*2. **Заде, Л. А.** Основы нового подхода к анализу сложных систем и процессов принятия решений / Л. А. Заде // Математика сегодня.— М.: Знание, 1974.— С. 5–49.*

*3. **Zadeh, L. A.** Fuzzy sets / L. A. Zadeh // Information and Control.— 1965.— P. 338–353.*

*4. **Підручник** для студентів вищих навчальних закладів за напрямком «Телекомунікації» з дисциплін СП, ТОТСМ, ТЕСЗ.-К ДУТ 2014-700с з. іл. Бібліогр. в кінці розд. ISDN 966-575-039-9 [Електронний ресурс].— Режим доступу:*

http://www.dut.edu.ua/ua/lib/1/category/1116/view/684

*5. **Narendra, K. S.** Bck propagation in dynamical systems containing neural networks [Електронний ресурс] / K. S. Narendra, K. Parthasarathy.— Режим доступу:*

https://ac.els-cdn.com/0888613X9290014Q/1-s2.0-0888613X9290014Q-main.pdf?_tid=7c90fedc-f5d8-11e7-b7aa-00000aab0f6c&acdnat=1515569761_83620b6a11dd5631dff6b78324e61b2e

Рецензент: доктор техн. наук, професор **В. В. Вишнівський**, Державний університет телекомунікацій, Київ.

Ю. В. Мельник, К. П. Сторчак

ПОСТРОЕНИЕ ОБОБЩЕННОЙ НЕЙРОСЕТЕВОЙ МОДЕЛИ ИЕРАРХИЧЕСКОГО УПРАВЛЕНИЯ СЕТЬЮ СВЯЗИ

Определена математическая модель иерархического управления, а также представлена модель объекта контроля и диагностики при нечетких условиях воздействий и управления.

Ключевые слова: критерии управления; модель управления; нечеткое множество; система контроля; сеть связи.

Yu. V. Melnik, K. P. Storchak

CONSTRUCTION OF A GENERALIZED NEURAL NETWORK MODEL OF HIERARCHICAL CONTROL OF A COMMUNICATION NETWORK

The article defines a mathematical model of hierarchical control and a model of the object of control and diagnostics under fuzzy conditions of impacts and control.

Keywords: management criteria; management model; fuzzy set; control system; communication network.

УДК 004.8+65.05+681.5

В. В. ВИШНІВСЬКИЙ, доктор техн. наук, професор;
Ю. І. КАТКОВ, канд. техн. наук, доцент;
С. О. СЄРИХ, канд. техн. наук, доцент,
Державний університет телекомунікацій, Київ

Роль і місце інформаційної інфраструктури під час виникнення явища критичності організаційної системи

Розглянуто загальні положення щодо організаційних систем із критичною інфраструктурою та умови реорганізації як напрямку дослідження невідповідності інфраструктури організаційної системи в результаті впливу можливих викликів або загроз, які можуть призвести до критичного стану будь-який важливий елемент цієї системи або інших систем. Виконано аналіз термінів для опису впливу на організаційну систему з критичною інфраструктурою, що викликають необхідність її реорганізації. Подано математичну модель оцінювання рівня критичності організаційної системи з критичною інфраструктурою.

Ключові слова: організаційні системи з критичною інфраструктурою; інфраструктура організаційної системи; виклики; загрози; реорганізація.

Вступ

Уся історія розвитку людського суспільства є процес удосконалення організаційних форм його діяльності, ускладнення структури організації людей і засобів виробництва внаслідок розвитку поділу суспільної праці, забезпечення органами управління взаємодії елементів складних організаційних (організаційно-технічних або організаційно-соціальних) систем через обмін ресурсами та інформацією між ними.

Початок XXI сторіччя характеризується новим явищем у розвитку організаційних систем — революційним упровадженням засобів телекомунікації, автоматизації та інтелектуалізації в усі процеси управління. Природно, що за умов інформатизації та інтелектуалізації суспільства виникають виклики та загрози безпосередньо для інформаційної інфраструктури будь-яких організаційних систем. Виклики та загрози стосуються деяких уразливих об'єктів (елементів організаційної системи), наслідком чого є її нестійкій стан у вигляді кризових ситуацій її функціонування. Так, для систем управління

енергетикою це яскраво ілюструють події з відімкнення підстанцій у Нью-Йорку чи Москві. Економічні збитки внаслідок відмови уразливого об'єкта вартістю в кілька тисяч сягають сотень мільйонів. Вочевидь, це змушує чинити протидію цим викликам та загрозам, забезпечуючи захист уразливих об'єктів або вдаватись до асиметричних дій щодо джерел цих викликів та загроз.

Постановка завдання

Під час розв'язання завдань системою управління складними організаційними системами за умов впливу викликів та загроз на уразливі елементи інфраструктури організаційних систем постає необхідність автоматизації розробки варіантів управлінських рішень, скажімо з прискорення адаптації (скорочення часу адаптації або зменшення витрат матеріальних ресурсів) до нових умов функціонування на основі впровадження новітніх інформаційних технологій (телекомунікаційних, технологій автоматизації, інтелектуальних, штучного інтелекту тощо) та організації відповідної системи інформаційної безпеки для запобігання кризовим явищам. Відомо, що для автоматизації прийняття рішень необхідно розв'язати проблему формалізації процесів адаптації складної організаційної системи до нових умов функціонування з урахуванням імовірних загроз і впливів. Це дасть змогу визначати методи оцінювання показників критичності та створювати рекомендації з протидії критичним ситуаціям. Звідси виникає необхідність формалізації явища критичності для складної організаційної системи та розробки методів оцінювання показників критичності за допомогою моделі інформаційної безпеки складної організаційної системи з критичною інфраструктурою (ОСКІ). Це завдання особливо актуальне для розробки моделей управління інтелектуальними системами управління.

Аналіз останніх публікацій

Постановка такого завдання вже неодноразово пропонувалася в теорії організації складних систем [1–5]. Дослідженню управлінської діяльності керуючих органів присвячено багато праць, де пропонуються різноманітні моделі управління об'єктом керування. Наприклад, здійснено дослідження моделей ієрархічних систем управління [7], моделей загальної теорії систем [7; 8], моделі організації систем [2; 4], моделі самоорганізації в нерівноважних системах [9; 10], моделі стійкості системи [11], моделі адміністративної поведінки [12], моделі структурної організації та стратегічного управління [13–18]. Аналогічні питання розглянуто у [19], але для інфраструктури національної безпеки без урахування інтелектуалізації суспільства. Проте рівень інтелектуалізації суспільства необхідно враховувати, коли йдеться про визначення критичності складної організаційної системи. Аналіз праці у галузі забезпечення безпеки складної організаційної системи показав, що загальної кількісної оцінки та моделі, яка одночасно враховувала б інформатизацію та інтелектуалізацію, не існує.

Основна частина

Для формалізації процесів адаптації складної організаційної системи до нових умов функціонування, що характеризується інформатизацією та інтелектуалізацією, для створення математичних моделей аналізу ситуацій протидії інформаційним викликам і загрозам та розробки варіантів рішень на основі відповідного математичного апарату необхідно введення низки взаємозв'язаних понять.

***Організаційна система* (ОС)** — це сукупність дієвих чинників і засобів, організована у вигляді системної структури для виконання заданого переліку функцій (завдань) при досягненні встановлених цілей [21]. Для розвитку процесу поділу суспільної праці в певній галузі виробництва створюється відповідна інфраструктура.

Інфраструктура — це комплекс взаємозв'язаних обслуговуючих структур, що становлять і/або забезпечують основу для розв'язання проблеми (задачі). Наприклад, інфраструктура, що забезпечує загальні умови функціонування економіки, включає в себе енергетичні, транспортні, телекомунікаційні мережі, інформаційні, логістичні системи тощо.

Криза організаційної структури — це небезпечний і нестійкий перехідний стан, коли наявна організаційна структура, призначена для розв'язання певних завдань, стає неадекватна цим завданням, що призводить до непередбачуваних ситуацій. Характерними ознаками кризи є порушення відповідності між попитом і пропозицією, між потребами і їх задоволенням. Природа кризи приховується в наявності уразливого об'єкта щодо певної загрози.

Загроза — це потенційні або реальні дії, що можуть спричинити порушення існуючого стану функціонування організаційної системи через збої в технології управління. Загроза може бути передумовою виникнення порушення одного чи кількох аспектів безпеки, неприпустимого ризику під час прийняття керуючих рішень.

Уразливий об'єкт — це слабка ланка в організаційній системі, нездатна протистояти шкідливим впливам (загрозам), дія яких порушує технологію управління. Якщо цей об'єкт посідає важливе місце

в системі, то його пошкодження (втрата) може призвести до катастрофічних наслідків. Розрізняють людську, технічну та інформаційну уразливість. Людська уразливість виникає внаслідок психологічних впливів. Технічна — результат виникнення несправності в механізмах управління системою. Інформаційна уразливість є наслідком непередбачуваного впливу інформації на процес прийняття рішень. Загроза і уразливий об'єкт — це передумови виникнення критичного стану інфраструктури.

Критичній стан інфраструктури (організаційної системи) виникає тоді, коли її потенційно уразлива структура внаслідок дії середовища раптово втрачає задані властивості та набуває інших властивостей, які не могли бути передбачені при її проектуванні. Для запобігання кризовому стану в організаційній системі здійснюються заходи з її реформування завдяки застосуванню методів цільового управління і відповідних технологій управління.

Реформування — це перетворення, удосконалення законодавчим шляхом будь-якої галузі державного або суспільного життя. Передбачає два напрямки дій: нормативно-правовий і організаційно-технічний. Нормативно-правовий напрямок пов'язаний зі змінами в нормативно-правових актах, а організаційно-технічний напрямок передбачає перебудову системи управління, модернізацію всієї інфраструктури, зміну її організаційної структури, технічне переоснащення, зміну способів застосування тощо. Реформування організаційних систем є еволюційною формою вирішення керівництвом множини нових завдань за допомогою заходів вдосконалення організаційних відносин у діючих структурах.

Реорганізація — це процес перетворення, перебудови, зміни структури та функцій установи (організації), удосконалення організаційних відносин у діючих структурах, пристосування технологій управління до потреб цільового управління. Реорганізація виступає організаційно-технічним напрямком реформування. Особливість процесів реорганізації — їх поступовість і неухильність щодо вдосконалення організаційно-технічних відносин у постійно діючих структурах організаційної системи при нейтралізації можливих наслідків прояву загрози, що може створити критичний стан цієї системи. Нейтралізація негативних наслідків такого стану тягне за собою низку нових завдань, які наявна структура здебільшого не здатна вирішувати в межах існуючих організаційно-штатних структур постійно діючої організаційної системи. Тому її результатом є зміни в цих організаційно-штатних структурах.

Зрештою поняття «реорганізація» передбачає вдосконалення організаційних відносин у діючих структурах за допомогою нейтралізації можливого прояву негативної дії виклику або загрози на технологію управління в кібернетичному просторі. Реорганізація доцільна тільки в такій організаційній системі, де існує можливість появи критичного стану інфраструктури, тобто кризи в організаційній структурі. Звідси пропонується реорганізацію пов'язувати з передумовами виникнення критичного стану елементів системи, а при висвітленні цього явища йтиметься про згадувану вже *організаційну систему з критичною інфраструктурою*.

Система з критичною інфраструктурою, або критична система, — це сукупність фізичних або віртуальних систем і засобів, настільки важливих для держави, що їх вихід із ладу або знищення може призвести до згубних наслідків у сфері оборони, економіки, охорони здоров'я та безпеки нації [20]. Це поняття охоплює ключові сектори, де є уразливі об'єкти: органи управління; інформаційні і телекомунікаційні системи та мережі; енергетику; транспорт; фінансові системи тощо. Їх стан має вплив на рівень воєнної, економічної, екологічної та інших видів безпеки.

Кібернетичний простір (вид інформаційного простору) — середовище, що перебуває під юрисдикцією держави (установи, фірми) і в якому здійснюється створення, зберігання та поширення інформації. Наприклад, основними складовими захищеного інформаційного простору держави можуть бути інформаційна інфраструктура виробничого об'єднання з відповідними показниками захищеності, а також елементи та засоби інформаційної інфраструктури.

Інформаційна інфраструктура — це система організаційних структур (комплекс систем, установ, служб, частин і підрозділів, необхідних для функціонування органів управління), що забезпечують функціонування і розвиток інформаційного простору країни (установи, фірми) і засобів інформаційної взаємодії. Зазначена інфраструктура включає в себе сукупність інформаційних центрів, банків даних і знань, систем зв'язку, що забезпечує доступ споживачів до інформаційних ресурсів, необхідних для управління організаційними системами, сервісні та інтелектуальні підсистеми. Наприклад, вона може складатись із підсистем, поданих на рис. 1.

Інформаційна інфраструктура, як випливає з рис. 1, має частинні структури, що відповідають за другорядні функції: за створення, накопичення, зберігання та поширення інформаційної продукції; за її виробництво та поширення: за виробництво інформаційних технологій; за сервісне та інтелектуальне обслуговування елементів інфраструктури. Результатом функціонування інформаційної інфраструктури є створення захищеного інформаційного простору для організаційних структур.

Рис. 1. Складові інформаційної інфраструктури

Матеріально-технічною основою процесів інформатизації та інтелектуалізації органів управління в сучасних умовах правомірно вважати інформаційну систему (ІС).

Інформаційна система — це множина взаємозв'язаних матеріальних і програмних об'єктів (засобів і комплексів інформатизації, засобів їх забезпечення, засобів інтелектуалізації, сервісів), що безпосередньо беруть участь у забезпеченні надання інформаційних послуг користувачам для прийняття рішення. Поняття ІС об'єднує множину взаємозв'язаних об'єктів (автоматизовані аналітичні, розрахункові, довідкові, телекомунікаційні, інтелектуальні системи інформаційної інфраструктури сучасної організаційної системи), що безпосередньо беруть участь у наданні інформаційних та інтелектуальних послуг в інформаційному просторі.

Уразливість в інформаційній системі є подією, за якої компрометується один або кілька аспектів безпеки інформації (доступність, конфіденційність, цілісність і достовірність). Наявність уразливого об'єкта створює слабку ланку, що може призвести до порушення безпеки інформації. Природно, що впливи загрози на технологію управління можуть викликати критичний стан будь-якої організаційної системи, яка через це стає ОСКІ. Звідси правомірно передбачати залежність безпеки будь-якої організаційної системи від рівня інформаційної безпеки. Тому сьогодні під час реорганізації організаційних систем необхідно враховувати процеси, пов'язані з упровадженням новітніх інформаційних технологій.

Безпека ОСКІ — це стан правових норм і відповідний їм стан організаційно-технічних заходів, що гарантує відсутність неприпустимого ризику, пов'язаного з ухваленням стратегічних рішень та захистом ресурсів у всіх ланках управління.

Об'єктом забезпечення безпеки в ОСКІ є ефективне функціонування соціальних і технічних складових ОСКІ. Соціальними об'єктами є політичний устрій, суспільні установи тощо. Технічними об'єктами є матеріальні та інформаційні ресурси, інфраструктура, інформаційні технології, інформаційні системи, що застосовуються в системі управління. Для забезпечення безпеки створюється система безпеки ОСКІ.

Система безпеки ОСКІ — це організована сукупність суб'єктів (органів управління та посадових осіб, об'єднаних цілями та завданнями щодо захисту інтересів у заданій сфері (політичній, економічній, інформаційній, воєнній), об'єктів захисту та об'єктів забезпечення, що здійснюють узгоджену діяльність на основі прийнятих вимог, методів і засобів.

Функції системи безпеки ОСКІ включають у себе захист інтересів у певній сфері; захист інтересів об'єкта (установи, фірми, суспільства, держави) від внутрішніх та зовнішніх викликів і загроз; упровадження сучасних інформаційних технологій; забезпечення безпеки інформаційних і телекомунікаційних систем, які створюють інформаційний простір для організаційних систем; запобігання впливу негативних чинників на функціонування інформаційних систем.

Отже, інформатизація з інтелектуалізацією стає системоутворюючим фактором. Але ці процеси породжують суперечності між поліпшенням умов удосконалення організаційних відносин у діючих структурах і необхідністю постійного адекватного реагування технологій управління на появу нових викликів та загроз, які призводять до кризи організаційних структур, дезорганізації технологій управління в процесах функціонування організаційної системи. Інформаційна інфраструктура стала ахіллесовою п'ятою сучасних організаційних систем і перетворила їх на системи з критичною інфраструктурою. Практично всюди, де є застосування засобів інформатизації органів управління небезпечними технологічними об'єктами, виникають принципово нові умови впливу і прояви загроз через уразли-

вість об'єктів інформаційних систем і, як наслідок, необхідність організації безпеки в ОСКІ. У таких системах стає актуальним поняття безпеки ОСКІ.

Для будь-якої ОСКІ можна визначити множину ознак при класифікації потенційних загроз її безпеці. Тут зазначимо, що загрози або створюють «вікно» небезпеки, або «відчиняють» вікна небезпеки для завдання шкоди зловмисником (або порушником) безпеки.

Вікно небезпеки системи з критичною інфраструктурою — це проміжок часу від моменту, коли з'являється можливість використати уразливі об'єкти в ОСКІ, і до моменту, коли вікно ліквідується. Тоді рівень безпеки можна тлумачити так, як це запропоновано на рис. 2.

Небезпека (рівень безпеки ОСКІ) — це ступінь відповідності системи цілям у ситуації, що склалася. Він характеризується кількісними та якісними показниками, взятими для його оцінювання.

Загальною кількісною оцінкою небезпеки ОСКІ можна запропонувати показник на основі відомого підходу Б. В. Васильєва [3], коли кількісний рівень безпеки ОСКІ має оцінюватися ступенем готовності організаційної системи до виконання поточного переліку завдань, тобто показник $\Phi_б$ визначає ефективність дії системи безпеки (рівень небезпеки).

$$\Phi_б = \frac{\Phi_г}{\Phi_{г0}}, \tag{1}$$

де $\Phi_г$ — показник готовності до застосування ОСКІ в реальних умовах; $\Phi_{г0}$ — значення того самого показника, але визначеного за умови, що система функціонує найкращим чином (ідеально).

Особливістю підходу Б. В. Васильєва є те, що показник $\Phi_б$ визначає ефективність дії системи безпеки (рівень небезпеки) і водночас аналітично пов'язаний із показником $\Phi_г$ ефективності функціонування ОСКІ. Це дає змогу на основі заданих вимог до готовності ОСКІ сформулювати вимоги до системи безпеки визначенням деякого мінімально припустимого рівня безпеки ОСКІ.

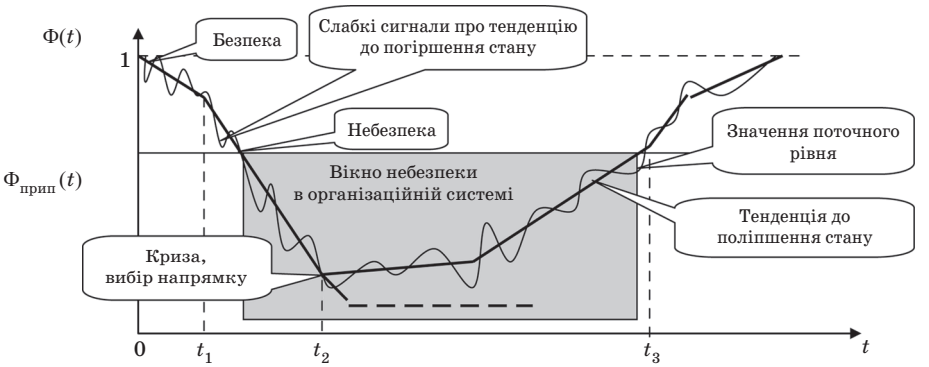

Рис. 2. Рівень безпеки $\Phi(t)$

Зазначимо, що рис. 2 ілюструє основні фази критичного стану. Вважається, що вікно небезпеки виникає випадково та існує протягом непередбачуваного часу. Адже за цей час неодмінно відбуваються такі події: стають відомими загрози та їх дія; знаходяться засоби їх нейтралізації або усунення; ці засоби мають бути встановлено в ОСКІ для її захисту. Також бачимо, що в моменти t_1 і t_3 нас цікавить стан системи, оцінювання якого здійснюється за обчисленим критерієм $\Phi_{прип}(t)$.

Цей критерій фактично визначає готовність до виконання завдань структурними елементами ОСКІ, а в критичний момент t_2 нас буде цікавити, як вийти з критичного стану, а це, по суті, інший за змістом показник, що встановлює якість керованості під час переходу. Звідси пропонується загальним показником вважати

$$\Phi_б(t) = \begin{cases} G(t), \text{ якщо } \Phi_б(t) \geq \Phi_{прип}, \\ \Phi(t), \text{ якщо } \Phi_б(t) < \Phi_{прип}. \end{cases} \tag{2}$$

Тут $G(t)$ — готовність до використання ОСКІ в поточному режимі функціонування (або експлуатації) для виконання відомого переліку завдань; $\Phi(t)$ — показник, що характеризує адаптацію ОСКІ до виконання нових завдань; $\Phi_{прип}(t)$ — припустиме значення, яке характеризує рівень безпеки ОСКІ.

Визначений зміст комплексного показника рівня безпеки $\Phi_б$ характеризує вплив загрози та ефективність заходів із реорганізації щодо її нейтралізації.

Висновки

♦ Вікна небезпеки і засоби їх виконання зловмисником в ОСКІ з'являються постійно; трактування проблеми безпеки ОСКІ для різних категорій суб'єктів і об'єктів може істотно різнитися; для кожної ОСКІ існує своя система забезпечення захисту; успіх стосовно організації безпеки ОСКІ може гарантувати тільки комплексний підхід, що поєднує різноманітні заходи, наприклад інформаційного, організаційного, процедурного характеру.

♦ В основу забезпечення безпеки будь-якої ОСКІ має бути покладено наукове обґрунтування таких положень: доктрини як сукупності концепцій; стратегії як сукупності способів досягнення цілей; концепції як компактної теорії, що застосовується для розробки політики безпеки, а також програм досягнення визначених цілей у системі забезпечення безпеки і профілів захисту складових ОСКІ. Тут виникає необхідність розгляду змісту реорганізації ОСКІ. Вирішення цього завдання передбачає визначення методології забезпечення реорганізації ОСКІ як логічної організації понять, показників, закономірностей, методів оцінювання рівня інформаційної безпеки і заходів із реорганізації, що мають вплив на рівень цієї безпеки. Практичним результатом є обґрунтування завдань, складу і принципів побудови системи забезпечення інформаційної безпеки держави (юридичної особи), яка знайде місце в доктринах, концепціях, політиках і програмах організації безпеки установ та організацій.

Список використаної літератури

1. ***Богданов, А.*** *Наука об общественном сознании: Краткий курс идеологической науки в вопросах и ответах / А. Богданов.— [3-е изд.].— Петроград, Москва: Книгоиздательское товарищество «Книга», 1923.— 314 с.*

2. ***Богданов, А. А.*** *Всеобщая организационная наука (Тектология) / А. А. Богданов: в 2-х кн.— М.: Книга, 1912; 2-е изд. 1925; переиздание 1989.— Книга 1.— 304 с. Книга 2.— 351 с.*

3. ***Месарович, М.*** *Теория иерархических многоуровневых систем / М. Месарович, Д. Мако, И. Такахара; пер. с англ.— М.: Мир, 1970.— 340 с.*

4. ***Мильнер, Б. З.*** *Теория организаций / Б. З. Мильнер.— М.: ИНФРА-М, 1999.— 336 с.*

5. ***Иванова, Т. Ю.*** *Теория организации / Т. Ю. Иванова, В. И. Приходько и др.— СПб.: Питер, 2004.— 269 с.*

6. ***Месарович, М.*** *Основания общей теории систем / М. Месарович.— М.: Мир, 1966.— 244 с.*

7. ***Гиг, Дж. Ван.*** *Прикладная общая теория систем / Дж. Ван Гиг.— Кн. 1, 2.— М.: Мир, 1981.— 340 с.*

8. ***Боулдинг, К.*** *Общая теория систем — скелет науки / К. Боулдинг.— М.: Прогресс, 1969.— 224 с.*

9. ***Николос, Г.*** *Самоорганизация в неравновесных системах. От диссипативных структур к упорядоченности через флуктуации / Г. Николос, И. Пригожин.— М.: Мир, 1979.— 512 с.*

10. ***Хакен, Г.*** *Синергетика / Г. Хакен.— М.: Мир, 1980.— 404 с.*

11. ***Горский, Ю. М.*** *Основы гомеостатики (Гармония и дисгармония в живых, природных, социальных и искусственных системах) / Ю. М. Горский.— Иркутск: Изд-во ИГЭА, 1998.— 337 с.*

12. ***Саймон, Г.*** *Административное поведение / Г. Саймон, Дж. Марш; пер. с англ.— М.: Мир, 1974.— 245 с.*

13. ***Берталанфи, Л. фон.*** *Общая теория систем: критический обзор / Л. фон Берталанфи.— М.: Прогресс, 1969.— 382 с.*

14. ***Ансофф, И.*** *Стратегическое управление / И. Ансофф.— М.: Мир, 1980.— 340 с.*

15. ***Сетров, М. И.*** *Основы функциональной теории организации / М. И. Сетров.— Л.: Наука, 1972. — 187 с.*

16. ***Акофф, Р.*** *Планирование будущего корпорации / Р. Акофф; пер. с англ.— М.: Прогресс, 1985.— 230 с.*

17. ***Виханский, О. С.*** *Стратегическое управление / О. С. Виханский.— М.: Мир, 1986.— 230 с.*

18. ***Ансофф, И.*** *Стратегическое управление / И. Ансофф.— М.: Мир, 1980.— 340 с.*

19. ***Даник, Ю. Г.*** *Національна безпека: запобігання критичним ситуаціям: монографія / Ю. Г. Даник, Ю. І. Катков, М. Ф. Пічугін.— Житомир: Рута, 2006.— 386 с.*

20. ***Лапин, Н. И.*** *Теория и практика социального планирования / Н. И. Лапин, Э. М. Коржева, Н. Ф. Наумова.— М.: Политиздат, 1975.— 245 с.*

Рецензент: доктор техн. наук, доцент **В. В. Онищенко,** Державний університет телекомунікацій, Київ.

В. В. Вишневский, Ю. И. Катков, С. А. Серых

РОЛЬ И МЕСТО ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПРИ ВОЗНИКНОВЕНИИ ЯВЛЕНИЯ КРИТИЧНОСТИ ОРГАНИЗАЦИОННОЙ СИСТЕМЫ

Рассмотрены общие положения об организационных системах с критической инфраструктурой. Исследован случай несоответствия инфраструктуры организационной системы в результате воздействия возможных вызовов или угроз, которые могут привести в критичное состояние любой важный элемент этой системы или других систем. Представлена математическая модель оценки уровня критичности организационной системы с критичной инфраструктурой.

Ключевые слова: организационные системы с критичной инфраструктурой; инфраструктура организационной системы; вызовы; угрозы; реорганизация.

V. V. Vyshnivskyi, Yu. I. Katkov, S. A. Serikh

ROLE AND LOCATION OF INFORMATION INFRASTRUCTURE IN THE EVE OF THE ORGANIZATIONAL SYSTEM CRITICALITY

This paper examines the general provisions of organizational systems with a critical infrastructure. Reasons for reorganization are shown. The direction of the study of the infrastructure of the organizational system is indicated after the impact of possible challenges or threats. A mathematical model for assessing the level of criticality of an organizational system with a critical infrastructure is provided.

Keywords: organizational systems with a critical infrastructure; infrastructure of the organizational system; challenges; threats; reorganization.