УДК 004.056

Телелим В. М., д.військ.н., професор;
Даник Ю. Г., д.т.н., професор;
Зінченко А. О., д.т.н., доцент

Національний університет оборони України імені Івана Черняховського, Київ

Модель оцінювання вразливостей систем із критичною кібернетичною інфраструктурою

Резюме. У статті на основі представлення сукупності сучасних кібернетичних систем та зв'язків між ними у вигляді моделі неорієнтованого графа розроблено модель системи з критичною кібернетичною інфраструктурою. Зміна структури кібернетичної системи щодо нових завдань та (або) як реакція на деструктивні кібервпливи для збереження функціональної стійкості та здатності була описана рівнянням балансу "потреб-можливостей", яке у цьому випадку відображає функціональну залежність між величиною потреб для нейтралізації кібернетичних загроз і наявними можливостями.

Ключеві слова: кібернетична безпека, кібернетична система, критична кібернетична інфраструктура, модель.

Постановка проблеми. Протягом останніх десятиліть у життя стрімко увійшли нові поняття і реалії кібернетичної сфери, кіберпростору, кіберзагроз тощо. До того ж вони охоплюють майже всі аспекти діяльності громадян, суспільства, держав і світової спільноти в цілому та знаходяться в безперервному активному розвитку. Особлива увага приділяється питанням кібернетичної безпеки, до сфери якої відносять все, що пов'язано з управлінням електронними, інформаційними та безпосередньо кібернетичними системами, включаючи соціотехнічні системи. Крім того, розглядаються питання їх функціонування - від антивірусного забезпечення окремої персональної обчислювальної машини до безпеки систем управління підприємств, відомств і держав, від окремих особистостей і складових соціуму до соціуму в цілому.

Аналіз останніх досліджень і публікацій. Кількість публікацій на зазначені теми у мережі *Internet* більш ніж чисельна. Уведення у пошукову сторінку *Google* запиту "*кібернетична безпека*" видає близько 40 000 посилань. Аналогічний запит англійською мовою "*cyber security*" видає вже 330 000 000 посилань. З аналізу цих посилань видно, що галузь знань "кібернетична безпека" знаходиться у стадії активного формування. До того ж, єдині погляди, стійкий категорійний апарат і єдина методологія досі не сформувалися. Існує низка підходів, які викладені у наукових статтях, виступах на конференціях і симпозіумах, програмних документах і законодавчих міжнародних і національних актах різних країн [1-4]. Значну увагу у відомих публікаціях приділяють вразливостям кіберсистем, але питання їх кількісного оцінювання для систем із критичною кібернетичною інфраструктурою досі потребує вирішення. У цій статті системи з критичною кібернетичною інфраструктурою розглядаються з класичних позицій "вінерівської кібернетики", як науки про загальні закономірності процесів управління і передачі інформації в живих організмах, суспільстві та машинах [5]. Саме тому, далі будемо оперувати визначенням *кібернетичної безпеки* як станом захищеності управління в усіх сферах за якого забезпечується його ефективне здійснення. Таким чином, незважаючи на природу процесів управління і не прив'язуючись до конкретного виду технічної, ергатичної або суспільної системи управління, система управління як така була, є і надалі залишатиметься об'єктом кібернетичної безпеки. Першочерговими завданнями, які покладатимуться на систему кібернетичної безпеки, будуть завдання з виявлення та пошуку об'єктів із критичною кібернетичною інфраструктурою, а також організація їх кібернетичного захисту для унеможливлення виникнення процесів ланцюгової реакції та, як наслідок, кібернетичного колапсу в економіці, фінансах, політиці, військовій сфері та в державі в цілому [6, 7].

Метою статті є розроблення моделі оцінювання вразливостей систем із критичною кібернетичною інфраструктурою.

Виклад основного матеріалу. Система управління незалежно від її цільового призначення та природи походження є базовою основою будь-якої кібернетичної системи. Сукупність усіх кібернетичних систем, які існують у живій і неживій природі та зв'язків

між ними можливо подати у вигляді моделі неорієнтованого графа.

Вершинами графа є кібернетичні системи різної природи, а ребрами – зв'язки між ними. У зваженому графі можна виділити кібернетичні системи, вплив на які матиме фатальні та катастрофічні наслідки для усієї моделі взаємодії кібернетичних систем, а у складі будь-якої кіберсистеми існують аналогічні критичні елементи, порушення роботи яких породжує синергію процесів деструкції. Такі кібернетичні системи називають кібернетичними системами з критичною кібернетичною інфраструктурою. Як видно з графової моделі, кібернетичні системи з критичною кібернетичною інфраструктурою містять значну кількість зв'язків між собою і з іншими кібернетичними системами. Руйнування будь-якого з цих зв'язків потенційно може призвести до ефекту "ланцюгової реакції", що, як наслідок, зруйнує всю управлінську структуру.

Кібернетичні системи з критичною кібернетичною інфраструктурою виступають ключовим елементом у забезпеченні сталого функціонування та взаємодії всіх інших систем. Кібернетична інфраструктура охоплює безліч елементів критичної інфраструктури держави.

Розв'язання проблеми кібернетичної безпеки істотно стримується через відсутність єдиного підходу до виявлення та пошуку власне "об'єкта" кібернетичної безпеки. На прикладі об'єктів із критичною кібернетичною інфраструктурою розкриємо сутність цього процесу, але перед цим розглянемо відомі рішення у цій галузі. Основу більшості відомих досліджень присвячених розробленню методів виявлення та пошуку об'єктів з критичною кібернетичною інфраструктурою складає методологія експертного аналізу. Її базисом виступають методи експертного оцінювання. Однак, як відомо, застосування методів експертного оцінювання пов'язано з розв'язанням проблеми пошуку доступної вихідної інформації щодо можливої шкоди, яка наноситься "еталонному об'єкту з критичною кібернетичною інфраструктурою". Також методам експертного оцінювання притаманні й інші недоліки: достовірність і надійність результатів дослідження залежать від компетентності експертів; суб'єктивність методу; трудомісткість процедури збору інформації; потреба у високопрофесійних спеціалістах для проведення опитування. З огляду на високу технологічність, швидкість розвитку, кількість галузей застосування кібернетичних систем і їх взаємозв'язок застосування методу експертного оцінювання виглядає недоцільним.

Окремої уваги потребують моделі, що використовуються експертами для оцінювання кібернетичної інфраструктури. Основний недолік цих моделей полягає у тому, що дослідження об'єктів з критичною кібернетичною інфраструктурою здійснюються без урахування критичної мережевої архітектури до якої вони входять. Тим часом, без урахування критичної мережевої архітектури та її аналізу істотно знижується адекватність моделі і, відповідно, достовірність отримуваних оцінок.

Можливим підходом до усунення зазначеного недоліку є застосування для аналізу об'єктів із критичною кібернетичною інфраструктурою системного підходу. За такої умови критична кібернетична інфраструктура розглядається як велика складна система і характеризується такими атрибутами: необмежена кількість варійованих об'єктів і параметрів системи; важкопрогнозована поведінка об'єктів із великою кількістю взаємозв'язків.

Проте кількість подібних центрів тяжіння невелика, що обґрунтовано теорією мереж, що самоорганізуються, в роботах Альберто Барабаши [8]. За цією теорією великі мережеві структури (наприклад, Інтернет, соціальні мережі тощо), які здавалися раніше неструктурованими, тобто випадковими, насправді мають складну внутрішню організацію і є такими, що самоорганізуються, з кількома ключовими "вузлами" або центрами тяжіння.

Крім того, будь-яка неструктурована (пуасонівска) мережа під впливом набору загальновідомих правил і законів, у першу чергу економічного і соціального характеру, через певний час (після деякого числа ітерацій) набуває відповідної структури, без будь-якої зовнішньої дії, організовуючись навколо найважливіших критичних вузлів.

Валентність (кількість зв'язків) будь-якого вузла мережі, що самоорганізується, підпорядкована степеневому закону розподілу, який визначає ймовірність взаємодії вершин $P(k)$ з іншими k вершинами (вузлами)

$$P(k) = 2m^2 / k^3, \qquad (1)$$

де m – кількість вершин;

k – вузли мережі, які задіяні в процесі самоорганізації.

Згідно із законом (1) кількість вузлів $P(k)$ у мережі, яка має k зв'язків з іншими вузлами, пропорційна величині $k^{-1}m$.

За аналогією система з критичною кібернетичною інфраструктурою може бути подана критичною мережевою архітектурою, пов'язаних між собою за визначеними законами елементів (об'єктів), які входять до її складу. До того ж, слід відмітити, що кількість "найбільш важливих" серед таких об'єктів є величиною зліченною й обмежується їх певною кількістю.

Центри тяжіння в кожному секторі критичної кібернетичної інфраструктури формуються відповідно до різних законів: економічних, соціального розвитку, еволюції та інших, які дають змогу із сукупності раніше неструктурованих об'єктів формувати мережі, що самоорганізуються. Саме поява подібних центрів тяжіння призводить до самоорганізації мережі й можливості її ефективного функціонування.

Вочевидь саме тому у всіх сучасних імітаційних моделях основним підходом до розв'язання такої задачі є розроблення відповідних методів із використанням теорії графів, яка дає змогу наочно представити комплексні взаємозв'язки між об'єктами і розробити математичні моделі, які описують рівень взаємодії і взаємозалежності між ними. У зв'язку з цим критична кібернетична інфраструктура, як велика складна система стратегічного масштабу і подається у вигляді зваженого орієнтованого або неорієнтованого графа, вершини якого – об'єкти, а ребра – зв'язки між ними.

Зміна структури кібернетичної системи щодо нових завдань (упровадження або вилучення окремих підсистем, які призначені для виконання відповідних процесів) може бути описана рівнянням балансу "потреб-можливостей", яке вважаємо функцією початкових даних про величину потреб для нейтралізації кіберзагрози і наявності можливостей їх забезпечення

$$\frac{dA(t)}{dt} = F(t,s) - D(t,F,s), \qquad (2)$$

де $A(t)$ – показники структури кібернетичної системи з критичною кібернетичною інфраструктурою, що змінюються протягом деякого часу *t*;

$F(t,s)$ - потік ресурсів, який надається зовнішнім середовищем для зниження ризику реалізації кібернетичної загрози в кібернетичній системі з критичною кібернетичною інфраструктурою, за рахунок яких вона адаптується до нових умов;

$D(t,F,s)$ - вихідний потік перероблених ресурсів із системи з критичною кібернетичною інфраструктурою (не з *F*-потоку), які вона віддає іншим системам у вигляді послуг (готової продукції);

s - елементарний процес виконання визначеної послуги.

Вираз (2) описує кібернетичну систему, яку побудовано за принципом відкритої архітектури, її структура змінюється залежно від появи нових завдань, які виникають унаслідок нейтралізації кіберзагрози. В умовах невизначеності наслідків впливу $\nu(t)$ кіберзагроз прогнозування значень $D(t,F,s)$ можливе на основі деяких закономірностей цих впливів. Йдеться про те, що прояв реалізації кіберзагрози супроводжується порушенням порядку, а це викликає підвищення невизначеності та неорганізованості. Для нейтралізації кіберзагрози необхідно завчасно реорганізувати відповідну структуру шляхом введення нового порядку.

Для цього орган управління визначає керуючий вплив $u(t)$, а саме для управління балансом витрат ресурсів у $F(t,s)$ і $D(t,F,s)$ – потоках у *s*-му процесі. Саме тому доцільне введення керуючих впливів у рівняння (2) в умовах кібернетичних впливів $U_F(t,u_\nu)$ і $U_D(t,u_\nu)$, тобто

$$\frac{dA(t)}{dt} = F(t,s)U_F(t) - D(t,F,s)U_D(t), \qquad (3)$$

де $U_F(t)$ і $U_D(t)$ набувають негативних або позитивних значень у певні моменти часу для коригування параметрів існуючої структури.

Зміст виразу (3) у тому, що за певних значень керуючих впливів $U_F(t)$ і $U_D(t)$ структура може бути незмінною тільки при $\frac{dA(t)}{dt} = 0$. У противному випадку керуючий вплив $U_F(t,u_\nu)$ діє на $F(t,s)$-потік, змінюючи залежно від цілей витрату ресурсів у ньому; $U_D(t,u_\nu)$ регулює витрату ресурсів у $D(t,F,s)$-потоках. Саме тут вплив загрози можна розглядати як появу нових завдань і контролювати значенням. Звідси сукупність значень $D(t,F,s)$ створюватиме ряд, в якому можна очікувати наявність тенденції (тренду), циклічної (стаціонарної) і випадкової складових.

Для вирішення завдання побудови ряду, який відображає динаміку змін завдань (відповідно до структури), як правило, застосовується процесорний підхід О. О. Богданова [9]. Цей підхід дає змогу розглядати систему як сукупність

процесів щодо забезпечення її потреб. Кожен процес складається із сукупності операцій, які об'єднані певною технологією управління. Ефективність процесу оцінюється ступенем досягнення корисного ефекту, з використанням притаманного йому критерію (вимоги). Звідси виникає можливість застосування індексного методу для оцінювання забезпеченості безпеки від кіберзагроз.

Особливістю моделі є те, що вона відображає поведінку системи з критичною кібернетичною інфраструктурою на момент непередбачуваної зміни її структури, яка відбувається у результаті кібернетичного впливу. Відомі ж моделі такої властивісті не мають. Розроблена модель додатково забезпечує підвищення своєчасності й ефективності вирішення завдань кібернетичною системою за призначенням в умовах кібернетичного впливу, що, як наслідок, призводить до забезпечення збереження можливості нею стійкого виконання тих зі старих завдань, необхідність у вирішенні яких зберігається при рівні ризику прийнятих рішень, не вище припустимого або заданого.

Таким чином, на основі розробленої моделі кібернетичної системи з критичною кібернетичною інфраструктурою та приведеного аналізу можна дійти таких висновків:

корисний ефект системи визначається кількістю визначених, покладених і вирішених нею завдань, кожне з яких спрямоване на досягнення певної вимоги;

корисний ефект від функціонування сукупності елементів, які складають систему в умовах невизначеності, буде тим більшим, чим більше буде їх організованість в ієрархію;

процес зміни структури кібернетичної системи з критичною кібернетичною інфраструктурою є процесом виконання (досягнення) вимоги, що встановлює вищий орган управління та відображається траєкторією розвитку до кожного процесу.

Це надає можливість застосування *постулатів*:

ступінь організованості системи визначає якість вирішення нею завдання;

загальна структура системи складається із сукупності віртуальних структур, кожна з яких націлена на вирішення певного завдання (задоволення потреби);

кожна така віртуальна структура під дією органу управління (процес організовування) переходить до ефективніших станів щодо певних цілей (вимог);

аналіз та формалізоване оцінювання об'єднання віртуальних структур у певні кіберсистеми надає можливість отримати обґрунтовані вимоги до дій органів управління, які їх застосовують для виконання завдань за призначенням.

Висновки. Традиційний показник якості управління існує для замкнених (стійких) кібернетичних систем, у визначених межах змінних, за відповідної цілям структури системи. При втраті функціональної стійкості цієї системи поняття якості управління не існує, а для нової структури буде своя якість управління. Застосування лінійних моделей для оцінювання керуючих впливів доцільне, коли малі відхилення вхідних збурень нейтралізуються стійкістю системи. Для випадку, коли досить малий керуючий вплив виявляється у значних відхиленнях стану, що призводить до його критичності, треба враховувати фактичний прояв нелінійності, для цього потрібні інші методи. У критичний момент доцільно визначати тенденції розвитку і темп зміни показників щодо орієнтирів (вимог), які описуються рівнянням балансу "потреб-можливостей" певної структури.

Під час реорганізації є очевидним здійснення оцінювання якості управління через показник керованості, який треба тотожно замінити на оцінку ступеня порядку (організованості) за обмежень на стійкість, оперативність і ризик. Новим моментом тут є оцінювання організованості через її складові технічної та організаційної готовності до виконання завдань за допомогою коефіцієнта організованості, що відображатиме ефективність дії органів управління під час процесів реорганізації. Це дає змогу діагностувати стан кібернетичної системи за допомогою відомих показників, наприклад, фрактальною розмірністю, значення якої свідчить про той чи інший стан системи і його зміни, які можуть призвести до розвитку кризового стану.

Під час реорганізації необхідно контролювати кожний процес виконання завдання. Наслідком цього є можливість формально визначити сукупності завдань: *базових,* виконання яких організовано; *асоціативних,* для виконання яких треба організувати в структуру деяку сукупність сил і засобів. Для кожного завдання існує своя *віртуальна структура.* До того ж із сукупності віртуальних структур для базових завдань складається базова структура, яка існує постійно. Із сукупності асоціативних завдань складається змінна частина структури. Віртуальні структури потрібно об'єднувати в загальну лінійно-функціональну структуру, яка є найпоширенішим для застосування видом структури.

Для врахування можливих впливів кіберзагрози слід враховувати її математичну модель (2), що дасть змогу визначити заходи, здійснення яких призведе до зміни структури кібернетичної системи для завчасного виявлення її проявів і визначення заходів із нейтралізації передумов виникнення критичних ситуацій при її реалізації. Для визначення впливів кіберзагрози

формується певна кількість поточних значень $D(t,F,s)$, на основі якої практично створюватиметься повна сукупність оцінок відповідності системи її функціональному призначенню. Отриманий у результаті фільтрації тренд дає змогу, наприклад, визначати напрям розвитку, а кут його нахилу – швидкість змін, що відбуваються.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. С. Гнатюк, М. Рябий, В. Лядовська, “Визначення критичної інформаційної інфраструктури та її захист: аналіз підходів”, Зв’язок, № 4, С. 3-7, 2014.
2. С. Гнатюк, В. Лядовська, “Критерії визначення елементів критичної інфраструктури держави”, Матеріали XXIII всеукр. наук.-практ. конф. Інноваційний потенціал світової науки — XXI сторіччя. Запоріжжя: Вид-во ПГА, С. 55-57, 2013.
3. A. Wenger, V. Mauer, M. Cavelty “International critical information infrastructure protection hand-book 2008-2009”, Center for Security Studies, ETH Zurich, 2009.
4. О. Довгань, “Критична інфраструктура як об’єкт захисту від кібернетичних атак”, Матеріали наук.-практ. конф. Інформаційна безпека: виклики і загрози сучасності. К: НА СБ України, С. 17-20, 2013.
5. Винер Н. Нелинейные задачи в теории случайных процессов. - М.: ИЛ, 1961.
6. Даник Ю. Г., Грищук Р. В. Основи кібернетичної безпеки: монографія; за заг. ред. проф. Ю. Г. Даника. Житомир: ЖНАЕУ, 2016. - 636 с.
7. Національна безпека: запобігання критичним ситуаціям: Монографія / Ю. Г. Даник, Ю. І. Катков, М. Ф. Пічугін К.: МО України. – Житомир: Рута, 2006. – 388 с.
8. Albert-László Barabási & Réka Albert (October 1999). “Emergence of scaling in random networks”. Science 286 (5439): 509–512. DOI:10.1126/science.286.5439.509.
9. А. А. Богданов (Малиновский) Всеобщая организационная наука: Тектология: В 2 книгах. Москва: Книга, 1912.

Стаття надійшла до редакції 30.08.2018

Телелим В. М., д.воен.н., профессор
Даник Ю. Г., д.т.н., профессор;
Зинченко А. А., д.т.н., доцент
Национальный университет обороны Украины имени Ивана Черняховського, Киев

Модель оценки уязвимостей систем с критической кибернетической инфраструктурой

Резюме. В статье на основе представления совокупности кибернетических систем и связей между ними в виде модели неориентированного графа разработана модель системы с критической кибернетической инфраструктурой. Изменение структуры кибернетической системы относительно новых задач и (или) как реакция на деструктивные киберугрозы для сохранения функциональной устойчивости и способности описана уравнением баланса “потребностей-возможностей”. Приведенное уравнение отражает функциональную зависимость между величиной потребностей для нейтрализации кибернетических угроз и имеющимися возможностями.

Ключевые слова: кибернетическая безопасность, кибернетическая система, критическая кибернетическая инфраструктура, модель.

V. Telelym, DsM, professor;
Y. Danyk, DsT, professor;
A. Zynchenko, DsT, assistant professor
National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv

The vulnerability assessment model for systems with critical cybernetic infrastructure

Resume. In the article, based on the representation of the aggregate of cybernetic systems and the relationships between them in the form of an undirected graph model, a model of a system with a critical cybernetic infrastructure was developed. Changing the structure of the cybernetic system with respect to new tasks and (or) as a reaction to destructive cyber threats to preserve functional stability and ability is described by the balance equation of “needs-opportunities”. The above equation reflects the functional relationship between the magnitude of the needs for neutralizing cyber threats and the available opportunities.

Keywords: cybernetic security, cybernetic system, critical cybernetic infrastructure, model.