УДК 004.056.5 Doi: https://doi.org/10.32918/nrs.2021.1(89).07

Дослідження проблеми кіберживучості об'єктів критичної інформаційної інфраструктури

■ **Комаров Максим Юрійович**
Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України, м. Київ, Україна
ORCID: https://orcid.org/0000-0002-5739-8959

■ **Гончар Сергій Феодосійович**, д-р техн. наук
Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України, м. Київ, Україна
ORCID: https://orcid.org/0000-0002-9978-8998

■ **Дімітрієва Дар'я Олександрівна**
Державне підприємство «Державний науково-технічний центр з ядерної та радіаційної безпеки», м. Київ, Україна
ORCID: https://orcid.org/0000-0002-9029-0456

У статті розглядається підхід до оцінки кіберстійкості критичної інформаційної інфраструктури, яка функціонує в умовах протиборства двох та більше сторін. Результатом оцінки є значення загального критерію здатності об'єкта критичної інформаційної інфраструктури виконувати цільову функцію в конкретний момент часу. Запропонована методика оцінки кіберживучості об'єктів критичної інформаційної інфраструктури Об'єднаної енергосистеми України, як інструмента для підвищення ефективності управління критичною інфраструктурою, а також для обґрунтування нових методів і засобів протиборства в кіберпросторі. Наведено визначення поняття кіберживучості. Зазначено властивості управління, що визначають кіберстійкість системи. Розглянуто модель інформаційного протиборства в кіберпросторі. Наведено властивості процесу управління: адекватність, оптимальність, оперативність, стійкість, скритність. Здійснено класифікацію об'єктів критичної інформаційної інфраструктури за ознаками, що впливають на забезпечення кіберстійкості, зокрема структурною організацією. Подано визначення одноланкового та багатоланкового об'єкта критичної інформаційної інфраструктури. Наведена класифікація багатоланкових об'єктів критичної інформаційної інфраструктури за ознакою функціональної однорідності: багатоланкові однорідні та багатоланкові неоднорідні. Наведено узагальнений показник кіберстійкості. Отримано залежності рівня кіберстійкості від стану об'єкта критичної інфраструктури та наведено методику і алгоритм їх розрахунку. Подано схему відповідності класу стану об'єкта критичної інформаційної інфраструктури рівню кіберживучості. Описано узагальнений алгоритм методики оцінки кіберстійкості об'єктів критичної інформаційної інфраструктури.

Ключові слова: Об'єднана енергосистема України, об'єкти критичної інфраструктури, кібербезпека, кіберживучість, кіберстійкість.

Функціонування об'єктів критичної інформаційної інфраструктури (КІІ) в такому специфічному середовищі, як кіберпростір, пов'язане з вразливостями системи кіберзахисту і кіберзагрозами, та вимагає розробки нового інструментарію забезпечення стійкості функціонування в умовах кібератак. Управління стійкістю функціонування об'єктів КІІ Об'єднаної енергосистеми України ґрунтується на знаннях про стан об'єктів управління, стан середовища функціонування і впливи, які відбуваються. Невід'ємним елементом систем управління об'єктів КІІ є низка підсистем підтримки ухвалення рішень. Можливості системи управління безпосередньо залежать від здатності підсистеми підтримки ухвалення рішень забезпечити особу, яка ухвалює рішення, якісно збалансованою інформацією, що характеризує реальні і прогнозовані стани об'єктів критичної інфраструктури та запропонувати обґрунтований вибір траєкторії досягнення мети. З огляду на це, розробка методики оцінки кіберживучості об'єктів КІІ, що функціонує в кіберпросторі, є актуальним завданням.

Пропонуємо розглянути методику оцінки кіберживучості об'єктів КІІ Об'єднаної енергосистеми України, що функціонує в кіберпросторі.

Новизна запропонованої методики полягає в оцінці складних технічних систем, які мають високий ступінь критичності. Практична значимість наведеної методики полягає в можливості її застосування для підвищення ефективності управління критичною інфраструктурою, а також для обґрунтування нових методів і засобів протиборства в кіберпросторі.

Високий ступінь автоматизації управління і глобалізації інформаційних систем через інформаційно-телекомунікаційні мережі загального користування (ІТКМ ЗК) призвів до формування глобального інформаційного суспільства і нового середовища його функціонування – кіберпростору, що ставить об'єкти КІІ, серед іншого, в залежність від ступеня захищеності інформаційно-телекомунікаційних систем.

Кібернетичне протиборство – різновид інформаційної боротьби, під час якої здійснюється кібернетичний вплив на апаратно-програмні комплекси автоматизованих систем (АС) об'єкта кібервпливів, спрямований на порушення їх нормального функціонування, що ставить об'єкти КІІ в залежність від ступеня захищеності інформаційно-телекомунікаційних систем.

Аналіз відкритих джерел [1]–[4], присвячених забезпеченню безпеки КІ, надійності та стійкості функціонування АС об'єктів КІІ показав, що в них практично не розглянуті питання, пов'язані:

з розробкою моделей і методів з побудови системи оцінки стану об'єктів КІІ;

з розробкою науково-методичного апарата побудови автоматичної системи збору та приведення до єдиного вигляду інформації, що характеризує стан КІІ в умовах деструктивних інформаційних впливів (ДІВ);

з розробкою моделей і методів адаптивного управління КІІ, що враховують поточний і прогнозований стан об'єктів КІІ в умовах ДІВ.

Отже, існує необхідність у розробці підходів до побудови системи оцінки сталості функціонування КІІ.

Під поняттям кіберживучості [5] розуміється здатність інформаційної системи виконувати свої функції в умовах здійснення ДІВ, які виникають унаслідок протиборства щонайменше двох сторін, водночас відбувається спільне використання загального ресурсу (глобального інформаційного простору), управління яким має розглядатися як цілеспрямований вплив двох (і більше) підсистем управління, які прагнуть поширити керуючий вплив одна на одну (Рисунок 1).

Зауважимо, що незважаючи на суттєве спрощення та ідеалізацію, модель, наведена на Рисунку 1, дозволяє сформулювати найважливіші властивості, притаманні процесам управління в умовах здійснення ДІВ: адекватність, оптимальність, оперативність, стійкість і скритність.

Розглянемо ці властивості більш детально, з погляду функціонування об'єктів КІІ в кіберпросторі в умовах застосування нового виду зброї – кіберзброї.

Адекватність. Адекватність управління полягає в здатності системи здійснювати перетворення інформації про стан об'єкта, отриманої від підсистеми моніторингу, в керуючий інформаційний вплив (КІВ), на основі якого об'єкт управління переходить до стану, який відповідає ситуації, що склалася. Вочевидь коректність перетворень багато в чому залежить від достовірності отриманої інформації про стан і правильності визначення цільової функції об'єкта управління. Отже, властивість адекватності значною мірою залежить від

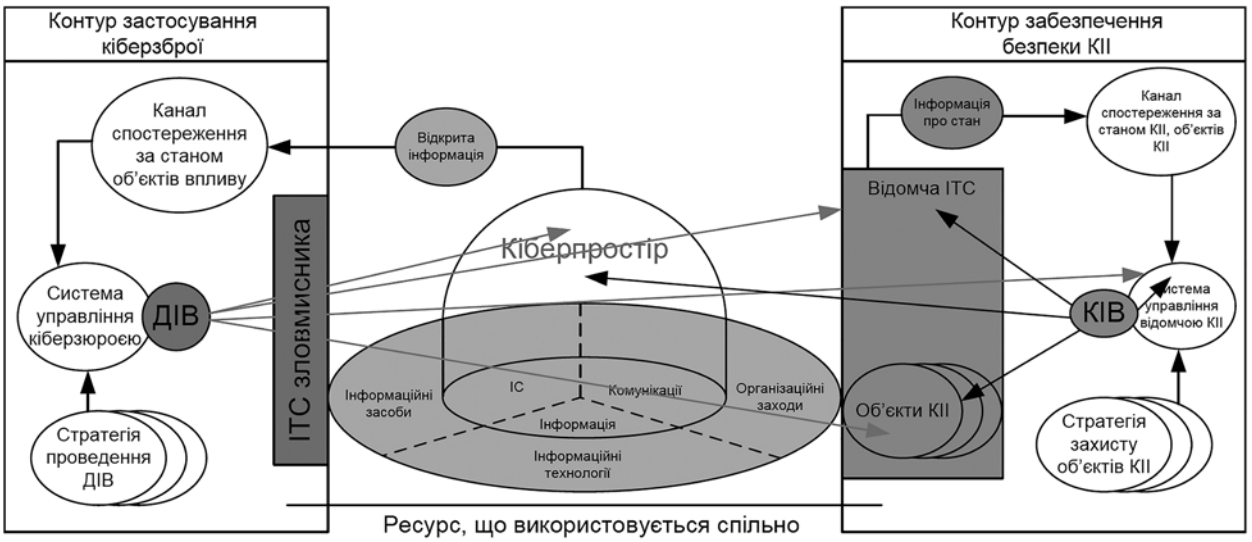

Рисунок 1 – Модель інформаційного протиборства в кіберпросторі

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

достовірності і повноти інформації, коректності операцій перетворення інформації та їх послідовності.

Оптимальність. Під оптимальністю управління розуміється вибір таких керуючих впливів, за яких точно досягається екстремальне значення деякого критерію, що характеризує якість управління. Зазвичай намагаються мінімізувати втрати в системі, що зазнає впливу, – грошові втрати або інші ресурси, що підлягають втраті. Інакше кажучи, оскільки всі допустимі траєкторії призводять до мети, і кожна з них характеризується певною витратою ресурсів (часом, додатковим навантаженням на обчислювальні ресурси тощо), то в розумінні «кращого» споживання цих ресурсів (з погляду доцільності їх споживання) існує краща траєкторія. Якщо в процесі управління система «рухається» в просторі ситуацій саме цією траєкторією, то кажуть, що управління оптимальне.

Оперативність. Оперативність управління – це здатність системи перетворювати інформацію відповідно до часових обмежень. Інакше кажучи, оперативністю є властивість управління перетворювати інформацію відповідно до темпу зміни поточної ситуації. Залежно від виду операції, яка домінує в тому чи іншому процесі управління, розрізняють оперативність семантичного (смислового) перетворення (наприклад, вироблення рішення) та оперативність перетворення інформації (наприклад, оперативність передачі даних або виконання якихось розрахунків) тощо.

Стійкість. Стійкість управління визначається здатністю системи управління виконувати свої функції в складних обставинах, що різко змінюються, в умовах деструктивних впливів різної природи протиборчої сторони (сторін). Як правило, стійкість є інтегральною властивістю, що визначається живучістю, завадостійкістю і надійністю, під якими розуміється здатність здійснювати управління в умовах впливу всіх деструктивних видів, технічних і програмних відмов, а також помилкових дій технічного персоналу і посадових осіб, зберігаючи водночас значення всіх показників управління в установлених межах.

Скритність. Властивість процесу управління зберігати в таємниці від протиборчої сторони факт, час і місце перетворення інформації, а також її зміст і належність до керуючих об'єктів.

Деструктивні інформаційні впливи (кібератаки) в кібернетичному просторі є збурюючим впливом, система управління об'єктом має компенсувати ці збурення, а загалом об'єкт та система управління повинні бути стійкими до цих збурень, тобто бути кіберстійкими (cyber stability). Одним з видів стійкості є кіберстійкість об'єкта КІІ, під якою в цій статті розуміється, здатність системи управління об'єкта КІІ виконувати свої функції в складних, різко мінливих обставинах в умовах ДІВ.

Під час оцінки кіберстійкості об'єктів КІІ, як складових елементів КІІ, що функціонує в кіберпросторі, виникає низка проблем, пов'язаних зі складністю самих об'єктів КІІ, складністю і різнорідністю зв'язків між ними і умовами спільного із супротивником використання ресурсів ІТКМ ЗК.

Вочевидь існують досить різноманітні об'єкти КІІ [6] і для подальшого їх розгляду доцільно провести їх декомпозицію за ознаками, що впливають на забезпечення кіберстійкості:

За структурною організацією:

Одноланкові і багатоланкові.

Одноланковий об'єкт КІІ – це самодостатній об'єкт, який володіє всією необхідною структурою для виконання цільової функції (самостійний одиничний (базовий) елемент).

Прикладом одноланкової структури можуть виступати окремі АС.

Багатоланковий об'єкт КІІ – об'єкт, який являє собою структурне послідовне об'єднання декількох одноланкових об'єктів КІІ в єдину систему в рамках виконання єдиної цільової функції.

За функціональною однорідністю:

Багатоланкові однорідні і багатоланкові неоднорідні.

Багатоланковий однорідний об'єкт КІІ – об'єкт, який являє собою структурне об'єднання декількох одноланкових об'єктів КІІ, що виконують однакову цільову функцію, в єдину систему в межах виконання єдиної цільової функції.

Прикладом багатоланкової однорідної структури є багатоінтервальна (складна) мережа передачі даних, що складається з різнотипних одноланкових систем передачі даних.

Багатоланковий різнорідний об'єкт КІІ – об'єкт, який являє собою структурне об'єднання декількох одноланкових об'єктів КІІ, що виконують різні функції, наприклад, інформаційно-телекомунікаційна мережа, інформаційні системи тощо.

Об'єкти КІІ, які використовують ІТКМ ЗК, як правило, є багатоланковими. Водночас, склад окремих ланок цих ліній залежить від обраних маршрутів проходження інформації по ІТКМ ЗК, а також відомчих інформаційно-телекомунікаційних систем.

З огляду на вищезазначене пропонується ввести деякий узагальнений показник кіберстійкості.

Узагальнений показник кіберстійкості одноланкового об'єкта КІІ має вигляд:

$$K_{ОКІІ}^{уп} = K_{ОКІІ}^{жив} \times K_{ОКІІ}^{зах} \times K_{ОКІІ}^{над}, \qquad (1)$$

де: $K_{ОКІІ}^{уп}$ – узагальнений показник кіберживучості;

$K_{ОКІІ}^{жив}$ – **кіберживучість** об'єкта КІІ, яка трактується як здатність збереження його працездатності (виживання) в умовах виходу з ладу технічних засобів обробки інформації внаслідок ДІВ, тобто, по суті, – внесок кожного базового елемента

одноланкового об'єкта КІІ у виконання ним цільової функції;

$K_{ОКІІ}^{зах} = (1 - P_{ЗКА}) \times (1 - P_{ЦКА})$ – **кіберзахищеність** одноланкового об'єкта КІІ, що трактується як ймовірність забезпечення виконання цільової функції об'єкта КІІ із заданою якістю в умовах застосування «загальних» і цілеспрямованих ДІВ;

$P_{ЗКА}$ і $P_{ЦКА}$ – ймовірності ураження технічних засобів обробки інформації, що входять до об'єкта КІІ, загальними ($P_{ЗКА}$) та цілеспрямованими ($P_{ЦКА}$) ДІВ;

$K_{ОКІІ}^{над}$ – **кібернадійність** одноланкового об'єкта КІІ, під якою розуміється ймовірність забезпечення виконання цільової функції об'єкта КІІ протягом визначеного часового інтервалу в умовах виникнення різних подій ($i = 1, \ldots, N$) – програмних та технічних відмов засобів об'єкта КІІ внаслідок ДІВ, де

$$K_{ОКП}^{над} = \Pi_{i=1}^{N} K_{ОКІІНАДі}(1 - P_i), \quad (2)$$

де P_i – імовірність i-ої події ($i = 1, \ldots, N$)

До об'єктів КІІ вже на етапах проєктування висуваються досить жорсткі вимоги з технічної надійності і передбачається низка спеціальних заходів щодо запобігання технічним і програмним відмовам технічних засобів обробки інформації (наприклад, завдяки кластеризації серверів [7], через резервування окремих компонентів). Відповідно до цього в завданнях оцінки кіберстійкості КІІ цілком допустимо вважати ймовірність програмних та технічних відмов за умови своєчасного і якісного проведення технічного обслуговування зневажливо малою, тобто $P_{ТН}=0$, де $P_{ТН}$ – імовірність технічного неспрацювання. У цьому разі кібернадійність одноланкового об'єкта КІІ буде визначатися як:

$$K_{ОКІІ}^{о} = K_{ОКІІ}^{жив} \times K_{ОКІІ}^{пом}, \quad (3)$$

Якщо вважати виходи з ладу ланок КІІ в умовах ДІВ незалежними подіями [8], кіберстійкість багатоланкового об'єкта КІІ ($K_{ОКІІстб}$) може бути знайдена із виразу:

$$K_{ОКІІстб}(N) = \prod_{i=1}^{N} K_{ОКІІоі}, \quad (4)$$

де N – кількість різних шкідливих подій, зумовлених ДІВ;

$K_{ОКІІоі}$ – кіберстійкість i-го одноланкового об'єкта КІІ.

Кібернадійність багатоланкового об'єкта КІІ трактується як ймовірність забезпечення виконання цільової функції об'єкта КІІ протягом визначеного часового інтервалу в умовах виникнення програмних помилок і технічних збоїв одноланкових об'єктів КІІ, з яких складається багатоланковий.

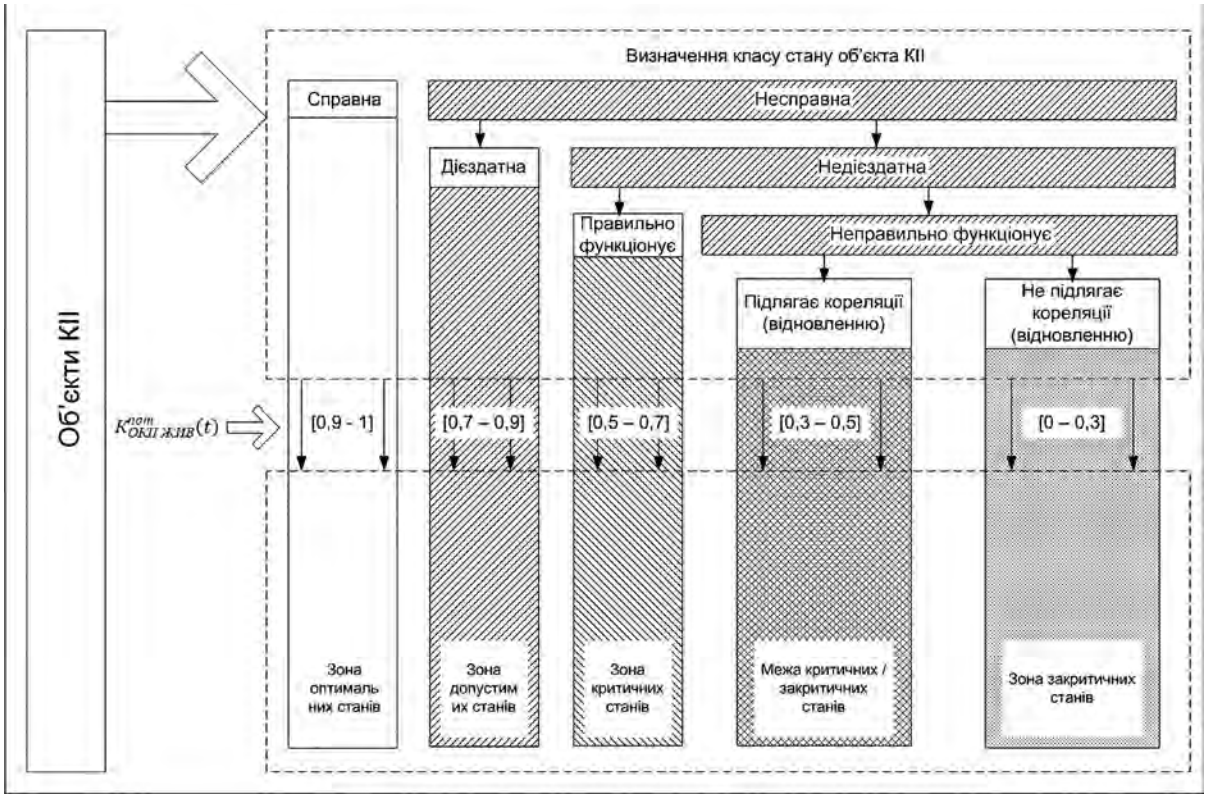

Рисунок 2 – Схема відповідності класу стану об'єкта КІІ рівню кіберживучості

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

Тобто кіберстійкість багатоланкового об'єкта КІІ має розраховуватися як спільна *N*-мірна функція розподілу ймовірності збереження працездатності одночасно *N* ланок, які складають цей багатоланковий об'єкт КІІ:

$$K_{OKIIсб}\left(K_{OKIIco1,\ldots,K_{OKIIcoN}}\right)= \\ =P\left\{K_{OKIIco1}\geq K_{OKIIconomp},\ldots,K_{OKIIcoN}\geq K_{OKIIocnomp}\right\}, \quad (5)$$

де $K_{OKIIсб}(N)$ – кіберстійкість багатоланкового об'єкта КІІ;

$K_{OKIIco1}$ – кіберстійкість першого одноланкового об'єкта КІІ;

$K_{OKIIconomp}$ – потрібна кіберстійкість першого одноланкового об'єкта КІІ;

$K_{OKIIcoN}$ – кіберстійкість *N*-го одноланкового об'єкта КІІ;

$K_{OKIIocnomp}$ – потрібна кіберстійкість *N*-го одноланкового об'єкта КІІ.

Основою розрахунку кіберстійкості багатоланкових об'єктів КІІ є розрахунок показників кіберзахищеності і кіберживучості окремих ланок об'єкта КІІ.

Тому, необхідно розробити методику розрахунку показників кіберзахищеності і кіберживучості об'єкта КІІ, причому визначальною властивістю з погляду можливості виконання об'єктом КІІ цільової функції буде кіберживучість, а кіберзахищеність буде складовою частиною функції.

Методика оцінки кіберживучості об'єктів КІІ

Зважаючи на те, що властивості, які характеризують кіберживучість об'єкта КІІ в умовах здійснення ДІВ – Ω, починають проявлятися тільки після того, як об'єкт зазнав впливу, то міра живучості має визначатися умовною імовірністю збереження працездатності, за умови, що система отримала локальне пошкодження.

Під показником кіберживучості одноланкового об'єкта КІІ, $K_{ОКІІ\ ЖИВ}$, будемо розуміти умовну ймовірність невиходу кінцевого стану об'єкта КІІ за межі заданої області безпечних станів S^{I} простору безпечних станів S у разі проведення ДІВ S_0.

$$K_{OKIIЖИВ}=P\left[\left(S-s_0<S^{I}\right)/\Omega\right]. \quad (6)$$

З огляду на розуміння функціональної вразливості системи V_S, під якою будемо розуміти ймовірність виходу кінцевого стану системи із заданої безпечної області S^{I}, справедливо:

$$K_{ОКІІ\ ЖИВ}=1-V_S, \quad (7)$$

а в конкретній точці часового інтервалу, що досліджується:

$$K_{ОКІІ\ ЖИВ}(t)=1-V_S(t). \quad (8)$$

Критерієм оцінки кіберживучості одноланкового об'єкта КІІ будемо розглядати вираз:

$$K^{пот}_{OKIIЖИВ}(t)\geq K^{mp}_{OKIIЖИВ}(t) \quad (9)$$

де $K^{пот}_{OKIIЖИВ}(t)$ – поточний рівень кіберживучості одноланкового об'єкта КІІ, а $K^{mp}_{OKIIЖИВ}(t)$ – потрібний рівень його кіберживучості в умовах здійснення ДІВ.

Також визначимо наступний критерій здатності об'єкта КІІ виконувати цільову функцію в умовах ДІВ $W_б$ (див. вираз (10)).

Для визначення поточного показника кіберживучості $K^{пот}_{OKIINЖИВ}(t)$ введемо такі рівні кіберживучості (див. вираз (11)).

Узагальнені результати, отримані у виразах (10) і (11), та їх візуалізація наведені на Рисунку 2.

$$W_б=\begin{cases}K^{пот}_{ОКІІЖИВ}(t)>0{,}9-\text{об'єкт КІІ повністю дієздатний}\\ 0{,}7\leq K^{пот}_{ОКІІЖИВ}(t)<0{,}9-\text{об'єкт КІІ загалом дієздатний}\\ 0{,}5\leq K^{пот}_{ОКІІЖИВ}(t)<0{,}7-\text{об'єкт КІІ обмежений(основна мета)}\\ 0{,}3\leq K^{пот}_{ОКІІЖИВ}(t)<0{,}5-\text{об'єкт КІІ недієздатний(підлягає відновленню)}\\ K^{пот}_{ОКІІЖИВ}(t)\leq 0{,}3-\text{об'єкт КІІ недієздатний(не підлягає відновленню)}\end{cases} \quad (10)$$

$$K_{ОКІN\ ЖИВ}(t)=\begin{cases}K^{тек}_{ОКІ\ ЖИВ}(t)\text{-}K^{тр}_{ОКІ\ ЖИВ}(t)>0-\text{ оптимальний рівень}\\ K^{тек}_{ОКІ\ ЖИВ}(t)\text{-}K^{тр}_{ОКІ\ ЖИВ}(t)=0-\text{допустимий рівень}\\ K^{тек}_{ОКІ\ ЖИВ}(t)\text{-}K^{тр}_{ОКІ\ ЖИВ}(t)<0-\text{критичний рівень}\\ K^{тек}_{ОКІ\ ЖИВ}(t)=0-\text{надкритичний рівень}\end{cases} \quad (11)$$

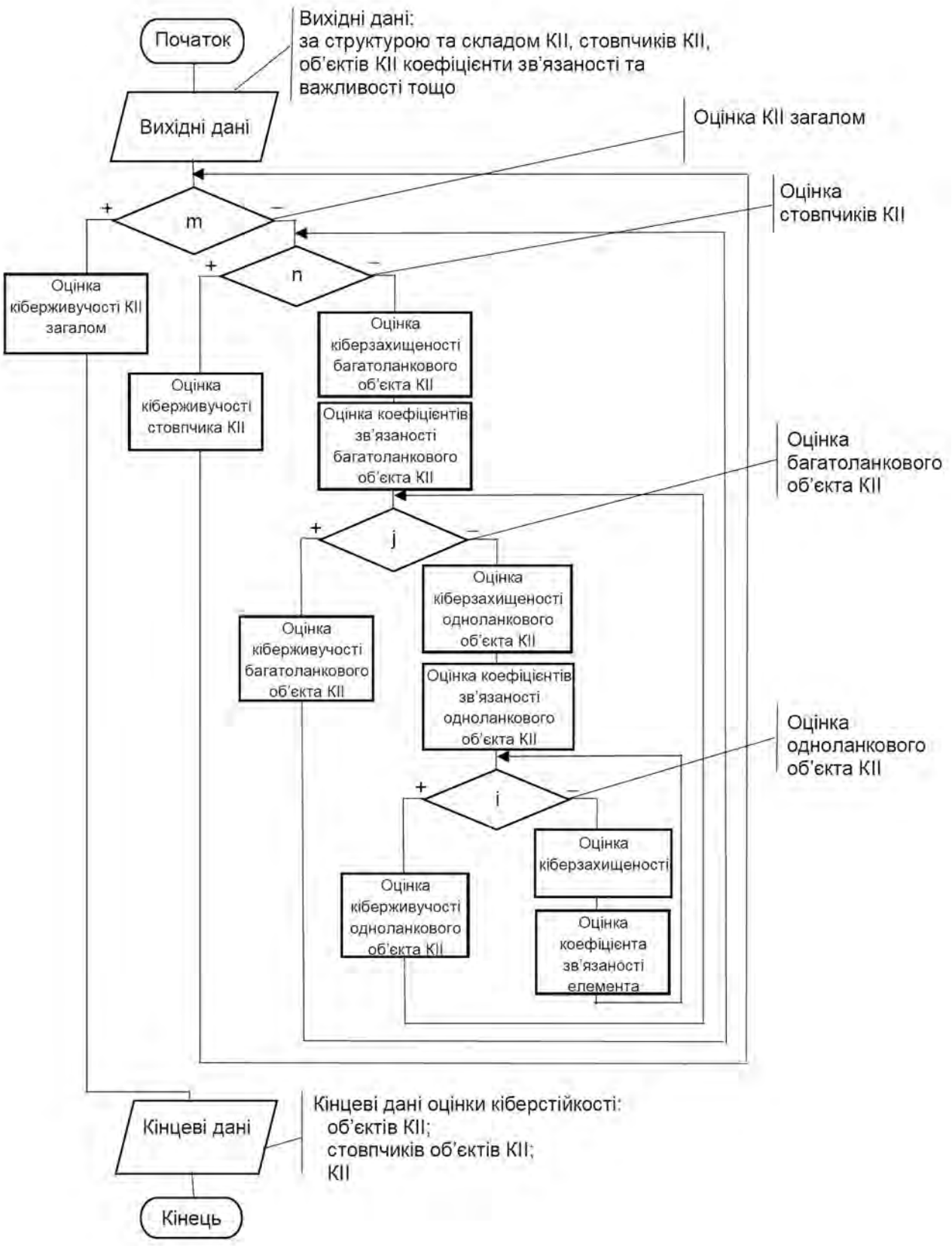

Рисунок 3 – Узагальнений алгоритм методики оцінки кіберстійкості КІІ

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

Методика оцінки кіберстійкості охоплює такі етапи, що схематично зображені на Рисунку 3:

1. Оцінка кіберживучості кожного об'єкта КІІ окремо.

1.1. Оцінка кіберживучості одноланкового об'єкта КІІ.

Рівень кіберзахищеності – ймовірність збереження працездатності *i*-го елемента в умовах ДІВ.

Оцінити коефіцієнт пов'язаності *i*-го елемента і його внесок в цільову функцію об'єкта КІІ.

1.2. Оцінка кіберживучості багатоланкового об'єкта КІІ.

Рівень кіберзахищеності – ймовірність збереження працездатності *j*-го одноланкового об'єкта КІІ в умовах реалізації ДІВ.

Оцінити коефіцієнт пов'язаності *j*-го одноланкового об'єкта КІІ та його внесок у цільову функцію багатоланкового об'єкта КІІ.

2. Оцінка кіберживучості взаємодіючих об'єктів КІІ (стовпчиків об'єктів КІІ).

Рівень кіберзахищеності – ймовірність збереження працездатності *n*-го багатоланкового об'єкта КІІ в умовах реалізації ДІВ.

3. Оцінка кіберживучості КІІ через суму стійкості її елементів з урахуванням їх коефіцієнта зв'язаності.

Оцінка кіберживучості КІІ загалом відповідно до поточного стану КІІ і ступеня важливості в певний момент часу виконання ними функцій.

Під час розробки методики оцінки стійкості об'єктів КІ, що функціонують у кіберпросторі, було запропоновано введення такої властивості, як кіберстійкість. Необхідність введення такої властивості зумовлена специфічним середовищем функціонування мережевої інфраструктури об'єктів КІІ (кіберпростір), застосуванням нового виду зброї – кіберзброї, і, як наслідок, появою нових вразливостей і загроз для КІІ і об'єктів КІІ Об'єднаної енергосистеми України. Запропонована методика завдяки декомпозиції КІІ на окремі об'єкти КІІ з урахуванням коефіцієнтів зв'язаності і ступеня важливості функцій, які виконуються в цей момент, дозволяє здійснити оцінку кіберстійкості КІІ відповідно до заданого рівня. Отриманий результат, відповідно до розробленої схеми відповідності стану об'єкта КІІ рівню захищеності (Рисунок 2), дозволяє однозначно оцінити стан кіберзахищеності КІІ від кібератак (ДІВ).

Висновки

1. Доступність критичної інформаційної інфраструктури впливає на її захищеність, яка напряму залежить від ступеня володіння відповідними організаціями засобами деструктивних кібервпливів, які створюють необхідні підстави для виникнення та здійснення ефективного протиборства у кіберпросторі.

2. Функціонування об'єктів критичної інформаційної інфраструктури у кіберпросторі породжує нові вразливості та загрози, потребуючи створення нового інструментарію забезпечення безпеки КІІ, під якою розуміється стан її захищеності, що забезпечує стале функціонування в умовах кібератак різної інтенсивності.

3. Об'єкти КІІ доцільно класифікувати за ознаками, що впливають на забезпечення кіберстійкості функціонування: за структурною організацією – одно ланкові, багатоланкові; за функціональною єдністю – багатоланкові однорідні, багатоланкові неоднорідні.

4. Узагальнений показник кіберстійкості охоплює показники кіберживучості, кіберзахищеності та кібернадійності КІІ.

Список використаної літератури

1. Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури. Монографія. К.: «Альфа Реклама», 2019. 176 с.

2. Мохор В. В., Гончар С. Ф., Дибач О. М. Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури. *Ядерна та радіаційна безпека*, 2019. № 2(82). С. 4-8. doi: 10.32918/nrs.2019.2(82).01.

3. Ерохин В. В., Погонышева Д. А., Степченко И. Г. Безопасность информационных систем: учебное пособие. М.: «Флинта», 2016. 184 с.

4. Чио К., Фримэн Д. Машинное обучение и безопасность. Пер. с анг. А.В. Снастина. М.: ДМК Пресс, 2020. 388 с.

5. Шаньгин В. Ф. Информационная безопасность и защита информации. М.: «ДМК Пресс», 2014. 702 с.

6. Hentea M. Improving security for SCADA control systems. *Interdisciplinary Journal of Information, Knowledge, and Management*. 2008. Vol. 3, P. 73-86. doi: 10.28945/91.

7. Izadi M., Hosseinian S. H., Dehghan S., Fakharian A., Amjady N. A critical review on definitions, indices, and uncertainty characterization in resiliency-oriented operation of power systems. *International Transactions on Electrical Energy Systems*. 2021. V. 31(1). doi: 10.1002/2050-7038.12680.

8. Krings A., Oman P. A simple GSPN for modeling common mode failures in critical infrastructures. *Proceedings of the 36th Annual Hawaii International Conference on System Sciences, 2003*. Big Island, HI, USA, 2003, HICSS 2003, P. 10-19. doi: 10.1109/HICSS.2003.1174908.

References

1. Honchar S.F. (2019). *Assessment of cybersecurity risks of information systems of critical infrastructure objects*. Monograph. K.: Alpha Advertising. 176 p.

2. Mokhor, V., Gonchar, S., Dybach, O. (2019). Methods for the total risk assessment of cybersecurity of critical infrastructure facilities. *Nuclear and Radiation Safety*, 2(82), 4-8. doi: 10.32918/nrs.2019.2(82).01.

3. Erokhin V. V., Pogonysheva D. A., Stepchenko I. G. (2016). *Security of information systems*: a tutorial. M .: Flinta.184 p.

4. Chio K., Freeman D. (2020). *Machine learning and security*. Transl. from eng. A.V. Snustina. Moscow: DMK Press. 388 p.

5. Shangin V. F. (2014). *Information security and information protection*. M .: DMK Press.702 p.

6. Hentea M. (2008). Improving security for SCADA control systems. *Interdisciplinary Journal of Information, Knowledge, and Management*. Vol. 3, 73-86. doi: 10.28945/91.

7. Izadi, M., Hosseinian, S. H., Dehghan, S., Fakharian, A., Amjady, N. (2021). A critical review on definitions, indices, and uncertainty characterization in resiliency-oriented operation of power systems. *International Transactions on Electrical Energy Systems*, 31 (1). doi: 10.1002/2050-7038.12680.

8. Krings, A., Oman, P. (2003). A simple GSPN for modeling common mode failures in critical infrastructures. Paper presented at the *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*, HICSS 2003, 10-19. doi: 10.1109/HICSS.2003.1174908.

Study of the Cyber Survivability of Critical Information Infrastructure Objects

Komarov M.[1], Honchar S.[1], Dimitriieva D.[2]

[1] G.E. Pukhov Institute for Modelling in Energy Engineering of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
[2] State enterprise «State Scientific and Technical Center for Nuclear and Radiation safety», Kyiv, Ukraine

The article considers an approach to assess the cyber resilience of a critical information infrastructure (CII), which functions under confrontation between two or more parties. Assessment result is the value of the general criterion of CII object ability to perform the target function at a specific point of time. A method to assess the cyber survivability of critical information infrastructure objects of the United Energy System of Ukraine is proposed. The definition of cyber survivability is presented. The management properties that determine the cyber resilience of the system are presented. The model of information confrontation in cyberspace is considered. The properties of the management process are presented: adequacy, optimality, efficiency, resilience, secrecy. Critical infrastructure objects are classified on grounds affecting cyber resilience, in particular, structural organization. The definition of single-link and multi-link object of critical information infrastructure is presented. The classification of multi-link objects of critical information infrastructure based on functional homogeneity is presented: multi-link homogeneous and multi-link inhomogeneous. A generalized indicator of cyber resilience is presented. The dependences of cyber resilience level on the state of critical infrastructure object are obtained and the method and algorithm of their calculation are presented. The diagram of correspondence of the class of CII object state to the level of cyber survivability is presented. The generalized algorithm of a technique to estimate cyber resilience of objects of a critical information infrastructure is described.

Keywords: United Energy System of Ukraine, critical infrastructure objects, cybersecurity, cyber survivability, cyber resilience.

Отримано 15.01.2021