УДК 004.056:004.7

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 1, pp. 35-43

ДИНАМІКА КІЛЬКОСТІ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

І.В. Кононович

Одеська національна академія харчових технологій
вул. Канатна, 112, м. Одеса, 650039, Україна; e-mail: kononovich@mail.ru

В статті розглядається динаміка інцидентів інформаційної безпеки інфокомунікаційних мереж, запропоновано гіпотезу щодо її коливального характеру та розроблена модель «зловмисник-захисник» на основі моделі Лоткі – Волтерра. Отримані результати дозволяють підвищити ефективність роботи систем інформаційної безпеки та формалізувати напрямки подальших досліджень щодо розробки нових ефективних систем інформаційної безпеки інфокомунікацій з використанням методів нелінійної динаміки.

Ключові слова: інформаційна безпека, інциденти, нелінійна динаміка, комп'ютерне моделювання, інформаційно-комунікаційні мережі

Вступ

Інформаційна безпека критично важливих інфраструктур держави, зокрема, кібербезпека інформаційно-комунікаційних систем (інфокомунікацій), увійшла в число найбільш значимих задач науки і практики. Інфокомунікації стали складними і постійно змінюються. Динамічний характер об'єкта захисту приводить до труднощів аналітичного описання систем інформаційної безпеки. Це ставить, за словами Д. У. Гіббса, «одною з головних цілей теоретичного дослідження – знайти точку зору, з якої предмет представляється найбільш простим [1; епіграф до § 1.2]». Методичною основою для створення моделей і теорії динаміки кількості інцидентів інформаційної безпеки можуть стати нелінійна динаміка та комп'ютерне моделювання.

Основними математичними моделями в теорії захисту інформації, які з 90-х років минулого століття є «доказовою теоретичною базою для побудови сучасних систем захисту інформації» і класифікація яких дана в [2; § 4.4], стали: для дискреційної політики безпеки – модель Харісона – Руззо – Ульмана, модель Take-Grant; для мандатної політики та моделей безпеки інформаційних потоків – модель конфіденційності Белла-ЛаПадула, модель цілісності Біба, модель Байба, модель Кларка Вілсона, див. [3; § 3.3-3.5]; для ймовірнісних моделей – модель системи безпеки з повним перекриттям, ігрова модель, ланкова модель Байба. Популяризуються також моделі, що дозволили внести нові вклади Юдіним О.К., Корченко О.Г. та Конаховичем Г.Ф. у оцінку ефективності захисту інформаційних ресурсів – узагальнені концепції побудови систем безпеки інформації, структурні моделі організації систем безпеки мереж, див. [4; § 7.2-7.5], та інші.

В цілому моделі охоплюють функціональні аспекти, детермінований та, частково, стохастичний характер функціонування систем безпеки. Динамічні аспекти процесів, характерні для процесів різних видів безпеки та катастроф, розглядаються із застосуванням методів нелінійної динаміки у піонерській роботі російських вчених під редакцією Малінецького Г.Г. [1].

Перелік літератури з нелінійної динаміки (синергетики), починаючи з робіт її основоположників Г. Хакена та І. Пригожина і до робіт нинішньої пори, див. [5], став

неоглядним. При цьому, багато дослідників відмічають застосовність методів нелінійної динаміки до вирішення задач у багатьох галузях на стику фізики і хімії [6], біології, екології [7], соціології й економіки [8], психології, управління [9]. Успішність побудови основ математичної теорії безпеки та ризику [1], феноменологічних моделей не рівноважних соціально-економічних систем [8], та багатьох інших, обумовлені переносом моделей фізико-хімічних реакцій у дані галузі та використанням нелінійної динаміки й комп'ютерного моделювання.

Що стосується досліджень загальної динаміки процесів забезпечення інформаційної безпеки та кібербезпеки у складних інформаційно-комунікаційних системах (ІКС) та мережах, то таких досліджень поки що не достатньо.

Метою даної роботи є підвищення ефективності розробки систем інформаційної безпеки ІКС за рахунок створення й аналізу моделей нелінійної динаміки інцидентів інформаційної безпеки.

Обґрунтування методики досліджень

Застосування методів нелінійної динаміки для моделювання процесів забезпечення інформаційної безпеки надає ряд можливостей та умов. Система інформаційної безпеки ІКС є складною системою. Для спрощення моделі застосовують процедури редукції. «В основі таких процедур – поділ динамічних змінних на групи у відповідності з характерними у часі перемінами змінних, оцінюваних у рамках окремо взятого рівняння із повної системи, див. [10; вступ, с. 26]». У системі виділяють дуже швидкі за часом та дуже повільні процеси. Тоді повільно змінювані процеси можна вважати стаціонарними і в описаннях моделі повільно змінювані змінні замінити на їх стаціонарні значення. Таким способом вдається звести змістовне описання об'єкта до двох – трьох диференційних рівнянь. «Хорошою рисою таких моделей ... являється наявність невеликого числа базових моделей, дослідження яких дозволяє ефективно будувати та вивчати великі класи моделей різноманітних явищ. ... Можна будувати вкрай прості нелінійні математичні моделі, які являються глибокими і змістовними [11; с. 19]».

«Існує практичний спосіб редукції системи рівнянь (великої розмірності) до рівнянь набагато меншої розмірності, що надає можливість дати змістовне описування об'єкта на основі усього тільки двох-трьох диференційних рівнянь. Принцип редукції сотень, рівнянь до системи рівнянь набагато меншої розмірності основується на принципі простоти, див. [8; вступ, § 4] принципі мінімуму та «вузького місця», див. [8; вступ, § 2]». У таких системах можуть виникати структури колективної поведінки ... та можливі автоколивальні процеси, див. [8; вступ, § 6], а також «мають місце степенні закони розподілу та явища самоорганізованої критичності, див. [1; глава 2, § 3]».

Система інформаційної безпеки ІКС є відкритою не рівноважною системою в тому смислі, що вона активно обмінюється із своїм оточенням інформацією. Основним математичним апаратом є якісна теорія диференційних рівнянь. Синергетичний підхід та відповідні моделі можуть стати важливим елементом досліджень масштабних систем інформаційної безпеки.

Розглянемо однорідну мережу із K об'єктів (комп'ютерів). Нехай на кожному з об'єктів є L уразливостей. Так що у мережі сумарно є

$$z = K \cdot L \qquad (1)$$

уразливостей. Візьмемо систему, яка складається із множини об'єктів захисту на вузлах мережі, які мають вразливості, із зловмисників, які створюють потік атак на мережу, із працівників служби безпеки, які виявляють і протидіють атакам та ліквідують виявлені вразливості. Атака закінчується зломом системи, якщо у мережі знаходиться хоча б

одна із уразливостей, відповідно. Інтерес успішних зловмисників полягає у тому, щоб було багато вразливостей (і працівників служби безпеки, бо число останніх свідчить про цінність інформаційних ресурсів, які захищаються). Інтерес одного працівника служби безпеки полягає у відсутності зловмисників. Інтерес корпорації працівників служби безпеки вимагає деякої малої кількості зловмисників для підтримки професійного рівня працівників. Повна відсутність зловмисників приводить до ліквідації служби безпеки. «Інтерес» уразливостей вимагає, щоб працівників служби безпеки було мало. Задача працівників служби безпеки полягає у ліквідації вразливостей. Інтерес усієї системи вимагає підтримання мінімальної чисельності зловмисників, працівників служби безпеки і вразливостей. У такій постановці задача схожа на задачі, які вирішуються у класичній моделі «хижак - жертва». У біології ця модель вивчається з метою визначення умов, за яких підтримується екологічно рівноважна кількість взаємозалежних популяцій при заданих природних ресурсах та екологічної рівноваги. У нашому випадку представляє інтерес аналіз умов за яких мінімізується кількість уразливостей і, відповідно, атак.

Конструювання моделі динамічних процесів інформаційної безпеки

Відносно змінної z – сумарної кількості вразливостей у мережі (1), можна сказати наступне. Відомо, за даними ЗМІ, що кількість помилок, які залишались у перших версіях операційної системи (ОС) Windows, було близько 200. У сучасних версіях ОС помилок, які призводять до вразливостей від атак, значно більше за об'єктивних причин. Доказом цього є нескінченний потік оновлень, які розсилаються на комп'ютери легальних користувачів. Розміри програмного коду стали настільки гігантськими, що повне тестування ОС стало неможливим за показниками часу і вартості [12; § 9.2, рис. 9.1]. А методи автоматизованого генерування надійних програм та методологія створення проактивних систем інформаційної безпеки, розвинуті поки що недостатньо [13,14]. З моменту початку експлуатації ОС число помилок у системі поступово зменшується. Помилки знаходять і виправляють розробники, а також добросовісні користувачі. За помилками полюють зловмисники. Потік спроб зловмисників знайти вразливість є стохастичним. Але слід вважати, що якщо у мережі є вразливість, то вона, рано чи пізно, буде знайдена і використана для атаки. Тому функцію потоку атак будемо пов'язувати із функцією числа вразливостей не стохастичними, а детермінованими залежностями.

У пропонованій моделі динамічних процесів інформаційної безпеки ресурсом будемо вважати вразливості системи інформаційної безпеки, характеристикою яких буде загальне число вразливостей (незалежно від їх типу). Початкову кількість уразливостей можемо обчислювати за формулою $z = n \cdot N$, де n – кількість уразливостей в ОС; N – кількість інсталяцій даної операційної системи. Між хакерами та персоналом служби безпеки йде боротьба за кінчений ресурс. Хакери споживають ресурс-вразливості для здійснення атак. Служби безпеки виявляють атаки, аналізують вразливості й закривають або ліквідують ресурс-вразливості.

Система, що розглядається, є системою із запізнюванням. Запізнювання виникає внаслідок проведення роботи по аналізу атак: виділення характерного «синдрому» вірусу чи атаки, виявлення та ліквідація вразливості тощо. Запізнення виникає і як соціально-психологічне явище, наприклад, за необхідності навчання користувачів, фахівців та осіб, що приймають рішення. «Тут ми стикаємося з ефектом Касандри, про який майже завжди згадують очевидці найбільших лих – багато, а інколи й більшість людей не слідують застереженням, ігнорують попередження щодо небезпеки і завчасно не розпочинають ніяких заходів, які допомогли б їм врятуватись, див. [1; вступ, § 3]». Тут мало знати закономірності, передбачати інциденти з безпекою, створювати механізми захисту. Треба домогтись, щоб це було зрозуміло людям і ними

використано. Ще однією причиною запізнювання є прискорення зміни технологій і звикання до них. Згідно концепції лауреата Нобелівської премії Алвіна Тоффлера «... існує гранична швидкість сприймання людиною змін [1; глава 1, § 3]». А за час одного покоління зараз змінюють одна одну декілька технологій. Люди, особливо старшого віку, можуть мати труднощі з перенавчанням і сприйманням нових загроз.

У даному разі може постати питання, чи правомірний перехід до розгляду мережі, а точніше до «колективу» об'єктів захисту, замість того, щоб надійно захистити кожен об'єкт окремо. Тоді, так здавалося б, що й загальна безпека буде забезпечена. Але стан інформаційної безпеки сьогодні не дозволяє самостійно забезпечити надійний захист. Виявлення та протидія атакам на комп'ютерну мережу не під силу окремим її вузлам. Крім того, «поняття безпеки є системним. Воно залежить від того, які системи ми аналізуємо, а які для нас байдужі та розглядаються як зовнішнє оточення. ... Під системою будемо розуміти циклічну або поліциклічну систему зв'язків, здатну підтримувати власне існування. Здатність до такої самопідтримки або гомеостазу за допомогою циклічної структури зв'язків і будемо розглядати як основну прикмету системи. ...

Безпекою системи будемо називати відсутність можливих порушень (або відсутністю причин, що викликають порушення) гомеостазу системи на протязі деякого проміжку часу [1; глава 2, § 4]». Там же стверджується: «Якщо останню сукупність (мережу, – K) розглядати як складне системоутворююче середовище, то прийдемо до висновку, що прості системи можуть існувати лише у складному середовищі, а у простих середовищах системи повинні бути складними. ... Для підтримки гомеостазу, тобто для компенсації несприятливих зовнішніх впливів (або для розривання небажаних зв'язків), системі потрібна деяка мінімальна складність. Певне, чим складніша система, тим більше впливів вона здатна компенсувати. Якщо система не достатньо складна, щоб вижити у ризикованому середовищі, то вона виживає не одиничними особинами, а колоніями, великими групами. ... Мабуть, таким чином добирається потрібна складність. Цінність однієї особини невелика, смертність висока, колонія існує за рахунок високої швидкості розмноження. ... Дещо такого роду відтворюють моделі типу хижак-жертва».

Також, згідно закону У. Росс Ешбі щодо необхідного різноманіття: «Кількість регулювання має бути не меншою різноманіття збурень, проти якого направлене регулювання [15; глава 11/8-11/10, гл.13/1]». Складність поведінки системи протидії повинна перевищувати складність поведінки атакуючої системи. Звідси випливає і висловлювання Є.А. Касперського щодо «важливості складних технологій в епоху складних атак [16]». Підтвердженням сказаного може служити протікання боротьби з вірусами, під час якої нормалізувати ситуацію (за виключенням «бойових вірусів») вдалося, створивши централізовані служби, де концентровані досвідчені спеціалісти з аналізу вірусів, і розгалужену систему розсилки актуальних баз даних «синдромів» цих вірусів й оперативної модифікації засобів антивірусного захисту.

Оскільки загрози стали виходити від багатоелементної системи, то для аналізу систем протидії природним є використати методи синергетики або нелінійної динаміки. Саме синергетика як теорія сумісних дій, вивчає виникнення у складної системи, що складається із взаємодіючих елементів, нових властивостей, якими окремі елементи не володіють.

Історично першою найпростішою лінійною моделлю у цій області була модель народонаселення, запропонована у 1798 р. Т. Мальтусом, і вирішеною ще у 1202 р. Л. Фібоначчі [10; глава 2.3, пример 2]:

$$\frac{dN}{dt} = \alpha N,\ N(0) = N_0,\ \alpha = const > 0. \qquad (2)$$

Фізичний смисл моделі у тому, що швидкість росту населення, за відсутності стримуючих факторів або протидії, пропорційна чисельності населення N. Вирішенням цього рівняння є $N(t) = N_0 e^{\alpha t}$. Вирішення має сингулярність: $N(t) \to \infty$ при $t \to \infty$. Модель можна застосувати для описування росту населення, біологічних вірусів, а також росту числа комп'ютерних вірусів в умовах, коли нема ніякого антивірусного захисту й віруси мають необмежений доступ до потрібних їм ресурсів середовища.

В реальних умовах є обмеження росту – або закінчуються ресурси, коли заражені всі комп'ютери, або віруси знищуються, коли проти них ведеться боротьба. «У 1835 р. Л.А. Кетле і П.Ф. Ферхюльст, а в 1920 р. повторно Р. Пірл і Л.Д. Рід, відкрили, що чисельність виду N змінюється у відповідності з законом, який задається логістичним рівнянням

$$\dot{N} = r\left(1 - \frac{N}{K}\right)N, \tag{3}$$

де K – середній розмір популяції;

N – чисельність популяції;

r – мальтузіанський коефіцієнт лінійного росту.

Середній розмір популяції – K залежить від ємності середовища, тобто від кількості їжі, розміру ареалу заселення. Логістичний закон добре описує динаміку росту простих біологічних і комп'ютерних вірусів, див. [1; глава 9, § 1.1]». Але логістичний закон не застосовний для моделювання більшості інших видів атак на комп'ютерні мережі, бо не враховує фактор запізнення.

Результати, отримані в нелінійній динаміці, дозволяють сформулювати наступну гіпотезу.

Довгострокові процеси забезпечення інформаційної безпеки, як і процеси у численних складних природних системах, можуть мати коливальний, циклічний характер і мають періоди зростання і спадання. Одним із механізмів коливальності пов'язаний з тим, що система забезпечення інформаційної безпеки являється системою із запізненням. В них результат впливу позначається не відразу, а через певний час h – час запізнення. На вироблення заходів протидії та їх впровадження витрачається певний час. Так, хвилі нових вірусів встигають розповсюдитись, поки не будуть оновлені всі антивірусні засоби.

Для описування систем, що схильні до різких циклічних коливань «у 1948 р. Г.Хатчинсон запропонував наступне узагальнення рівняння (3):

$$\dot{N} = r\left(1 - \frac{N(t-h)}{K}\right)N(t), \tag{4}$$

де h – час запізнення.

Введення додатної постійної h – це спроба врахувати фактор запізнення. Рівняння описує наступну ситуацію: вид заселений у однорідному середовищі, міграційні фактори не суттєві, мається задана кількість їжі, яка відновлюється при зменшенні численності популяції, див. [1; гл.9, § 1.1, формула (3)]». Ситуація з комп'ютерним вірусом описується у такій моделі так: комп'ютерний вірус розповсюджується у однорідній комп'ютерній мережі, є задана кількість комп'ютерів, які можуть бути заражені. Рішення рівняння (4) має періодичний коливальний характер. Його аналіз є предметом іншої роботи. Тут лише зробимо зауваження, що період коливальних процесів у системах із запізненням може бути значно більшим, ніж час запізнення. Для випадку, що розглядається у цій роботі, більш придатна модель

«хижак - жертва». Існують численні добре вивчені модифікації цієї моделі. Задача зводиться до вибору модифікації моделі, удосконалення її та адекватної інтерпретації у термінах систем інформаційної безпеки.

Із декількох різновидів моделі «хижак-жертва» (див. [1; § 5.1, формула (29)] та [17; упражнения 1.15, 4.9, 4.12]) оберемо як зразок модель Лоткі – Волтерра, удосконалений варіант якої описано та проаналізовано аналітично у [1, ; глава 9, § 5.1, формула (29)] та [18; формула 1]. Покажемо, що цю модель можна удосконалити, перетворивши її у модель «хакер - захисник». Позначимо за x – кількість атак на комп'ютерну мережу, що виконуються зловмисниками, це аналог «жертв»; за y – кількість операцій, що виконуються захисниками комп'ютерної мережі, це аналог «хижаків»; за z – кількість уразливостей у мережі, ця змінна характеризує «ресурси». Кількість уразливостей у комп'ютерах, які можуть бути атаковані, враховується у «ресурсах» за формулою (1). Середнє значення цих величин позначимо великими буквами, відповідно – X_c, Y_c, Z_c. Динаміку чисельності взаємодіючих популяцій захисника $x(t)$ та хижака $y(t)$ будемо моделювати системою рівнянь

$$\begin{cases} \dot{x}(t) = r_x\left[1 + a\left(1 - \dfrac{y(t)}{Y_c}\right) - \dfrac{x(t-h_x)}{X_c}\right]x(t) \\ \dot{y}(t) = r_y\left[\dfrac{x(t)}{X_c} - \dfrac{y(t-h_y)}{Y_c}\right]y(t) \end{cases}, \tag{5}$$

де r_x та r_y – мальтузіанські коефіцієнти росту;

h_x та h_y – середній час затримки, відповідно, аналізу (планування) атаки хакером й впровадження засобів протидії та пошуку вразливості захисником;

X_c та Y_c – середні кількості операцій для атак та з ліквідації атак, відповідно;

a – коефіцієнт тиску захисників на хакерів, який визначає ефективне зменшення середньої кількості дій хакерів за умови збільшення активності захисників (хижаків);

Коефіцієнт тиску захисників на хакерів – a визначає ефективне зменшення кількості операцій хакерів по плануванню, підготовці та здійснення атак. Його можна визначити неявним чином

$$X_c(a) = \frac{X_c(0)}{1+a}. \tag{6}$$

На практиці кількість уразливостей мережі поступово зменшується внаслідок діяльності служби безпеки та вдосконалення теорії безпеки. Але часта зміна технологій і потік нових версій підвищують стрибкоподібно число вразливостей. Кількість уразливостей доводиться вважати поновлюваним ресурсом.

Проведемо аналіз цієї моделі при початкових умовах на інтервалі часу $\{h_x \ldots 0\}$ від: $x(0) = 1$, $y(0) = 1$, які були характерні на початку масового використовування комп'ютерів в Україні.

Аналіз моделі динаміки кількості інцидентів інформаційної безпеки

Фізичний смисл моделі, яка представлена системою рівнянь (5), можна зрозуміти порівнявши її з іншими моделями. Так, якщо виключити члени, які описують взаємні зв'язки, система рівнянь розпадається. При цьому, якщо нема захисників ($a = 0$), то перше рівняння перетворюється на рівняння Хатчинсона (4). Якщо, крім того,

виключити запізнення ($h_x = 0$), то маємо логістичне рівняння. А якщо, крім того, далі зняти самообмеження на ріст кількості атак ($X_c \to \infty$), то перше рівняння стає рівнянням мальтузіанського росту. Якщо нема хакерів ($x(t) = 0$), що важко собі уявити, та виключити фактор запізнювання, то із другого рівняння (5) випливає, що захисники поступово «вимирають». Якщо у моделі, тобто системі рівнянь (5), виключити запізнення з обох рівнянь ($h_x = 0; h_y = 0$), то модель стає канонічною, яка ретельно проаналізована аналітично та чисельно, див. [11; глава 8, пример 1] та [7; глава 2, § 3]. Блок-схема Simulink для моделі Лоткі-Волтерра наведена у [7; приложение А.4]. Щодо моделі із запізненням (5), то вона досліджена значно менше. У [17; глава 4 и упражнение 4.9] розроблена методика розрішення диференційних рівнянь із запізненням та надано приклад розрахунку для простої моделі «хижак-жертва», що схожа на модель (5).

Для спрощення моделі (5) при чисельному розрахунку зменшують кількість параметрів за допомогою заміни. Слідуючи [17; формули (3), (4)], робимо заміни: $t = h_x\tau$, $x(h_x\tau) = X_c N_1(\tau)$, $y(h_y\tau) = Y_c N_2(\tau)$ і далі, позначивши $\lambda_1 = r_x h_x$, $\lambda_2 = r_y h_y$, $h = h_y / h_x$, та перепозначивши τ через t , отримуємо

$$\begin{cases} \dot{N}_1(t) = \dfrac{\lambda_1}{1+a}\left[1 + a\left(1 - N_2(t)\right) - N_1(t-1)\right]N_1(t), \\ \dot{N}_2(t) = \lambda_2\left[N_1(t) - N_2(t-h)\right]N_2(t). \end{cases} \qquad (7)$$

З практичних міркувань для моделювання нами була створена програма проведення розрахунків за формулою (5).

Результати одного з прогонів моделі при $r_x = 1.28$, $r_y = 0.99$, $a = 0.9$, $h_x = 1$, $h_y = 0.4$, $X_c = 35$, $Y_c = 25$, показані на рис. 1.

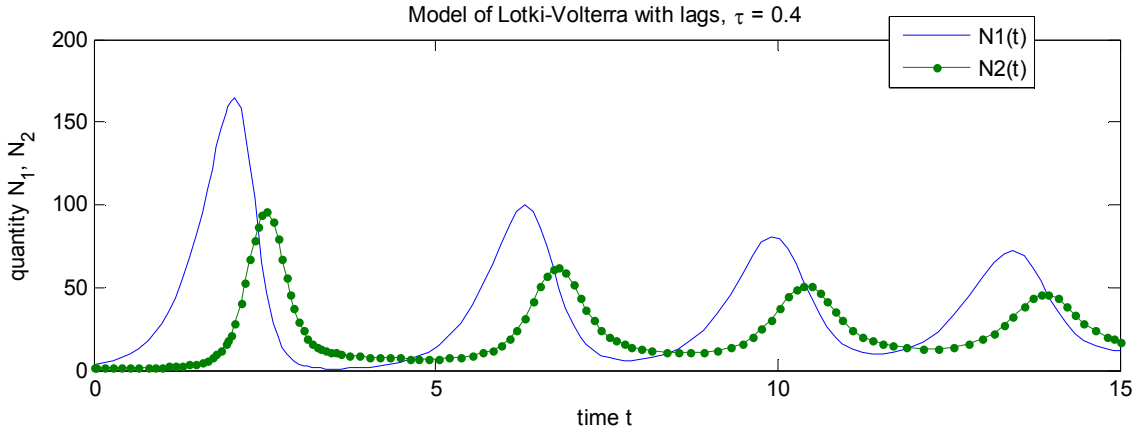

Рис. 1. Розрахунки моделі Лоткі-Волтерра в середовищі MATLAB

До недоліків розглянутої моделі динаміки кількості інцидентів інформаційної безпеки можна віднести її якісний характер. «Число функціонально значимих «резонансів» у реальних сигналах (системах) ... може досягати декількох сотень. При цьому, внаслідок взаємозв'язків у системі та впливів сторонніх факторів різного виду, у тому числі, випадкових, продуцьовані системою сигнали нестаціонарні, див. [10; вступ, с. 27]». Це стосується й великих систем інформаційної безпеки. Продовжуємо цитату: «Всі ці фактори «маскують» чисто хаотичні компоненти

сигналів. ... Таке різноманіття динамічних факторів неможливо врахувати у рамках модельного розгляду».

Висновки

Запропонована у даній статті модель «зловмисник-захисник» на основі моделі Лоткі-Волтерра підтвердила гіпотезу щодо коливального характеру динаміки інцидентів інформаційної безпеки та дозволяє чітко визначити напрямки подальших досліджень щодо розробки методів та побудови систем захисту інформації, а також створити концептуальні моделі попередження атак та формалізувати, на основі методів нелінійної динаміки, можливості превентивних систем для підвищення ефективності їх вибору й формулюванню вимог при їх проектуванні та розробки. Розроблена модель взаємовпливу порушника і захисника в системах захисту інформації дозволяє визначити сукупність заходів різного характеру для організації комплексної системи інформаційної безпеки в інформаційно-комунікаційних системах. Вибір адекватної моделі та розрахунок її кількісних характеристик на основі експериментальної статистики й розробка прогнозу є метою подальшої роботи.

Список літератури

1. Управление риском / [Электронный ресурс] под ред. Г.Г. Малинецкого. – М.: РАН, 2000. – 249 с. – Режим доступа: http://risk.keldysh.ru/risk/risk.htm.
2. Гайворонський, М. В. Безпека інформаційно-комунікаційних систем / М.В. Гайворонський, О.М. Новіков. – К.: Видавнича група ВНУ, 2009. – 608 с.
3. Богуш, В.М. Теоретичні основи захищених інформаційних технологій: навч. посіб. / В.М. Богуш, О.А. Довидьков, В.Г. Кривуца. – К.: ДУІКТ, 2010. – 454 с.
4. Юдін, О.К. Захист інформації в мережах передачі даних / Юдін О.К., Корченко О.Г., Конахович Г.Ф. – К.: Вид-во ТОВ «НВП»ІНТЕРСЕРВІС», 2009. – 716 с.
5. Гленсдорф, П. Термодинамическая теория структуры, устойчивости и флуктуаций: Пер с англ. / Гленсдорф П Пригожин И. Изд. 2-е. – М.: Едиториал УРСС, 2003. – 280 с. (Синергетика: от прошлого к будущему).
6. Малинецкий, Г.Г. Нелинейная динамика и хаос. Основные понятия: Учебное пособие. / Г.Г. Малинецкий. - М.: КомКнига, 2006. – 240 с. (Синергетика: от прошлого к будущему).
7. Тарасевич, Ю.Ю. Математическое и компьютерное моделирование. Вводный курс: Учебное пособие. / Ю.Ю. Тарасевич. – М.: Эдиториал УРСС. 2004. 2004. – 152 с.
8. Милованов, В.П. Неравновесные социально-экономические системы: синергетика и самоорганизация. / В.П. Милованов. – М.: Эдиториал УРСС, 2001. – 264 с.
9. Колесников, А.А. Синергетические методы управления сложными системами: Теория системного синтеза. / А.А. Колесников. – М.: КомКнига, 2006. – 240 с.
10. Тимашев, С.Ф. Фликер-шумовая спектрскопия: информация в хаотических сигналах. / С.Ф. Тимашев. – М.: ФИЗМАТЛИТ, 2007. – 248 с.
11. Малинецкий, Г.Г. Математические основы синергетики. Хаос, структура, вычислительный експеримент. / Г.Г. Малинецкий. – М.: КомКнига, 2005. – 312 с. (Синергетика : от прошлого к будущему).
12. Шураков, В.В. Надежность программного обеспечения систем обработки данных: Учебник. / В.В. Шураков. – М.: Финансы и статистика, 1987. – 272 с.
13. Петренко, С.А. Вычисления с памятью критически важных информационных систем в условиях кибератак / С.А. Петренко, А.Г. Ломако, О.Н. Омелченкова, А.В. Зотова // Защита информации. INSIDE, – № 6, 2012. – с. 58-69.
14. Казарин, О.В. Методология обеспечения проактивной безопасности комп'ютерных систем / О.В. Казарин, В.Ю. Скиба // Защита информации. INSIDE, – № 2, 2013. – с. 52-60.
15. Эшби, У.Р. Введение в кибернетику / У. Р. Эшби; [Пер. с англ. Д.Г. Ламути. Под ред. В.А. Успенського]. – М.: Изд-во „Иностр. лит.", 1959. – 432 с.
16. Отчет «Лаборатории Касперского»: Java под ударом – эволюция эксплойтов в 2012-2013 гг. – 26 с. – Режим доступа: http://www.securelist.com/ru/analysis/208050816/Otchet_Laboratorii_Kasperskogo_Java_pod_udarom_evolyutsiya_eksploytov_v_2012_2013_gg.

17. Шампайн, Л.Ф. Решение обыкновенных дифференциальных уравнений с использованием МАТЛАБ: Учебное пособие / Л.Ф. Шампайн, И. Гладвел, С. Томпсон. Пер. с англ. – СПб.: Издательство «Лань», 2009. – 304 с. (Учебники для вузов. Специальная литература).
18. Кащенко, С.А. Релаксационные колебания в системе с запаздываниями, моделирующей задачу «хищник-жертва» / С.А. Кащенко // Моделирование и анализ информационных систем. Т.20, № 1 (2013). 52 – 98 с.

ДИНАМИКА КОЛИЧЕСТВА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

И.В. Кононович

Одесская национальная академия пищевых технологий
ул. Канатная, 112, г. Одесса, 650039, Украина; e-mail: kononovich@mail.ru

В статье рассматривается динамика инцидентов информационной безопасности инфокоммуникационных сетей, предложена гипотеза относительно ее колебательного характера и разработана модель «злоумышленник-защитник» на основе модели Лотки – Волтерра. Полученные результаты позволяют повысить эффективность работы систем информационной безопасности и формализовать направления дальнейших исследований по разработке новых эффективных систем информационной безопасности инфокоммуникаций с использованием методов нелинейной динамики.
Ключевые слова: информационная безопасность, инциденты, нелинейная динамика, компьютерное моделирование, информационно-коммуникационные сети

DYNAMICS OF THE NUMBER OF INFORMATION SECURITY INCIDENTS

Irina V. Kononovich

Odessa National Academy of Food Technologies
112, Kanatnaja str., Odessa, 650039, Ukraine; e-mail: kononovich@mail.ru

The dynamics of incidents of informative security of communication networks is examined in the article, a hypothesis is offered in relation to its oscillatory nature was proposed. The simulator «hacker-defender» on the basis of the model is Lotki –Volterra was developed. The obtained results allow to improve the efficiency of information security systems and formalize directions for further research to develop new effective information security systems of communication using the methods of nonlinear dynamics.
Keywords: information security, incidents, nonlinear dynamics, computer simulation, infocommunication networks