УДК 003.26:004.7(056.55):621.39(045)

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 4, pp. 339-346

МОДЕЛІ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІЗ ЗАПІЗНЮВАННЯМ РЕАГУВАННЯ НА ІНЦИДЕНТИ

І.В. Кононович[1], Д.А. Маєвський[2], Р.С. Подобний[2]

[1]Одеська національна академія харчових технологій
вул. Канатна, 112, Одеса, 65039, Україна; e-mail: kononovich@mail.ru
[2]Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: vl_kononovich@ukr.net

Розглядається проблема впливу запізнювання реагування на інциденти із захищеністю інформаційних ресурсів в системах кібербезпеки інформаційного простору. Визначено, що динамічні властивості взаємодіючих систем типу «порушення безпеки – підтримка безпеки» досліджена ще недостатньо. Відомі інструментарії аналізу й оцінки захищеності інформації та результати досліджень не дають можливості враховувати вплив запізнювання реагування на інциденти з кібербезпекою. На основі аналізу теорії й моделей запізнювання та аналізу динаміки систем захисту інформації розроблена методика дослідження впливу запізнювання в системах кібербезпеки. Порівнюються моделі із запізнюванням Хатчинсона, Лотки-Вольтерра та Аронсона. Методика та досліджені моделі дають можливість створювати більш гнучкі засоби виявлення, обробки та ліквідації наслідків інцидентів кібербезпеки та оцінювати рівень захищеності інформації на основі статистичних даних і на якісних оцінках, зроблених за допомогою нелінійних моделей із запізнюванням.

Ключові слова: захист інформації, інформаційна безпека, загрози, вразливість, атака, кібербезпека, ризики інформаційної безпеки, нелінійна динаміка, модель систем із запізнюванням

Вступ

Триваюче загострення критичної ситуації у сфері кібербезпеки високотехнологічних систем, критичних інформаційних ресурсів, інформаційного простору країни та кіберпростору вимагає вирішення багатьох наукових і технологічних проблем. Зростають різноманітність, складність і технологічність загроз та засобів впливу, збільшується кількість вразливостей елементів сучасного кіберпростору внаслідок його надзвичайної гнучкості. При цьому, існуючі засоби та заходи захисту не здатні в повному обсязі протидіяти наявній множині загроз. Згідно висловлювання Касперського настав час «важливості складних технологій (безпеки) в епоху складних атак» [1]. Тому загальною проблемою є вдосконалення та підвищення ефективності систем забезпечення інформаційної безпеки з урахуванням ризиків безпеки сучасного кіберпростору та високотехнологічних систем. Новою проблемою, яка стає темою досліджень, є використання в сфері кібербезпеки прогностичних можливостей нелінійної динаміки та синергетики, зокрема, врахування впливу запізнювання з прийняттям рішень та реагуванням на інциденти з кібербезпекою. Для побудови ефективних комплексних систем захисту інформації в інформаційно-комунікаційних системах необхідно проводити аналіз, моделювання та оцінку ризиків із врахуванням запізнювання реагування на порушення політики кібербезпеки.

Аналіз існуючих досліджень. Огляд теорії запізнювання стосовно систем синхронізації та інших галузей подано у [2]. Показано, що запізнювання у взаємодіях приводить до суттєвих змін і ускладненню динаміки ансамблю. Як найбільш типова

властивість таких систем відмічена «періодичність у залежності динамічних режимів системи від величини запізнювання». Періодичний характер залежності величини захищеності інформації у часі та залежності амплітуди захищеності від величини запізнювання реагування на інциденти з кібербезпекою прогнозовано у роботах з участю автора [3, 4]. Дана робота є продовженням і узагальненням цих робіт. Складні системи удосконалюються завдяки процесам інтеграції, конвергенції й уніфікації, які стимулюються застосуванням інформаційних технологій. Інтегральний підхід «до множини різних ризиків» безпеки обґрунтовується у [5]. Для дослідження динаміки захищеності інформаційних ресурсів почали використовувати моделі динамічних систем, які мають аналоги різної природи: фізичної, хімічної, біологічної, соціальної, економічної, інформаційної тощо. Застосовується математичний апарат, який став класичним для вивчення моделей розповсюдження інфекційних хвороб, біологічних та інших об'єктів [6]. Огляд сучасного стану аналітичних моделей розповсюдження червів та оцінки впливу запізнень заходів з протидії мережевим хробакам зроблено в [7]. Детальні математичні дослідження систем із запізнюванням, що моделюють задачу типу «хижак-жертва» на основі рівнянь Хатчинсона проведені у [8]. Однією з головних причин ризиків інформаційної безпеки є «людський фактор» і, зокрема, запізнювання в прийнятті нагальних рішень щодо застосування заходів і засобів захисту. Запізнювання виникає як технологічне, соціальне і психологічне явище. Нові покоління технологій непередбачено виявляються вразливими. Потрібен час для вироблення протидії. Необхідне відповідне навчання користувачів, фахівців та осіб, що приймають рішення. Запізнювання може виникати внаслідок звикання до технологій і недооцінки ризиків. Запізнювання прийняття рішень щодо захисту інформації стало одним із важливих проблем безпеки. Вплив запізнювання прийняття заходів захисту інформації на ризики інформаційної безпеки науковцями і практиками досліджено недостатньо. Існуючі оцінки захищеності інформації у переважній більшості базуються на статистичних підходах, орієнтуються на статичні моделі і слабо враховують динамічний характер взаємодій у кіберпросторі. Відомий інструментарій аналізу та оцінки ризиків не дає можливості враховувати вплив запізнювання у прийнятті рішень щодо заходів захисту інформації з урахуванням їх динаміки.

Метою роботи є розробка в рамках системного аналізу методів дослідження та аналіз впливу запізнювання у прийнятті рішень із захисту інформації на рівень захищеності інформаційних ресурсів за допомогою порівняння моделей із запізнюванням на основі рівняння Хатчинсона, моделі Лоткі-Вольтерра та системи рівнянь Аронсона і виділення найбільш типових властивостей, які характерні для систем із запізнюванням у зв'язках.

Системи із запізнюванням за характером взаємодії можна поділити на наступні класи. Системи із внутрішніми взаємодіями, які отримали назву систем із внутрішньовидовою конкуренцією за ресурси. Характерним прикладом таких систем є модель на основі рівняння Хатчинсона. Системи із природною (ймовірнісною) міжсистемною взаємодією, які називають міжвидовою конкуренцією. Реакції обох систем пропорційні дії противної сторони. Типовим прикладом таких систем є модель Лоткі-Вольтерра. Системи із коливальною регулярною міжсистемною взаємодією, так звані, системи із синхронізацією. Амплітудна динаміка таких систем вивчена Аронсоном на «взаємній синхронізації двох автогенераторів» [2]. На основі численних даних моделювання є підстави вважати, що в усіх випадках взаємодія системи «зловмисник – захисник» відбувається коливальним способом.

Внутрішньо-системні запізнювання. Рівняння Хатчинсона

Системи забезпечення інформаційної безпеки є системами із часовим запізнюванням. В них результат впливу або ліквідації цього впливу проявляється не

відразу, а через певний час τ – час запізнювання. Розглянемо вплив запізнювання з прийняття і виконання рішень щодо заходів захисту інформації на ризик інформаційної безпеки. У найпростіших випадках ризик пропорційний частоті вдалих атак, які привели до завдання шкоди. Тоді частота вдалих атак може бути мірою ризику інформаційної безпеки. «Рівнянням із запізнюванням прийнято називати рівняння відносно невідомої функції $x(t)$, що пов'язує швидкість зміни функції $x(t)$ з її значеннями в поточний момент часу t та з її значеннями в певний момент часу $t-\tau$, де постійна $\tau > 0$» [9]. Дослідимо вплив запізнювання з прийняття рішень щодо захисту інформації на частоту атак за допомогою простої моделі – рівняння Хатчинсона:

$$N'(t) = r(1-\frac{N(t-\tau)}{K})N(t), \tag{1}$$

де: τ – час запізнювання.

Найпростішим дискретним аналогом рівняння Хатчинсона є рівняння [10]:

$$N_{n+1} = r\left(1 - N_{n-\tau}/K\right)N_n \tag{2}$$

де $\tau \in \{0,1,2,...\}$, приймає дискретні значення

Якщо у (1) покласти $\tau = 0$, то рівняння Хатчинсона перетворюється у рівняння Ферхюльста [11]. Рівняння (1) і (2) мають просту інтерпретацію для систем забезпечення інформаційної безпеки. Маємо: динамічний процес у системі з обмеженим обсягом однорідних інформаційних ресурсів K, наприклад, у мережі є K однакових, вразливих до атак, типових комп'ютерів; t – час; n – величина дискретного відліку часу (модельний час). У системі відбувається боротьба за ресурси. Змінна N відображає поточне число реалізованих загроз. Параметр r – коефіцієнт росту кількості вдало реалізованих атак. Параметр r/K – коефіцієнт стримування росту кількості атак, або коефіцієнт внутрішньо-системної конкуренції. Він характеризує процес «опору середовища». Опір середовища пояснюється, по-перше, обмеженими доступними ресурсами, а, по-друге, тим, що кількість ресурсів (неуражених активів) поновлюється внаслідок впровадження засобів та заходів захисту, які, проте, можуть мати нові вразливості.

Оскільки потік реалізованих атак є дискретним потоком подій, то для аналізу моделі Хатчинсона доцільно вибрати відображення (2). Порядок проведення математичного експерименту наступний. Задаємо кількість інформаційних ресурсів – K. Для кожної пари параметрів r і τ знаходимо рівняння руху

$$N_{i+1}(r,\tau) = r\left(1 - N_{i-\tau}/K\right)N_i;\ i = [1,2,...,i_{\max}]. \tag{3}$$

Далі знаходимо функцію, яка описує поверхню:

$$M(r,\tau) = \max\left(N_{i+1}(r,\tau)\right). \tag{4}$$

Недолік моделі запізнювання у системі інформаційної безпеки на основі рівняння Хатчинсона полягає у тому, що коефіцієнт опору середовища не змінюється і не залежить від зовнішніх факторів. Коефіцієнт відновлених комп'ютерів не залежить від кількості атак. Такий недолік усувається у наступній моделі.

Запізнювання при стохастичній міжсистемній взаємодії. Модель Лоткі-Вольтерра

Цю модель інтерпретовано в термінах систем інформаційної безпеки і запропоновано автором для вивчення систем безпеки із запізнюванням у роботі [4]. Модель представлена у наступному вигляді. Введені позначення: x – кількість атак на комп'ютерну мережу, що виконуються зловмисниками, це аналог «жертв»; y –

кількість операцій, що виконуються захисниками комп'ютерної мережі, це аналог «хижаків». Середнє значення цих величин позначимо великими літерами, відповідно – X_c, Y_c. Динаміка чисельності взаємодіючих популяцій захисника $x(t)$ та хижака $y(t)$ моделюється системою рівнянь [8]:

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

де r_x та r_y – мальтузіанські коефіцієнти росту;

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

X_c та Y_c – середні кількості операцій-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.

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

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

Для спрощення моделі (5) при чисельному розрахунку зменшують кількість параметрів за допомогою заміни. Слідуючи [12; формули (3), (4)], робимо заміни: $t = h_x\tau$, $x(h_x\tau) = X\,N_1(\tau)$ $y(h_y\tau) = Y\,N_2(\tau)$, і далі, позначивши $\lambda_1 = r_x h_x$, $\lambda_2 = r_y h_y$, $h = h_y / h_x$, та знову перепозначивши τ через t, отримуємо

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

Звернемо увагу, що рівняння (7) можна вивести із рівняння Хатчинсона (1), при $K = 1$, у яке включаються додаткові члени $(\lambda_1 a N_2(t)N_1(t)), (\lambda_2\ N_1(t)N_2(t))$, щоб «описати пригнічуючі впливи, які чиняться кожним видом на свого конкурента» [13].

При проведенні математичного експерименту величину запізнювання дій хакера можна вважати незмінною і змінювати запізнювання дій «захисника». Можна зафіксувати також параметри активності хакера та тиску на нього: $\lambda_1 = const$; $a = const$. Для кожної пари параметрів λ_2 і h знаходимо рівняння руху $N_1(t, \lambda_2, h)$, вирішуючи систему рівнянь (7) чисельним способом; знаходимо функцію, яка описує поверхню

$$M(r, \tau) = \max\left(N_1(t, \lambda_2, h)\right). \tag{8}$$

Основні труднощі математичного експерименту полягають у знаходженні раціональних інтервалів зміни параметрів λ_2 і h та фіксації параметрів λ_1, a. Нас цікавлять випадки, коли можна попередити максимальні ризики інформаційної безпеки.

Запізнювання при регулярній міжсистемній взаємодії. Системи із синхронізацією

Аналізувати запізнювання у системі кібербезпеки з позицій синхронізації має сенс за таких причин. Моделювання показує, що інтенсивність атак та інтенсивність впливу

на порушення політики безпеки (реагування на інциденти з кібербезпекою) мають тенденцію до коливального характеру. Тому корисно визначити як параметри синхронізуючого коливального процесу протидії атакам впливають на коливальний процес самих атак і виробити відповідні заходи зменшення останніх. Вважається, що модель взаємодії із запізнюванням Аронсона є найбільш універсальною, на відміну від моделей Хатчинсона і Лоткі-Вольтерра. Як і раніше, нас цікавить опис процесів із амплітудною динамікою.

У [2] розглядається ансамбль із двох зв'язаних систем Ван-дер-Поля. Такий ансамбль описується наступною системою рівнянь для амплітуд і фаз:

$$\begin{cases} dr_1/dt = r_1\left(1 - k\gamma - r_1^2\right) + r_2\gamma\cos\varphi, \\ dr_2/dt = r_2\left(1 - k\gamma - r_2^2\right) + r_1\cos\varphi, \\ d\varphi/dt = \Delta + q_1 r_1^2 - q_2 r_2^2 - \left(r_1/r_2 + r_2/r_1\right)\sin\varphi. \end{cases} \quad (9)$$

Тут r_1 та r_2 – амплітуда коливань автогенераторів; відповідно – це кількість атак і кількість відновлених комп'ютерів;

$\varphi = \theta_1 - \theta_2$ – різниця фаз коливань;

y – сила зв'язку;

k – тип зв'язку (задамо $k = 1$);

Δ – параметр, що визначає частотне розлаштування між автогенераторами;

q_1 та q_2 – задають залежність частоти коливань від амплітуди у незв'язаних системах.

«Найбільш цікавим ефектом, який виявлено у системі (9), являється так зване вимирання коливань. Даний ефект полягає у тому, при зв'язуванні автогенераторів коливання в них припиняються і амплітуди r_i приймають нульові значення. З точки зору фазового простору, цей ефект відповідає стійкому в цілому стану рівноваги на початку координат» [2]. З точки зору кібербезпеки, такий ефект можна трактувати як існування умов, за яких активність порушників кібербезпеки можна звести до нульового значення. У [2] показано, що стан рівноваги може бути стійким лише за умови $|\Delta| > 2/k$.

«Простір параметрів системи (9) розбивається на три області з якісно різною поведінкою, ([2, рис. 3а]). За малих розлаштувань Δ та великих силах зв'язку y в системі спостерігається синхронізація, при якій автогенератори коливаються з постійною різницею фаз. За великих розлаштуваннях і слабких зв'язках динаміка системи являється асинхронною – різниця фаз автогенераторів необмежено зростає. У випадку великих розлаштувань та сильних зв'язках у системі відбувається вимирання коливань» [2].

Таким чином, ефект взаємодії із запізнюванням полягає у тому, що взаємодія між системами «часто приводить до якісної зміни динаміки системи в цілому [2]». Ритми взаємодії систем узгоджуються і налаштовуються одне до одного. Синхронізація нелінійних систем різної природи часто виявляється заснованою на якісно схожих між собою динамічних механізмах.

Результати математичних експериментів

Для прикладу і для виявлення типових властивостей моделей із запізнюванням розглянемо модель на основі рівняння Хатчинсона. Після аналізу нерухомих точок, досліджуємо рівняння руху. На серії рис. 5, а, б, в, г наведені рівняння руху, отримані за формулою (3) у залежності від коефіцієнту росту – r та величини запізнювання – τ. Маємо відповідно: а – швидко зменшувану кількість атак; б – виникнення затухаючих

коливань; в – регулярний коливальний процес; г – детермінований хаос. Далі досліджувався вплив на максимальну кількість реалізованих атак у залежності від коефіцієнту росту – r та величини запізнювання – τ (рис. 6.). На графіку відображені значення максимуму кількості реалізованих атак лише в області стійкості моделі. На рис. 7 наведено фактичні затримки T у залежності від коефіцієнту росту – r та величини запізнювання – τ. Фактична затримка оцінюється модельним часом від початку моделювання, до першого максимуму. Отримані результати носять не кількісний, а якісний характер. «Так, стало цілком ясно, що навряд чи можливий ефективний кількісний аналіз (навіть при використанні ЕОМ з їх колосальними можливостями) природної екосистеми навіть у «малому», без чого важко розраховувати на побудову яких-небудь більш або менш адекватних прогнозів щодо динаміки цих систем у «цілому»» [14, с. 8]. Кількісні оцінки можливі лише після уточнення моделей та доведення їх адекватності на основі широкого експериментального та статистичного матеріалу.

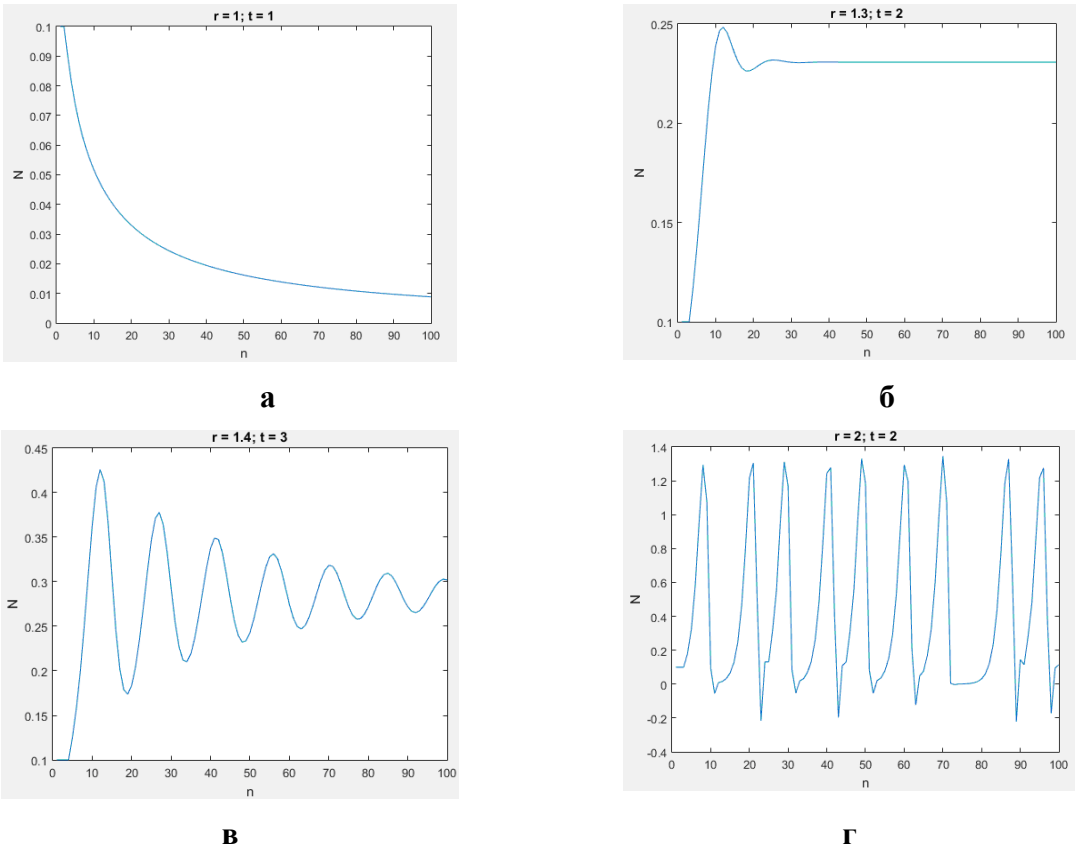

Рис. 5. Графіки рівняння руху в моделі Хатчинсона.

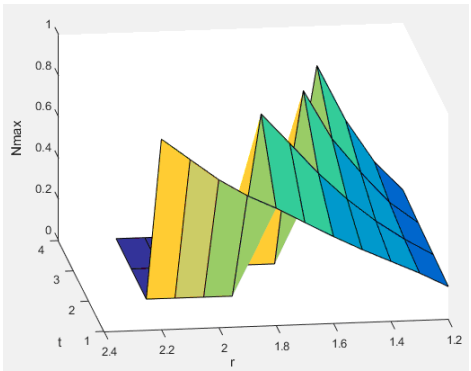

Рис. 6. Залежність максимальної кількості реалізованих атак від коефіцієнту росту – r та величини запізнювання – τ в моделі Хатчинсона

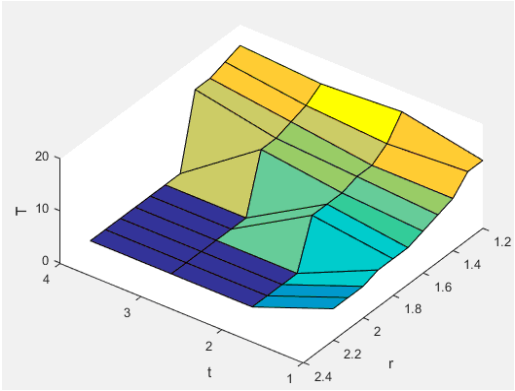

Рис. 7. Залежність фактичної затримки реагування від коефіцієнту росту – r та величини запізнювання – τ в моделі Хатчинсона

Висновки

В рамках системного аналізу розроблено методи дослідження та проведено якісний аналіз впливу запізнювання у прийнятті рішень із захисту інформації на рівень захищеності інформаційних ресурсів за допомогою порівняння моделей із запізнюванням на основі рівняння Хатчинсона, моделі Лоткі-Вольтерра та системи рівнянь, досліджених Аронсоном. Виділені найбільш типові властивості, які характерні для систем із запізнюванням у взаємозв'язках. Темою подальших досліджень може стати експериментальна та статистична перевірка адекватності моделей на реальних системах.

Список літератури

1. 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.
2. Клиньшов, В.В. Синхронизация автоколебательных сетей с запаздывающими связями / В.В. Клиньшов, В.И. Некоркин // УФН. СПб.:– 2013. – Т. 183. – № 12. – С. 1323 – 1336.
3. Кононович, В.Г. Вплив затримки прийняття заходів із захисту інформації на ризики інформаційної безпеки / В.Г. Кононович, І.В. Кононович, Ю.В. Копитін, С.В. Стайкуца // Безпека інформації. – Київ: НАУ, 2014. – Т. 20. – № 1. – С. 83 – 91.
4. Кононович, І.В. Динаміка кількості інцидентів інформаційної безпеки / І.В. Кононович // Інформатика та математичні методи в моделюванні. – Одеса, 2014. – Т. 3. – №3. – С. 35-43.
5. Управление риском / [Электронный ресурс] под ред. Г.Г. Малинецкого. – М.: РАН, 2000. – 249 с. – Режим доступа: http://risk.keldysh.ru/risk/risk.htm.
6. Захарченко, А.А. Черводинамика: причины и следствия / А.А. Захарченко // Защита информации. Конфидент. – 2004. – №2.– С. 50–55.
7. Котенко, И.В. Аналитические модели распространения сетевых червей / И.В. Котенко, В.В. Воронцов // Труды СПИИРАН. Вып. 4. – СПб.: Наука. 2007. – С. 208-224. – Режим доступа: http://www.proceedings.spiiras.nw.ru/data/src/2007/04/00/spyproc-2007-04-00-15.pdf.
8. Кащенко, С.А. Релаксионные колебания в системе с запаздываниями, моделирующей задачу «хищник–жертва» / С.А. Кащенко // Модели и анализ информационных систем. – 2013. – Т. 2. – № 1 (2013) – Ярославль.– С. 52-98.
9. Тарасевич, Ю.Ю. Избранные вопросы математического моделирования и численных методов. – Режим доступа: http://window.edu.ru/resource/936/38936/files/aspu03.pdf.
10. Гусаров, А.Н. Модель запаздывания действия антивирусов при распространении в сетях комп'ютерных угроз / А.Н. Гусаров, Д.О. Жуков // Известия ОрелГТУ. Серия «Информационные системы и технологии». – 2008. – № 1-2/269(544). – С. 67–72.
11. Долгий, Ю.Ф. Математические модели динамических систем с запаздыванием : учеб. пособие / Ю.Ф. Долгий, П.Г. Сурков. – Екатеринбург : Изд-во Урал, ун-та, 2012. – 122 с.

12. 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).
13. Дж. М. Смит. Модели в екологии / Дж. М. Смит. – М.: Мир, 1976. – 183 с.
14. Тутубалин, В.Н. Математическое моделирование в экологии: Историко-методологический анализ. Монография / В.Н. Тутубалин, Ю.М. Барабашева, А.А. Григорян и др. // – М.: Языки русской культуры, 1999. – 208 с.

МОДЕЛИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ С ЗАПАЗДЫВАНИЕМ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

И.В. Кононович[1], Д.А. Маевский[2], Р.С. Подобный[2]

[1]Одесская национальная академия пищевых технологий
ул. Канатная, 112, Одесса, 65039, Украина; e-mail: kononovich@mail.ru
[2]Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: vl_kononovich@ukr.net

Рассматривается проблема влияния запаздывания реагирования на инциденты с защищенностью информационных ресурсов в системах кибербезопасности информационного пространства. Известные инструментарии анализа и оценки защищенности информации и результаты исследований не дают возможности учитывать влияние запаздывания реагирования на инциденты с кибербезопасностью. На основе анализа теории и моделей запаздывания и анализа динамики систем защисты информации разработана методика исследования влияния запаздывания в системах кибербезопасности. Сравниваются модели с запаздыванием Хатчинсона, Лотки-Вольтерра и Аронсона. Методика и исследованные модели дают возможность оценивать уровень защищенности информации на основе статистических данных и качественных оценок, выполненных с помощью нелинейных моделей с запаздыванием.

Ключевые слова: защита информации, информационная безопасность, угрозы, уязвимость, атака, кибербезопасность, риски информационной безопасности, нелинейная динамика, модель систем с запаздыванием

MODELS OF SYSTEM OF THE CIBERSECURITY PROVIDING WITH DELAY OF REACTION ON INCIDENTS

I.V. Kononovich[1], D.A. Mayevskiy[2], R.S. Podobniy[2]

[1]Odessa national academy of food technologies
112, Rope Str, Odessa, 65039, Ukraine; e-mail: kononovich@mail.ru
[2]Odessa national polytechnic university,
1, Shevchenko Str, Odessa, 65044, Ukraine; e-mail: konrac1993@gmail.com

The problem of influencing of delay of reaction on incidents with protected of informative resources in the systems of cibersecurity informative space is examined. It is certain that dynamic properties of the interactive systems of type of security «breach is support of safety» is yet not enough explored. Known tools of analysis and estimation of protected of information and the results of researches do not enable to take into account influence of delay of reaction on incidents with cibersecurity. On the basis of analysis of theory and models of delay and analysis of dynamics of the systems of defence of information the developed method of research of delay in the systems of cibersecurity. Models with the Chatshinson, Aronson and Lotki-Volterra delay are compared. A method and explored models enable to create more flexible facilities of exposure, treatment and liquidation of consequences of incidents of cibersecurity and to estimate the level of protected of information on the basis of statistical information and on the high-quality estimations done by nonlinear models with the delay.

Keywords: information security, information security, threat, vulnerability, attack, cyber security, information security risks, nonlinear dynamics model systems with delay