УДК 004.415.056.5(075)
DOI: https://doi.org/10.17721/ISTS.2024.7.11-23

Сергій ТОЛЮПА, д-р техн. наук., проф
ORCID ID: 000-0002-1919-9174
e-mail: tolupa@i.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Анатолій ШЕВЧЕНКО, бригадний генерал
ORCID ID: 0000-0003-2723-0378
e-mail: anatolii.shevchenko@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Андрій КУЛЬКО, асп.
ORCID ID:0009-0006-1185-0774
e-mail: kulko452@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КРИТИЧНИХ ІНФРАСТРУКТУР

В с т у п . *Стрімкий розвиток інформаційних технологій за останні два десятиліття вплинув на функціонування особливостей об'єктів критичної інфраструктури. Ці технології почали використовувати не лише як засіб обміну та оброблення інформації, а і як інструмент для заподіяння шкоди. Захист державних інтересів у політичному контексті є першоосновою забезпечення національної безпеки країни, що пояснює необхідність створення та постійний розвиток потужної кібернетичної безпеки. Об'єкти критичної інфраструктури є складними, просторово розподіленими, багатокомпонентними системами, стійка робота яких критично важлива для функціонування економіки та життєдіяльності суспільства. Вони мають багаторівневу структуру, яка включає: рівень технічних компонентів; соціальний рівень; організаційний рівень і рівень державного управління.*

М е т о д и . *Порівняно інформаційні системи і за допомогою методу оцінювання дослідження захищеності систем покращенно й оптимізовано систему захисту інформації.*

Р е з у л ь т а т и . *Результатом роботи є дослідження критичних інфраструктур як соціотехнічних систем, що потребують оцінювання складних взаємодій між технічними, соціальними й організаційними рівнями системи. Тому критичну інфрастуктуру варто розглядати як єдине ціле. Необхідно наголошувати на одночасному спільному розгляді технічних, організаційних і соціальних факторів, що визначають стан системи та динаміку її розвитку. Щоб забезпечити безпеку таких систем, потрібно вийти за межі традиційного підходу до оцінювання проєктних ризиків і перейти до нової парадигми, що ґрунтується на забезпеченні безпеки критичної інфраструктури за критерієм стійкості до позапроєктних впливів. У зв'язку з необхідністю включити до розгляду позапроєктні аварії на критичній інфраструктурі, межі досліджень мають бути суттєво розширені. Заходи щодо забезпечення безпеки повинні бути спрямовані не лише на створення захисних бар'єрів, покликаних попередити реалізацію проєктних аварій, що постулюються, але і на підвищення стійкості та живучості критичної інфраструктури у разі позапроєктних впливів, тобто зосередитися на запобіганні великомасштабним катастрофам і тривалим перервам у функціонуванні, а побудова багатокритеріальної моделі для оцінювання рівня захищеності об'єктів критичної інфраструктури дасть повнішу картину стану об'єкта критичної інфраструктури.*

В и с н о в к и . *Наявні нині методики безпеки технічних систем розроблено для систем, що мають чіткі межі і добре визначені переліки загроз. Для цих систем можуть бути створені бази даних зі статистики аварій, які дозволяють кількісно оцінювати та верифікувати моделі. Вказані методики, що базуються на побудові сценарних "дерев" (моделі типу "дерево" подій, "дерево" відмов), розроблені без урахування позапроєктних впливів і не дозволяють належно врахувати складність критичних інфраструктур, функціонування яких визначається взаємодією технічних, організаційних і соціальних. факторів.*

К л ю ч о в і с л о в а : *кібербезпека, об'єкти критичної інфраструктури, інформаційні системи, стійкість, кіберпотужність.*

Вступ

У багатьох країнах реалізується концепція критичної інфраструктури, яка дозволяє зосередитися на системах, мережах та окремих об'єктах, руйнування чи порушення роботи яких матиме серйозні негативні наслідки для національної

ISSN 2707-1758

безпеки. Стрімкий розвиток інформаційно-комунікаційних технологій за останні два десятиліття вплинув на функціонування особливостей об'єктів критичної інфраструктури. Ці технології почали використовувати не лише як засіб обміну й оброблення інформації, а і як інструмент для заподіяння шкоди. Захист державних інтересів у політичному контексті є першоосновою гарантування національної безпеки країни, що пояснює необхідність створення та постійний розвиток потужної кібернетичної безпеки.

Об'єкти критичної інфраструктури є складними, просторово розподіленими, багатокомпонентними системами, стійка робота яких критично важлива для функціонування економіки та життєдіяльності суспільства. Об'єкти критичної інфраструктури (ОКІ) мають багаторівневу структуру, яка включає: рівень технічних компонентів (машини, обладнання й апаратура); соціальний рівень (персонал, що обслуговує технічні компоненти критичної інфраструктури); організаційний рівень (взаємодія служб компанії, що експлуатує ОКІ) та рівень державного управління (нормативні та органи контролю, які здійснюють нагляд і державне регулювання у сфері діяльності КІ). Складність критичних інфраструктур (КІ) обумовлено: складністю їхньої структури (складними взаємозалежностями та нелінійними зв'язками між компонентами й рівнями системи, а також між різними компонентами КІ); складним характером явищ і процесів, що спостерігаються в ході експлуатації ОКІ (Бірюков, & Кондратов, 2012).

Метою статті є те, що ОКІ представляють собою технічні об'єкти, на яких зберігають, переробляють / перетворюють або транспортують / передають небезпечні речовини, енергії та / або інформаційні потоки. Ці об'єкти можуть бути джерелами важких аварій і катастроф, які є предметом традиційного аналізу ризиків, на основі якого будують карти ризиків для територій розміщення об'єктів критичних інфраструктур і приймають рішення про будівництво або модернізацію останніх.

Огляд літератури. Нині розв'язання питань забезпечення безпеки критичної інфраструктури та управління станом їхньої захищеності описано в роботах вітчизняних і зарубіжних дослідників, а саме: В. Л. Бурячка, С. С. Бучика, С. О. Гнатюка, С. П. Євсеєва, С. В. Казмирчука, О. Г. Корченка, О. О. Кузнецова, І. Ю. Субача, T. Ptaceka, G. Elmasry, P. Albers, O. Camp та ін.

Процес розвитку та впровадження новітніх інформаційних технологій забезпечують безпрецедентні умови для накопичення і використання інформації, а також створюють фундаментальну залежність від їхнього нормального функціонування всіх сфер життєдіяльності суспільства та держави: економіки, політики, сфери національної та міжнародної безпеки тощо. Така залежність стає вразливим місцем у функціонуванні систем і об'єктів критичних національних інфраструктур і дає можливість негативно налаштованим елементам й угрупованням скористатися нею для реалізації протиправних дій у кібернетичному просторі шляхом порушення цілісності, доступності й конфіденційності інформації та нанесення шкоди інформаційним ресурсам й інформаційним системам. У цьому разі особливе занепокоєння викликає можливість застосування інформаційних технологій у кібернетичному просторі в інтересах здійснення воєнно-політичного та силового протиборства, тероризму і проведення хакерських атак, що нині досить актуально, враховуючи воєнний стан (Довгань, 2013, с. 17–20).

Інформаційна сфера, яка є одним з основних факторів розвитку сучасного суспільства, активно впливає на стан соціально-політичної та економічної галузей діяльності. Складність процесів, які відбуваються в розподілених інформаційних системах (РІС), постійно зростає. Це призводить до того, що РІС, які використовують для зберігання інформації, обміну інформацією та розв'язання різного типу завдань у всіх сферах людської діяльності, можуть стати об'єктом зловживань.

Кожна розподілена інформаційна система ОКІ має свої особливості, які обумовлені сферою її застосування. Важливість і відповідальність задач, розв'язуваних за допомогою розподілених систем у реальному масштабі часу, обумовили високі вимоги до надійності цих систем, у яких, найчастіше, неможливе проведення технічного обслуговування під час функціонування, і відмова всієї розподіленої інформаційної системи, або її окремих компонентів може призвести до негативних наслідків.

Дослідження сучасних науково обґрунтованих підходів підвищення ефективності складних технічних систем дозволили дійти висновку, що за останні роки сформувався новий пріоритетний підхід, який пов'язаний із забезпеченням в інформаційній системі властивості функціональної стійкості ОКІ.

Властивість функціональної стійкості КІ розглядають як можливість складної технічної системи, до якої належать усі без винятку компоненти КІ, успішно завершити поставлене завдання за регламентованої кількості змін у стані

самої системи, тобто зберегти її працездатність після прояву припустимої кількості відмов і зовнішніх дестабілізувальних впливів (Гнатюк, & Лядовська, 2013, с. 55–57).

Функціональна стійкість спрямована, в першу чергу, на поліпшення характеристик відмовостійкості й живучості, але не обов'язково показників надійності окремих комплектувальних елементів. Оскільки теорія функціональної стійкості перебуває у стадії розвитку, то формування основних показників функціональної стійкості є важливим напрямом наукових досліджень.

Проблему функціональної стійкості інформаційних систем досліджували в роботах О. А. Машкова, О. В. Барабаша, Д. М. Обідіна, Ю. В. Кравченка, О. А. Кононова. Питання відмовостійкості систем аналізували в роботах А. А. Авіжиєніса, В. А. Машкова, О. Ю. Ільїна, Ю. М. Коростіля, В. А. Савченка та інших учених.

Методи

За допомогою методу дослідження порівняно інформаційні системи. Методом оцінювання дослідження захищеності систем покращенно й оптимізовано систему захисту інформації.

Результати

Наявність тісних взаємозв'язків між компонентами КІ є їхньою принципово важливою особливістю, яка визначально впливає на характер їхнього функціонування у штатних і позаштатних ситуаціях. З одного боку, пов'язаність елементів КІ підвищує їхню ефективність, дозволяючи раціонально використовувати та перерозподіляти наявні ресурси й потужності, а з іншого – робить їх схильними до великомасштабних катастроф, величезний розмір збитків від яких не дозволяє нехтувати ними, незважаючи на низьку ймовірність реалізації ризиків.

Щодо аналізу ризиків взаємопов'язаних інфраструктурних систем, то доводиться мати справу з двосторонніми залежностями між компонентами КІ, тому прийнято говорити про взаємозалежність елементів КІ. Ці взаємозалежності існують як для елементів, що належать до однієї інфраструктури, так і для елементів різних інфраструктур. В останньому випадку говорять про взаємозалежності між різними ОКІ (Юдін, & Пирогов, 2016, с. 88).

Наявність сильних зв'язків між елементами КІ робить їх схильними до каскадних сценаріїв аварій, які охоплюють велику кількість об'єктів інфраструктури, причому хід реалізації аварії визначається структурою зв'язків між елементами. Крім масштабів потенційних аварій, наявність внутрішньо- та міжінфраструктурних залежностей визначально впливає на динаміку поширення аварій, призводячи до реалізації комбінованих механізмів досягнення граничних станів, різкої інтенсифікації процесів деградації та потоку відмов елементів КІ.

Через складну структуру ОКІ та складний характер взаємодій між значною кількістю елементів можливості сценарного аналізу за допомогою традиційного інструментарію (дерев подій, дерев відмов, баєсових мереж, нейронних мереж) виявляються обмеженими. Для опису розвитку збурень у критичних інфраструктурах застосовують мережні моделі, які активно використовують математичний апарат теорії графів. Мережі є надзвичайно гнучкою абстракцією, яка може широко застосовуватися у вивченні інфраструктурних систем. Причому може бути побудована ієрархія математичних моделей різної складності, що дозволяють описати різні аспекти ризиків інфраструктурних систем щодо можливих ініціюючих впливів. За допомогою зазначених моделей вдається описати багато властивостей та особливостей мережних систем: хаос, самоорганізація, статистичні розподіли, критичність.

Прийнято виокремлювати три типи взаємозалежностей між компонентами інфраструктурних систем, які можуть бути між компонентами й однієї інфраструктури, і різних інфраструктур.

Фізичні взаємозв'язки, які спостерігають, коли речовина, енергія або інформація фізично передається від одного компонента до іншого компонента (тої чи іншої) інфраструктури. У цьому разі вихідний продукт, який створюється або переробляється однією інфраструктурою, використовується як вхідний продукт компонентом іншої інфраструктури. Очевидно, що аварії в компонентах однієї КІ можуть викликати каскади відмов, що поширюються на компоненти іншої КІ.

Кібервзаємозалежність є інформаційно залежною, якщо стан її елементів залежить від інформації, що передається інформаційною мережею. У зв'язку зі швидким розвитком інформаційних технологій, система управління будь-якою системою залежить від якості роботи інформаційної мережі.

Територіальні взаємозалежності – інфраструктури, компоненти яких розміщені територіально безпосередньо близько один від одного і можуть зазнавати безпосереднього впливу у надзвичайних ситуаціях на компонентах іншої інфраструктури (Бурячок, & Толюпа, 2015, с. 288).

Особливість сучасних КІ полягає в тому, що вони стають транскордонними, а в деяких випадках – глобальними. Просторова довжина КІ,

ISSN 2707-1758

поряд із наявністю тісних взаємозв'язків між ними, робить їхнє функціонування залежним від величезної кількості факторів, пов'язаних зі станом природно-техногенно-соціального середовища в різних регіонах світу. Значний обсяг небезпечних речовин, енергії та інформації, що зберігаються, транспортуються та переробляються критичними інфраструктурами, а також їхня величезна роль в економіці та житті людей, зумовлюють можливість великомасштабних аварій на ОКІ та тяжкість наслідків, що виникають у разі таких аварій, для населення й об'єктів економіки. Складність критичних інфраструктур значно перешкоджає створенню ефективних систем захисту, оскільки стає практично неможливим провести детальний сценарний аналіз системи, виявити всі значущі небезпечні сценарії та визначити комплекс заходів і бар'єрів захисту, спрямованих на парирування всіх можливих загроз.

Разом із тим аналіз практики, що склалася у сфері функціонування ОКІ, свідчить, що їхнє проєктування, будівництво й експлуатацію *здійснюють* відповідно до традиційної парадигми технічного забезпечення безпеки технічних систем (ТЗ). Ця парадигма передбачає: аналіз можливих сценаріїв розвитку відмов у системі; ідентифікацію найбільш значущих сценаріїв; створення захисних бар'єрів, вкладених у попередження цих сценаріїв.

Структурна складність ОКІ, їхня винятково важлива роль у життєдіяльності людей і функціонуванні економіки, а також тяжкість наслідків, що неминуче виникають у разі аварій на КІ, повинні визначити особливий порядок і спеціальні вимоги у сфері забезпечення їхньої безпеки. Сучасні тенденції у сфері забезпечення безпеки критичних інфраструктур передбачають формування нової парадигми, яка має доповнити традиційні зусилля щодо забезпечення безпеки КІ системою заходів, спрямованих на підвищення їхньої стійкості до можливих екстремальних впливів.

Врахування особливостей критичних інфраструктур у розробленні стратегії забезпечення їхньої захищеності. Як зазначено, сучасні об'єкти критичної інфраструктури є складними технологічними системами, функціонування яких визначається взаємодією технічних, соціальних, організаційних та управлінських факторів. Традиційний підхід до моделювання технологічних систем, що широко використовується у забезпеченні їхньої безпеки, передбачає декомпозицію системи на технічну, соціальну й організаційну підсистеми, які потім розглядають окремо в межах відповідних дисциплін. У такому випадку не враховують ні взаємні впливи підсистем, ні їхню взаємодію на системному рівні.

Варто зазначити, що зусилля захисту ОКІ традиційно фокусуються на технічних аспектах. Завдяки цьому досягнуто значного прогресу у сфері забезпечення надійності технічних компонентів КІ. Однак можливості цього підходу близькі до вичерпання. Це пов'язано з тим, що КІ більше неспроможні розглядатися як переважно технічні системи, а стають дедалі більше техносоціальними системами.

Завдяки бурхливому розвитку інформаційних технологій в останні десятиліття ОКІ стають все складнішими. Це означає, що в оцінюванні безпеки КІ з'являється дуже багато чинників, які підлягають обліку. Це відбувається внаслідок складних нелінійних взаємодій між компонентами КІ, сильної зв'язаності між різними підсистемами, а також того, що КІ та навколишнє середовище починають змінюватися швидше, ніж вони можуть бути описані й досліджені. Тому виникає ситуація нестачі інформації про КІ і, отже, обмеженість можливостей прогнозування їхньої поведінки й управління ними. Причому на певних режимах неможливо детально описати закони функціонування КІ й розробити правила управління.

Відмінність між повністю визначеними та не повністю визначеними системами стає надзвичайно важливою у розробці комплексу заходів щодо безпеки. Особливість деяких систем полягає у тому, що виявляється неможливим повний опис їхньої поведінки та прогнозування їхнього стану за різних умов і на різних режимах експлуатації. Внаслідок цього для таких складних систем, як критичні інфраструктури, практично неможливо створити закритий перелік проєктних впливів, яким система може піддаватися протягом її експлуатації. У зв'язку із цим традиційна стратегія забезпечення безпеки КІ, заснована на розробленні комплексу захисних бар'єрів, покликаних парирувати проєктні впливи, не може бути успішною.

Тому необхідно розробити методи забезпечення безпеки, що дають змогу мати справу з недовизначеними системами. Потрібно використовувати підходи, що розвиваються в межах нового бачення, що отримало назву *теорія забезпечення стійкості технічних систем до екстремальних впливів* (Resilience Engineering). Цей напрям концентрує увагу на створенні систем, які здатні: продовжувати (принаймні частково) виконувати запропоновані ним функції після того, як вони отримають пошкодження, зазнавши позапроєктних впливів; досить швидко відновлювати свій початковий функціональний рівень після позапроєктного впливу.

Принципи забезпечення стійкості критичної інфраструктури. Стійкість до екстремальних впливів є ключовим поняттям у випадках позапроєктних впливів і позапроєктних сценаріїв аварій у складних технічних системах, до яких належать КІ. Сучасні інфраструктурні системи (системи водо-, електро- і газопостачання, транспортні, телекомунікаційні мережі) стають дедалі складнішими, взаємозалежними, динамічно змінюваними, дедалі більше виявляють нелінійні властивості. У зв'язку із цим стає неможливо заздалегідь – у процесі проєктування – спрогнозувати багато несприятливих подій або їхнє поєднання, а також сценарії відмов, які вони ініціюють, і, отже, заздалегідь передбачити повний комплекс захисних заходів, що дозволяє побудувати системи захисту від вичерпного переліку позапроєктних впливів / сценаріїв. На перший план у такому разі виходить завдання підвищення стійкості інфраструктурних систем до проєктних впливів. Традиційні заходи щодо зниження ризику та забезпечення безпеки, що передбачають створення систем захисту від проєктних впливів та аварій, повинні доповнюватися заходами щодо забезпечення стійкості до позапроєктних впливів та аварій. У такій постановці, крім традиційних питань, на які доводиться відповідати під час забезпечення безпеки технічних систем, – "які проєктні сценарії відмови можуть відбутися в системі?" і "яких захисних заходів потрібно вжити, щоб запобігти цим сценаріям?", повинні доповнюватися питанням: "Що потрібно зробити, щоб забезпечити стійкість системи стосовно заздалегідь невідомих екстремальних впливів?".

Під стійкістю ТЗ до екстремальних впливів розуміють здатність системи, що зазнала позапроєктного впливу, підтримувати певний рівень експлуатаційних характеристик і повертатися на нормальний рівень функціонування (тобто відновлюватися) протягом певного інтервалу часу. Система, стійка до екстремальних впливів, має відповідати таким вимогам:

- живучість, тобто здатність функціонувати та певною мірою виконувати запропоновані функції за наявності локальних ушкоджень, що виникають унаслідок екстремальних впливів;
- надмірність, тобто наявність резервних зв'язків, альтернативних шляхів передачі навантаження та дублювальних елементів, які можуть бути задіяні у надзвичайній ситуації;
- ресурсозабезпеченість, тобто наявність у системі ресурсів, які можуть бути задіяні у разі екстремальної дії;
- здатність до швидкого відновлення, яка визначається інтервалом часу, протягом якого пошкодження можуть бути ліквідовані, тобто система буде відновлена і вийде на номінальний рівень.

Інфраструктуру вважають стійкою, якщо їй властиві низька ймовірність відмови, незначна шкода, що реалізується у разі відмови (кількість постраждалих, економічна й екологічна шкода) та малий час відновлення системи (повернення системи у нормальний стан із виходом у штатний режим експлуатації та на штатну потужність / продуктивність).

Формування багатокритеріальної моделі для оцінювання рівня захищеності об'єктів критичної інфраструктури. До багатокритеріального класу належать такі завдання: оцінювання рівня захисту об'єктів критичної інфраструктури від ризику стороннього кібервпливу. Для колегіального розв'язання цих завдань в умовах невизначеності та конфліктності між існуючими методами математичного моделювання, методами формування та дослідження узагальнених показників якості з використанням графоаналітичних та подібних підходів, експертними методами розв'язання складних завдань оцінювання та вибору будь-яких об'єктів, зокрема і спеціальних об'єктів призначення, а також аналізу та прогнозування ситуацій із великою кількістю суттєвих факторів, найраціональнішими та визначальними є експертні методи. Вони дають можливість глибше дослідити явища, які суттєво впливають на рівень захисту як держави в цілому, так і її окремих об'єктів інформаційної та кібернетичної інфраструктури від впливу внутрішніх і зовнішніх кібернетичних втручань і загроз, визначити найбільш важливе і значуще в цих процесах, не оминаючи тих деталей і взаємозв'язків, без яких неможливо побудувати модель досліджуваної проблеми. Метою цієї моделі є оцінка готовності об'єктів інформаційної та кіберінетичної інфраструктури для безпечного функціонування в умовах стороннього кібервпливу та встановлення вимог до власних систем кібербезпеки на основі так званого "індексу кіберпотужності". Його величина залежить від виявлених відхилень від стандартного режиму роботи систем і мереж інтелектуальної власності й інформаційних технологій, а також апаратного та програмного забезпечення за допомогою аналізу чотирьох основних категорій, кожна з яких включає багато узагальнених показників, а саме:

- існуюча нормативно-правова база; ставлення влади до забезпечення кібербезпеки; наявність національної стратегії кібербезпеки (доктрини

ISSN 2707-1758

тощо); наявність нормативно-правового забезпечення сфери кібербезпеки; наявність міжнародних зобов'язань країни у сфері кібербезпеки; наявність співпраці між державними та приватними структурами у сфері кібербезпеки; стан розвитку політики кіберзахисту; рівень активності керівництва країни щодо кіберзахисту; рівень активності інформаційної та кібернетичної інфраструктури з питань кіберзахисту;

- умови соціально-економічного розвитку держави; рівень освіти, науки і техніки; частка населення з вищою освітою; частка населення зі знанням іноземної мови, зокрема й англійської; частка дослідно-конструкторських робіт із кібербезпеки; рівень виконання науково-дослідної та дослідницько-конструкторської роботи (дослідження та розробки) інженерно-технічним персоналом; рівень розвитку інноваційного середовища; стан витрат на науково-дослідну та дослідницько-конструкторську роботу; стан патентної та раціоналізаторської роботи (кількість патентів); стан залучення приватного та венчурного капіталу;
- наявність розгалуженої технологічної інфраструктури: якісний стан технологічної інфраструктури; рівень використання мережі інтернет (включно з розподілом точок доступу Wi-Fi); рівень використання мобільного зв'язку та соціальних мереж; рівень упровадження технологічної інфраструктури; рівень фінансування впровадження інформаційно-комунікаційних технологій (щодо валового внутрішнього продукту); рівень безпеки послуг;
- ступінь використання ІКТ та інформаційно-технологічного забезпечення у розвитку інформаційного суспільства; використання ІКТ у корпоративних мережах, інтелектуальних транспортних системах; використання інтернет-ресурсів для розміщення пропозицій щодо надання товарів і послуг; замовлення товарів і послуг.

На основі наведених показників, які характеризують здатність об'єктів критичної інфраструктури забезпечувати кібербезпеку та підтримувати безпечні функції власних об'єктів інформаційної та кібернетичної інфраструктури, можна побудувати ієрархічну схему їхніх показників (табл. 1), у якій значення попереднього рівня "I" визначається значеннями відповідних показників 1-го рівня. Цю категорію приведено у відповідність із набором специфічних показників, які у свою чергу представлено елементарними характеристиками, які називають індексами.

Таблиця 1

Ієрархічна схема рівня критичності кібербезпеки

Рівень 1–4	Категорії	Індикатори	Індекси
Критичність кібербезпеки, якій згідно з вихідними параметрами присвоюють рівень	Наявність нормативної бази	Ставлення керівництва держави до питань кібербезпеки	$A1_1, A1_2, A1_3, A1_4$
		Стан розвитку політики кіберзахисту	$A2_1, A2_2$
	Стан соціально-економічного розвитку держави	Освітній, науково-технічний рівень	$B1_1, B1_2, B1_3, B1_4$
		Іноваційне середовище та рівень розвитку	$B2_1, B2_2$ $B2_3$
	Наявність розгалуженої технологічної інфраструктури	Якісний стан технологічної інфраструктури	$C1_1, C1_2$
		Рівень упровадження технологічної інфраструктури	$C2_1, C2_2$
	Ступінь використання ІКТ та ІБ	Використання інформаційно-комунікаційних технологій у локальній мережі	$D1_1, D1_2$
		Використання інтернет-ресурсів у комерційній діяльності	$D2_1, D2_2$

Кожній категорії рівня 2, кожному показнику рівня 3 та кожному показнику рівня 4 ієрархії за правилом, наприклад за допомогою експертного опитування, може бути присвоєно певний номер (табл. 2). Обов'язковою умовою такого присвоєння є врахування того, що вага категорій, показників та індексів одного рівня завжди має дорівнювати одиниці.

Значення категорій і показників якості визначають способом наведеним у табл. 3.

Таблиця 2

Значення вагових коефіцієнтів категорій і показників рівня критичності КС

Позначення категорій і показників критичності	Вагові коефіцієнти категорій і позначення показників	Вагові коефіцієнти категорій і показників	Сума вагових коефіцієнтів показників
Наявність нормативної бази	g_1	0,26	
Ставлення держави до питань кібербезпеки	a_1	0,75	1,0
Розроблення політики кіберзахисту держави	a_2	0,25	
Стан соціально-економічного розвитку держави	g_2	0,25	
Освітній, науково-технічний рівень	b_1	0,68	1,0
Рівень розвитку іноваційного середовища	b_2	0,32	
Наявність розгалуженої технологічної інфраструктури	g_3	0,26	
Якісний стан технологічної інфраструктури	c_1	0,22	1,0
Рівень упровадження технологічної інфраструктури	c_2	0,78	
Ступінь використання ІКТ та ІБ	g_3	0,23	
БІКТ	d_1	0,71	1,0
Використання ресурсів інтернету	d_2	0,29	

Таблиця 3

Порядок визначення категорій і показників рівня критичної кібербезпеки

Наявність нормативно-правової бази – $\begin{cases} a_1 - < The\ attitude\ of\ the\ leadership\ to\ cybersecurity > \\ +a_2 - < The\ state\ of\ cyber\ defense\ policy\ development\ > \end{cases}$, де a_1 і a_2 – вагові коефіцієнти відповідних ідентифікаторів рівня 3, де $a_1 + a_2 = 1$	(1)
Ставлення керівництва до кібербезпеки – $a1_1 \cdot A1_1 + a1_2 \cdot A1_2 + a1_3 \cdot A1_3 + a1_4 \cdot A1_4 = \sum_i a1_i \cdot A1_i\,; i = \overline{1,4}$, де $a1_1, a1_2, a1_3, a1_4$ – вагові коефіцієнти рівня 3 для $A1_1, A1_2, A1_3\ \ A1_4$; $a1_1 + a1_2 + a1_3 + a1_4 = \sum_i a1_i = 1$	(2)
Стан розвитку політики кіберзахисту – $a2_1 \cdot A2_1 + a2_2 \cdot A2_2 = \sum_i a2_i \cdot A2_i\,; i = \overline{1,2}$, де $a2_1, a2_2$– вагові коефіцієнти відповідних показників рівня 3 для $A2_1\ and\ A2_2$,; $a2_1 + a2_2 = \sum_i a2_i = 1$	(3)
Стан соціально-економічного розвитку – $\begin{cases} b_1 - (\text{level of education, science and technology}) \\ b2 - (\text{the level of development of the innovation environment}) \end{cases}$, де $b_1\ and\ b_2$ – вагові коефіцієнти відповідних показників рівня 3 $cb_1 + b_2 = 1$	(4)
Рівень освіти, науки і техніки – . $b1_1 \cdot B1_1 + b1_2 \cdot B1_2 + b1_3 \cdot B1_3 + b1_4 \cdot B1_4 = \sum_i b1_i \cdot B1_i\,; i = \overline{1,4}$, де $b1_1, b1_2, b1_3, b1_4$ – вагові коефіцієнти відповідних показників рівня 4 для $B1_1, B1_2, B1_3\ and\ B1_4$; $b1_1 + b1_2 + b1_3 + b1_4 = \sum_i b1_i = 1$	(5)

ISSN 2707-1758

Закінчення табл. 3

Рівень розвитку інноваційного середовища – $b2_1 \cdot B2_1 + b2_2 \cdot B2_2 + b2_3 \cdot B2_3 = \sum_i b2_i \cdot B2_i\,; i = \overline{1,3}$, де $b2_1, b2_2, b2_3$ – вагові коефіцієнти відповідних показників рівня 4 для $B2_1, B2_2, B2_3$; $$b2_1 + b2_2 + b2_3 = \sum_i b1_i = 1$$	(6)
Наявність розгалуженої технологічної інфраструктури – $\begin{cases} c_1 - \text{(qualitative state of technological infrastructure)} \\ c_2 - \text{(the level of implementation of technology infrastructure)'} \end{cases}$ де c_1 та c_2 – вагові коефіцієнти відповідних ідентифікаторів рівня 3 з $c_1 + c_2 = 1$	(7)
Стан розвитку політики кіберзахисту – $c1_1 \cdot C1_1 + c1_2 \cdot C1_2 = \sum_i c1_i \cdot C1_i\,; i = \overline{1,2}$, де $c1_1, c1_2$ – вагові коефіцієнти відповідних показників рівня 4 для $C1_1\ and\ C1_2$,; $$c1_1 + c1_2 = \sum_i c1_i = 1$$	(8)
Рівень реалізації технологічної інфраструктури – $c2_1 \cdot C2_1 + c2_2 \cdot C2_2 = \sum_i c2_i \cdot C2_i\,; i = \overline{1,2}$, де $c2_1, c2_2$ – вагові коефіцієнти відповідних показників 4 рівня для $C2_1\ and\ C2_2$,; $$c2_1 + c2_2 = \sum_i c2_i = 1$$	(9)
Ступінь використання ІКТ та ІБ – $\begin{cases} d_1 - \text{(use of ICT)} \\ d_2 - \text{(Using the Internet)'} \end{cases}$ де d_1 і d_2 – вагові коефіцієнти відповідних ідентифікаторів рівня 3 з $d_1 + d_2 = 1$	(10)
Використання ІКТ – $d1_1 \cdot D1_1 + d1_2 \cdot D1_2 = \sum_i d1_i \cdot D1_i\,; i = \overline{1,2}$, де $d1_1, d1_2$ – вагові коефіцієнти відповідних показників рівня 4 для $D1_1\ and\ D1_2$,; $$d1_1 + d1_2 = \sum_i d1_i = 1$$	(11)
Застосування інтернету – $d2_1 \cdot D2_1 + d2_2 \cdot D2_2 = \sum_i d2_i \cdot D2_i\,; i = \overline{1,2}$, де $d2_1, d2_2$ – вагові коефіцієнти відповідних показників рівня 4 для $D2_1\ and\ D2_2$,; $$d2_1 + d2_2 = \sum_i d2_i = 1$$	(12)

Використовуючи формули (2), (3), (5), (6), (8), (9), (11) і (12) з табл. 3 та застосовуючи дані анкети експерта, який регулює значення індексів та їхніх вагових коефіцієнтів, можна розрахувати значення показників рівня 3, таких як:

- створення державного керівництва для забезпечення кібербезпеки;
- стан розробки політики кіберзахисту;
- освітній, науково-технічний рівень;
- рівень розвитку інноваційного середовища;
- якісний стан технологічної інфраструктури;
- рівень фінансування технологічної інфраструктури;
- використання інформаційно-комунікаційних технологій;
- використання інтернет-ресурсів.

Експертна анкета для оцінювання рівня критичності кібербезпеки за параметрами наявності нормативно-правової бази на тему ставлення влади до питань кібербезпеки

Для визначення значення індексів експерт відповідає на такі питання:

- *$A1_1$ – чи має держава національну стратегію кібербезпеки (доктрину, концепцію тощо)?*
- *$A1_2$ – чи функціонує в державі система нормативного забезпечення кібербезпеки?*
- *$A1_3$ – чи виконуються міжнародні зобов'язання у сфері кібербезпеки на державному рівні?*
- *$A1_4$ – чи існує співпраця державних і приватних структур у сфері кібербезпеки?*

Відповіді на перше запитання:

- стратегія зрозуміла з чітко визначеними цілями та часовими межами;
- стратегія нечітка, незрозуміла або формальна;
- стратегія тільки розробляється;
- стратегії немає.

Відповідні значення показників 1,0; 0,4; 0,2; 0.

Ваговий коефіцієнт $a1_1$, що відповідає показнику $A1_1$, має значення 0,4.

Відповіді на друге запитання:

- законодавство охоплює всі аспекти кібербезпеки;
- є певні закони, але лише деякі з них виконуються;
- є певні закони, але жоден із них не виконується;
- законодавство не сформоване.

Відповідні значення показників 1,0; 0,6; 0,2; 0.

Ваговий коефіцієнт $a1_2$, що відповідає показнику $A1_2$, має значення 0,3.

Відповіді на третє запитання:

- держава практично виконує міжнародні договори;

- держава ратифікувала підписані міжнародні договори;
- держава приєдналася до міжнародних договорів;
- держава не має підписаних міжнародних зобов'язань.

Відповідні значення показників 1,0; 0,6; 0,2; 0.

Ваговий коефіцієнт $a1_3$, що відповідає показнику $A1_3$, має значення 0,2.

Відповіді на четверте питання:

- держава доклала значних зусиль для розвитку державно-приватного співробітництва.
- держава докладала активні, але недостатні зусилля для розвитку державно-приватного співробітництва.
- державно-приватне партнерство не реалізовано.

Відповідні значення показників 1,0; 0,5; 0.

Ваговий коефіцієнт $a1_4$, що відповідає показнику $A1_4$, має значення 0,1.

Отже, значення вагового коефіцієнта показників становлять 0,4; 0,3; 0,2; 0,1.

Експертна анкета для оцінювання рівня критичності кібербезпеки за параметрами доступності нормативно-правової бази для розроблення політики протидії кіберзлочинності

Для визначення показників $A2_1$ та $A2_2$ експерт відповідає на запитання:

- A21 – який рівень державного лідерства у сфері кіберзахисту?
- A22 – який рівень активності інформаційної та кібернетичної інфраструктури в кібербезпеці?
- Відповіді на перше запитання:
- у державі створено орган виконавчої влади з питань кіберзахисту, діяльність якого визнана ефективною (значення показника 1,0);
- є певні недоліки в діяльності органу виконавчої влади з питань кіберзахисту (значення показника 0,5);
- орган виконавчої влади з питань кіберзлочинності в державі відсутній (значення показника 0).

Показник $A2_1$ відповідає ваговому коефіцієнту $a2_1$, значення якого становить 0,5.

Відповіді на друге запитання:

- рівень реакції суб'єктів інформаційної та кіберінфраструктури на прояв сторонніх кіберінвестицій високий середній (значення індикатора 1,0);
- рівень реагування суб'єктів інформаційної та кібернетичної інфраструктури на прояв сторонніх кібернетичних впливів є періодичним і спонтанним (значення показника 0,5);
- суб'єкти інформаційної та кіберінфраструктури не займаються питаннями стороннього кібервпливу (значення індикатора 0).

Показник $A2_2$ відповідає ваговому коефіцієнту $a2_2$, значення якого становить 0,5.

Експертна анкета для оцінювання рівня критичності кібербезпеки за параметрами стану соціально-економічного розвитку держави на рівні освіти, науки і технологій

Для визначення показників експерт відповідає на такі запитання:

- *$B1_1$ – який відсоток населення держави має вищу освіту? (визначається як відсоток молоді віком від 18 до 22 років, яка здобуває освіту за денною формою навчання, до загальної кількості студентів зазначеного віку в країні).*
- *$B1_2$ – яка частина населення в державі знає іноземну мову, особливо англійську? (визначається на базі державного центру вивчення англійської мови).*
- *$B1_3$ – яка частина науково-дослідних робіт у державі присвячена дослідженням питань кібербезпеки? (визначається на основі інформації реєстраційного органу НДДКР).*
- *$B1_4$ – який рівень залучення до виконання НДДКР напряму кібербезпеки інженерно-технічного персоналу? (визначається як кількість спеціалістів, які задіяні у виконанні НДДКР на 1 млн населення країни).*

Наступні відповіді на перше запитання "високий"; "середній"; "низький" зі значеннями показників 1,0; 0,5; 0.

Показник $B1_1$ відповідає ваговому коефіцієнту $b1_1$, значення якого становить 0,2.

Відповіді на інші питання збігаються з попередніми і мають такі вагові коефіцієнти:

- $b1_2$, значення якого дорівнює 0,2;
- $b1_3$, значення якого 0,3;
- $b1_4$, значення якого 0,3.

Експертна анкета для оцінювання рівня критичності кібербезпеки за параметрами стану соціально-економічного розвитку держави за рівнем розвитку інноваційного середовища.

Для визначення показників експерт відповідає на такі запитання:

- B2 1 – який стан витрат у державі на НДДКР у сфері кібербезпеки? (визначається як відношення поточних і капітальних витрат на НДДКР до рівня ВВП);
- B22 – який стан державного патенту та інноваційної діяльності у сфері кібербезпеки? (визначається як кількість патентних заявок на 1 млн населення країни);
- B23 – яка умова залучення приватного та венчурного капіталу у сферу кібербезпеки? (визначається відсотком приватного та венчурного капіталу до рівня ВВП країни).

ISSN 2707-1758

Наступні відповіді на всі запитання:

- "достатній" зі значенням 1,0;
- "середній" зі значенням 0,5;
- "недостатній" зі значенням 0.

Відповідно, значення вагових коефіцієнтів $b2_1$, $b2_2$ та $b2_3$ показників становлять 0,3; 0,4; 0,3.

Експертна анкета для оцінювання рівня критичності кібербезпеки за параметрами наявності розгалуженої технологічної інфраструктури для статусу якості технологічної інфраструктури

Для визначення значення показників $C1_1$ та $C1_2$ експерт відповідає на такі запитання:

- *$C1_1$ – який рівень використання інтернету? (вказує кількість інтернет-користувачів на 100 осіб; розраховується на основі інформації JiWire (Wi-Fi-бази даних – точка доступу в 142 країнах));*
- *$C1_2$ – який рівень використання мобільних і соціальних мереж? (вказує кількість користувачів мобільного зв'язку на 100 осіб у відсотках від кількості користувачів до загальної кількості користувачів інтернету).*

У першому випадку відповіді "високий" зі значенням показника 1,0; "середній" зі значенням показника 0,5; "низький" зі значенням показника 0; відповідають ваговому коефіцієнту $c1_1$, значення якого становить 0,5.

Відповідно, відповіді на друге запитання відповідають попереднім і їхній ваговий коефіцієнт $c1_2$ також має значення 0,5.

Експертна анкета для оцінювання рівня критичності кібербезпеки на основі наявності розгалуженої технологічної інфраструктури за рівнем технологічної інфраструктури. впровадження .

Для визначення значення показників $C2_1$ і $C2_2$ експерт відповідає на такі запитання:

- *C21 – який рівень фінансування заходів із впровадження ІКТ? (визначається як відсоток загального обсягу програмного забезпечення, обладнання та IT-послуг до рівня ВВП);*
- *C22 – який рівень безпеки послуг? (вказує на кількість серверів, які використовують технологію шифрування даних для захисту даних обміну трафіком).*

У першому випадку "достатній" зі значенням показника 1,0 відповіді; "середній" зі значенням показника 0,5; "недостатній" зі значенням показника 0; відповідають ваговому коефіцієнту $c2_1$, значення якого становить 0,5.

Згідно з наведеними вище даними, відповіді на друге запитання відповідають попереднім і їхній ваговий коефіцієнт $c2_2$ також має значення 0,5.

Експертна анкета для оцінювання рівня критичності кібербезпеки за ступенем використання ІКТ та ІТС за рахунок застосування інформаційно-комунікаційних технологій у локальній мережі

Для визначення значення показників $D1_1$ експерт $D1_2$ відповідає на такі запитання:

- D11 – який рівень використання ІКТ у корпоративних мережах?
- D12 – який рівень використання ІКТ в інтелектуальних транспортних системах?
- Відповіді на перше запитання:
- широке використання корпоративних мереж по всій країні (значення 1,0);
- рівень розвитку корпоративних мереж досить високий (значення 0,6);
- розробляються плани впровадження корпоративних мереж (значення 0,2);
- в країні немає корпоративних мереж (значення 0).

Зазначимо, що показник $D1_1$ відповідає ваговому коефіцієнту $d1_1$, значення якого становить 0,5.

Відповіді на друге запитання:

- високий рівень використання ІТС для розв'язання важливих функцій (зі значенням 1,0);
- рівень використання ІТС для розв'язання важливих функцій нижче середнього рівня (зі значенням 0,5);
- інтелектуальних транспортних систем не існує (зі значенням 0).

Показник $D1_2$ відповідає ваговому коефіцієнту $d1_2$, значення якого також дорівнює 0,5.

Експертна форма для оцінювання рівня критичності кібербезпеки за ступенем використання ІКТ та ІТС із метою використання інтернет-ресурсів у торгівлі

Для визначення значення показників $D2_1$ експерт $D2_2$ відповідає на такі запитання:

- *D21 – який відсоток користувачів інтернету розміщують пропозиції щодо надання товарів і послуг?*
- *D22 – який відсоток інтернет-користувачів замовляють товари та послуги?*

Відповіді на питання показника $D2_1$:

- більше 55 відсотків (значення показника 1,0);
- від 25 до 54 відсотків (значення показника 0,5);
- 0 до 24 відсотків (значення показника 0).

Ідентифікатор $D2_2$ визначається ваговим коефіцієнтом $d2_1$ і його значення становить 0,5.

Наступні відповіді на друге питання:

- більше 80 відсотків (значення показника 1,0);
- від 40 до 79 відсотків (значення показника 0,5);
- 0 до 39 відсотків (значення показника 0).

Відповідно, показнику $D2_2$ відповідає ваговий коефіцієнт $d2_2$, значення якого становить 0,5.

За формулами (1), (4), (7) і (10) розраховують значення комплексних показників (категорій) другого рівня, такі як:

а) наявність нормативної бази ($G_1^{\text{факт}}$);

б) стан соціально-економічного розвитку держави ($G_2^{\text{факт}}$);

в) наявність розгалуженої технологічної інфраструктури ($G_3^{\text{факт}}$);

г) ступінь використання ІКТ та ІТС ($G_4^{\text{факт}}$).

Індекс кіберпотужності ($G_{sec.level}$) з погляду експерта можна розрахувати за такою формулою:

$$G_{sec.level} = (\sum_{i=1}^{n}(g_i \times G)) \times 100\%, \qquad (13)$$

де g_i – ваговий коефіцієнт s категорій другого рівня ієрархії G_i^{fact} ; n – кількість категорій (в цьому випадку n4).

Рішення щодо спроможності держави протистояти кібератакам здійснюватиметься за 100-бальною шкалою за таким правилом:

- якщо 90 $< g_{sec.level} <$ 100, то рівень захисту держави від ризику зовнішнього кібервпливу вважають достатньо високим для забезпечення безпечного функціонування її об'єктів інформаційної та кіберінфраструктури;
- якщо 45 $< g_{sec.level} <$ 90, то рівень захисту держави від ризику зовнішнього кібервпливу можливий для забезпечення безпечного функціонування її об'єктів інформаційної та кіберінфраструктури;
- якщо $g_{sec.level} <$ 45, то рівень захисту держави від ризику зовнішнього кібервпливу вважають недостатнім для забезпечення безпечного функціонування її об'єктів інформаційної та кіберінфраструктури.

Дискусія і висновки

Існуючі нині методики безпеки технічних систем розроблено для систем, що мають чіткі межі і добре визначені переліки загроз. Для цих систем можуть бути створені бази даних зі статистики аварій, які дозволяють кількісно оцінювати та верифікувати моделі. Ці методики, що базуються на побудові сценарних "дерев" (моделі типу "дерево" подій, "дерево" відмов), були розроблені без урахування позапроєктних впливів і не дозволяють належно врахувати складність критичних інфраструктур, функціонування яких визначається взаємодією технічних, організаційних і соціальних факторів.

У зазначених методиках аварії, що розвиваються в технічних системах, розглядають як лінійні послідовності подій. Ці моделі мають обмежені можливості, коли доводиться описувати розвиток аварій у складних техносоціальних системах, як критичні інфраструктури, які передбачають нелінійні взаємодії між компонентами, петлі зворотних зв'язків, множинні джерела аварій тощо. Традиційний підхід до моделювання аварій не дозволяє описувати сценарії відмов у складних системах, які, зазвичай, відбуваються не внаслідок окремої події, що ініціює (технічної відмови елемента системи або помилки оператора), а є наслідком кількох взаємопов'язаних факторів, що діють на різних рівнях системи. До цих факторів належать технічні відмови, людські помилки, зовнішні екстремальні впливи, латентні умови, пов'язані з такими аспектами, як практика управління діючою системою або етнокультурні особливості персоналу, зовнішні ініціювальні події.

Дослідження критичних інфраструктур як соціотехнічних систем потребує оцінювання складних взаємодій між технічними, соціальними й організаційними рівнями системи. Тому КІ варто розглядати як єдине ціле. Причому необхідно наголошувати на одночасному спільному розгляді технічних, організаційних і соціальних факторів, що визначають стан системи та динаміку її розвитку. Щоб забезпечити безпеку таких систем, необхідно вийти за межі традиційного підходу до оцінювання проєктних ризиків і перейти до нової парадигми, що ґрунтується на забезпеченні безпеки КІ за критерієм стійкості до позапроєктних впливів. У зв'язку з необхідністю включити до розгляду позапроєктні аварії на КІ, межі досліджень мають бути суттєво розширені. Заходи щодо забезпечення безпеки повинні бути спрямовані не тільки на створення захисних бар'єрів, покликаних попередити реалізацію проєктних аварій, що постулюються, але і на підвищення стійкості та живучості КІ у разі позапроєктних впливів, тобто зосередитися на запобіганні великомасштабним катастрофам і тривалим перервам у функціонуванні.

Можливість позапроєктних впливів, що мають низьку ймовірність реалізації та тяжкі наслідки, має враховуватися під час оцінювання захищеності критичних інфраструктур. Це вимагатиме реалізації додаткових заходів, спрямованих на підвищення стійкості КІ у випадку позапроєктних впливів.

Нова парадигма забезпечення безпеки КІ й інших складних систем має концентрувати увагу не лише на створенні захисних бар'єрів і реалізації охоронних заходів, спрямованих на парирування проєктних аварій, а й на підвищенні стійкості КІ щодо позапроєктних аварій. Причому новий підхід до забезпечення безпеки КІ, що розробляється, має розглядатися не як заміна, а скоріше як доповнення до традиційного підходу.

ISSN 2707-1758

Отже, запропонована стратегія дасть можливість отримати кількісну оцінку рівня захисту ОСІ від ризику зовнішнього кібернетичного впливу, встановити організаційні вимоги до власних систем кібернетичної безпеки та розробити заходи, спрямовані на підвищення їхньої ефективності. Підставою для таких дій може бути виявлення відхилень від нормального режиму роботи ІР, ІТ-систем і мереж, а також відповідного програмного й апаратного забезпечення, зокрема і виявлення таких ознак:

- поломка окремих компонентів електронних систем;
- зміна алгоритмів функціонування програмного забезпечення в ІТ-системах і системах управління мережами;
- несанкціоновані зміни файлів (їхніх розмірів і останньої дати модифікації);
- порушення безпеки обміну інформацією, протоколів передачі даних вхідного або вихідного трафіку, а також прав доступу до ІР-користувачів;
- уповільнення завантаження і роботи ПК;
- зменшення обсягу оперативної пам'яті;
- виконання неконтрольованих процесів тощо.

Крім того, у процесі завантаження ОС може виявлятися багато помилок, через неможливість збереження файлів у потрібних каталогах, а також незрозумілі системні повідомлення, музичні та візуальні ефекти.

Внесок авторів: Сергій Толюпа – концептуалізація; методологія; аналіз джерел; Анатолій Шевченко – збір емпіричних даних та їхня валідація; емпіричне дослідження; Андрій Кулько – підготування огляду літератури або теоретичних засад дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Бірюков, Д., & Кондратов, С. (2012). *Захист критичної інфраструктури, проблеми та перспективи впровадження в Україні.* Національний інститут стратегічних досліджень.

Гнатюк, С., & Лядовська, В. (2013,). Критерії визначення елементів критичної інфраструктури держави. У Р. Сущенко, Л. Веремеєнко, Д. Шелунцов (Ред.). *Матеріали XXIII Всеукраїнської практичної конференції. Іноваційний потенціал світової науки XXI століття* (с. 55–57). Національна академія СБУ. https://zp.edu.ua/

Довгань, О. (2013). Критична інфраструктура як об'єкт захисту від кібернетичних атак. У Н. М. Мармоленко, О. П. Власенко, С. В. Ангелуца, Н. М. Лашкет (Ред.). *Інформаційна безпека: виклики та загрози сучасності: матеріали науково-практичної конференції* (с. 17–20). Національна академія СБУ. https://er.nau.edu.ua/bitstream/NAU/27208/1/2013

Юдін, А., & Пирогов, Г. (2013). Аналіз та оцінка нормативних документів, що використовуються для забезпечення інформаційної безпеки систем Smart Grid. *Правова, нормативна та метрологічна функціональність системи захисту інформації в Україні*, 1, 88.

Бурячок, В., Толюпа, С., Толубко, В., & Хорошко О. (2022). Інформаційна та кібербезпека: соціотехнічний аспект. У С. Даков, О. Торошанко, Я. Шестак, Ю. Бабенко (Ред.). *VII міжнародна науково-практична конференція: Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)* (с. 288). Київський національний університет імені Тараса Шевченка. https://pcsits.knu.ua/

REFERENCES

Buryachok, V., Tolyupa, S., Tolubko, V., & Khoroshko, O. (2022). Information and cyber security: socio-technical aspect. In S. Dakov, O. Toroshanko, Ya. Shestak, Yu. Babenko. *VII international scientific and practical conference, Problems of cyber security of information and telecommunication systems (PCSITS)* (p. 288). Taras Shevchenko National University of Kyiv [in Ukrainian]. https://pcsits.knu.ua/

Biryukov, D., & Kondratov, S. (2012). *Protection of critical infrastructure, problems and prospects of implementation in Ukraine*. National Institute of Strategic Studies [in Ukrainian].

Dovgan, O. (2013). Critical infrastructure as an object of protection against cyber attacks. In N. M. Marmolenko, O. P. Vlasenko, S. V. Angelutsa, N. M. Lashket (Eds.). *Information security: modern challenges and threats: materials of the scientific and practical conference* (pp. 17–20). National Academy of the Security Service of Ukraine [in Ukrainian]. https://er.nau.edu.ua/bitstream/NAU/27208/1/2013

Hnatyuk, S., & Lyadovska, V. (2013,). Criteria for determining the elements of the state's critical infrastructure. In R. Sushchenko, L. Veremeyenko, D. Sheluntsov (Eds.). *Materials XXIII All-Ukrainian pr. Conference. Innovative potential of global science of the 21st century* (pp. 55–57). National Academy of the Security Service of Ukraine [in Ukrainian]. https://zp.edu.ua/

Yudin, A., & Pirogov, G. (2013). Analysis and assessment of regulatory documents used to ensure information security of Smart Grid systems. *Legal, regulatory and metrological functionality of the information protection system in Ukraine*, 1, 88 [in Ukrainian].

Отримано редакцією журналу / Received: 17.03.24
Прорецензовано / Revised: 27.03.24
Схвалено до друку / Accepted: 13.05.24

Serhii TOLIUPA, DSc (Engin.), Prof.
ORCID ID: 000-0002-1919-9174,
e-mail: tolupa@i.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Anatoliy SHEVCHENKO, brigadier general
ORCID ID: 0000-0003-2723-0378
e-mail: anatolii.shevchenko@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Andriy KULKO, PhD Student
ORCID ID:0009-0006-1185-0774,
e-mail: kulko452@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

FEATURES OF ENSURING SECURITY OF CRITICAL INFRASTRUCTURES

B a c k g r o u n d . *The rapid development of information technologies over the past two decades has impacted the functioning of critical infrastructure facilities. These technologies have begun to be used not only for the exchange and processing of information, but also as a tool for reducing harm. The protection of sovereign interests in the political context is the primary basis for ensuring the national security of the country, which explains the need for the creation and constant development of strong cyber security. Critical infrastructure facilities are foldable, spaciously distributed, rich in component systems, the stability of the robot is critical for the functioning of the economy and the livelihood of the household. They have a rich structure, which includes: a range of technical components; social rheum; organizational level and level of state governance.*

M e t h o d s . *For monitoring information systems and methods for assessing the security of systems.*

R e s u l t s . *The investigation of critical infrastructures as socio-technical systems will require an assessment of the complex interactions between the technical, social and organizational levels of the system. Therefore, it is important to look at critical infrastructure as a whole. In this case, it is necessary to speak at a one-hour close examination of the technical, organizational and social factors that indicate the structure of the system and the dynamics of its development. Schobstecchita to the nonsense of such systems, it is not possible to pray beyond the traditions of the tradition to the zziki projected Riziki, to go to the new paradigmes, and the blessing of the nonsense of the critical sinfrastructure for the criterly wrecks to the designed areas. Due to the need to include the consideration of design basis accidents on critical infrastructure, the scope of surveillance may be expanded accordingly. Come to the point of ensuring the safety of those responsible not only for the creation of dry-barriers that occur ahead of the implementation of project-based accidents that are postulated, but also for the improvement of the resistance and survivability of critical infrastructure times beyond the project inflows, in order to focus on avoided large-scale disasters and troubling interruptions in the functioning of , and the creation of a rich criteria model for assessing the level of security of critical infrastructure objects will give a more comprehensive picture of the status of the critical infrastructure object.*

C o n c l u s i o n s . *The current safety methods for technical systems are divided into systems that have clear boundaries and well-defined danger flows. For these systems, a database of accident statistics can be created, which allows for precise evaluation and verification of models. These methods, which are based on case-by-case scenario "trees" (models of the type "tree" of ideas, "tree" of views), were fragmented without the coordination of design inputs and do not allow for proper management of the complexity of critical infrastructures functioning in is determined by the interaction of technical, organizational and social factors.*

K e y w o r d s : *cyber security, critical infrastructure facilities, information systems, resilience, cyber power.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.