Ярослав ДОРОГИЙ
Доктор технічних наук, доцент, професор кафедри прикладної математики та інформатики
Донецький національний технічний університет, кафедра ПМІ, Дрогобич, Україна
ORCID: 0000-0003-3848-9852
cisco.rna@gmail.com

Цуркан Василь
Кандидат технічних наук, доцент, доцент спеціальної кафедри №5
Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського, Київ, Україна
ORCID: 0000-0003-1352-042X
v.v.tsurkan@gmail.com

КІБЕРБЕЗПЕКА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІД ЧАС ВІЙСЬКОВОЇ ЗАГРОЗИ

Анотація. Критична інфраструктура є основою стабільності будь-якої держави, оскільки вона забезпечує життєво важливі функції суспільства, зокрема енергетичні, водопостачальні, транспортні та інформаційні системи. В умовах сучасних кіберзагроз та військових конфліктів, таких як агресія росії проти України, кібербезпека критичної інфраструктури набуває особливої важливості. Кібератаки можуть не тільки порушити роботу інфраструктури, але й призвести до серйозних економічних, соціальних та гуманітарних наслідків. У статті розглядаються основні види кіберзагроз, зокрема DDoS-атаки, шкідливі програми та віруси, атаки на енергетичну інфраструктуру, фінансові кібератаки, а також цілеспрямовані атаки на військові об'єкти та інформацію. Зокрема, в Україні під час військового конфлікту значно зросла кількість атак, що впливають на державні органи, фінансові установи та енергетичні системи. Прикладом таких атак є відомий вірус "NotPetya", який призвів до значних пошкоджень інформаційних систем та фізичних об'єктів інфраструктури. Захист критичної інфраструктури вимагає комплексного підходу, включаючи розробку національної стратегії кібербезпеки, інтеграцію кіберзахисту в загальну стратегію національної безпеки, створення систем моніторингу та оперативного реагування на кіберзагрози, а також впровадження резервних систем та планів відновлення після атак. Важливим елементом є також підготовка фахівців у сфері кібербезпеки, зокрема через спеціалізовані програми навчання та сертифікації. В умовах постійних кіберзагроз Україна розробляє та впроваджує різноманітні нормативно-правові акти для покращення захисту критичної інфраструктури. Створення ефективної системи кібербезпеки є одним з основних пріоритетів для забезпечення національної безпеки та стабільності держави в умовах сучасної війни.

Ключові слова: кібербезпека, критична інфраструктура, кіберзагрози, військова агресія, захист інформаційних систем.

1. ВСТУП

Критична інфраструктура є основою стабільності держави, охоплюючи енергетику, транспорт, водопостачання, фінансові установи та зв'язок. Від її роботи залежить національна безпека та життєдіяльність громадян. Зі зростанням цифровізації ці об'єкти стають вразливими до кіберзагроз, що можуть призвести до серйозних економічних і соціальних наслідків, особливо під час військових загроз, коли кібератаки можуть бути частиною гібридних стратегій агресора.

Забезпечення кібербезпеки критичної інфраструктури є надзвичайно актуальним, особливо в умовах війни, коли збройний конфлікт супроводжується кібератаками. Держави повинні мати стратегії захисту критичних об'єктів, що включають технічні та організаційні заходи для забезпечення фізичної та інформаційної безпеки. Враховуючи численні кібератаки на українські енергетичні, фінансові та комунікаційні системи, що спричинили серйозні наслідки, проблема кіберзахисту стає особливо важливою. Останні

дослідження підтверджують вразливість цих об'єктів у військовому конфлікті та підкреслюють необхідність вдосконалення стратегій захисту.

Метою публікації є аналіз сучасних кіберзагроз для критичної інфраструктури України та розробка рекомендацій щодо вдосконалення заходів кіберзахисту.

2. РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

Види кіберзагроз під час військової агресії. В умовах військової агресії проти України, кіберзагрози набувають особливого значення, оскільки вони можуть бути використані для паралізації державних і комерційних структур, а також для втручання в особисту діяльність громадян. Важливо зазначити, що з 2014 року Україна стикається з серйозними кіберзагрозами з боку державних та недержавних акторів, і більшість цих атак здійснюються під час або на фоні військового конфлікту.

Класичні кібератаки. DDoS-атаки та шкідливі програми є серйозними загрозами для критичної інфраструктури України. У 2017 році потужні DDoS-атаки вплинули на роботу урядових установ, фінансових структур та енергетичних компаній, порушивши функціонування портальних систем та електронних послуг. Для захисту критичних об'єктів від таких атак важливо розвивати механізми безпеки, включаючи інтеграцію з міжнародними мережами захисту. Окрім цього, шкідливі програми, такі як вірус "NotPetya", стали однією з найбільш руйнівних атак на українську інфраструктуру, зупинивши підприємства, знищивши дані та порушивши роботу фінансових і логістичних систем. Такі атаки доводять, що кіберзагрози можуть не лише порушити інформаційні системи, а й мати руйнівний вплив на фізичні об'єкти критичної інфраструктури.

Атаки на енергетичну інфраструктуру. Враховуючи залежність України від енергетичної інфраструктури, саме ця сфера є однією з найбільш уразливих. Українська енергетична система вже неодноразово ставала мішенню для кібератак, які спричиняли відключення електрики в регіонах, що підвищує ризик виникнення гуманітарних катастроф. Окрім цього, атаку на енергетичні об’єкти може бути використано для порушення життєдіяльності держави на стратегічному рівні — зокрема для зупинки роботи підприємств оборонної промисловості чи транспорту.

Фінансові кібератаки. Фінансовий сектор є важливим елементом для стабільності держави, і атаки на фінансові системи України можуть призвести до дестабілізації економічної ситуації. Враховуючи військові дії та присутність агресора в кіберпросторі, українські банки та платіжні системи стали частими об’єктами для кібератак. Атаки на платіжні системи або банківські платформи, а також спроби маніпулювати транзакціями є серйозною загрозою для економічної безпеки країни.

Цілеспрямовані атаки на військові об'єкти та інформацію. Військові об'єкти є стратегічною мішенню для кібератак під час війни. На прикладі України можна побачити, як атаки на комп'ютерні мережі збройних сил використовуються для отримання конфіденційної інформації, а також для саботажу або дезорганізації роботи військових. В умовах війни агресор використовує кібератаки для дестабілізації управління та командних пунктів, що робить боротьбу з такими нападами важливим пріоритетом для національної безпеки.

Захист критичної інфраструктури України від кіберзагроз. Захист критичної інфраструктури України від кіберзагроз є ключовим аспектом національної безпеки. Враховуючи військову агресію з боку рф, Україна змушена адаптувати свою кіберстратегію до нових умов і викликів. Розробка комплексних заходів захисту

критичних об'єктів інфраструктури вимагає не тільки технічних, а й організаційних і правових змін.

Розробка національної стратегії кібербезпеки. Україна розробила ряд нормативно-правових актів для створення ефективної системи кібербезпеки, яка включає правила взаємодії державних органів, приватного сектору та громадських організацій. Зокрема, документ [1] визначає основні принципи забезпечення кібербезпеки, а також передбачає взаємодію держави та бізнесу у питаннях захисту від кіберзагроз. Крім того, у 2021 році було розроблено Стратегію кібербезпеки України [2], яка націлена на побудову комплексної системи захисту критичної інфраструктури.

Інтеграція кібербезпеки в національні стратегії безпеки. Інтеграція кібербезпеки в національні стратегії безпеки передбачає створення координаційних органів, що здійснюють постійний моніторинг загроз і забезпечують реагування на кіберінциденти. В Україні створено Національний координаційний центр кібербезпеки, що відповідає за моніторинг ситуації в кіберпросторі та надає оперативні рекомендації щодо захисту критичних об'єктів інфраструктури.

Моніторинг кіберзагроз та оперативне реагування. Моніторинг кіберзагроз є основою системи захисту. В Україні для цього були розроблені спеціальні програмні продукти та платформи, зокрема, система CERT-UA (команда реагування на комп'ютерні інциденти), яка відповідає за виявлення, попередження і реагування на кіберінциденти. Моніторинг здійснюється з використанням сучасних технологій, таких як Zabbix, Nagios, та інші, що дозволяє здійснювати проактивний контроль за станом інформаційних систем критичних об'єктів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Кібербезпека критичної інфраструктури є ключовим аспектом національної безпеки, особливо в умовах військової загрози. Україна стикається з постійними кіберзагрозами, включаючи DDoS-атаки, шкідливі програми та цілеспрямовані напади на енергетичні, фінансові та інші важливі об'єкти. Актуальність удосконалення механізмів захисту критичних інфраструктурних систем зростає з кожним роком, зокрема через розробку нових нормативно-правових актів та інтеграцію з міжнародними системами захисту.

Необхідно продовжувати розробку нових технологій для захисту критичної інфраструктури, зокрема в області виявлення та протидії новим типам кіберзагроз. Також важливо досліджувати ефективність національних стратегій кібербезпеки та розвивати навчання і підготовку кадрів у сфері кіберзахисту, що сприятиме посиленню стійкості інфраструктури до кібератак.

ПОСИЛАННЯ

1. "Pro osnovni zasady zabezpechennya kyberbezpeky Ukrayiny: Zakon Ukrayiny, 5 zhovtnya 2017 roku, No. 2163-VIII," Verkhovna Rada Ukrayiny, 2017. [Online]. Available: https://zakon.rada.gov.ua/laws/show/2163-19. [Accessed: Nov. 2, 2024].
2. "Ukaz Prezydenta Ukrayiny vid 26 serpnya 2021 roku No. 447/2021 'Pro Stratehiyu kyberbezpeky Ukrayiny'," Prezydent Ukrayiny, Aug. 26, 2021. [Online]. Available: https://zakon.rada.gov.ua/laws/show/447/2021. [Accessed: Nov. 2, 2024].

Статтю прийнято до опублікування __.__.20__