УДК: 65.012.8 DOI 10.33111/mise.100.2

Бєгун А. В., к.е.н.,
професор кафедри комп'ютерної математики та інформаційної безпеки,
Осипова О. І., к.е.н.,
доцент кафедри економіко-математичного моделювання,
Урденко О. Г.,
аспірант кафедри комп'ютерної математики та інформаційної безпеки,
ДВНЗ «КНЕУ імені Вадима Гетьмана»

Biehun A. V., PhD in Economics,
Professor of the Computer Mathematics and Information Security Department,
Osypova O. I., PhD in Economics,
Associate Professor of the Economic and Mathematical Modelling Department,
Urdenko O. G., Postgraduate Student of the
Computer Mathematics and Information Security Department,
SHEI KNEU named after V. Hetman

ПРО ОДНУ З СИТУАЦІЙНИХ МОДЕЛЕЙ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

ABOUT ONE OF THE SITUATIONAL MODELS OF THE INFORMATION SECURITY MANAGEMENT OF THE ENTERPRISE

Анотація. *Теорія управління інформаційною безпекою економічних систем створила багато ефективних механізмів швидкого і точного вибору управляючих дій на об'єкт за даними його стану. До найважливіших серед них слід віднести концепцію ситуаційного управління складними об'єктами на основі різноманітних технологій моделювання.*

Серед загальної кількості моделей і методів управління інформаційною безпекою організації систем найконструктивнішим для дослідження критичних процесів можуть бути використані ситуаційні. Головною перевагою і щільною якістю таких моделей є корисність для кількісного прогнозу інформаційних ризиків, а також для апріорної оцінки та оптимізації заходів щодо їх зменшення або перерозподілу. Більш того, якісний і кількісний аналіз ситуаційних моделей може також сприяти не тільки виявленню «вузьких місць», але і розробці найефективніших стратегій удосконалення інформаційної безпеки. В якості прикладу розглядається задача одного класу моделей — так званих діаграм причинно-наслідкових зв'язків. До таких моделей звичайно відносять: а) мережу стохастичної або детермінованої структури; б) граф станів і переходів; в) дерево надзвичайних станів і дерево подій. До того ж основними перевагами таких семантичних моделей слід віднести наочність, інформативність і можливість враховувати велику кількість тих суттєвих факторів, які реально супроводжують функціонування конкретних компонентів організаційної системи.

Особливість до практичного застосування даних діаграм пов'язана з можливістю переходу від семантичного (змістовного) рівня представлення об'єктів і процесів, до синтаксичного (знакового). Досягається цей процес наступною формалізацією вказаних діаграм, яка проводиться з ме-

тою отримання на їх основі відповідних аналітичних моделей, що найбільш пристосовані для аналізу і оброблення за допомогою сучасних математичних і машинних методів.
Ключові слова: *дерево подій; ситуаційна модель; діаграма причинно-наслідкових зв'язків; надзвичайна ситуація.*

Abstract. *The theory of information security management of economic systems has created many effective mechanisms for quick and accurate selection of control actions for the object according to its condition. Among the most important among them is the concept of situational management of complex objects based on various modeling technologies. Among the total number of models and methods of information security management of the organization of systems the most constructive for the study of critical processes can be used situational. The main advantage and dense quality of such models is the usefulness for quantitative forecasting of information risks, as well as for a priori assessment and optimization of measures to reduce or redistribute them. Moreover, qualitative and quantitative analysis of situational models can also help not only to identify «bottlenecks», but also to develop the most effective strategies to improve information security. As an example, we consider the problem of one class of models — the so-called diagrams of causation. Such models usually include: a) a network of stochastic or deterministic structure; b) graph of states and transitions; c) emergency tree and event tree. In addition, the main advantages of such semantic models include clarity, informativeness and the ability to take into account a large number of those significant factors that actually accompany the functioning of specific components of the organizational system. The peculiarity of the practical application of these diagrams is associated with the possibility of transition from the semantic (content) level of representation of objects and processes, to the syntactic (symbolic). This process is achieved by the following formalization of these diagrams, which is carried out in order to obtain on their basis the appropriate analytical models that are best suited for analysis and processing using modern mathematical and machine methods.*
Keywords: *event tree; situational model; causal diagram; emergency situation.*

Вступ. Інформаційна складова є ведучим сегментом у діяльності будь-якого підприємства і чинить вплив на всі елементи його функціонування. Разом зі зростаючою залежністю від цифрових технологій, які пов'язані з поширенням обсягів інформації, підвищується рівень загроз інформаційних атак на інформаційні ресурси та інфраструктуру. Ці атаки становляться складнішими, цілеспрямованішими і масштабнішими, часто погрожують критичним елементам інформаційної інфраструктури економічної системи.

Аналіз останніх публікацій. З цього приводу є доцільним дослідження і створення цілісної системи управління інформаційною безпекою, яка б проводила моніторинг прошарку нестабільних ситуацій і приймала рішення на виникнення конкретного інциденту [5, 6].

Розгляд концепцій ситуаційного управління інформаційною безпекою (СУІБ) економічних суб'єктів дозволяє зробити два основних висновки. По-перше, основні методологічні передумови

реалізації ситуаційного управління розроблені на дуже високому рівні абстракції і не доведені до рівня структуризації систем різноманітного класу. По-друге, спроби розробити достатньо обгрунтовану концепцію СУІБ суб'єктів господарювання слід визнати незавершеною, так як відсутня надійна методологічна основа дослідження джерел і причин виникнення управлінських ситуацій. Тому головна позиція при розробці концепції рішення ситуаційних задач управління інформаційною безпекою полягає у такому: ситуація, яка виникла або передбачена проблемною, може враховуватися вирішеною тільки в тому випадку, коли виконане відпрацювання і реалізація управлінських рішень, що ліквідують той стан організації, її елементів та елементів зовнішнього середовища, який є проблемним. Тобто, кожному типу конкретної ситуації повинна відповідати своя послідовність процедур управління з її інформаційним забезпеченням, критеріями і методами прийняття рішень, своїми об'єктами управлінських дій. Тим самим забезпечується можливість адаптації структури управління до умовам функціонування організації, які динамічно змінюються у зовнішньому середовищі та його елементів. Таким чином, концепція полягає у розробці комплексу методів і засобів, які направлені на виявлення та вирішення проблем, що виникають на всіх етапах функціонування організації. Ці методи і засоби включають класифікатор управлінських ситуацій, топологію процедур управління, структуру інформаційного забезпечення тощо. Розробка основних положень концепції у теоретичному і методичному плані повинна виконуватися таким чином. По-перше, необхідно дослідити причини і джерела виникнення ситуацій, а також об'єкти на які можуть бути направлені дії з метою вирішення ситуацій. По-друге, необхідно розробити методи і моделі формувань процедур управління, що є адекватними цілям розв'язання всій сукупності ситуацій. По-третє, необхідно виявити послідовність, обсяг і змістову різноманітність інформаційних процесів, оскільки вони є основою для розроблення системи інформаційного і технічного забезпечення технологій розв'язання ситуаційних задач управління.

Однією з автономних задач є задача пошуку методів і моделей доповнення ситуаційними елементами реалізації нових організаційно-економічних зв'язків, які виникають при розв'язанні всієї сукупності ситуацій або з найбільш значимих з них. Природно, що на різних етапах реалізації цієї концепції необхідно розв'язувати цілий ряд задач статичного і динамічного аспектів управління: великі обсяги даних, оцінка потенціалу управлінських кадрів, стандарти інформаційної безпеки тощо.

Викладення основного матеріалу. Теорія управління інформаційною безпекою економічних систем створила багато ефективних механізмів швидкого і точного вибору управляючих дій на об'єкт за даними його стану. До найважливіших серед них слід віднести концепцію ситуаційного управління складними об'єктами на основі різноманітних технологій моделювання.

Серед загальної кількості моделей і методів управління інформаційною безпекою організації систем найконструктивнішим для дослідження критичних процесів можуть бути ситуаційні.

Головною перевагою і щільною якістю таких моделей є корисність для кількісного прогнозу інформаційних ризиків, а також для апріорної оцінки та оптимізації заходів щодо їх зменшення або перерозподілу. Більш того, якісний і кількісний аналіз ситуаційних моделей може також сприяти не тільки виявленню «вузьких місць», але і розробці найефективніших стратегій удосконалення інформаційної безпеки. В якості прикладу розглянемо задачу одного класу моделей — так званих діаграм причинно-наслідкових зв'язків. До таких моделей звичайно відносять:

а) мережу стохастичної або детермінованої структури;

б) граф станів і переходів;

в) дерево надзвичайних станів і дерево подій.

До того ж основними перевагами таких семантичних моделей слід віднести наочність, інформативність і можливість враховувати велику кількість тих суттєвих факторів, які реально супроводжують функціонування конкретних компонентів організаційної системи.

Особливість до практичного застосування даних діаграм пов'язана з можливістю переходу від семантичного (змістовного) рівня представлення об'єктів і процесів, до яких притаманний процес моделювання, до синтаксичного (знакового).

Досягається цей процес наступною формалізацією вказаних діаграм, яка проводиться з метою отримання на їх основі відповідних аналітичних моделей, що найпристосованіші для аналізу і оброблення за допомогою сучасних математичних і машинних методів [2, 3].

До теперішнього часу вже накопичено певний досвід застосування ситуаційних графо-аналітичних моделей для зниження ризику техногенний катастроф. Такий досвід може виявитися корисним у попередженні та обслуговуванні загроз і викликів іншого походження, наприклад, для підприємств з неоднорідною структурою. Мабуть найперспективнішим у цьому відношенні

слід вважати діаграми: «дерево надзвичайних подій» і «дерево подій» та його можливих руйнівних наслідків.

При створенні таких діаграм доцільно користуватися такими правилами:

а) давати чіткі визначення категоріям моделі (події, причини і умови їх появи), виконувати декомпозицію складних подій на прості, виявляти спільні передумови та розділяти їх, встановлювати час і місце появи причин і передумов, які пов'язані із зовнішніми факторами;

б) дерево подій слід будувати з використанням методу дедукції — від головної події до її передумов (в зворотній послідовності);

в) дерево результатів — метод індукції — від центральної події до можливих руйнівних наслідків для інформаційних, матеріальних і природних ресурсів.

Такі правила можна представити у вигляді дерева надзвичайної події і дерева подій.

В якості об'єкту моделювання будемо розглядати деяке гіпотетичне цифрове підприємство і його оточення — цифрове суспільство. Предметом дослідження виступають об'єктивні закономірності появи і попередження надзвичайної ситуації, яка пов'язана із можливістю підриву життєдіяльності цифрового підприємства, його метою — оцінювання і зниження відповідної ймовірності та збитку конкретної структурної частини підприємства.

Під подією (Х), зображеним посередині рис. 1, розуміється надзвичайна ситуація, що виникла на підприємстві, наприклад, внаслідок оголошення (І) в ньому надзвичайного стану і розколу (Л) керівництва компанії. Пояснимо також, що подія (Х) одночасно є «головним» для дерева події, і «центральним» — для дерева подій — результатів цієї надзвичайної ситуації.

Дерево подій будується дедуктивно, від головного події (Х) до ймовірних причин, рознесених за трьома рівнями, не рахуючи вихідних передумов. При цьому, крім уже згаданих 2-х причин першого рівня — (І) і (Л), у ньому враховані також дві передумови другого рівня — (В) і (Е) і чотири передумови третього рівня — (А), (Б), (Г) і (Д), а також 12 вихідних подій-передумов.

Зокрема, алфавітний код подій, включених у дерево подій, означає, наприклад, такі причини: (В) — виникнення в країні масових хвилювань і заворушень, (Е) — загальний страйк працівників муніципального транспорту, (А) — різке збільшення тарифів на енергоресурси, (Б) — спустошення полиць магазинів, (Г) — падіння курсу національної валюти і (Д) — страйк службовців місцевого транспорту.

У свою чергу, цифровий код вихідних передумов цього ж дерева вказує на такі небажані події:

1, 2 — відповідна скупка іноземцями акцій газових і електроенергетичних компаній країни;

3 — небувалий перш сплеск злочинності;

4 — заворушення, викликані масовим розпродажем і безконтрольної скупки землі, а також її виведенням з використання за призначенням;

5, 6 — припинення імпорту товарів масового попиту і вичерпання їх державних запасів відповідно;

7 — відмова іноземних кредиторів від відстрочок у виплаті державного боргу;

8 — різке падіння світових цін на експортовані країною мінерально-сировинні і паливно-енергетичні ресурси;

9 — страйк водіїв транспорту всіх великих міст країни;

10, 11 — відмова службовців колійного або локомотивного господарства галузі від виходу на роботу через її непродумані реструтурізації;

12 — саморозпуск уряду й обох палат парламенту.

Моделювання руйнівних наслідків досліджуваної надзвичайної ситуації здійснюється за допомогою дерева результатів (права частина діаграми), яке будувалося зліва направо, тобто від центральної події до його конкретним реалізаціям. При цьому передбачається, що дана ситуація може розвиватися далі за одним із трьох сценаріїв: (В) — конурентна боротьба, (М) — рейдерське захоплення, (Р) — заміна менеджменту акціонерами компанії. Ці події першого рівня дослідження, а також алфавітні коди всіх інших рівнів-розгалужень правій частині діаграми (рис. 1) зображені в її відповідних вузлах.

Вважається також, що кожен з перелічених трьох сценаріїв, в подальшому буде розвиватися залежно від створеної ситуації.

Наприклад, конкурентне протистояння може а) спровокувати зовнішню агресію і завершиться поглинанням (О) підприємства, або б) крахом (К) підприємства або в) закінчиться масовими звільненнями (4) і фінансовими (5) втратами (Ж).

Подібні альтернативи можуть мати місце і в рейдерському захопленні: швидке придушення опору (9) або тривала спроба облоги (10) рейдерів, і у зборів акціонерів (зміна керівництва (11) підприємства або проведеної ним політики (12), або — того та іншого разом).

Природно, що кожен варіант розвитку надзвичайної ситуації буде характеризуватися своєю ймовірністю — Q_{rs} і збитком — Y_{rs}. Так само як і те, що деякі з результатів можуть бути в подальшому

піддані деталізації, наприклад, подібно до того, як це зроблено для подій (О), (Ж) і (К), що мають додаткові результати — (1-3), (4 -5) і (6-8) відповідно. При цьому результати (О) і (К) в подальшому відрізняються між собою лиш можливостями і розмірами втрачених а) природних (1, 6) б) матеріальних (2, 7) і в) людських (3, 8) ресурсів підприємства, а результат (Ж) — тільки рівнем збитків для двох останніх.

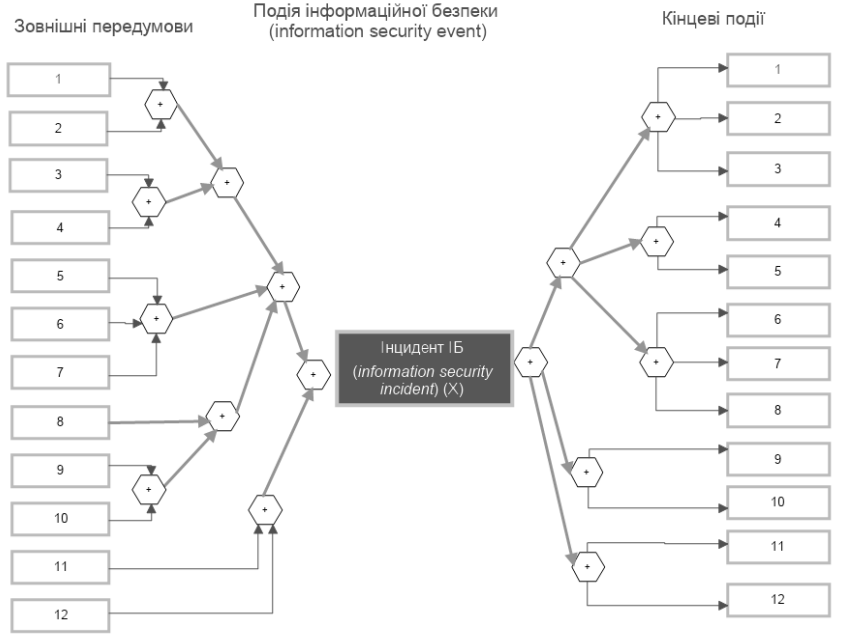

Рис. 1. Діаграма надзвичайної події типу «дерево»

Основною перевагою подібних ситуаційних моделей служить їх придатність як для аналізу умов виникнення і попередження різноманітних надзвичайних подій, так і для синтезу рекомендацій щодо їх попередження і зниження небажаних наслідків. Проілюструємо — як це робиться на прикладі якісного і кількісного системного аналізу зображеної вище діаграми.

У процесі якісного аналізу дерева надзвичайної події, використовуємо так звані «мінімальні поєднання» передумов, що складаються з найменшого числа його вихідних подій і втрачають властиві їм властивості при видаленні бодай одного з них: а) *пропускні* — достатні для появи головної події і б) *відсічні* — гарантують

його відсутність. У нашому випадку може бути виявлено 18 мінімальних пропускних поєднань: 14 *дуплетів* — 3,12; 3,12;4,12; 4,13; 7,12; 7,12; 8,12; 8,12; 9,12; 9,12; 10,12; 10,12; 11,12; 11,12 та 4 *триплетів* [4] — 1,2,12; 1,2,12;5,6,12; 5,6,12, — а також 5 мінімальних відсічних поєднань: один дуплет — 11,12 і ще 4 сполучення, які включають у себе по дев'ять вихідних подій-передумов — 1,3-5,7-11; 2,3-5,7-11; 1,3-6, 7-11 і 2,3-6,7-11.

За допомогою виявлених мінімальних поєднань дерева подій можна судити про значимість або критичність кожної вихідної передумови, тобто про внесок у дотримання умов, необхідних для прояву або попередження досліджуваної небезпечної події. Не заглиблюючись в суворіші способи оцінки такого вкладу, відзначимо лише таку його характерну ознаку. Виявляється, що міра значущості конкретної передумови — обернено пропорційна кількості інших суміжних з нею подій мінімального пропускного поєднання, і — пропорційна числу, яке містить її мінімальне відсічне поєднання.

Отже, можна стверджувати, що з врахованих тут подій нижнього рівня лівій частині діаграми (рис. 1), найкритичнішими для даної надзвичайної ситуації виявилися передумови 11 і 12, найменш 1, 2 і 5, 6, тоді як всі інші можна вважати якісно рівнозначними. Справді, хоча виникнення будь-якої з передумов 3, 4, 7-11 і супроводжується одним і тим же внеском в умови появи події, що 11 і 12 (всі вони як би пропускають сигнал, мало не головної події), але вплив останньої пари на нього недопущення (перетин сигналу) значно вище. Інакше кажучи, для того щоб гарантувати неможливість появи моделюємої надзвичайної ситуації, необхідно не допускати в умовах надзвичайного стану ні саморозпуску управління компанією (12) ні розколу (11) між акціонерами і керівником компанії.

Змістовіші висновки і рекомендації можна отримати за допомогою кількісного аналізу діаграми, проведеного на основі відповідних аналітичних залежностей. Для дерева подій, це — функція, яка описує структуру, яка забезпечує проходження сигналу від його вихідних передумов до основної події. Наприклад, використовуючи алфавітно-цифрові коди для передумов дерева подій й позначаючи символами «$\cup$» і «$\cap$» оператори диз'юнкції (логічне додавання) і кон'юнкції (логічне множення), нескладно сформувати таку структурну функцію для лівої частини даної ситуаційної моделі:

$$X=И\cap Л=(В\cup Г\cup Е)\cap Л=[(А\cup 3\cup 4\cup Б)\cup Г\cup(9\cup Д)]\cap Л=$$
$$=[[(1\cap 2)\cup 3\cup 4\cup (5\cap 6)]\cup(7\cup 8)\cup(9\cup 10\cup 11)]\cap Л=$$
$$=[[(1\cap 2)\cup 3\cup 4\cup (5\cap 6)]\cup(7\cup 8)\cup(9\cup 10\cup 11)]\cap(12\cup 11). \quad (1)$$

Для дерева ж можливих результатів справедливо наступний аналітичний вираз, який дозволяє спрогнозувати розміри ризику (величини середнього збитку — $M_r[Y]$, очікуваного в разі моделювання і надзвичайної ситуації:

$$R = M_r[Y] = \sum_{k=1}^{m} Q_{rk} Y_{rk} , \qquad (2)$$

де Q_{rk} , Y_{rk} — значення умовної ймовірності та розміру збитків від кожного (m = 12) з результатів розташованих у правій частині цього дерева.

Апріорну кількісну оцінку, тобто прогноз ймовірності *виникнення* надзвичайної ситуації *Q(X)* доцільно проводити двома способами:

а) за допомогою структурної функції (1) після її згортання за правилами булевої алгебри і заміни операторів «$\cup$» і «$\cap$» на арифметичні дії «+» і «·», і алфавітно-цифрових кодів змінних — на ймовірності появи відповідних подій-передумов;

б) шляхом послідовного зміцнення дерева подій (тобто згортання від низу до верху тих його гілок, які утворені за допомогою передумов і вузлів «і», «або») в події з еквівалентними параметрами, які розраховуються за такими формулами:

$$P_{(*)} = P_1 \cdot P_2 \cdots P_n = \prod_{i=1}^{n} P_i ;$$

$$P_{(+)} = 1 - (1 - P_1)(1 - P_2) \cdots (1 - P_m) = 1 - \prod_{i=1}^{s} (1 - P_i), \qquad (3)$$

де $P_{(*)}$ і $P_{(+)}$ — ймовірності виникнення подій, утворених логічним добутком і складанням зумовлених їх передумов;

n, s — кількість подій передумов дерева подій, об'єднаних конкретним вузлом типу «і», «або», відповідно;

P_i — величина ймовірності появи кожної події-передумови.

Співмножники, які входять до правої частини формул (3), можуть бути знайдені за допомогою різноманітних методів апріорної та апостеріорної оцінки — експертних, модельних, статистичних. Якщо ж моделюються умови виникнення унікальної (статистично не відтворюється) надзвичайної ситуації, наприклад, — подібно тільки що розглянутої, то значення P_i краще всього визначати методом експертних оцінок, за умови подання цих ймовірностей в вигляді нечітких чисел. Найзручніше це досягається шляхом попередньої апроксимації лівої і правої гілок функції приналежності відповідних чисел так званими (*L*) і (*R*) формами [2].

У цьому випадку наближена інтервальна оцінка міри можливості головної події також здійснюється за формулами (1) і (3), тобто за допомогою структурної функції або послідовної декомпозиції дерева події. Особливість полягає в тому, що замість правих частин виразу (3) використовуються відповідні рекурентні формули [1], параметрами яких служать не точкові оцінки ймовірності P_i, а тріади чисел, відповідних: а) найможливішим, б) оптимістичним і в) песимістичним значенням.

Подібним чином — як модельні, експертні або статистичні оцінки, можуть бути знайдені й вихідні дані, які необхідні для прогнозу ризику за формулою (2). При визначенні її параметрів, слід також пам'ятати, що Q_{rk} є умовними ймовірностями, а відповідні їм результати кожного рівня утворюють повну групу незалежних подій. Інакше кажучи, при побудові дерева подій, слід враховувати як умовний характер результатів, так і всі ті комбінації, поява яких не суперечить об'єктивно діючим законів.

Через об'єктивні причини тут не наводяться будь-які вихідні дані про параметри P_i, Q_{rk}, Y_{rk} і вже тим більше — не проводяться засновані на них кількісні розрахунки. Перш за все, — розуміючи, а) цінність подібного ситуаційного моделювання полягає не в точному кількісному прогнозі ймовірності *Q(X)* і / або ризику $M_r[Y]$, а — в оцінці ефективності різноманітних стратегій щодо недопущення або пом'якшення наслідків цих небажаних ситуацій; б) а також заради часу, необхідного для проведення практично непотрібних обчислень. Так, наприклад, якщо оцінена дослідником ймовірність *Q(X)* або збиток $M_r[Y]$ перевищать максимально допустимі значення, то він зобов'язаний запропонувати розумні заходи щодо усунення виниклої проблеми.

Виходом з таких ситуацій може бути впровадження додаткових організаційних та інших заходів, спрямованих на попередження надзвичайних подій, або на зниження шкоди від них у разі появи. Очевидно також, що такий захід буде пов'язаний з певними витратами і деякої результативністю, — не обов'язково пропорційної вкладеним коштам. В цих умовах доцільна попередня оцінка ефективності подібних заходів та їх оптимізація з якимись критеріями. Вирішення цього важливого завдання може бути здійснено також за допомогою розглянутих тут ситуаційних моделей типу «дерево». Для визначення ефекту $\Delta Q(X)$ або $\Delta M_r[Y]$, очікуваного від конкретного заходу, необхідно провести розрахунки за формулами (1-3) за новими (зменшених у результаті впровадження) значеннями вихідних даних: а) ймовірності P_i критичних передумов

дерева події або б) ймовірності Q_{rk} і збитку Y_{rk} від найруйнівніших сценаріїв дерева подій. При цьому загальна схема оцінки ефективності конкретних заходів може бути представлена таким чином: $\Delta P_i \to \Delta Q(X) \to \Delta M_r[Y]$ та $\Delta Q_{rk} \to \Delta M_r[Y]$, $\Delta Y_{rk} \to \Delta M_r[Y]$ відповідно.

Висновки. Незважаючи на простоту запропонованої моделі, основна її мета — ілюстративна, слід зробити деякі висновки та кількісні оцінки, які дуже складно отримати без моделювання.

Ситуаційна модель дозволяє виконувати ранжування факторів, які враховані деревом події в якості вихідних подій-передумов. Дійсно, по-своєму внеску у створення й руйнування причинного ланцюга надзвичайної ситуації, всі вони можуть бути розділені на якісно різноманітні групи. Акцентування цієї обставини буде істотно позначатися на виявленні «вузьких» місць забезпеченні інформаційної безпеки, а значить — і на їх усунення.

Використання запропонованої моделі відкриває перспективу для оптимізації відповідної діяльності. Справді, альтернативних заходів можна запропонувати багато, ефект від кожного з них і витрати на впровадження — різні, а наявні в розпорядженні коштів — як правило не вистачає. Звідси — необхідно знаходити та приймати оптимальне рішення.

При оцінці заходів, які проводяться на основі запропонованих моделей, буде забезпечуватися вища точність прогнозу їх ефективності. Справа в тому, що тут доведеться оперувати абсолютними оцінками ймовірності та / або ризику, достовірність яких низька, а — відносними (різниця вкладу одних і тих же факторів, які вимірюються при інших рівних умовах), що є вірогіднішим.

Бібліографічні посилання

1. Белов П.Г. Теоретические основы системной инженерии безопасности. — М.: ГНТП «Безопасность», 1996. — 424 с.
2. Дюбуа Д., Прад А. Теория возможностей. Приложения к представлению знаний в информатике. — М.: Радио и связь, 1990. — 288 с.
3. В.І. Жлуктенко, А.В. Бєгун. Стохастичні моделі в економіці:монографія — К.:КНЕУ — 2007. — 288 с.
4. Kumamoto H., Henley E. Probabiliustic risk assessment and management for engineers and scientists IEEE Press. 1996. — 597 p.
5. ISO/IEC TR 18044:2004 «Information technology. Security techniques. Information security incident management».

6. ISO/IEC 27035:2011 «Information technology. Security techniques. Information security incident management».
7. BS 25999-1:2006 «Business continuity management. Code of practice».

Статтю подано до редакції 21.11.2020

УДК: 303.732 DOI 10.33111/mise.100.3

Джалладова І. А., д.ф.-м.н.,
професор кафедри комп'ютерної математики та інформаційної безпеки,
ДВНЗ «КНЕУ імені Вадима Гетьмана»

Dzhalladova I. A., Doctor of Physic Mathematical Sciences,
Professor of the Department of Computer Mathematics and Information Security,
SHEI KNEU named after V. Hetman

СИСТЕМНИЙ АНАЛІЗ ЗАГРОЗ СОЦІОКІБЕРНЕТИЧНОЇ БЕЗПЕКИ В УМОВАХ ПАНДЕМІЇ

SYSTEM ANALYSIS OF SOCIOCYBERNETIC SECURITY IN A PANDEMIC CONDITIONS

Анотація. *Метою роботи є системний аналіз логічних, структурних зв'язків між різними загрозами соціокібернетичної безпеки. При чому включаємо в розгляд широкий спектр різних складових, різних розумінь соціокібернетичної безпеки: безпеку технічних систем, безпеку кіберпростору, безпеку кібер-фізичних систем тощо. Все майже не вивчено і не досліджено в цілому. Поняття «соціо-кіберфізичні системи» — взагалі новий, але перспективний інноваційний напрям. CPS (2006) — це системи, які складаються із різних об'єктів штучних підсистем, контролерів, які поєднуються в єдине ціле. Додаючи термін «social» маємо на увазі, що в будь-яку із перелічених підсистем додаємо людину і суспільство. Джерелом появи складних систем можна вважати появу найскладніших, різноманітних механізмів, що запропоновано внаслідок засвоєння наукою автоматизованих, сенсорних та інших систем. Соціокібернетичні системи засновано на інженерному моделюванні та здатні пристосовуватись до широкого спектра змін. Стаття є актуальною і перспективною науковою роботою. Перспективною є ідея створити опис певного механізму, який би на кшталт «комбайна з кліщами», спостерігаючи за різними аспектами підсистем, збирав би і аналізував до якої із підсистем віднести склад, якість загроз, і вже тоді обирав би відповідний алгоритм дій. Упродовж тисячоліть побудовано сотні тисячі різних методів та інструментів, але в сучасних умовах жодний не є готовим. Власно ситуація з COVID-19 це показала. Гнучкість розуму і комбінація різних методів це єдиний ключ у сфері моделювання різних процесів, у тому числі процесів, пов'язаних*