КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.779
УДК 004.056.5:005.8

Сидоренко Вікторія Миколаївна
к.т.н., доцент, доцент кафедри комп'ютерних інформаційних технологій
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID ID: 0000-0002-5910-0837
v.sydorenko@ukr.net

Максимець Андрій Володимирович
старший інженер
Інститут спеціального зв'язку та захисту інформації
Національний технічний університет України
Київський політехнічний інститут імені Ігоря Сікорського, Київ, Україна
ORCID ID: 0000-0003-3551-0628
andy.west.corp@gmail.com

МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КРИТИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ В УМОВАХ ВПЛИВУ ВНУТРІШНІХ ТА ЗОВНІШНІХ ДЕСТАБІЛІЗУЮЧИХ ЧИННИКІВ

Анотація. Сучасна критична інфраструктура (КІ) держави складається з інформаційних, енергетичних, транспортних та інших стратегічно важливих об'єктів, які забезпечують безперервне функціонування суспільства та економіки. Особливу роль у її захисті відіграють критичні інформаційні системи (КІС), які забезпечують обробку, зберігання та передачу даних, необхідних для управління ключовими секторами/підсекторами інфраструктури. В умовах зростання кіберзагроз, воєнних викликів та дестабілізуючих чинників (ДЧ) визначальним фактором захищеності та стабільності функціонування КІ держави є забезпечееня стійкості КІС. У статті проведено аналіз існуючих підходів до забезпечення стійкості за ключовими критеріями: надійність, стійкість до фізичних загроз, кібербезпека, оперативність відновлення, гнучкість та адаптивність, координація управління ризиками, фінансова та ресурсна забезпеченість, сприйнятливість до ДЧ. Визначено сильні та слабкі аспекти національних підходів, а також встановлено необхідність врахування критерію сприйнятливість до ДЧ, оскільки його вплив залишається недостатньо дослідженим, особливо в умовах сучасних загроз. Розроблено модель забезпечення стійкості КІС, що дозволяє критичним системам функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після впливу внутрішніх та зовнішніх ДЧ. Наступні дослідження будуть спрямовані на удосконалення повноти множини функцій захищеності, що дозволить підвищити рівень кібербезпеки та стійкості (резильєнтності) КІ в умовах воєнного стану та післявоєнного відновлення.

Ключові слова: критична інфраструктура; об'єкти критичної інфраструктури; кібербезпека; критичні інформаційні системи; стійкість; забезпечення стійкості; функції захисту; дестабілізуючі чинники.

ВСТУП

Сьогодні критична інфраструктура (КІ) нашої держави перебуває під постійними загрозами, що спричинені як зовнішніми, так і внутрішніми факторами. Військові конфлікти, кібератаки, техногенні аварії та природні катаклізми можуть значно послабити функціонування ключових об'єктів, що забезпечують життєдіяльність країни. У такій ситуації необхідно впроваджувати ефективні механізми оцінки ризиків, прогнозування потенційних загроз і розробки стратегій швидкого реагування, що дозволять мінімізувати наслідки кризових ситуацій.

Особливої уваги набуває питання стійкості КІ, що визначено на законодавчому рівні. Відповідно до Закону України «Про критичну інфраструктуру» [1], забезпечення її безперервного функціонування є одним із ключових пріоритетів державної політики. Реалізація цього завдання вимагає застосування сучасних методів аналізу, які дозволяють оцінювати рівень загроз, визначати потенційні вразливості та формувати ефективні механізми захисту.

Забезпечення стійкості КІ є важливим напрямом наукових досліджень, що вимагає пошуку нових моделей і методів. Розробка універсальних підходів до оцінки ризиків та прогнозування ймовірності відмови інформаційних систем дозволить підвищити ефективність управління кібербезпекою, підвищить стан захищеності КІ та надасть можливість розробки рекомендацій щодо стійкості КІ в умовах воєнного стану.

Постановка проблеми. У законодавстві України поряд із поняттям інформації використовується термін «інформаційна система» (ІС), який має низку різних визначень. Узагальнююче визначення трактує ІС як взаємопов'язану, організовану сукупність підприємств, підрозділів, фахівців, нормативно-правового забезпечення, комплексу організаційних та технічних заходів, інформаційних технологій і ресурсів, що забезпечують інформаційні процеси. До таких процесів належать створення, поширення, використання, зберігання та утилізація інформації [2]. В контексті забезпечення стійкості ІС ключовим завданням є розробка механізмів, які дозволять мінімізувати вплив ДЧ та забезпечити безперервність функціонування.

Окрему категорію становлять критичні інформаційні системи (КІС), під якими розуміють ті ІС, що є ключовими для забезпечення національної безпеки, економіки, охорони здоров'я та інших важливих сфер. Порушення або знищення таких систем може призвести до серйозних наслідків для держави та суспільства. Через високу значущість цих систем особливу увагу слід приділяти їхній захищеності та стійкості до зовнішніх і внутрішніх загроз.

Термін «інформаційний ресурс» визначається як будь-яка сукупність інформації незалежно від її змісту, часу чи місця створення [2]. Це визначення дозволяє відносити до інформаційних ресурсів як організовану, так і неорганізовану інформацію, а також продукти, створені на її основі. Інформаційні ресурси відіграють важливу роль у функціонуванні КІ, оскільки забезпечують підтримку стратегічних галузей, таких як освіта, виробництво, медицина, право та соціальна сфера. Для гарантування їхньої стійкості необхідно враховувати не лише технологічні аспекти, а й загрози інформаційній безпеці, що можуть призвести до порушення функціонування системи.

Рис. 1. Базові принципи забезпечення стійкості (резильєнтності) КІ

Стійкість є фундаментальною властивістю будь-якої системи, оскільки вона визначає здатність протистояти впливу зовнішніх і внутрішніх ДЧ. Базові принципи стійкості КІ (рис. 1) описують набір принципів, ключових дій і вказівок для підвищення рівня стійкості в національному масштабі та покращення безперервності критично важливих послуг, таких як енергетика, транспорт, водопостачання, водовідведення, відходи та цифровий зв'язок, та забезпечують ефективне функціонування охорони здоров'я, освіти, оборони тощо [3].

Відповідно до загальної теорії систем, однією з атрибутивних характеристик є самозбереження, яке можливе лише за умови ефективної нейтралізації загроз та мінімізації потенційних втрат. Забезпечення стійкості інформаційних та технічних систем вимагає комплексного підходу, що включає оцінку ризиків, розробку механізмів адаптації та вдосконалення заходів безпеки. Оцінка стійкості може проводитися як кількісними, так і якісними методами [4], що дозволяє формувати стратегії для підвищення захисту КІ та зменшення негативного впливу кризових ситуацій.

Зазначені твердження свідчать про наявність важливого наукового завдання щодо проведення аналізу існуючих підходів до забезпечення стійкості та розробки універсальної моделі забезпечення стійкості КІС в умовах впливу внутрішніх та зовнішніх ДЧ.

Аналіз останніх досліджень і публікацій. Забезпечення належного рівня захисту КІ є пріоритетним завданням держави, оскільки від її стійкості залежить безпека громадян, економічна стабільність та обороноздатність країни. Аналіз наявних досліджень у цій сфері дозволяє оцінити існуючі підходи, визначити ключові ризики та сформувати ефективні стратегії підвищення захищеності критичних об'єктів. Для вирішення завдань пов'язаних з забезпеченням захищеності та стійкості КІС проведемо аналіз сучасних публікацій, опишемо існуючі підходи до визначення стійкості та проведемо їх порівняльний аналіз.

У роботі Плахотнюка Р. [5] досліджено питання забезпечення стійкості КІ України в умовах сучасних викликів. Автор аналізує основні загрози, що постають перед КІ, зокрема кіберзагрози, фізичні атаки та організаційні недоліки. У статті запропоновано заходи з удосконалення системи управління стійкістю інфраструктури та механізми мінімізації ризиків.

Мурасов Р. і Мельник Я. [6] у своїй роботі розглядають методи оцінювання захищеності кіберпростору об'єктів КІ. Автори аналізують сучасні підходи до кібербезпеки, визначають вразливості та пропонують алгоритми підвищення рівня захисту ІС, що функціонують у межах КІ.

Дослідження Бойка О. [7] присвячене державній політиці та державному управлінню у сфері захисту КІ. У статті розглянуто законодавчі та нормативні акти, що регулюють цей напрям, а також запропоновано напрями вдосконалення управлінських процесів. Особливу увагу приділено міжнародному досвіду та можливості його адаптації в Україні.

Сокіран М. [8] у своїй роботі аналізує систему принципів адміністративно-правового забезпечення стійкості критичної інформаційної інфраструктури України. Автор розглядає правові аспекти забезпечення кіберстійкості, визначає основні виклики та пропонує правові механізми їх подолання.

У роботі Суходолі О. [9] акцентовано увагу на стійкості критичної енергетичної інфраструктури та забезпеченні життєдіяльності громад. Автор аналізує основні ризики для енергетичного сектору та розглядає підходи до підвищення його захищеності в умовах кризових ситуацій.

Гордієнко С. Г. та Доронін І. М. [10] досліджують інформаційно-правові аспекти захисту КІ. У статті розглянуто чинне законодавство та міжнародні нормативно-правові акти у сфері інформаційної безпеки, проаналізовано їхній вплив на регулювання захисту критичних об'єктів.

Шевченко Н. І. та Плахотнюк Р. В. [11] у своїй роботі пропонують методичні підходи до оцінювання стійкості функціонування об'єктів КІ в умовах особливого періоду функціонування економіки України. Дослідження містить методи оцінювання ризиків та підходи до управління кризовими ситуаціями у критичних секторах.

Яременко О. І. та Страхніцький Я. І. [12] аналізують теоретичні підходи до визначення дефініції КІ як об'єкта державного управління. У статті обґрунтовано необхідність формування єдиної термінологічної бази та визначено ключові характеристики КІ з точки зору державного управління.

У статті Ковальчука І. [13] розглядається питання захисту КІ з точки зору міжнародного досвіду та українських реалій. Автор проводить порівняльний аналіз підходів до захисту критичних об'єктів у різних країнах, акцентуючи увагу на можливостях адаптації світових практик до умов нашої держави.

Кириленко С. П. та Тищенко В. В. [14] досліджують моделі оцінювання ризиків для КІ в умовах збройного конфлікту. У роботі представлено підходи до аналізу загроз та розроблено методику оцінювання вразливостей об'єктів КІ в умовах воєнного стану.

У табл. 1, систематизовано та представлено детальний аналіз підходів до забезпечення стійкості описаних у проаналізованих джерелах за такими 8 критеріями (запропоновані авторами):

1. Надійність (RL) — рівень забезпечення безперервної роботи системи завдяки резервним ресурсам та альтернативним каналам постачання.
2. Стійкість до фізичних загроз (RPT) — здатність інфраструктури витримувати природні катастрофи, техногенні аварії, військові удари та інші фізичні впливи.
3. Кібербезпека (CS) — рівень захисту ІС, зокрема від кібератак, шкідливого програмного забезпечення та витоків даних.
4. Оперативність відновлення (RS) — швидкість і ефективність реагування на надзвичайні ситуації, здатність швидко відновити критично важливі функції.
5. Гнучкість та адаптивність (FLA) — можливість системи змінюватися у відповідь на нові загрози, впроваджувати інноваційні рішення та змінювати сценарії роботи.
6. Координація та управління ризиками (CRM) — ефективність взаємодії між державними, приватними та міжнародними партнерами у сфері захисту КІ.
7. Фінансова та ресурсна забезпеченість (FRS) — рівень фінансування заходів із забезпечення стійкості, наявність людських та матеріальних ресурсів для виконання запланованих заходів.
8. Сприйнятливість до ДЧ (SDF) — рівень впливу політичних, економічних, соціальних та інформаційних загроз на функціонування КІ.

Представлений у табл. 1 огляд підходів до забезпечення стійкості КІ показав, що найбільш важливими критеріями яким відповідають більша частина проаналізованих досліджень є надійність, оперативність відновлення та координація управління ризиками. Водночас менш дослідженими залишаються кібербезпека та фінансова забезпеченість, що вимагає подальших досліджень і вдосконалення методик захисту КІ. Крім того, встановлено, що сприйнятливість до ДЧ постає справжнім викликом, особливо в умовах сучасних загроз. Отримані результати можуть бути корисними для подальшого вдосконалення стратегій забезпечення стійкості КІ України.

Таблиця 1

Порівняльний аналіз підходів до забезпечення стійкості КІС

№	Назва	Критерії							
		RL	**RPT**	**CS**	**RS**	**FLA**	**CRM**	**FRS**	**SDF**
1.	Плахотнюк Р.	+	+	+/-	+	+	+	+/-	+/-
2.	Мурасов Р., Мельник Я.	+/-	-	+	+/-	+/-	-	+/-	-
3.	Бойко О.	+/-	+/-	-	+/-	-	+/-	-	-
4.	Сокіран М.	-	+/-	-	-	-	-	-	-
5.	Суходоля О.	+	+	+/-	+	+	+	+	+
6.	Гордієнко С., Доронін І.	+/-	-	+	+/-	-	-	-	-
7.	Шевченко Н., Плахотнюк Р.	+	+	+/-	+	+	+	+	+/-
8.	Яременко О., Страхніцький Я.	-	-	+/-	-	-	-	+/-	-
9.	Ковальчук І.	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-
10.	Кириленко С., Тищенко В.	+	+	+	+	+	+	+/-	+

З урахуванням зазначеного, вбачається за доцільне розробити універсальну модель забезпечення стійкості КІС, у якій будуть враховані всі перелічені функціональні особливості та переваги.

Метою статті є розроблення та дослідження моделі забезпечення стійкості КІС в умовах впливу внутрішніх та зовнішніх ДЧ.

ТЕОРЕТИЧНІ ОСНОВИ РОЗРОБКИ МОДЕЛІ

Побудова моделі забезпечення стійкості КІС

Ефективне забезпечення стійкості КІС можливе лише на основі комплексного використання всіх відомих моделей та підходів до вирішення цієї проблеми. Концепція такого комплексного підходу до захищеності має задовольняти розглянуту нижче сукупність вимог.

По-перше, мають бути розроблені та приведені до рівня регулярного використання усі необхідні механізми гарантованого забезпечення необхідного рівня захищеності КІС.

По-друге, мають бути наявними механізми практичної реалізації необхідного рівня захищеності КІС.

По-третє, необхідно мати у своєму розпорядженні засоби раціональної реалізації всіх необхідних заходів щодо захищеності КІС на базі досягнутого рівня розвитку науки і техніки.

По-четверте, повинні бути розроблені способи оптимальної організації та забезпечення всіх заходів щодо захищеності КІС в процесі її обробки.

З метою побудови єдиної концепції, яка задовольняє всю сукупність перелічених вимог, розроблено модель забезпечення стійкості КІС.

Під функцією захищеності КІС розуміють сукупність функціонально однорідних заходів, які регулярно здійснюються в ІС різними засобами та методами з метою створення, підтримки та забезпечення умов, об’єктивно необхідних для ефективного забезпечення стійкості КІС. Щоб множина функцій відповідала своєму призначенню, вони повинні задовольняти вимогам повноти. У цьому разі, забезпечуючи належним чином відповідний рівень виконання кожної з функцій зазначеної множини, і можливо гарантовано досягти необхідного рівня захищеності КІС.

Етап 1. Визначення множини функцій захищеності КІС.

Введемо повну множину функцій захищеності КІС $\mathbf{F}$:

$$\mathbf{F} = \{\bigcup_{i=1}^{n} \mathbf{F}_i\} = \{\mathbf{F}_1, \mathbf{F}_2, \ldots, \mathbf{F}_n\}, \quad (1)$$

де $\mathbf{F}_i \subseteq \mathbf{F}\ (i=\overline{1,n})$ — категорії функцій захищеності КІС, n — загальна кількість функцій захищеності.

Певні множини категорій $\mathbf{F}_i$ можуть бути представлені у вигляді підмножини потенційно можливих умов захищеності:

$$\mathbf{F}_i = \{\bigcup_{j=1}^{m_i} F_{ij}\} = \left\{F_{i1}, F_{i2}, ..., F_{im_i}\right\}, \quad (2)$$

де $F_{ij} \subseteq \mathbf{F}_i\ \ (i=\overline{1,n}, j=\overline{1,m_i})$ — функції забезпечення захищеності i-ї категорії, m_i — кількість функцій захищеності i-х категорій.

З урахуванням (2), вираз (1) можна представити у такому вигляді:

$$\mathbf{F} = \{\bigcup_{i=1}^{n} \mathbf{F}_i\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} F_{ij}\}\} = \{\{F_{11}, F_{12}, ..., F_{1m_1}\},$$

$$\{F_{21}, F_{22}, ..., F_{2m_2}\}, ..., \{F_{n1}, F_{n2}, ..., F_{nm_n}\}\}, (i=\overline{1,n}, j=\overline{1,m_i}).$$

Відповідно до запропонованого рішення введемо повну множину функцій захищеності КІС згідно [2], при $n=7$ з урахуванням (1), таким чином:

$$\mathbf{F} = \{\bigcup_{i=1}^{7} \mathbf{F}_i\} = \left\{\mathbf{F}_1, \mathbf{F}_2, \ldots, \mathbf{F}_7\right\},$$

де $\mathbf{F}_1$ — попередження всіх можливих умов, що можуть призвести до виникнення ДЧ; $\mathbf{F}_2$ — запобігання безпосередньому прояву ДЧ; $\mathbf{F}_3$ — виявлення ознак ДЧ; $\mathbf{F}_4$ — запобігання впливу ДЧ, спрямованих на порушення захищеності КІС; $\mathbf{F}_5$ — виявлення дій ДЧ, спрямованих на порушення захищеності КІС; $\mathbf{F}_6$ — локалізація (обмеження) впливу ДЧ; $\mathbf{F}_7$ — ліквідація наслідків впливу ДЧ.

Для множини категорій $\mathbf{F}_4$, при $n=4,\ \ m_4=2$ з використанням (2), представимо підмножину функцій таким чином:

$$\mathbf{F}_4 = \{\bigcup_{j=1}^{2} F_{4j}\} = \left\{F_{41}, F_{42}\right\},$$

де F_{41} — запобігання впливу ДЧ, які визначено та виявлено; F_{42} — запобігання впливу ДЧ, які визначено, але не виявлено.

Для множини категорій $\mathbf{F}_6$, при $n=6,\ \ m_6=2$ з використанням (2), представимо підмножину функцій таким чином:

$$\mathbf{F}_6 = \{\bigcup_{j=1}^{2} F_{6j}\} = \left\{F_{61}, F_{62}\right\},$$

де F_{61} — локалізація виявленого впливу ДЧ на інформацію; F_{62} — локалізація невиявленого впливу ДЧ на інформацію.

Для множини категорій $\mathbf{F}_7$, при $n=7,\ \ m_7=2$ з використанням (2), представимо підмножину функцій таким чином:

$$\mathbf{F}_7 = \{\bigcup_{j=1}^{2} F_{7j}\} = \left\{F_{71}, F_{72}\right\},$$

де F_{71} — ліквідація наслідків локалізованого та виявленго впливу ДЧ; F_{72} — ліквідація наслідків локалізованого та невиявленого впливу ДЧ.

$$\mathbf{F} = \{\bigcup_{i=1}^{n} \mathbf{F}_i\} = \{\bigcup_{i=1}^{7} \{\bigcup_{j=1}^{2} F_{4j}\}\{\bigcup_{j=1}^{2} F_{6j}\}\{\bigcup_{j=1}^{2} F_{7j}\}\} =$$

$$= \{\{F_1\},\{F_2\},\{F_3\},\{F_{41},F_{42}\},\{F_5\},\{F_{61},F_{62}\},\{F_{71},F_{72}\}\}, (i=\overline{1,n},\ j=\overline{1,m_i}).$$

Етап 2. Візуалізація структурної схеми моделі забезпечення стійкості.

Щоб довести повноту множини перерахованих функцій, розглянемо наведені на рис. 2 об'єднання подій, які потенційно можливі за умови виконання всіх функцій. Кожен із результатів є випадковою подією, а всі разом вони утворюють повну групу несумісних подій [2].

На рис. 2 представлено візуалізацію моделі забезпечення стійкості через опис функцій захисту КІС, а також наведено можливі наслідкові події від впливу ДЧ [2].

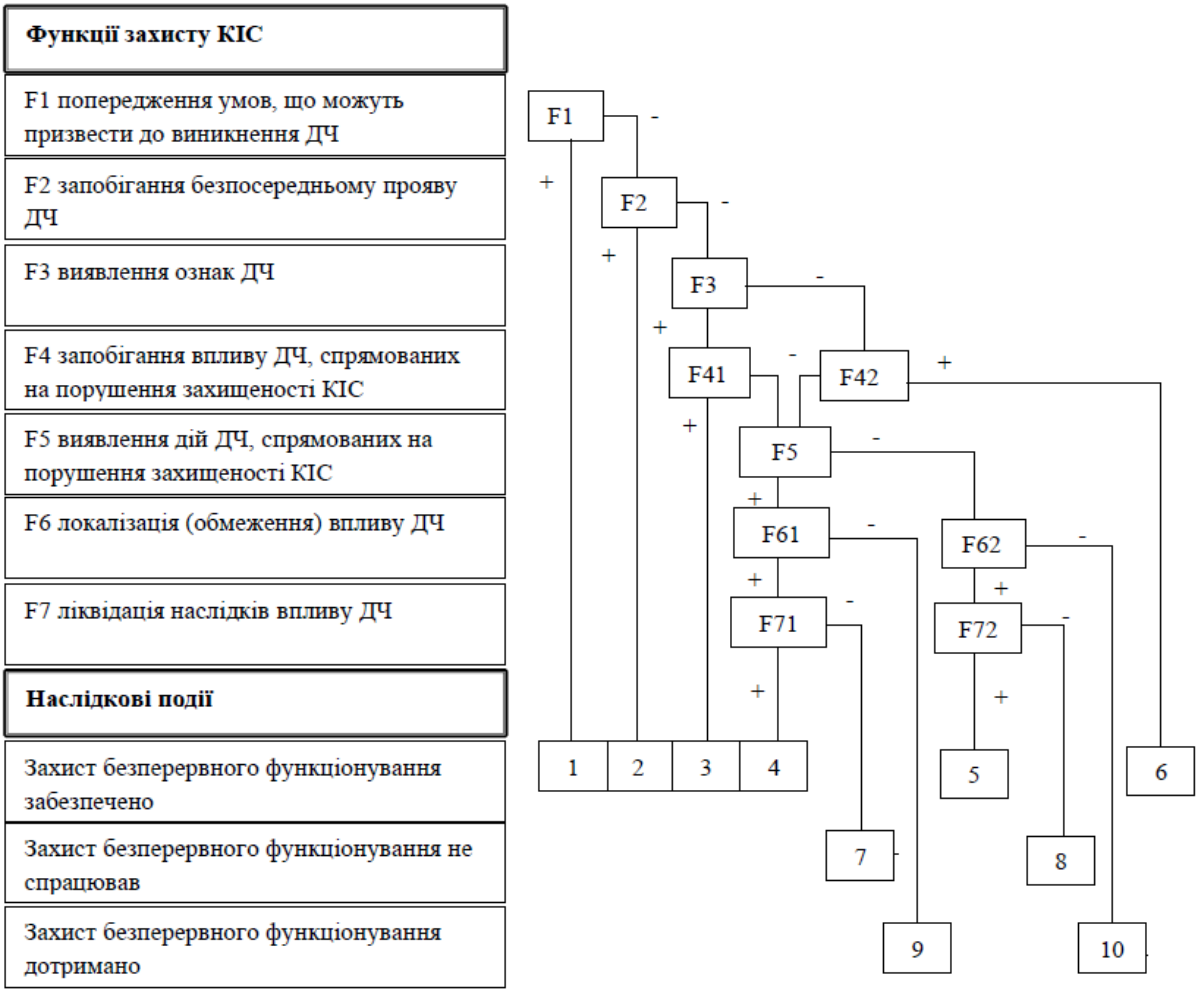

Рис. 2. Структурна схеми моделі забезпечення стійкості КІС

Етап 3. Визначення ймовірності захищеності КІС

Виходячи із визначення стійкості зазначеного у [1], опишемо можливість забезпечення стійкості як стан захищеності КІС, під час якого гарантується її спроможність виконувати повну множину функцій захисту та функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після впливу ДЧ будь-якого виду. Отже, визначемо стійкіть КІС за допомогою основ теорії

ймовірностей. Відповідно до рис. 2, сприятливими з точки зору захищеності КІС є результати 1–6, сума ймовірностей таких подій дорівнює 1 (ймовірність успішного захисту КІС) і буде свідчити про те, що захищеність КІС забезпечено — атаку не допущено. Позначивши ймовірність захищеності КІЧ через P_3 отримаємо:

$$P_3 = \sum_{m=1}^{6} P_m^i. \tag{3}$$

Також слід зазначити, що маючи сім категорій функцій захисту КІС, F7 це той випадок, коли атака відбулась і тепер необхідно швидко відновлювати захищеність КІС та ліквідовувати наслідки кібератаки (див. рис. 2, результат 7–8).

Етап 4. Реалізація моделі забезпечення стійкості відповідно до потенційно можливих умов виконання всіх функцій.

Позначимо через $P_k^{(У)}$ ймовірність успішного здійснення r-ї функції захищеності КІС, тоді для P_k^i будуть виконуватись такі вирази:

$$P_1^i = P_1^{(У)}, \tag{4}$$

$$P_2^i = (1-P_1^{(У)})P_2^{(У)}, \tag{5}$$

$$P_3^i = (1-P_1^{(У)})(1-P_2^{(У)})P_3^{(У)}P_{41}^{(У)}, \tag{6}$$

$$P_4^i = (1-P_1^{(У)})(1-P_2^{(У)})P_3^{(У)}(1-P_{41}^{(У)}) + (1-P_3^{(У)}) + (1-P_{42}^{(У)})P_5^{(У)}P_{61}^{(У)}P_{71}^{(У)}, \tag{7}$$

$$P_5^i = (1-P_1^{(У)})(1-P_2^{(У)})P_3^{(У)}(1-P_{41}^{(У)}) + (1-P_3^{(У)}) + (1-P_{42}^{(У)})(1-P_5^{(У)})P_{62}^{(У)}P_{72}^{(У)}, \tag{8}$$

$$P_6^i = (1-P_1^{(У)})(1-P_2^{(У)})(1-P_3^{(У)})P_{42}^{(У)}. \tag{9}$$

Вираз (4) це найкращий випадок захищеності КІС — він означає, що атака не відбулась, засоби захисту правильні і адекватні, Політики безпеки виконуються, і навіть більше того, прогностична функція моделювання (принцип прогнозування) застосована, ефективно працюють фахівці служби захисту інформації, а працівники, відповідно, виконують усі правила щодо захищеності КІС. У виразах (4) – (9) індекси при ймовірностях відповідають індексам при функціях захищеності КІС з рис. 2 і пояснень до нього. Важливо розуміти, що функція F7 — провал функціонування засобів захисту, оскільки в описі повної функції захисту визначено, що: F7 ліквідація наслідків, F71 локалізація виявленої дії ДЧ на інформацію, F72 локалізація не виявленої дії ДЧ на інформацію [2].

Підведемо підсумки та сформулюємо, що захищеність КІС повністю визначається ймовірністю успішного виконання функцій захисту, що можна описати виразом:

$$P_3 = f(\{P_r^{(У)}\}). \tag{10}$$

Слід розуміти, що ймовірність успішного захисту КІС цілком забезпечується ймовірністю успішного виконання r-ї функції захисту.

Щоб забезпечити достатній рівень захищеності інформації, що дорівнює $P_З^{(Д)}$, необхідно вибрати такі сукупність засобів і заходів захисту, щоб виконувалась кожна з функцій захисту, за яких виконується нерівність:

$$P_3 \geq P_З^{(Д)} \text{ або } f(\{P_r^{(У)}\}) \geq P_З^{(Д)}. \tag{11}$$

Таким чином, можна вважати доведеною повноту множини функцій захисту КІС, але з точністю до умови, що для кожної функції можна вибрати необхідні заходи та засоби захисту.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі проведено аналіз існуючих підходів до забезпечення стійкості КІС, за такими критеріями: надійність, стійкість до фізичних загроз, кібербезпека, оперативність відновлення, гнучкість та адаптивність, координація та управління ризиками, фінансова та ресурсна забезпеченість, сприйнятливість до ДЧ. Проведений детальний аналіз показав, що найбільш сильними аспектами національних підходів є надійність, оперативність відновлення та координація управління ризиками. Водночас слабшими місцями залишаються кібербезпека та фінансова забезпеченість, що вимагає подальших досліджень і вдосконалення методик захисту КІ. Крім того, сприйнятливість до ДЧ постає справжнім викликом, адже у більшості проаналізованих робіт цей критерій є недостатньо дослідженим, особливо в умовах сучасних загроз.

Розроблено модель забезпечення стійкості КІС, яка за допомогою уніфікованого опису функцій захищеності, розрахунку їх ймовірності успішного настання/не настання, можливості локалізації та ліквідації наслідків, дає можливість обрати сукупність засобів і заходів захисту, необхідних для виконання повної множини функцій та дозволяє забезпечити стійке функціонування КІС в умовах впливу внутрішніх та зовнішніх ДЧ.

Продовженням дослідження стане використання запропонованої моделі забезпечення стійкості КІС у майбутньому, після збільшення та удосконалення повноти множини функцій захищеності, що дозволить підвищити рівень кібербезпеки та стійкості (резильєнтності) КІ в умовах воєнного стану та післявоєнного відновлення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. On Critical Infrastructure, Law of Ukraine № 1182-IX. (2024) (Ukraine). https://zakon.rada.gov.ua/go/1882-20.
2. Babak, V. P., & Klyuchnikov, A. A. (2012). Theoretical foundations of information protection. Chernobyl (Kyiv region): Institute of Nuclear Power Plant Safety Problems, NAS of Ukraine.
3. United Nations Office for Disaster Risk Reduction (UNDRR). (2022). *Principles for resilient infrastructure*. https://www.preventionweb.net/publication/principles-resilient-infrastructure
4. Avtushenko, O. S., Gyrda, V. A., Kozhedub, Yu. V., & Maksymets, A. V. (2022). Analysis of methods, methods, mechanisms, and decision theory tools for modeling information protection systems. *Cybersecurity: Education, Science, Technology, 4(16),* 159–171. https://doi.org/10.28925/2663-4023.2022.16.159171
5. Plahotniuk, R. (2023). Ensuring the Resilience of Critical Infrastructure in Ukraine in the Face of Modern Challenges. *Economic Space, (172),* 45–58.
6. Murasov, R., & Melnyk, Y. (2023). Assessing the Security of Cyberspace of Critical Infrastructure Objects in Ukraine. *Modern Information Technologies, (3),* 98–112.
7. Boyko, O. (2023). State policy and public administration in the field of critical infrastructure protection. *Scientific Bulletin of the State University of Infrastructure and Technologies, (4(28)),* 65–79.
8. Sokiran, M. (2023). System of principles of administrative and legal support of the stability of the critical information infrastructure of Ukraine. *Scientific Journals of the Central University of Infrastructure and Technologies, (3(14)),* 85–97.
9. Sukhodolya, O. (2022). *Stability of critical energy infrastructure and community life*. Analytical report of the National Institute of Infrastructure and Technologies.
10. Gordienko, S. G., & Doronin, I. M. (2023). Information and legal aspects of the protection of critical infrastructure of Ukraine. *Legal Bulletin of Ukraine, (5),* 56–67.
11. Shevchenko, N. I., & Plahotniuk, R. V. (2024). Methodological approaches to assessing the stability of the functioning of critical infrastructure facilities in the conditions of a special period of the functioning of the economy of Ukraine. *Reforming the economy and innovative development strategies, 14(2),* 112–126.
12. Yaremenko, O. I., & Strahnitsky, Y. I. (2023). Theoretical approaches to determining the definition of critical infrastructure as an object of state administration. *Bulletin of State Administration, (2),* 47–58.

13. Kovalchuk, I. (2023). Critical Infrastructure Protection: International Experience and Ukrainian Realities. *Strategic Priorities, (1(10))*, 23–38.
14. Kyrylenko, S. P., & Tyshchenko, V. V. (2023). Risk Assessment Models for Critical Infrastructure in Armed Conflict. *Life Safety, (3(9))*, 74–88.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Viktoriia Sydorenko
PhD, Associate Professor,
Associate Professor of IT-Security Academic Department
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID ID: 0000-0002-5910-0837
v.sydorenko@ukr.net

Andrii Maksymets
Senior Engineer
Institute of Special Communication and Information Protection
National Technical University of Ukraine
Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine
ORCID ID:0000-0003-3551-0628
andy.west.corp@gmail.com

MODEL OF ENSURING THE STABILITY OF CRITICAL INFORMATION SYSTEMS UNDER THE INFLUENCE OF INTERNAL AND EXTERNAL DESTABILIZING FACTORS

Abstract. The modern critical infrastructure (CI) of the state consists of information, energy, transport and other strategically important facilities that ensure the continuous functioning of society and the economy. A special role in its protection is played by critical information systems (CIS), which provide processing, storage and transmission of data necessary for the management of key sectors/subsectors of the infrastructure. In the context of increasing cyber threats, military challenges and destabilizing factors (DF), the determining factor in the security and stability of the functioning of the state's CI is ensuring the stability of the CIS. The article analyzes existing approaches to ensuring stability according to key criteria: reliability, resistance to physical threats, cybersecurity, prompt recovery, flexibility and adaptability, coordination of risk management, financial and resource security, susceptibility to DF. The strengths and weaknesses of national approaches have been identified, and the need to take into account the criterion of susceptibility to DF has been established, since its impact remains insufficiently studied, especially in the context of modern threats. A model for ensuring the stability of CIS has been developed, which allows critical systems to function in a normal mode, adapt to constantly changing conditions, withstand and quickly recover from the impact of internal and external DF. Subsequent research will be aimed at improving the completeness of the set of security functions, which will allow to increase the level of cybersecurity and stability (resilience) of CIS in conditions of martial law and post-war recovery.

Keywords: critical infrastructure; critical infrastructure facilities; cybersecurity; critical information systems; stability; ensuring stability; protection functions; destabilizing factors.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. On Critical Infrastructure, Law of Ukraine № 1182-IX. (2024) (Ukraine). https://zakon.rada.gov.ua/go/1882-20.
2. Babak, V. P., & Klyuchnikov, A. A. (2012). Theoretical foundations of information protection. Chernobyl (Kyiv region): Institute of Nuclear Power Plant Safety Problems, NAS of Ukraine.
3. United Nations Office for Disaster Risk Reduction (UNDRR). (2022). *Principles for resilient infrastructure.* https://www.preventionweb.net/publication/principles-resilient-infrastructure
4. Avtushenko, O. S., Gyrda, V. A., Kozhedub, Yu. V., & Maksymets, A. V. (2022). Analysis of methods, methods, mechanisms, and decision theory tools for modeling information protection systems. *Cybersecurity: Education, Science, Technology, 4(16),* 159–171. https://doi.org/10.28925/2663-4023.2022.16.159171
5. Plahotniuk, R. (2023). Ensuring the Resilience of Critical Infrastructure in Ukraine in the Face of Modern Challenges. *Economic Space, (172),* 45–58.

6. Murasov, R., & Melnyk, Y. (2023). Assessing the Security of Cyberspace of Critical Infrastructure Objects in Ukraine. *Modern Information Technologies, (3),* 98–112.
7. Boyko, O. (2023). State policy and public administration in the field of critical infrastructure protection. *Scientific Bulletin of the State University of Infrastructure and Technologies, (4(28)),* 65–79.
8. Sokiran, M. (2023). System of principles of administrative and legal support of the stability of the critical information infrastructure of Ukraine. *Scientific Journals of the Central University of Infrastructure and Technologies, (3(14)),* 85–97.
9. Sukhodolya, O. (2022). *Stability of critical energy infrastructure and community life.* Analytical report of the National Institute of Infrastructure and Technologies.
10. Gordienko, S. G., & Doronin, I. M. (2023). Information and legal aspects of the protection of critical infrastructure of Ukraine. *Legal Bulletin of Ukraine, (5),* 56–67.
11. Shevchenko, N. I., & Plahotniuk, R. V. (2024). Methodological approaches to assessing the stability of the functioning of critical infrastructure facilities in the conditions of a special period of the functioning of the economy of Ukraine. *Reforming the economy and innovative development strategies, 14(2),* 112–126.
12. Yaremenko, O. I., & Strahnitsky, Y. I. (2023). Theoretical approaches to determining the definition of critical infrastructure as an object of state administration. *Bulletin of State Administration, (2),* 47–58.
13. Kovalchuk, I. (2023). Critical Infrastructure Protection: International Experience and Ukrainian Realities. *Strategic Priorities, (1(10)),* 23–38.
14. Kyrylenko, S. P., & Tyshchenko, V. V. (2023). Risk Assessment Models for Critical Infrastructure in Armed Conflict. *Life Safety, (3(9)),* 74–88.