КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (12), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.12.2935
УДК 004

Мальцева Ірина Робертівна
Старший науковий співробітник
Військовий інститут інформаційно–телекомунікаційних технологій, Київ, Україна
ORCID ID: 0000–0001–6073–4637
irenagold2402@gmail.com

Черниш Юлія Олександрівна
Старший науковий співробітник
Військовий інститут інформаційно–телекомунікаційних технологій, Київ, Україна
ORCID ID: 0000–0002–6626–5656
kobernikoi@ukr.net

Овсянніков Вячеслав Володимирович
Провідний науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0003-0186-6220
2081364@gmail.com

АНАЛІЗ МЕТОДИК ОЦІНКИ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Доступність критичної інфраструктури через кіберпростір, ставить забезпечення національної безпеки в залежність від ступеня її захищеності. Критична інфраструктура це безліч автоматизованих систем управління, за допомогою яких забезпечується взаємодія інформаційно-телекомунікаційних мереж, які вирішують завдання державного управління, питання обороноздатності, проблем безпеки та правопорядку та ін. Захищеність критичної інфраструктури безпосередньо залежить від володіння відповідними структурами новими видами зброї, від ступеня її ефективності, методів використання і засобів захисту від такої ж зброї ворога. Необхідно вирішити питання здійснення дієвого протиборства в кіберпросторі. Аналіз проблем в розробці методик оцінки функціональної стійкості критичної інфраструктури в умовах кібернетичного протиборства потребує визначення базових методів і критеріїв, які можуть бути застосовані в Україні для оцінки стійкості обєктів критичної інфраструктури. Кібернетична зброя, що здійснює деструктивні інформаційні впливи, не є зброєю в класичному сенсі, тому що не провадить фізичне ураження об'єкта атаки, а переводить його інформаційні та автоматизовані системи управління в кризовий режим функціонування. Процес протидії двох і більше сторін, в такому вигляді, є кібернетичним протиборством, що реалізовується при використанні спільного загального ресурсу – глобального інформаційного простору. На процес управління критичною інфраструктурою, кібернетичне протиборство накладає додаткові вимоги, щодо забезпечення сталого функціонування критичної інфраструктури. Стійкість при цьому є інтегральною властивістю, невід'ємно пов'язаною із середовищем функціонування. Кіберстійкість є інтегральним показником і визначається кібернадійністю, яка відображає можливість виконувати свої завдання в складній системі управління критичною інфраструктурою в умовах інформаційних деструктивних впливів.

Ключові слова: кібервразливості, кіберзброя, кіберпростір, кіберстійкість, критична інфраструктура, об’єкти критичної інфраструктури.

ВСТУП

Значне підвищення рівня автоматизованих комплексів управління, інформаційних технологій та інформаційних систем, створення єдиного інформаційного простору визначили виникнення і розвиток принципово нового об'єкта планетарного масштабу –

кіберпростору [1]. Феномен наявності і успішного функціонування даного об'єкта за відсутності досить розвиненої теорії, щодо нього, не відповідає практиці створення складних штучних систем [2-4]. При цьому мова йде про штучні впливи і штучне середовище його існування, що породжують в свою чергу нові, що де-факто склалися, але юридично не закріплені. Хоча вже з'явилися роботи з дослідження термінології в даній області [5, 6].

Постановка проблеми. Доступність критичної інфраструктури (КІ) через кіберпростір, ставить забезпечення національної безпеки в залежність від ступеня її захищеності. Під КІ будемо розуміти безліч автоматизованих систем управління, за допомогою яких забезпечується взаємодія інформаційно-телекомунікаційних мереж, які вирішують завдання державного управління, питання обороноздатності, проблем безпеки та правопорядку та ін. Порушення або припинення функціонування цих мереж (систем) призводить до настання важких наслідків. Захищеність КІ безпосередньо залежить від володіння відповідними структурами новими видами зброї (наприклад, кіберзброї, що відповідає середовищу її функціонування), від ступеня її ефективності, методів використання і засобів захисту від такої ж зброї ворога. Все перераховане створює необхідні передумови для виникнення і здійснення дієвого протиборства в кіберпросторі.

Аналіз останніх досліджень і публікацій. Організації безпеки КІ присвячено не так багато праць та досліджень. Питання управління безпекою КІ розглядали такі вітчизняні учені: В. Абрамов, Д. Бірюков, Д. Бобро, О. Їжак, Г. Ситник, А. Семенченко, О. Суходоля, В. Лядовська, С. Кондратов, С. Кулінська, В. Куйбіда, О. Насвіт, А. Пашков, І. Уряднікова, Л. Щаслива та ін. Дослідженню проблемних питань безпеки КІ присвячені праці А. Біаласа, А. Венгера, Д. Гритзаліса, Т. Келлі, А. Лазарі, В. Майєра, Д. Рехака, С. Ріналді, А. Фекете, П. Хокстада та ін. [7]. Дослідження з організації безпеки КІ, забезпечення надійності та сталого функціонування автоматизованих систем управління об'єктів КІ, які викладені в одній із робіт[5] показує , що в них не розглянуті питання, пов'язані з розробкою моделей, методів і методик [4] в цьому напрямі.

Мета статті. Метою даної статті є аналіз проблем в розробці методик оцінки функціональної стійкості КІ в умовах кібернетичного протиборства. Визначення базових методів і критеріїв, які можуть бути застосовані в Україні для оцінки стійкості обєктів КІ.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Кібернетична зброя, що здійснює деструктивні інформаційні впливи, не є зброєю в класичному сенсі, тому що не провадить фізичне ураження об'єкта атаки, а переводить його інформаційні та автоматизовані системи управління в кризовий режим функціонування. Процес протидії двох і більше сторін, в такому вигляді, є кібернетичним протиборством, що реалізовується при використанні спільного загального ресурсу – глобального інформаційного простору. Управління ним визначають як цільовий вплив двох і більше підсистем управління. В результаті протиборства в кіберпросторі порушується функціонування об'єктів КІ, і це може привести до небажаних ефектів, наприклад, до тимчасової втрати управління об'єктом або фізичного руйнування об'єктів КІ. Ця проблема набуває значної актуальності при вирішенні завдань забезпечення безпеки об'єктів КІ, що мають особливо важливе значення (хімічні заводи, атомні електростанції і т.п.), при руйнуванні яких може бути завдано фатальної шкоди прилеглим об'єктам і територіям, а також обслуговуючому персоналу і населенню. Так, за оцінкою експертів [8], ефект цільового застосування

кібернетичної зброї проти інформаційної системи порівняємо з ефектом застосування зброї масового ураження. Звідси випливає, що дії об'єктів КІ в кібернетичному просторі створюють нові вразливості і загрози і вимагають розробки нових інструментів, що забезпечували б безпеку КІ та які б гарантували стабільну працездатність в умоваxx атак будь–якої інтенсивності [5].

Проблема стійкості критичної інфраструктури

Розглянемо оцінку стійкості функціонування такої складної соціотехнічної системи, як КІ, за наступними ключовими моментами:

• оцінка стану об'єктів КІ;

• формування простору ознак функціонування КІ;

• створення і ведення єдиної розподіленої бази даних з оперативної аналітичної обробкою даних [4];

• адаптивне управління КІ, що враховує поточний і прогнозований стан об'єктів КІ в умовах деструктивних інформаційних впливів [4].

Розроблений науково–методичний апарат проектування автоматичної системи збору даних є малоефективним. Необхідно вирішити завдання приведення інформації до єдиного вигляду, що визначає стан КІ в умовах деструктивних інформаційних впливів.

Зі сказаного випливає, що існує потреба в розробці способів проектування системи оцінки функціональної стійкості КІ в умовах кібернетичного протиборства. При цьому треба відзначити, що представлена спрощена модель дозволяє сформулювати і описати найважливіші якості і властивості управління, що визначають кіберстійкість.

На процес управління КІ кібернетичне протиборство накладає додаткові вимоги, щодо забезпечення сталого функціонування КІ. Стійкість при цьому є інтегральною властивістю, невід'ємно пов'язаною із середовищем функціонування. Зі стійкістю в техно- і інфосфері все більш–менш визначено, чого не скажеш про кіберстійкість. Тут виникає ряд питань, пов'язаних з віртуальністю зазначеного середовища. Причому процеси, що відбуваються в ньому, надають прямий або непрямий вплив, позначаються на стійкості функціонування КІ в техно- і інфосфері. Кіберстійкість є інтегральним показником і визначається кібернадійністю, яка відображає можливість виконувати свої завдання в складній системі управління КІ в умовах інформаційних деструктивних впливів.

1. За організаційною структурою:

• одноланковий об'єкт КІ (складається з однієї ланки) має всі необхідні можливості для виконання одиничної цільової функції (самостійний базовий сегмент). Окремі комплекси засобів автоматизації можуть служити прикладом одноланкової структури.

• багатоланковий об'єкт КІ (складається з багатьох ланок) являє собою структурне послідовне з'єднання в єдину систему декількох одноланкових об'єктів КІ для досягнення єдиної цільової функції.

2. . За функціональною єдністю:

• однорідні багатоланкові об'єкти КІ – це об'єкти , утворені з послідовного з'єднання одноланкових об'єктів КІ в єдину систему, що мають єдину цільову функцію, для виконання цієї функції.

• неоднорідні багатоланкові об'єкти КІ – це об'єкти, утворені з послідовного з'єднання одноланкових об'єктів КІ і виконують різні цільові функції, наприклад інформаційні системи, системи обробки даних, телекомунікаційна мережа і т.д.

Наведена класифікація допомагає оцінити кіберстійкість як сукупність взаємопов'язаних складних організаційних систем (враховуючи коефіцієнт пов'язаності)

одноланкових об'єктів КІ (беручи до уваги індивідуальний внесок в виконання системою цільової функції).

При цьому під кіберстійкістю одноланкового об'єкта КІ будемо розуміти здатність його системи управління виконувати свої функції при всіх видах деструктивних інформаційних впливів.

Методика оцінки кіберстійкості

Методика оцінки кіберстійкості розбита на три етапи:

1. Оцінка кіберстійкості кожного об'єкта КІ окремо.

1.1 Виконати оцінку одноланкового об'єкта КІ:

• розрахувати ймовірність виходу з ладу і-го елементу в умовах деструктивних інформаційних впливів;

• визначити коефіцієнт пов'язаності і-го елементу і його внесок в цільову функцію об'єкта КІ;

• оцінити кіберживучість, тобто межу станів одноланкового об'єкта КІ.

1.2. Виконати оцінку багатоланкового об'єкта КІ.

• розрахувати ймовірність виходу з ладу j-го одноланкового об'єкта КІ в умовах деструктивних інформаційних впливів;

• визначити коефіцієнт пов'язаності j-го одноланкового об'єкта КІ і його внесок в цільову функцію багатоланкового об'єкта КІ; дати оцінку кіберживучості, тобто межі станів багатоланкового об'єкта КІ.

2. Оцінка кібестійкості взаємодіючих об'єктів КІ:

• розрахувати ймовірність відмови n-го багатоланкового об'єкта КІ в умовах деструктивних інформаційних впливів;

• визначити коефіцієнт пов'язаності n-го багатоланкового об'єкта КІ і його внесок в цільову функцію багатоланкового об'єкта КІ;

• дати оцінку кіберстійкості.

3. Оцінка кіберстійкості КІ визначається через суму значень стійкості її елементів з урахуванням коефіцієнта пов'язаності, що включає оцінку кіберживучості КІ в динаміці при виконанні нею своїх функцій.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

1. Доступність КІ ставить національну безпеку в залежність від ступеня її захищеності. Захищеність при цьому безпосередньо залежить від ступеня володіння відповідними структурами нового виду зброї – кіберзброї, що створює необхідні передумови для виникнення і здійснення ефективного протистояння в кіберпросторі.

2. Реалізація функцій об'єктів КІ в кіберпросторі створює нові вразливості і загрози, вимагаючи створення сучасних інструментів, що забезпечують безпеку КІ, тобто захищеність, що забезпечує стійке функціонування КІ в умовах атак будь–якої інтенсивності.

3. Об'єкти КІ доцільно класифікувати за ознаками, які впливають на забезпечення кіберстійкості функціонування: по організаційній структурі – одноланкові і багатоланкові; за функціональною єдністю – однорідні багатоланкові і неоднорідні багатоланкові.

4. Узагальнений показник кіберстійкості включає показники кіберстійкості і кібернадійності КІ.

5. Методика оцінки кіберстійкості представлена трьома послідовними етапами:

• оцінка кіберстійкості кожного окремо діючого об'єкта КІ;

• оцінка кіберстійкості об'єктів КІ діючих взаємно;

• оцінка кіберстійкості КІ через суму стійкості її елементів з урахуванням коефіцієнта пов'язаності, включаючи оцінку кіберживучості КІ в динаміці при виконанні нею своїх функцій.

Подальші дослідження слід проводити в напрямку розвитку і вдосконалення методів, способів та методик оцінки кіберстійкості об'єктів критичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про схвалення Концепції створення державної системи захисту критичної інфраструктури, Розпорядження Кабінету Міністрів України № 1009-р (2017) (Україна). https://zakon.rada.gov.ua/laws/show/1009-2017-р
2. Бірюков, Д. С. (2012). Захист критичної інфраструктури: Проблеми та перспективи впровадження в Україні (С. І. Кондратов, Ред.). НІСД.
3. Про схвалення Концепції створення державної системи захисту критичної інфраструктури, Розпорядження Кабінету Міністрів України № 1009-р (2017) (Україна). https://zakon.rada.gov.ua/laws/show/1009-2017-р
4. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України", Указ Президента України № 287/2015 (2020) (Україна). https://zakon.rada.gov.ua/laws/show/287/2015
5. Верголяс, О. *Реформування системи захисту та підвищення стійкості критичної інфраструктури України в розрізі актуальних загроз*. Куля News. https://coolyanews.info/reformuvannyasistemi–zahistu–ta–piidvischennya–stiijkostii–kritichnoyi–iinfrastrukturi–ukrayinii–v–rozriiziiaktual.html
6. Суходолі, О. М. (Ред.). (2015). Зелена книга з питань захисту критичної інфраструктури в україні : Зб. матеріалів міжнар. експерт. нарад. НІСД.
7. Мельничук, О. (2019). Управління критичною інфраструктурою держави: Базові методи та критерії ідентифікації об’єктів. Національна академія державного управління при Президентові України, 3(42), 13–27.
8. НБУ: створена міжвідомча робоча група щодо державної системи захисту об’єктів та сфер критичної інфраструктури у фінансовому секторі (Україна). https://bank.gov.ua/control/uk/publish/article?art_id=50755738.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (12), 2021
ISSN 2663 - 4023

Irina R. Maltseva
Senior Researcher
Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0001-6073-4637
irenagold2402@gmail.com

Yuliya O. Chernysh
Senior Researcher
Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-6626-5656
kobernikoi@ukr.net

Viacheslav V. Ovsiannikov
Leading researcher
Military Institute of Telecommunication and Information Technologies named after the Heroes of Kruty, Kyiv, Ukraine
ORCID ID: 0000-0003-0186-6220
2081364@gmail.com

ANALYSIS OF CYBER RESISTANCE ASSESSMENT METHODS OF CRITICAL INFRASTRUCTURE

Abstract. The availability of critical infrastructure through cyberspace makes national security dependent on the degree of its security. Critical infrastructure is a set of automated management systems, which provide the interaction of information and telecommunications networks that solve problems of public administration, defense, security and law enforcement, and others. The protection of critical infrastructure directly depends on the possession of the relevant structures of new weapons, the degree of its effectiveness, methods of use and means of protection against the same weapons of the enemy. It is necessary to address the issue of effective confrontation in cyberspace. The analysis of problems in the development of methods for assessing the functional stability of critical infrastructure in cyber confrontation requires the definition of basic methods and criteria that can be used in Ukraine to assess the stability of critical infrastructure. Cyber weapons, which carry out destructive information effects, are not weapons in the classical sense, because they do not physically damage the object of attack, but translate its information and automated control systems into a crisis mode of operation. The process of counteraction of two or more parties, in this form, is a cyber confrontation that is realized using a common common resource - the global information space. In the process of critical infrastructure management, cyber confrontation imposes additional requirements to ensure the sustainable operation of critical infrastructure. Stability is an integral property that is inextricably linked to the operating environment. Cyber resilience is an integrated indicator and is determined by cyber reliability, which reflects the ability to perform its tasks in a complex critical infrastructure management system in the context of information destructive influences.

Keywords: cyber vulnerabilities, cyber weapons, cyberspace, cyber resilience, critical infrastructure, critical infrastructure facilities.

REFERENCES

1. Pro skhvalennia Kontseptsii stvorennia derzhavnoi systemy zakhystu krytychnoi infrastruktury, Rozporiadzhennia Kabinetu Ministriv Ukrainy № 1009-r (2017) (Ukraina). https://zakon.rada.gov.ua/laws/show/1009-2017-r
2. Biriukov, D. S. (2012). Zakhyst krytychnoi infrastruktury: Problemy ta perspektyvy vprovadzhennia v Ukraini (S. I. Kondratov, Red.). NISD.
3. Pro skhvalennia Kontseptsii stvorennia derzhavnoi systemy zakhystu krytychnoi infrastruktury, Rozporiadzhennia Kabinetu Ministriv Ukrainy № 1009-r (2017) (Ukraina). https://zakon.rada.gov.ua/laws/show/1009-2017-r

4. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 6 travnia 2015 roku "Pro Stratehiiu natsionalnoi bezpeky Ukrainy", Ukaz Prezydenta Ukrainy № 287/2015 (2020) (Ukraina). https://zakon.rada.gov.ua/laws/show/287/2015
5. Verholias, O. Reformuvannia systemy zakhystu ta pidvyshchennia stiikosti krytychnoi infrastruktury Ukrainy v rozrizi aktualnykh zahroz. Kulia News. https://coolyanews.info/reformuvannyasistemi–zahistu–ta–piidvischennya–stiijkostii–kritichnoyi–iinfrastrukturi–ukrayinii–v–rozriiziiaktual.html
6. Sukhodoli, O. M. (Red.). (2015). Zelena knyha z pytan zakhystu krytychnoi infrastruktury v ukraini : Zb. materialiv mizhnar. ekspert. narad. NISD.
7. Melnychuk, O. (2019). Upravlinnia krytychnoiu infrastrukturoiu derzhavy: Bazovi metody ta kryterii identyfikatsii obiektiv. Natsionalna akademiia derzhavnoho upravlinnia pry Prezydentovi Ukrainy, 3(42), 13–27.
8. NBU: stvorena mizhvidomcha robocha hrupa shchodo derzhavnoi systemy zakhystu obiektiv ta sfer krytychnoi infrastruktury u finansovomu sektori (Ukraina). https://bank.gov.ua/control/uk/publish/article?art_id=50755738.