УДК 004.056, 004.75
© О. Гарасим[12], Ю. Гарасим[13], П. Гаранюк[1], І. Гаранюк[1], 2013

ЗАСТОСУВАННЯ ТЕОРІЇ ХАОСУ В РИЗИК-МЕНЕДЖМЕНТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Запропоновано підхід до вирішення одного із найактуальніших завдань у сфері інформаційної безпеки та ризик-менеджменті – прогнозування ризику реалізації загроз. Наведено перелік конкретних дій до виконання для вирішення поставленого завдання на основі застосування теорії хаосу.

One of the most important tasks in the information security and risk management field solving approach is proposed in the paper. The practical recommendations to solve the task of threats risk prediction by applying chaos theory are given.

1. ВСТУП

В роботі досліджено можливість практичного застосування теорії хаосу [1, 2] в задачах галузі інформаційної безпеки (ІБ), зокрема:

– підсистемі ризик-менеджменту ІБ,
– системі менеджменту інформаційної безпеки (СМІБ) загалом,
– підвищенні ефективності та оптимізації режимів роботи систем захисту інформації (СЗІ),
– прогнозуванні векторів розвитку чинників дестабілізації (ЧД), які мають невизначений характер тощо.

За цих умов хаос розглянуто не лише як наслідок динамічної нестійкості структури СЗІ (логічної, фізичної), наприклад, в корпоративних мережах зв’язку (КМЗ), що належить до класу складних систем [3], як джерело руйнівної сили, але і як порядку (узгодженого функціонування) у сфері ІБ.

1. Зв’язок завдання із важливими науковими та практичними проектами

Одним із завдань, наприклад, СМІБ є необхідність здійснення процесу ризик-менеджменту. Ризик-менеджмент – процес управління ризиками, що є особливо актуальним за умов невизначеності, коли подальше уточнення інформації є неможливим або існує обмеженість у фінансуванні, наявності статистичних даних, динамічності та складності реалізації атак тощо. Підхід боротьби з наслідками реалізованих загроз (реактивний) не є ефективним, на цей час заходи ІБ повинні бути спрямовані на створення проактивного захисту інформації (інфо-

[12] Національний університет «Львівська політехніка»
[13] ТзОВ «ІТ Капітал»

рмаційних активів) – захист від нових, ще не реалізованих, невідомих загроз, а не на її відновлення, що, в свою чергу, повинно враховуватися на етапі проектування СЗІ в КМЗ наділяючи її властивістю живучості [4].

Не всі методи та засоби (наприклад, стрес-тестування, прогнозування кризових ситуацій в економіці, умовний VaR, нейронні мережі, теорія глобального ризик-фактору) [5], які застосовуються для систем із стабільним розвитком подій можуть застосовуватися за умов нестабільності (невизначеності впливу ЧД). Проте, існує можливість і необхідність застосовувати адекватні кількісні методи для оцінки ризиків ІБ. Велику користь експертам надає наявність навичок, практичного досвіду, методик здійснення ризик-менеджменту та консалтингова підтримка в плануванні забезпечення неперервності функціонування та оцінки ризиків [6].

Їх застосування обмежене такими аспектами:

– неточність прогнозу,
– навчання за наявності різнорідних та суперечливих даних,
– вимагають достатньо великих обсягів даних, щоб здійснювати самонавчання та прогнозування.

Це, в свою чергу, вимагає значних затрат часу; передбачає не контрольованість і закритість від експерта процесу прогнозування. Жодний з підходів не враховує форс-мажорних подій. Тому, в хаотичній, непередбачуваній поведінці подій у галузі ІБ вони не можуть точно спрогнозувати умови, за яких система знаходитиметься в стані рівноваги (в межах гомеокінетичного плата) [7], умови переходу КМЗ з одного стану в інший (роботоздатний, аварійний, нероботоздатний тощо), поведінку дій зловмисника, вектор атак (рис.1), ймовірність виникнення нових загроз тощо.

Рис. 1. Вектори загроз на прикладі системи управління виявлення/запобігання витоку інформації

Актуальним завданням для СМІБ компанії є здійснення своєчасного прогнозування потенційних загроз на початковому етапі проектування технологічних (бізнес) процесів та відповідно автоматичне або напівавтоматичне корегування власної роботи. Це зекономило б час і витрати, які могли б з'явитися через зміни в проекті на завершальному етапі впровадження або після початку функціонування системи.

Теорія хаосу надає можливість розглядати хаотичну систему як впорядковану, в короткотерміновому періоді і визначити її межі в довготерміновому періоді. Таким чином, лише деякі аспекти хаотичної системи залишаються непередбачуваними. Застосовуючи теорію хаосу до галузі ІБ ми отримуємо можливість використовувати нові методи аналізу даних (повідомлення про події або інциденти ІБ як співробітниками компанії, так і технічними системами: антивірус, між мережевий екран, веб-фільтр, виявлення/запобігання атакам, запобігання витоку даних тощо) і виявлення прихованих закономірностей. Там, де колись поведінку складної системи вважали випадковою і жодних закономірностей не шукали, вважаючи, що їх просто не існує, сьогодні можемо впорядкувати. Саме тому, підхід теорії хаосу є ефективним для вирішення завдань ІБ.

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

На цей час описати поведінку складних нелінійних динамічних систем, до складу яких автори відносять СЗІ в КМЗ, дає можливість математичний апарат теорії хаосу [8]. Складною називатимемо систему, що складається з множини взаємодіючих складових (наприклад, підсистем антивірусного захисту, захисту від витоку конфіденційної інформації, виявлення та запобігання атакам, управління інформацією та подіями ІБ, між мережевого екранування тощо), внаслідок чого з'являється підвищена вимога до такої властивості як живучість (оскільки кожна система, маючи властивість живучості, у взаємодії з іншими системами може стати єдиною точкою відмови загальної системи), а під нелінійною – рекурсію і нелінійні, динамічні, непостійні, неперіодичні завдання. Таким чином, теорія хаосу є інструментом для дослідження поведінки динамічних складних системи, який базується на математичних концепціях рекурсії або набору диференційних рівнянь, що описують її.

Вважають, що хаос – вища форма порядку [9]. Проте, правильніше вважати хаос іншою формою порядку в будь-якій динамічній системі. За порядком, у звичайному його розумінні, слідує хаос, а за хаосом – порядок. І, якщо визначати хаос як неструктурованість, тоді всередині нього формується своя, особлива форма порядку. Тобто будь-який хаос, має визначену форму – атрактор [10].

Використовуючи теорію хаосу в процесі управління СЗІ в КМЗ [11] отримуємо можливість здійснювати аналіз даних (про стан СЗІ, про вразливості, загрози, ризики) в режимі реального часу або максимально до нього наближеному, що уможливлює практичне застосування проактивного підходу. Крім цього, знаючи кризисні вектори розвитку атак, отримуємо змогу вдосконалювати СМІБ, передбачивши розвиток подій у КМЗ.

До переліку найперспективніших застосувань теорії хаосу у сфері інформаційної безпеки належить «хаотичне управління». Якщо дослідити множину випадків комп'ютерних злочинів, то можна спостерігати певні закономірності, проте, завжди існуватимуть фактори, які залишаються поза увагою. З однієї сторони невизначені фактори ускладнюють процес прогнозування впливу ЧД на СЗІ в КМЗ, але з іншої сторони можемо створювати ЧД для зловмисників, щоб змінити вектор атак у напрямку зручнішого для організації (використання «ефекту метелика», аналогія з технологією honey pot). Таким чином матимемо змогу впливати і, відповідно, керувати хаотичними процесами у галузі ІБ. Нестійкість означає те, що незначними змінами у функціонування СМІБ, отримуємо нову непрогнозовану поведінку зловмисника, але вплив якої буде віддаленим від кризисної точки дестабілізації СЗІ в КМЗ.

Згідно теорії хаосу, якими б не були хаотичні процеси СЗІ в КМЗ, вони прагнутимуть до однієї форми – атрактора [12]. Атрактор характеризує поведінку в просторі протягом певного часу і є одним із інструментів аналізу хаосу. Один з атракторів Лоренца має такий вигляд [13]

$$\begin{cases} \dfrac{dx}{dt} = -a \times x + a \times y, a > 0 \\ \dfrac{dy}{dt} = r \times x - y - x \times z, r > 0 \\ \dfrac{dx}{dt} = b \times z + x \times y, b > 0 \end{cases} \quad (1)$$

Іншим інструментом теорії хаосу є фрактал [14], хоч він і є протилежністю хаосу. Головна відмінність між хаосом і фракталом полягає в тому, що перший є динамічним явищем, а другий – статичним. Під динамічною властивістю хаосу розумітимемо непостійність і неперіодичність зміни траєкторій розвитку ЧД (векторів атак).

Виокремимо основні принципи до аналізу загроз інформаційної безпеки:

– для того, щоб прогнозувати вектори реалізації ЧД, необхідно накопичувати якомога більше інформації про стан ІБ і факторів, які на неї впливають (кількість та тип внутрішніх користувачів, кількість та тип

компонентів ІТ інфраструктури та підсистем захисту інформації, необхідність забезпечувати режим конфіденційності, мотиви порушників, як зовнішніх, так і внутрішніх, їх кількість та кваліфікацію, місце розташування, сфера діяльності, лояльність керівництва тощо). Чим більше інформації, тим точнішою буде оцінка ризику і прогноз розвитку вектору атак;

– незначні відмінності в початкових умовах можуть зумовити значні відмінності в розвитку вектору атак. Тому, прогнозування можливе лише в короткострокових термінах. Забезпечується процедура періодичного прогнозування;

– основна і, зазвичай, прихована структура завжди може бути визначена і змінена. Структура визначає поведінку. Дослідження загроз за допомогою хаосу дає змогу визначити основну їх структуру і, змінюючи підходи в управлінні ІБ, можна керувати ризиками.

3. ВИОКРЕМЛЕННЯ ЗАВДАННЯ ДОСЛІДЖЕННЯ

До недавна вважалося, що існують два класи процесів [15]: перші описуються динамічними системами, де майбутнє однозначно визначається минулим – процеси цього класу детерміновані, оборотні і повністю передбачувані. Межі прогнозу стану таких систем практично необмежені. Приклади таких систем – від так званих «ідеальних» маятників в класичній фізиці до реальних космічних об’єктів в астрономії. Другі ж – випадкові процеси, де майбутнє ніяк не залежить від минулого. Межі прогнозу таких систем повністю відсутні.

Проте, було виявлено [16], що існує третій клас процесів, які формально описуються динамічними системами, але їх поведінка може бути передбачена лише на невеликий проміжок часу (оскільки всі фактори не можуть бути враховані у процесі прогнозування). Цей клас процесів отримав назву «динамічного хаосу» [17]. Наведемо порівняння підходів прогнозування подій ІБ, інцидентів, інцидентів ІБ, кризових станів між процесами СЗІ в КМЗ, який є поліномінально обмеженим і можливим для виконання.

Виникнення ЧД є хаотичним процесом. Причина хаотичної поведінки розвитку ЧД полягає у відмінності початкових умов. Навіть найменші розбіжності в даних, на етапі проектування СЗІ в КМЗ, в процесі рекурсії зумовлює експоненційне накопичення помилок і відповідно їх стохастичну розбіжність [18].

Таблиця 1

Порівняння підходів прогнозування подій ІБ, інцидентів, інцидентів ІБ, кризових станів

Реальні системи та процеси	Теорія та моделі досліджень	Можливості прогнозування	Межі прогнозу
Динамічні	Теорія динамічних систем; неперервні моделі.	Майбутнє однозначно визначається минулим, процеси детерміновані і повністю прогнозовані.	Необмежені
Стохастичні	Теорія ймовірності та математична статистика; ймовірнісно-статистичні моделі.	Майбутнє жодним чином не залежить від минулого, процеси цілком непередбачувані.	Відсутні
«Динамічний хаос»	Теорія складності та самоорганізованої кризисності; моделі ієрархічних систем та нелінійної динаміки.	Поведінка може бути передбачена лише на короткий проміжок часу.	Обмежені

На це впливають складні непередбачувані дії зловмисників, кількість та рівень важливості інформаційних активів компанії, наявні елементи захисту даних. Все це та багато інших факторів є початковими умовами у розвитку ЧД, що зумовлює динамічність і нестабільність забезпечення ІБ організації. Чинники дестабілізації ж мають одну ціль – дестабілізувати нормальну роботу КМЗ, набираючи вигляду атрактора, структуру якого будемо досліджувати за допомогою теорії хаосу.

Будь-який атрактор має певні розміри [19], тому експоненційна розбіжність двох траєкторій не може тривати нескінченно. Рано чи пізно «траекторії подій» знову зійдуться (є малоймовірним) або пройдуть поруч одна з одною.

Швидкість сходження-розходження траекторії є мірою хаосу, тобто чисельним показником хаотичності самої системи. Іншою статистичною мірою хаосу є розмірність атрактора [20].

4. АНАЛІЗ ОТРИМАНИХ РЕЗУЛЬТАТІВ

Несуттєві відмінності в початкових умовах для прогнозування впливу ЧД на СЗІ в КМЗ збільшуються і стають суттєвими в результаті рекурсії. Проте, незважаючи на це, графік атрактора буде виглядати однаковим при цих неточностях. Системи будуть мати абсолютно різні значення в будь-який заданий момент часу, але графік атрактора залишиться тим самим. Тому, він описує загальну поведінку системи. Основною проблемою в цьому випадку є інтерпретація фазово-просторових діаграм, які представляють загальну поведінку системи за умов невизначеності впливу чинників дестабілізації.

У таких складних системах як СЗІ в КМЗ з внутрішньо структурованою відносною ентропією (мірою невизначеності, що характеризує внутрішню невпорядкованість системи) [21], заданої частотним розподілом компонентів, маємо

$$\widetilde{H} = -\frac{1}{\lg S} \cdot \sum_{i=1}^{n} p_i \cdot \lg p_i, \qquad (2)$$

де $\widetilde{H}$ – відносна ентропія (коефіцієнт стиснення інформації). Може визначатися відношенням поточної ентропії системи (розраховується за формулою К. Шеннона [22]) до максимальної ентропії системи (розраховується за формулою Р. Хартлі [23]);

S – кількість станів (подій, режимів роботи тощо). У цьому дослідженні це, по-перше, кількість співробітників, що безпосередньо впливають на рівень операційних ризиків ІБ; по-друге, рівень показника ROI (повернення інвестицій в ІБ);

p_i – ймовірність появи дискретної події, що має поєднання терміна «хаос» з термінами або «хаос», або «порядок».

Величина порядку визначається за формулою (3):

Порядок

$$(R) = 1 - \widetilde{H}. \qquad (3)$$

Ймовірність визначається на основі таких варіантів поєднань порядку і хаосу (згідно формули (3)), що виникають на межі системи «СМІБ – порушник»: 1) поєднання хаосу з однієї сторони з порядком на іншій; 2) порядок однієї сторони переходить в хаос іншої; 3) хаос однієї сторони переходить в порядок іншої сторони; 4) порядок – у новий порядок; 5) хаос – у новий хаос.

У варіантах поєднання терміну «хаос» з термінами «порядок» і «хаос» налічується 5 термінів. З точки зору терміну «хаос» загальна кількість термінів «хаос» і «порядок» в розглянутих варіантах становить величину 10–1=9 штук. За допомогою програми для збору, аналі-

зу, статистики загроз, яка була раніше розроблена і описана в [24] отримуємо відносну ентропію для події «загроза з боку працівників»

$$\widetilde{H}_{p_i=6/9} = \frac{0.08489}{\lg S}. \qquad (4)$$

З вищесказаного випливає, що лише на області хаосу можна досягнути вищого рівня ІБ. При цьому найвищий рівень успіху несе поєднання «хаос-хаос», ймовірність появи якого $p_i = 2/9$. Підставивши отримане значення ймовірності в формулу (2), отримаємо

$$\widetilde{H}_{p_i=2/9} = \frac{0.14516}{\lg S}. \qquad (5)$$

Формули (4) і (5) описують межі областей стохастичного (ймовірнісного) хаосу. Ці межі-траєкторії представимо рис. 2.

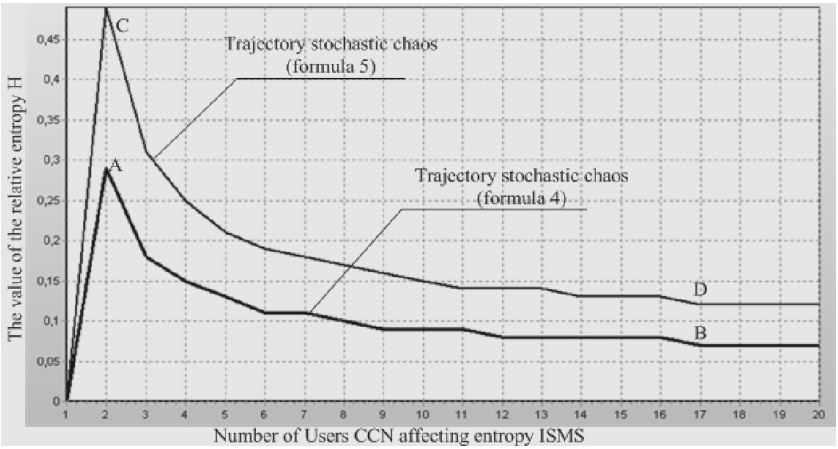

Рис. 2. Траєкторії та області стохастичного хаосу

Як показано на рис. 2, під траєкторією 1CA знаходиться область стохастичного хаосу, повне використання якого надасть максимальний рівень захисту. Пояснюється таке твердження практикою, згідно з якою, чим більша невизначеність у поведінці системи, тим ефективнішою виявляється стохастична модель.

Праві частини кривих 1CD і 1AB, тобто криві CD і AB схожі із правою частиною графічного зображення нормального закону розподілу випадкової величини x (закон Гаусса [25]), який описується формулою [26]

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} \cdot e^{-\frac{(x-a)^2}{2\sigma^2}}, \qquad (6)$$

де σ – середньоквадратичне відхилення випадкової величини x від центра розсіювання а (від центру розподілу ймовірностей);

a – параметр, як центр розсіювання, дорівнює математичному сподіванню випадкової величини x.

При $x = a$ функція $f(x)$ має найбільше значення, рівне $1/\sigma\sqrt{2\pi}$, тобто відстані від точок С і А (рис. 2) до точок середньої лінії траєкторії відносної ентропії операційного ризику при $x = a = 2$ [26]. При цьому, зауважимо, величина ординати точки А становить 0,2819 одиниць відносної ентропії, а величина ординати точки С складає 0,4822 одиниць відносної ентропії. Знаючи середню величину ординати нелінійної траєкторії відносної ентропії операційного ризику для кожної з двох траєкторій стохастичного хаосу (рис. 2) можна визначити відповідні величини загальних операційних ризиків з таких рівностей:

$$\frac{1}{\sigma_{o.o.p.(6/9)}\sqrt{2\pi}} = 0.2819 - h_{o.o.p.(p_i=6/9)}, \qquad (7)$$

$$\frac{1}{\sigma_{o.o.p.(6/9)}\sqrt{2\pi}} = 0.4822 - h_{o.o.p.(p_i=2/9)}. \qquad (8)$$

Визначення величин ординат середніх ліній траєкторій відносної ентропії операційних ризиків, тобто $h_{o.o.p.(p_i=6/9)}$ та $h_{o.o.p.(p_i=2/9)}$, можливо і необхідно здійснити за допомогою дивного атрактора.

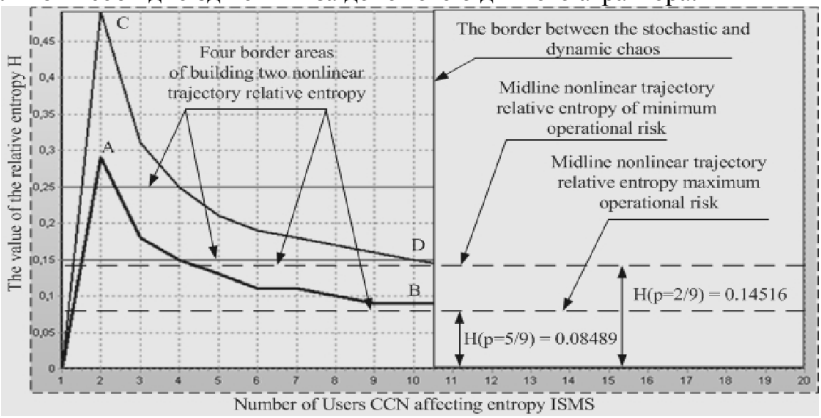

Рис. 3. Графічні пояснення до статичного і динамічного хаосу

Згідно рис. 3, відстані $h_{o.o.p.(p_i=6/9)} = 0.08489$ і $h_{o.o.p.(p_i=2/9)} = 0.14516$. У зв'язку з цим повернемося до формул (7) і (8). Підставивши в них отримані відстані, отримаємо такі залежності:

$$\frac{1}{\sigma_{o.o.p.(6/9)}\sqrt{2\pi}} = 0.2819 - h_{o.o.p.(p_i=6/9)} = 0.2819 - 0.08489 = 0.1,$$

$$\frac{1}{\sigma_{o.o.p.(2/9)}\sqrt{2\pi}} = 0.4822 - h_{o.o.p.(p_i=2/9)} = 0.4822 - 0.14516 = 0.3.$$

З цих залежностей отримуємо такі величини загальних операційних ризиків:

$$\sigma_{o.o.p.(6/9)} = \frac{1}{0.1970\sqrt{2\cdot 3.14}} = 2.0256,$$

$$\sigma_{o.o.p.(2/9)} = \frac{1}{0.3370\sqrt{2\cdot 3.14}} = 1.1841.$$

Для визначення амплітуд коливань відносної ентропії операційних ризиків було використано правило «трьох сигм» (рис. 3). Результатом цього є чотири межі областей побудови двох нелінійних траєкторій відносної ентропії (одна область заштрихована), показані на рис. 4. Формули, що описують нелінійні траєкторії відносної ентропії операційних ризиків, мають такий вигляд:

$$f(S)_{(6/9)} = 0.08489 + 0.02761\cdot e^{-0.135585(10-S)}\cdot \sin(3.14S + 1.57), \quad (9)$$

$$f(S)_{(2/9)} = 0.14516 + 0.1\cdot e^{-0.135585(10-S)}\cdot \sin(3.14S + 1.57). \quad (10)$$

Другий член множника, що знаходиться в правій частині формул (9) і (10), показує, що в цих випадках амплітуди коливань необмежено зростають при необмеженому зростанні параметра S. Таке явище називається резонансом [27]. Починається резонанс на траєкторії лінії межі між областями стохастичного і динамічного хаосів, точніше в одній з її точок, в яку входять всі траєкторії. На рис. 3 за допомогою формули (9) побудовано криву траєкторії відносної ентропії операційних ризиків, яка поряд з іншими трьома показаними на рисунку траєкторіями притягається точкою F.

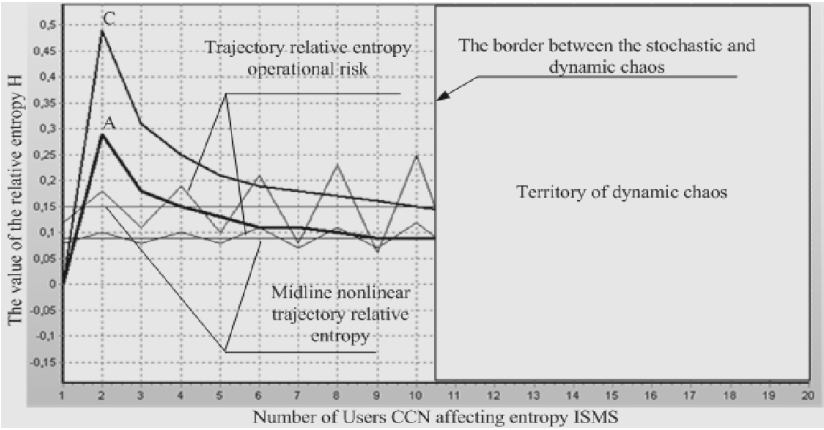

Рис. 4. Траєкторії області стохастичного хаосу

На рис. 4 представлено графічне зображення процесу функціонування СМІБ на обох областях хаосу. При цьому на області стохастичного хаосу показані всі її траєкторії з відповідними текстовими поясненнями. Таким чином, теорія хаосу є засобом боротьби з десабілізацією системи, є підходом до забезпечення ІБ, може застосовуватися для ліквідації слабких ланок захисту, бути інструментом аналізу і прогнозування в ризик-менеджменті.

5. ВИСНОВКИ

Теорія хаосу є перспективним інструментом у галузі ІБ, за допомогою якої, розроблятимемо управлінські підходи для аналізу СМІБ, оцінюватимемо ризики, прогнозуватимемо вплив чинників дестабілізації, управлятимемо ризиками і вдосконалюватимемо СЗІ в КМЗ. Корпоративна мережа зв'язку піддається множині чинників дестабілізації і, для того, щоб її адаптувати до умов нестабільності, наділити властивістю живучості та гнучкістю для забезпечення стабільності її функціонування запропоновано використовувати математичний аппарат теорії хаосу. Теорію хаосу використовуємо для обгрунтування, прогнозування подій у таких складних системах як СЗІ в КМЗ.

Оскільки теорія хаосу обгрунтовує важливість розроблення методик, методів, процедур, алгоритмів, правил прийняття рішень, вдається подолати складність та визначити приховані засоби для досягнення мети. Імітаційні графіки, які представлені в роботі доводять, що теорія хаосу має практичне застосування в завданнях ризик-менеджменту ІБ. Результати моделювання показують динаміку розвитку впливу чинників дестабілізації залежно від кількості осіб, які мають доступ до конфіденційної інформації.

Подальша робота спрямована на методах мінімізації впливу чинників дестабілізації і забезпечення властивістю живучості СЗІ в КМЗ.

1. Kyriazis M. Practical applications of chaos theory to the modulation of human ageing: nature prefers chaos to regularity [Електронний ресурс] режим доступу: http://www4.fct.unesp.br/docentes/ fisio/augusto/artigos%20cient% EDficos/artigo%20do%20caos.pdf 2. George T. Introduction to Chaos and It's Real World Applications [Електронний ресурс] режим доступу: http://www.csuohio.edu/sciences/ dept/physics/physicsweb/kaufman/yurkon/ chaos.html 3. About Complex Systems [Електронний ресурс] режим доступу: http://www.necsi.edu/guide/study.html 4. Гарасим Ю. Р. Аналіз систем захисту, які мають властивість живучості / Ю. Р. Гарасим // Військово-технічний збірник. – № 1 (4). – 2010. – С. 87-95 5. William D. Principles and Applications of Chaotic Systems [Електронний ресурс] режим доступу: http://cis.csuohio.edu/~munakata/publs/pdf/cacm95ch.pdf 6. Storkey I. Operational Risk Management and Business Continuity Planning for Modern State Treasuries / Storkey I. // International Monetary Fund. – Washington, 2005. – 32 p. 7. Дмитриев А. Детерминированный хаос и информационные технологии / Дмитриев А. // «Компьютерра №47». – 1998. – С. 50-54 8. Bautista-Thompson E. The classification of data sequences by similarity analysis of recurrence plot patterns / Bautista-Thompson E., Brito-Guevara R. / Seventh Mexican International Conference on Artificial Intelligence. – 2008. – P. 20-25. 9. Observations on The Application of Chaos Theory to Fluid Mechanics // Meridian International Research. – Wellesbourne, 2003. – 24 p. 10. Теория хаоса [Електронний ресурс] режим доступу: http://pro-forexinform.ru/teoriya-khaosa 11. Levy D. Chaos theory and strategy: theory, application,and managerial implication / Levy D. // Strategic Management Journal, Vol. 15. – Boston. – 1994. – P. 167-178. 12. Chaos Theory and Strange Attractors [Електронний ресурс] режим доступу: http://www.alunw.freeuk.com/chaos.html. 13. Атрактор Лоренца [Електронний ресурс] режим доступу: http://ec.snu.edu.ua/umkds/ nelinanalis/%D0%A0%D0%B0%D0%BC%D0%B0%D0%B7%D0%B0%D0%BD %D0% BE%D0%B2_%D0%9C%D1%83%D1%81%D0%B0%D1%94%D0%B2% D0%B0/sr4.htm. 14. Mendelson J. Chaos Theory and Fractals / J. Mendelson, E. Blumenthal [Електронний ресурс] режим доступу: http://www.tnellen.com/alt/chaos.html 15. Gumowski I. Dynamique chaotique: transformations ponctuelles, transition, ordre-désordre // Gumowski I., Mira Ch. – Cepadues, 1980. – 478 p. 16. Оганесян Т. За горизонтом предсказуемости / Оганесян Т., Переходцев Г. // «Эксперт», №27 (287). – 2001. – С. 31-33. 17. Vladimir I. Synergetic Phenomena in Active Lattices / Vladimir I.; Manuel G. – Berlin, 2002. – 361 p. 18. Bruce E. Nonlinear Dynamics and Chaos [Електронний ресурс] режим доступу: http://www.uam.es/personal_pdi/ciencias /dfaraco/docencia/modelizacion/ ELSKendall.pdf 19. Hunt B. The Theory of Chaotic Attractors / Brian R. Hunt, Judy A. Kennedy, Tien-Yien Li, Helena E. Nusse // Springer: New York, 2004. – 515 p. 20. Manneville P. Dynamique non lineaire et chaos [Електронний ресурс] режим доступу: http://e2phy.in2p3.fr/2005/documents/apres_ecole/Textes/Manneville_txt. pdf. 21. Козленко М. І. Ефективність застосування ймовірнісних характеристик

при формуванні широкосмугових випадкових сигналів в телекомунікаційних та комп'ютерних системах / Козленко М. І. / Вісник №4: Хмельницький національний університет. – Хмельницька, 2012. – С. 118-125. 22. Дулесов А. С. Применение подходов хартли и шеннона к задачам определения количества информации технических систем [Електронний ресурс] режим доступу: http://vernadsky.tstu.ru/pdf/2009/ 03/rus_16_2009_3.pdf. 23. Порфирьев Б. Н. Концепция риска, который никогда не равен нулю / Порфирьев Б. Н. // Энергия. – 1989. – № 8. – С. 38 51. 24. Гарасим О. Р. Аналіз захищеності мережі на основі консолідованих ресурсів загроз / О. Р. Гарасим, Л. Б. Чирун // Інформаційні системи та мережі: Вісник Національного університету «Львівська політехніка», № 699. – Львів, 2011. – С. 270-280 25. Gauss law [Електронний ресурс] режим доступу: http://teacher.nsrl.rochester.edu: 8080/phy122/LectureNotes/Chapter24/Chapter24.html. 26. Пискунов Н. С. Дифференциальное и интегральное исчисления для втузов. Т.2: Учебное пособие для втузов. – 13-е изд. / Пискунов Н. С. – М. : Наука, Главная редакция физико-математической литературы, 1985. – 500 с. 27. Азарєнков М. О. Теорія коливань та хвиль / М. О. Азарєнков, В. О. Гірка, В. І. Лапшин, В. І. Муратов. – Харків, 2005. – 154 с.