11 від 10 грудня 2024 р.)

Рецензенти:

О. А. Заярний – доктор юридичних наук, професор, професор кафедри інтелектуальної власності та інформаційного права Навчально-наукового інституту права Київського національного університету ім. Тараса Шевченка;

І. М. Доронін – доктор юридичних наук, доцент, керівник наукової лабораторії Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук».

Довгань О. Д., Ткачук Т. Ю.

Д 27 Кіберризики критичної інфраструктури: від аналізу загроз до впровадження рішень : наук.-практ. посіб. / О. Д. Довгань, Т. Ю. Ткачук. – Київ; Одеса : Фенікс, 2024. – 77 с.

ISBN 978-617-8430-50-4

Науково-практичний посібник присвячений комплексному висвітленню проблем кібербезпеки у сфері критичної інфраструктури. Розглядаються ключові аспекти аналізу кіберзагроз, механізми ідентифікації ризиків та ефективні підходи до їх нейтралізації. Посібник поєднує теоретичний аналіз із практичними рекомендаціями для організацій, що відповідають за функціонування критичних систем, зокрема в умовах підвищеного рівня кіберзагроз, зумовлених гібридними викликами сучасності.

Особливу увагу приділено адаптації міжнародного досвіду до національних реалій України, включаючи розроблення стратегій реагування, управління ризиками та впровадження інноваційних технологій. Видання орієнтовано на фахівців у галузі кібербезпеки, операторів критичної інфраструктури, науковців, представників державних органів, підрозділів сил безпеки й оборони, діяльність яких пов'язана із кіберзахистом критичної інфраструктури.

Посібник також буде корисним для студентів, слухачів, аспірантів і докторантів для поглиблення знань з кібербезпеки та інформаційно-аналітичної діяльності.

УДК 005.308+335/339

ISBN 978-617-8430-50-4

ЗМІСТ

ВСТУП

Критична інфраструктура є основою функціонування сучасного суспільства. Вона включає транспортні системи, енергетику, фінанси, зв'язок, охорону здоров'я та інші сфери, чия стабільна робота є ключовою для економічної та національної безпеки держави. Сучасні об'єкти критичної інфраструктури дедалі більше інтегруються у цифрове середовище, що підвищує їхню ефективність, але водночас робить вразливими до кіберзагроз. Ще у 2001 році експерти МКЧХ застерігали, що хакерські дії проти промисловості чи інфраструктури можуть призвести до тяжких наслідків для людей, якщо вивести з ладу критичні системи. У 2021 році держави на рівні ООН підтвердили, що кібероперації можуть серйозно вплинути на цивільну інфраструктуру і спричинити "спустошливі гуманітарні наслідки". На жаль, повномасштабне російське вторгнення в Україну вже на практиці продемонструвало реальність цих загроз: український кіберпростір став полем бою і голова Держспецзв'язку охарактеризував цю війну як "***першу у світі повномасштабну кібервійну".***

Європейський Союз, визнаючи зростаючу важливість кібербезпеки для захисту КІ, створив комплексну нормативну, організаційну та технічну базу для протидії кіберзагрозам. Успішний досвід ЄС у цьому напрямі може стати орієнтиром для України, особливо в умовах війни з рф, коли критична інфраструктура країни систематично стає об'єктом кібератак, спрямованих на дестабілізацію економіки та суспільного життя.

Критична інфраструктура охоплює основні об'єкти та системи, що забезпечують функціонування економіки, безпеки та здоров'я нації. До таких об'єктів належать енергетичні мережі, водопостачання, ядерні ресурси, авіація, а також системи харчування та сільського господарства. Порушення або знищення цих інфраструктур може мати серйозні наслідки для національної безпеки, економічної стабільності та громадського здоров'я.

Безпека життєво важливих системних мереж і ресурсів, від яких залежить функціонування економіки та суспільства, є ключовою складовою поняття кібербезпеки критичної інфраструктури. Захист таких інфра-

структур від кібератак є не лише обов'язковою умовою їх стійкого функціонування, але й потребує впровадження високоякісних, системних політик і заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів.

Захист критичної інфраструктури (ЗКІ) передбачає впровадження заходів та практик, спрямованих на забезпечення безперервної роботи цих систем та захист від потенційних загроз, таких як кібератаки, природні катастрофи та терористичні акти. Це включає використання систем управління та збору даних (SCADA) та промислових систем управління (ICS), які є ключовими для функціонування секторів, як-от енергетика, транспорт та сільське господарство. Однак захист критичної інфраструктури (КІ) в умовах цифрової трансформації стає дедалі складнішим завданням. Глобалізація, розвиток технологій і зростання взаємозв'язків між системами породжують нові ризики. Кібератаки на критичну інфраструктуру можуть не лише завдати економічних збитків, але й спричинити соціальні потрясіння, а також загрожувати життю громадян. У зв'язку з цим захист таких об'єктів стає стратегічним пріоритетом для урядів, бізнесу та міжнародних організацій.

Важливість ЗКІ полягає в наступному:

1. Забезпечення доступу до основних послуг: захист КІ гарантує надання таких послуг, як питна вода, електроенергія та харчові продукти, безперебійне постачання яких є критично важливим для громадського здоров'я та безпеки.

2. Захист ключових галузей: сектори, як-от хімічна промисловість, комунікації, екстрені служби, охорона здоров'я, інформаційні технології та транспорт, є життєво важливими для економіки. Успішна кібератака на ці галузі може мати руйнівні наслідки для пыдприэмств та організацій і становити значну загрозу для глобальної економіки та суспільства.

3. Пом'якшення різноманітних загроз: КІ вразлива до широкого спектру загроз, включаючи кібератаки, природні катастрофи та технічні збої. Виявлення та зменшення цих ризиків є необхідним для забезпечення цілісності та надійності цих систем.

4. Економічна безпека: стабільність національної та глобальної економіки залежить від надійної роботи КІ. Перебої можуть призвести до значних економічних втрат та довгострокових наслідків для економічної стабільності.

5. Співпраця: ефективний захист КІ вимагає тісної співпраці між державними установами та комерційними організаціями. Це сприяє впровадженню та управлінню ефективними заходами захисту та забезпечує комплексний підхід до безпеки.

6. Національна безпека: багато об'єктів КІ є невід'ємною частиною національної безпеки. Захист цих активів від фізичних та кіберзагроз є необхідним для підтримання національної оборони та громадської безпеки.

7. Стійкість до змін клімату: з огляду на зростання частоти та інтенсивності природних катастроф через зміну клімату, захист КІ від екстремальних погодних явищ стає все більш важливим для забезпечення безперервності та стійкості.

Дане дослідження присвячене комплексному аналізу кіберризиків для об'єктів критичної інфраструктури – від виявлення і аналізу сучасних кіберзагроз до впровадження рішень для їх нейтралізації. Особливу увагу приділено досвіду російсько-української війни як прикладу масштабного використання кібероперацій проти КІ та питанням відповідності таких дій нормам міжнародного гуманітарного права.

Структура роботи охоплює загальні питання кіберзахисту критичної інфраструктури (Розділ 1), типові кіберзагрози для таких об'єктів та конкретні кейси атак (Розділ 2), правові аспекти кібероперацій у контексті міжнародного гуманітарного права (Розділ 3), досвід ЄС у сфері кіберзахисту КІ та його значення для України (Розділ 4), а також визначає пріоритетні напрями стратегії захисту національної критичної інфраструктури (Розділ 5). Завершують дослідження висновки та рекомендації.