doi:https://doi.org/10.15407/emodel.41.01.043

УДК 519.7-004.65

С.Ф. Гончар, канд. техн. наук, **Р.П. Герасимов,**
В.В. Ткаченко, аспірант
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
(Україна, 03164, Київ, вул. Генерала Наумова, 15,
тел. +3809870000344, e-mail: sfgonchar@gmail.com)

Дослідження проблеми кіберживучості Об'єднаної енергосистеми України

Функціонування об'єктів критичної інфраструктури (КІ) в такому специфічному середовищі, як кіберпростір, пов'язане з уразливістю і загрозами та вимагає розробки нового інструментарію забезпечення стійкості в умовах комп'ютерних атак. Управління стійкістю функціонування КІ Об'єднаної енергосистеми (ОЕС) України ґрунтується на знаннях про стан об'єктів управління, стан середовища функціонування і про впливи, які відбуваються. Невід'ємним елементом таких систем управління є низка підсистем підтримки прийняття рішень. Можливості системи управління залежать від здатності підсистеми підтримки прийняття рішень забезпечити особу, що приймає рішення, якісно збалансованою інформацією, яка характеризує реальні і прогнозовані стани об'єктів КІ, та запропонувати обґрунтований вибір дій для досягнення мети. Розглянуто питання кіберстійкості інформаційної системи, її основні компоненти, властивості управління, що визначають кіберстійкість. Здійснено класифікацію об'єктів КІ. Отримано залежності рівня якості кіберстійкості від класу стану об'єкта КІ та наведено методику і алгоритм його розрахунку.

К л ю ч о в і с л о в а: кіберживучість, методика, властивість, інфраструктура, кіберстійкість, кіберпростір.

Методика оцінки критичної інфраструктури ОЕС України, що функціонує в кіберпросторі. Високий рівень автоматизації управління і глобалізації інформаційних систем (ІС) через інформаційно-телекомунікаційні системи (ІТС) загального користування (ЗК) зумовив формування глобального інформаційного суспільства і нового середовища його функціонування — кіберпростору, що ставить об'єкти критичної інфраструктури (КІ) в залежність від ступеня захищеності ІТС. Кібернетичне протиборство — різновид боротьби, в ході якої здійснюється кібернетичний вплив на апаратно-програмні комплекси автоматизованих систем (АС) противника, спрямований на руйнування їх нормального функціонування,

що ставить об'єкти КІ в залежність від ступеня захищеності транспортних ІТС.

Аналіз відкритих джерел, присвячених забезпеченню безпеки КІ, надійності і стійкості функціонування АС об'єктів КІ, свідчить про те, що в них практично не розглядаються питання, пов'язані з розробкою:

моделей і методів побудови системи оцінки стану об'єктів КІ;

науково-методичного апарату побудови АС збору та приведення до єдиного виду інформації, що характеризує стан КІ в умовах деструктивних інформаційних впливів (ДІВ);

моделей і методів адаптивного управління КІ, які враховують поточний і прогнозований стан об'єктів КІ в умовах ДІВ.

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

Кіберживучість є наслідком протиборства як мінімум двох сторін, що здійснюється при спільному використанні загального ресурсу (глобального інформаційного простору), управління яким слід розглядати як цілеспрямований вплив двох (і більше) підсистем управління, що прагнуть поширити керуючий вплив один на одного (рис. 1). При цьому треба відзначити, що, незважаючи на суттєве спрощення та ідеалізацію, модель, схему якої наведено на рис. 1, дозволяє сформулювати найважливіші властивості, притаманні будь-яким процесам управління, а саме адекватність, оптимальність, оперативність, стійкість та скритність.

Розглянемо дані властивості з точки зору функціонування об'єктів КІ в кіберпросторі в умовах застосування нового виду зброї — кіберзброї.

Адекватність управління полягає в здатності процесу здійснювати перетворення інформації про стан об'єкта, отриманої від підсистеми моніторингу, в керуючий інформаційний вплив (КІВ), внаслідок чого об'єкт управління переходить до стану, який відповідає ситуації, що склалася. Вочевидь коректність перетворень залежить здебільшого від достовірності отриманої інформації про стан і правильність визначення цільової функції об'єкта управління. Відтак, властивість адекватності в значній мірі залежить від достовірності і повноти інформації, коректності операцій перетворення інформації та їх послідовності.

Оптимальність — це є вибір таких керуючих впливів, за яких точно досягається екстремальне значення деякого критерію, що характеризує якість управління. Зазвичай намагаються мінімізувати втрати в системі, які піддаються впливу, а саме грошові витрати або втрати інших ресурсів. Оскільки всі допустимі дії приводять до мети і кожна з них пов'язана з певною втратою ресурсів (часу, додаткових навантажень на обчислювальні ресурси та ін.), для кращого споживання цих ресурсів (з точки зору доцільності) існує краща «траєкторія». Якщо в процесі управління система

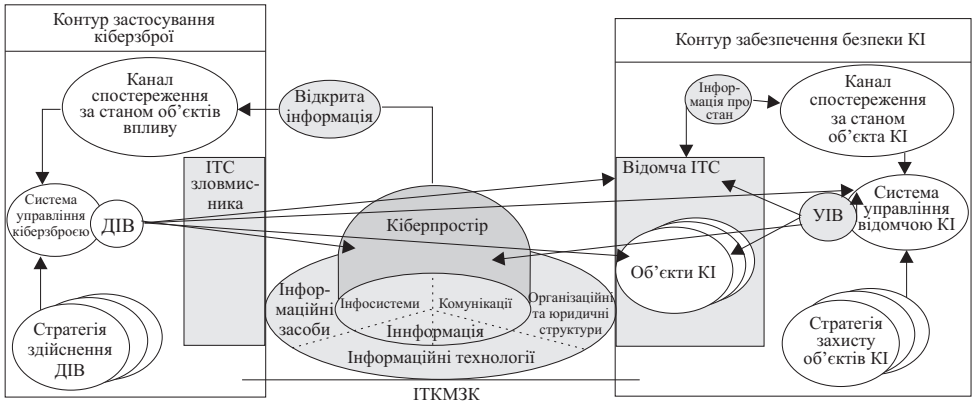

Рис. 1. Схема моделі інформаційного протиборства в кіберпросторі: УІВ — управління інформаційними впливами

«рухається» в просторі ситуацій саме по цій траєкторії, то кажуть, що управління оптимальне.

Оперативність — це є здатність процесу перетворювати інформацію відповідно до часових обмежень, тобто властивість управління перетворювати інформацію відповідно до темпу зміни поточної ситуації. Залежно від виду операції, яка домінує в процесі управління, розрізняють оперативність семантичного (смислового) перетворення (наприклад, вироблення рішення) та оперативність перетворення інформації (наприклад, оперативність передачі даних або виконання якихось розрахунків).

Стійкість управління визначається здатністю системи управління виконувати свої функції в складних обставинах, що різко змінюються, в умовах деструктивних впливів протиборчої сторони (сторін). Як правило, стійкість є інтегральною властивістю, що визначається живучістю, завадостійкістю і надійністю. Ці властивості забезпечують здатність здійснювати управління в умовах впливу всіх деструктивних видів, технічних і програмних відмов, а також помилкових дій технічного персоналу і посадових осіб, зберігаючи при цьому значення всіх показників управління у встановлених межах.

Скритність — це властивість процесу управління забезпечувати зберігання в таємниці від протиборчої сторони факт, час і місце перетворення інформації, а також її зміст і приналежність до керуючих об'єктів. Деструктивні інформаційні (комп'ютерні) атаки в кібернетичному просторі є збурюючим впливом. Система управління об'єктом повинна компенсувати ці збурення, а в цілому об'єкт і система управління повинні мати стійкість до цих збурень, тобто бути кіберстійкими (cyber stability).

Однією з визначених властивостей стійкості є кіберстійкість об'єкта КІ. Під цим в даному разі будемо розуміти здатність системи управління об'єкта КІ виконувати свої функції в складних, різко змінюваних обставинах в умовах ДІВ. При оцінці кіберстійкості об'єктів КІ як складових елементів КІ, яка функціонує у кіберпросторі, виникає ряд проблем, пов'язаних зі складністю об'єктів КІ, складністю і різнорідністю зв'язків між ними і умовами спільного з противником використання ресурсів транспортної ІТС.

Існують різноманітні об'єкти КІ, тому доцільно провести їх декомпозицію за ознаками, що впливають на забезпечення кіберстійкості.

За структурною організацією: одноланкові і багатоланкові об'єкти КІ.

Одноланковий — це самодостатній об'єкт, який має необхідну структуру для виконання цільової функції (самостійний одиничний (базовий) елемент), наприклад окремі автоматизовані системи.

Багатоланковий — це об'єкт, який є структурним послідовним об'єднанням декількох одноланкових об'єктів КІ в єдину систему в рамках виконання єдиної цільової функції.

За функціональною однорідністю: багатоланкові однорідні і багатоланкові неоднорідні об'єкти КІ.

Багатоланковий однорідний — це об'єкт, який є структурним об'єднанням декількох одноланкових об'єктів КІ, що виконують однакову цільову функцію, в єдину систему в рамках виконання єдиної цільової функції. Прикладом багатоланкової однорідної структури є багатоінтервальна (складна) мережа передачі даних, що складається з різнотипних одноланкових систем передачі даних.

Багатоланковий різнорідний — це об'єкт, який є структурним об'єднанням декількох одноланкових об'єктів КІ, що виконують різні функції, наприклад інформаційно-телекомунікаційна мережа (ІТКМ), ІТС тощо.

Для об'єктів КІ, які використовують ІТКМ ЗК, мережі передачі даних, що надаються, зазвичай є багатоланковими. При цьому склад окремих ланок цих ліній залежить від обраних маршрутів проходження інформації по ІТКМЗК, а також відомчих ІТС.

Узагальнений показник кіберстійкості одноланкового об'єкта КІ має вигляд

$$K_{\text{о.у}} = K_{\text{ж}} * K_{\text{з}} * K_{\text{н}}.$$

Тут $K_{\text{ж}}$ — кіберживучість об'єкта КІ, трактується як ймовірність збереження його працездатності (виживання) в умовах виходу з ладу технічних засобів обробки інформації, тобто внесок кожного базового елемента

одноланкового об'єкта КІ у виконання ним цільової функції; $K_{з}$ — кіберзахищеність одноланкового об'єкта КІ, трактується як ймовірність забезпечення виконання цільової функції об'єкта КІ із заданою якістю в умовах застосування загальних і цілеспрямованих деструктивних інформаційних впливів, $K_{з}=(1-P_{д})(1-P_{ц})$, де $P_{д}$ і $P_{ц}$ — ймовірності ураження технічних засобів обробки інформації, що входять до об'єкту КІ, цілеспрямованими і деструктивними інформаційними впливами; $K_{н}$ — кібернадійність одноланкового об'єкта КІ, трактується як ймовірність забезпечення виконання цільової функції об'єкта КІ протягом визначеного часового інтервалу в умовах виникнення програмних помилок, технічних збоїв і ненавмисних помилкових дій технічного персоналу та посадових осіб об'єкта КІ,

$$K_{i\text{н}} = \prod_{i=1}^{N} K_{i\text{н}}(1-P_{i}).$$

До об'єктів КІ вже на етапах проектування висуваються досить жорсткі вимоги з технічної надійності і передбачається ряд спеціальних заходів щодо запобігання технічних і програмних відмов технічних засобів обробки інформації (наприклад, у результаті кластеризації серверів, резервування окремих компонентів). У відповідності до цього в задачах оцінки кіберстійкості КІ цілком можливо вважати ймовірність технічних відмов при своєчасному і якісному проведенні технічного обслуговування зневажливо малою, тобто $P_{\text{т.н}} = 1$, де $P_{\text{т.н}}$ — ймовірність технічного неспрацювання. У даному випадку кібернадійність одноланкового об'єкта КІ визначається так:

$$K_{\text{о.у}} = K_{\text{ж}} * K_{\text{з}}.$$

Кіберстійкість багатоланкового об'єкта КІ можна визначити так:

$$K_{\text{б}}(N) = \prod_{i=1}^{N} K_{i\,\text{о.у}}. \qquad (1)$$

В іншому випадку кіберстійкість багатоланкового об'єкту КІ треба розраховувати як спільну N-мірну щільність розподілу ймовірності збереження працездатності одночасно N ланок, які складають даний багатоланковий об'єкт КІ:

$$K_{\text{б}}(N) = P\{K_{1\text{о.у}} \geq K_{\text{л}}, K_{N\ \text{о.у}} \geq K_{\text{л}}\},$$

де $K_{\text{л}}$ — кіберстійкість окремої ланки. При цьому будемо вважати, що вираз (1) може бути нижньою (гарантованою) оцінкою кіберстійкості багатоланкового (складного) об'єкта КІ. Основою розрахунку кіберстійкості

об'єктів КІ є розрахунок показників кіберзахищеності і кіберживучості окремих ланок об'єкта КІ. Отже, необхідно розробити методику розрахунку показників кіберзахищеності і кіберживучості об'єкта КІ. При цьому визначальною властивістю з точки зору можливості виконання об'єктом КІ цільової функції буде кіберживучість, а кіберзахищеність буде її складовою частиною.

Методика оцінки кіберживучості об'єктів КІ. У зв'язку з тим що властивості, які характеризують кіберживучість об'єкта КІ в умовах здійснення ДІВ, починають проявлятися тільки після того, як він піддався впливу, міру живучості необхідно визначати з урахуванням умовної ймовірності збереження працездатності при умові, що система отримала локальне пошкодження Ω.

Під показником кіберживучості одноланкового об'єкта КІ $K_{\text{о}}$ будемо розуміти умовну імовірність невиходу кінцевого стану об'єкта КІ за межі заданої області безпечних станів S^I простору безпечних станів S у випадку проведення ДІВ Ω:

$$K_{\text{о.ж}} = P\left[(\| S - s_0 \| < S^I)\ \Omega\right].$$

Враховуючи функціональну вразливість системи, яку розглядаємо як імовірність виходу кінцевого стану системи із заданої безпечної області $S^I - V^S$, запишемо $K_{\text{оКІж}} = 1 - V_S$, а в конкретній точці часового інтервалу, що досліджується, $K_{\text{о.ж}}(t) = 1 - V_S(t)$.

Критерієм оцінки кіберживучості одноланкового об'єкта КІ будемо вважати вираз $K_{\text{ж}}^{\text{п}}(t) \geq K_{\text{ж}}^{\text{потр}}(t)$, де $K_{\text{ж}}^{\text{п}}(t)$ — поточний рівень живучості одноланкового об'єкта КІ; $K_{\text{ж}}^{\text{потр}}(t)$ — потрібний рівень його живучості в умовах здійснення деструктивних інформаційних впливів.

Визначимо критерій $W_{\text{б}}$ здатності багатоланкового об'єкта КІ виконувати цільову функцію за наступними умовами ДІВ:

об'єкт КІ повністю дієздатний —

$$W_{\text{б}} = K_{\text{ж}}^{\text{п}}(t) > 0{,}9; \tag{2}$$

об'єкт КІ в цілому дієздатний —

$$W_{\text{б}} = 0{,}9 \leq K_{\text{ж}}^{\text{п}}(t) < 0{,}7; \tag{3}$$

об'єкт КІ обмежений (основна мета) —

$$W_{\text{б}} = 0{,}7 \leq K_{\text{ж}}^{\text{п}}(t) < 0{,}5; \tag{4}$$

об'єкт КІ недієздатний (підлягає відновленню) —

$$W_{\text{б}} = 0{,}5 \leq K_{\text{ж}}^{\text{п}}(t) < 0{,}3; \tag{5}$$

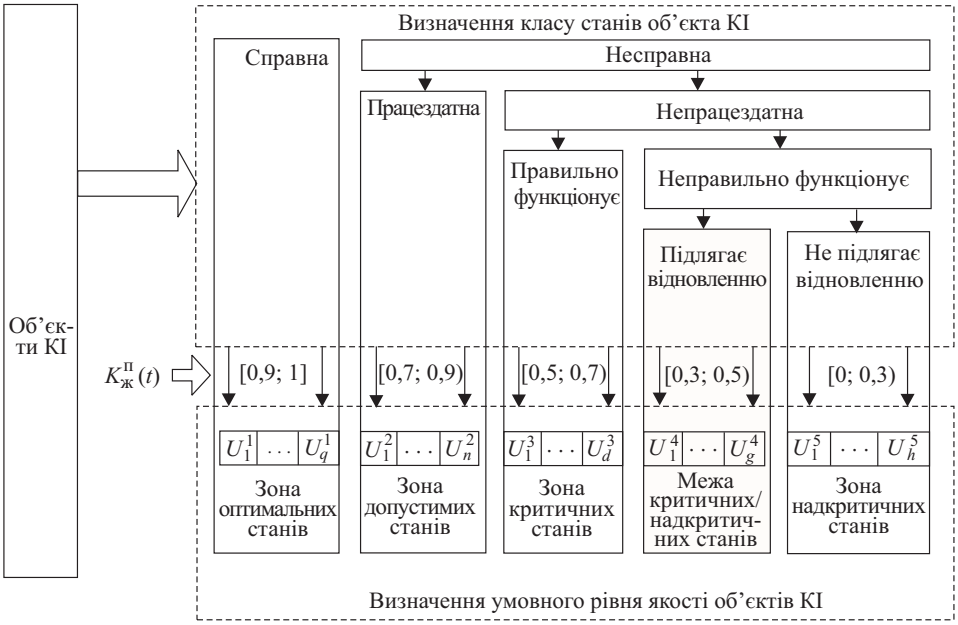

Рис. 2. Схема відповідності умовних рівнів якості класам станів об'єктів КІ

об'єкт КІ недієздатний (не підлягає відновленню) —

$$W_{б} = K_{ж}^{п}(t) \le 0{,}3. \tag{6}$$

Для визначення загального коефіцієнту живучості $K_{о.ж}^{з}(t)$ введемо наступні рівні кіберживучості:

оптимальний —

$$K_{ж}(t) = K_{ж}^{п}(t) - K_{ж}^{потр}(t) > 0; \tag{7}$$

допустимий —

$$K_{ж}(t) = K_{ж}^{п}(t) - K_{ж}^{потр}(t) = 0; \tag{8}$$

критичний —

$$K_{ж}(t) = K_{ж}^{п}(t) - K_{ж}^{потр}(t) < 0; \tag{9}$$

надкритичний —

$$K_{ж}(t) = K_{ж}^{п}(t) = 0. \tag{10}$$

Отримані за умовами (2)—(10) узагальнені результати наведено на рис. 2.

Методика оцінки кіберстійкості має наступні етапи:

1. Оцінка кіберстійкості кожного об'єкта КІ.

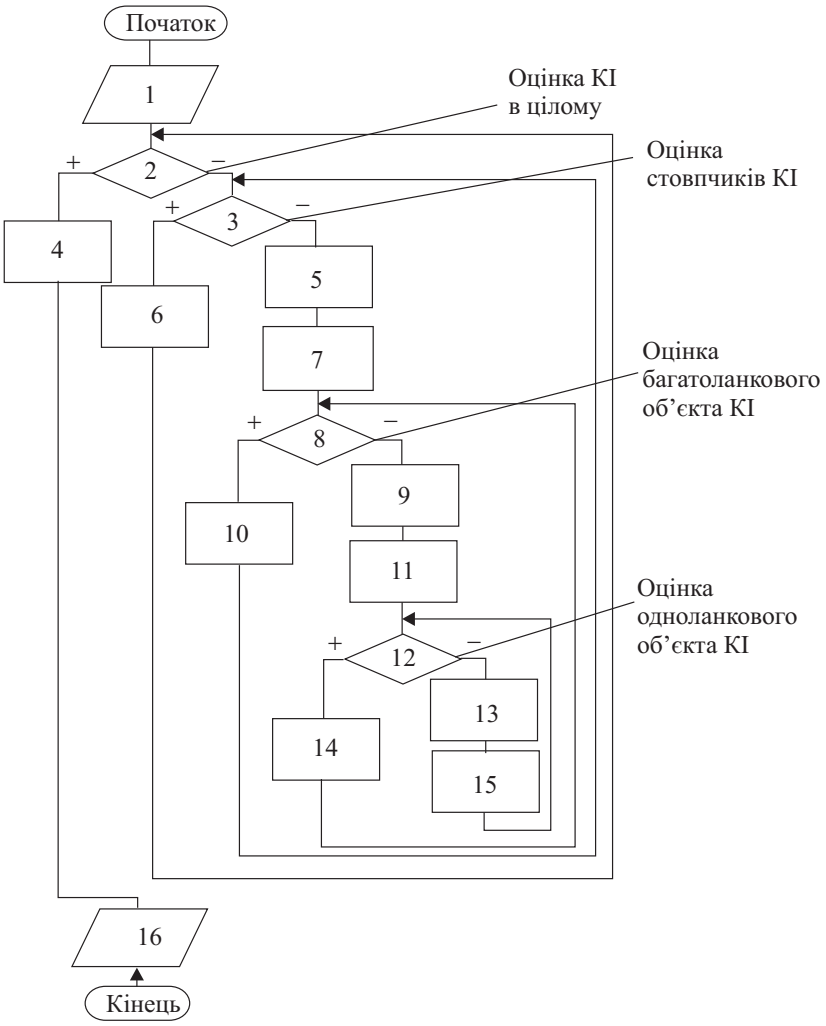

Рис. 3. Блок-схема узагальненого алгоритму методики оцінки кіберстійкості КІ: *1* — вихідні дані; *2* — *m*; *3* — *n*; *4* — оцінка кіберживучості КІ в цілому; *5* — оцінка кіберзахищеності багатоланкового об'єкта КІ; *6* — оцінка кіберживучості стовпчика КІ ; *7* — оцінка коефіцієнтів зв'язаності багатоланкового об'єкта КІ; *8* — *j*; *9* — оцінка кіберзахищеності одноланкового об'єкта КІ; *10* — оцінка кіберживучості багатоланкового об'єкта КІ; *11* — оцінка коефіцієнта зв'язаності одноланкового об'єкта КІ; *12* — *i*; *13* — оцінка кіберзахищеності елемента; *14* — оцінка кіберживучості одноланкового об'єкта КІ; *15* — оцінка коефіцієнта зв'язаності елемента; *16* — кінцеві дані

1.1.Оцінка одноланкового об'єкта КІ. Рівень кіберзахищеності — ймовірність виходу з ладу *i*-го елемента в умовах деструктивних інформаційних впливів. Оцінка коефіцієнта пов'язаності *i*-го елемента і його внесок в цільову функцію об'єкта КІ.

1.2. Оцінка багатоланкового об'єкта КІ. Рівень кіберзахищеності — ймовірність виходу з ладу *j*-го одноланкового об'єкта КІ в умовах реалізації деструктивних інформаційних впливів. Оцінка коефіцієнта пов'язаності *j*-го одноланкового об'єкта КІ та його внесок в цільову функцію багатоланкового об'єкта КІ.

2. Оцінка кіберстійкості взаємодіючих об'єктів КІ. Рівень кіберзахищеності — ймовірність виходу з ладу *n*-го багатоланкового об'єкта КІ в умовах реалізації деструктивних інформаційних впливів. Оцінка коефіцієнта пов'язаності *n*-го багатоланкового об'єкта КІ та його внесок у цільову функцію багатоланкового об'єкта КІ.

3. Оцінка кіберстійкості КІ через суму стійкості її елементів з урахуванням їх коефіцієнта пов'язаності. Оцінка кіберживучості КІ в цілому відповідно до поточного стану стовпчиків КІ і ступеня важливості в даний момент виконання ними функцій.

На рис. 3 наведено блок-схему алгоритму методики оцінки кіберстійкості КІ.

Таким чином, необхідність введення такої властивості, як кіберстійкість зумовлена новим середовищем функціонування мережевої інфраструктури ОЕС України (кіберпростір), застосуванням нового виду зброї, кіберзброї, і, як наслідок, появою нових вразливостей і загроз для КІ і об'єктів КІ ОЕС. Запропонована методика внаслідок декомпозиції КІ на окремі об'єкти з урахуванням коефіцієнтів зв'язаності і ступеня важливості функцій, які виконуються в даний момент, дозволяє здійснити оцінку стану захищеності КІ відповідно до заданого рівня якості. Це дає змогу однозначно оцінити стан захищеності КІ від комп'ютерних атак (деструктивних інформаційних впливів).

Висновки

Новизна запропонованої методики полягає в оцінці складних технічних систем, які мають високий ступінь критичності. Практична значимість розробленої методики полягає в можливості її застосування для підвищення ефективності управління КІ, а також для обґрунтування нових методів і засобів протиборства в кіберпросторі. Дану методику можна використовувати при розробці концептуальних рішень при побудові систем захисту інформації об'єктів КІ, а також при плануванні заходів із забезпечення безпеки інформації, що обробляється в спеціалізованих ІТС.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Корченко О.Г., Бурячок В.Л., Гнатюк С.О.* Кібернетична безпека держави: характерні ознаки та проблемні аспекти // Безпека інформації, 2013, **19**, № 1, с. 40—45.
2. *Мельник С.В., Тихомиров О.О., Лєнков О.С.* До проблеми формування понятійно-термінологічного апарату кібербезпеки // Зб. наук. праць Військового ін-ту КНУ ім. Тараса Шевченка, 2011, Вип. 30, с. 159—165.
3. *Тропина Т.Л.* Киберпреступность и кибертерроризм: поговорим о понятийном аппарате // Сб. науч. трудов междунар. конф. «Информационные технологии и безопасность», Вып. 3. Киев: НАН Украины, 2003, с. 173—181.

Отримано 10.12.18

REFERENCES

1. Korchenko, O.G., Buryachok, V.L. and Hnatyuk, S.O. (2013), “Cybernetic security of the state: characteristic features and problem aspects”, *Bezpeka informatsiyi*, Vol. 19, no. 1, pp. 40-45.
2. Melnyk, S.V., Tikhomirov, O. and Lenkov, O.S. (2011), “On the Problem of the Formation of the Conceptual-Terminological Device of Cyber security”, *Zb. nauk. prats Viyskovoho in-tu KNU im. Tarasa Shevchenka*, Vol. 30, pp. 159-165.
3. Tropina, T.L. (2003), “Cyber crime and cyber-terrorism: let’s talk about the conceptual apparatus”, *Sb. nauch. trudov mezhdunar. konf. «Informatsionnyye tekhnologii i bezopasnost»* [Scientific works of the Intern. conf. “Information Technology and Security”], Vol. 3, Kiev, NAS of Ukraine, pp. 173-181.

Received 10.12.18

С.Ф. Гончар, Р.П. Герасимов, В.В. Ткаченко

ИССЛЕДОВАНИЕ ПРОБЛЕМЫ КИБЕРЖИВУЧЕСТИ ОБЪЕДИНЕННОЙ ЭНЕРГОСИСТЕМЫ УКРАИНЫ

Функционирование объектов критической инфраструктуры (КИ) в такой специфической среде, как киберпространство, связано с уязвимостью и угрозами и требует разработки нового инструментария для обеспечения устойчивости в условиях компьютерных атак. Управление устойчивостью функционирования КИ Объединенной энергосистемы (ОЭС) Украины основано на знаниях о состоянии объектов управления, состояние среды обитания и действиях, которые происходят. Неотъемлемым элементом таких систем управления является ряд подсистем поддержки принятия решений. Возможности системы управления зависят от способности подсистемы поддержки принятия решений обеспечить лицо, принимающее решение, качественно сбалансированной информацией, характеризующей реальные и прогнозируемые состояния объектов КИ, и предложить обоснованный выбор действий для достижения цели. В связи с этим разработка методики оценки КИ, функционирующей в киберпространстве, является актуальной задачей.

К л ю ч е в ы е с л о в а: киберживучесть, методика, свойство, инфраструктура, киберстойкость, киберпространство.

S.F. Honchar, R.P. Herasymov, V.V. Tkachenko

INVESTIGATION OF THE PROBLEM OF CYBERSQUITY
OF THE UES OF UKRAINE AS A WHOLE

The operation of critical infrastructure objects in a specific environment such as cyberspace is associated with vulnerabilities and threats, and requires the development of new tools to ensure the sustainability of functioning in a computer attack. Management of the sustainability of the critical information infrastructure of the United Energy System of Ukraine is based on knowledge of the state of the objects of management, the state of the functioning environment and the effects that take place. An integral element of such control systems is a number of decision support subsystems. The capabilities of the management system directly depend on the ability of the decision support subsystem to provide the decision maker with a well-balanced information that characterizes the real and predicted states of the critical infrastructure objects and propose a reasonable choice of the trajectory for achieving the goal. In this regard, the development of a methodology for assessing the critical information infrastructure functioning in cyberspace is an urgent task.

K e y w o r d s: cyber life, technique, property, infrastructure, cyber resistance, cyberspace.

ГОНЧАР Сергій Феодосійович, канд. техн. наук, пров. наук. співр. Ін-ту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. У 1997 р. закінчив Вінницький національний технічний університет. Область наукових досліджень — теорія ризиків безпеки, кібербезпека об'єктів критичної інфраструктури, у тому числі в енергетичній галузі.

ГЕРАСИМОВ Ростислав Павлович, наук. співр. Ін-ту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. У 1980 р. закінчив Київський ін-т інженерів цивільної авіації. Область наукових досліджень — математичне і комп'ютерне моделювання, інформаційна безпека.

ТКАЧЕНКО Володимир Володимирович, аспірант Ін-ту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. У 1996 р. закінчив Київський військовий інститут управління та зв'язку. Область наукових досліджень — теорія ризиків безпеки, кібербезпека об'єктів критичної інфраструктури, у тому числі в енергетичній галузі.