УДК 003.26:004.7:053.072:519.876.5

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 2, pp. 116-126

МЕТОДИ ЗМЕНШЕННЯ ТУРБУЛЕНТНИХ ТА СИНГУЛЯРНИХ ЯВИЩ У МОДЕЛІ ДИНАМІКИ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ

І.В. Кононович

Одеська національна академія харчових технологій,
вул. Канатна, 112, Одеса, 65039, Україна; e-mail: kononovich@mail.ru

Розглядаються шляхи вирішення проблеми гіперболічного зростання кількості інцидентів кібербезпеки. Процес росту кількості інцидентів кібербезпеки представляється як перехідний процес, який описується математичною моделлю циклічної багатоетапної обробки інформаційних потоків із позитивними зворотними зв'язками. В моделі можуть виникати регулярні, квазіперіодичні коливання та динамічний хаос. У перехідний період можливі турбулентність та сингулярність. Запропоновано метод управління перехідним процесом, який підвищує стійкість системи, знижує ризик виникнення сингулярності та зменшують, у середньому вдвічі, викиди в зоні турбулентності. Як доповнення до математичної моделі, представлена логіко-лінгвістична модель процесів росту інцидентів. Пояснюються внутрішньо та зовнішньо системні причини недостатності застосовуваних сьогодні засобів забезпечення кібербезпеки. Для кардинального вирішення проблеми інцидентів інформаційної безпеки запропоновані позасистемні заходи, що забезпечують функціональну повноту засобів контролю доступів. Одним із засобів є технологія визначення ідентичності.

Ключові слова: кібернетична безпека, модель динамічної системи, турбулентність, сингулярність, біфуркації, управління безпекою, соціальна природа кібербезпеки

Вступ

Слідом за прискореним розвитком інфокомунікацій та інформаційних технологій швидко зростає кількість інцидентів кібербезпеки (КБ). Постає проблема моделювання таких явищ та пошук методів зупинки чи уповільнення росту інцидентів КБ.

Аналіз існуючих досліджень. Проблемі росту кількості і якості загроз, кількості інцидентів КБ присвячена величезний обсяг наукових і практичних робіт. Ці досягнення викладені, наприклад, в [1, 2]. Добре вивчені процеси розповсюдження і засоби боротьби з вірусами та іншими шкодоносними програмами [3, 4]. Для моделювання процесів боротьби з порушниками застосовані біологічні моделі [5, 6]. Статистика динаміки кількості інцидентів КБ видається регулярно, наприклад, [1, 7]. Але перехідні динамічні процеси досліджені недостатньо. Неясними залишаються питання, як зупинити гіперболічне зростання кількості інцидентів КБ, статистика яких залишається невтішною. Така ситуація схожа на аналогічну кризу інформаційних технологій внаслідок сингулярного переходу в процесі їх бурхливого розвитку [8]. Раніше автор приймав участь в обґрунтовуванні гіпотези щодо сингулярного характеру динаміки кількості інцидентів КБ. Представляє інтерес дослідження цієї динаміки окіл точок сингулярності. Стало ясно, що попередження сингулярних явищ не можливо без управління перехідними процесами.

В управлінні виробництвом, бізнесом, в державному управлінні, у військовій сфері, сфері кібернетичної безпеки широко застосовуються циклічні системи

управління. Такі циклічні управління реалізуються послідовністю мінімум із чотирьох етапів: планування, дії, перевірки, впливання. У стандарті ISO 9001:2008 рекомендується процесно-орієнтований підхід [9]. У військовій сфері будь-яку діяльність, із певною мірою наближення, представляють у вигляді типової кібернетичної моделі OODA, яка має такі її компоненти: Observe – спостерігай, Orient – орієнтуйся, Decide – вирішуй, Act – дій [10]. Подібні логігіко-лінгвістичні моделі застосовують у сфері інформаційної безпеки в системах виявлення кібератак [11]. Вказані моделі передбачають безперервне повторення циклу, який складається із чотирьох послідовних взаємодіючих процесів. На кожному витку такого циклу здійснюється взаємодія із зовнішнім середовищем, оцінка стану і ефективний вплив на нього. У той же час стала приділятись увага нелінійним моделям в соціально-економічній сфері та управлінні [12]. Проте, нелінійні фактори при циклічному управлінні також досліджені ще недостатньо. Особливо це стосується проблеми аналізу перехідних процесів і, стосовно КБ, ставить задачу управління деструктивними явищами у перехідний період.

Мета роботи. Спираючись на гіпотезу щодо сингулярного характеру динаміки кількості інцидентів КБ, на математичну і логіко-лінгвістичну модель, пояснити причини і фактори, що приводять до сингулярності та швидкого росту кількості інцидентів й виробити системні та позасистемні методи, засоби і механізми протидії росту кількості інцидентів КБ та запобіганню чи обходу сингулярностей.

Математична модель динаміки узагальненого циклічного інформаційного процесу

Забезпечення інформаційної безпеки, управління інформаційною безпекою, обробка та використання інформаційних потоків, розвиток інформаційних технологій являються інформаційними процесами. Створимо формальне описання певного узагальненого інформаційного процесу, який буде відображати основні характерні риси перелічених процесів. До типового представника узагальненого інформаційного процесу можна віднести процес, який реалізується організаційною структурою підготовки і реалізації інформаційного управління. «Управлінські рішення приймаються у різноманітних обставинах, включаючи кризові, і тим не менш вони повинні бути прийняті своєчасно, бути максимально обґрунтованими та забезпечувати найбільш повне і ефективне використовування наявних можливостей. … Основними складовими цього складного процесу являються: збирання та підготовка вхідних даних, побудова моделі розвитку ситуації, формулювання (прийняття) рішення керівником, конкретизація і деталізація рішення у плані реалізації інформаційного управління, доведення даного рішення до виконавців , а також організація, оперативне управління і контроль за його реалізацією [13]».

В сфері державного управління, де реалізуються сучасні світові стандарти інформаційної та організаційної культури, цикловий принцип управління отримав важливий розвиток. «На відміну від традиційних інформаційних служб, згадані фахівці виконують завдання якісно-змістовного перетворення інформації, функціонально поєднаного із науковою (виробництво нового знання) і управлінською (розробка варіантів рішень, сценаріїв) діяльністю. При цьому спостерігається організаційне відокремлення такої інформаційно-аналітичної діяльності від управлінської [14]». Виділений процес інформаційно-аналітичної діяльності, у свою чергу, складається з чотирьох кроків: виявлення вхідних вимог та даних; формування інформаційних ресурсів; витяг, придбання та генерація нових знань; доведення інформації, яка придатна для прийняття рішень щодо виконання конкретного завдання.

До характерних рис перелічених інформаційних процесів віднесемо мультиетапність процесів, циклічність процесів і наявність зворотних позитивних

зв'язків між сусідніми етапами обробки і використання інформації. Тоді динаміка цих процесів може бути описана єдиною математичною моделлю. Пропонується скористатись математичною моделлю циклічного управління КБ, у розробці якої автор приймав участь [15], яка формалізує дані моделі. Цикл перетворення даних в знання, рішення і управлінські дії можна представити як на рис. 1.

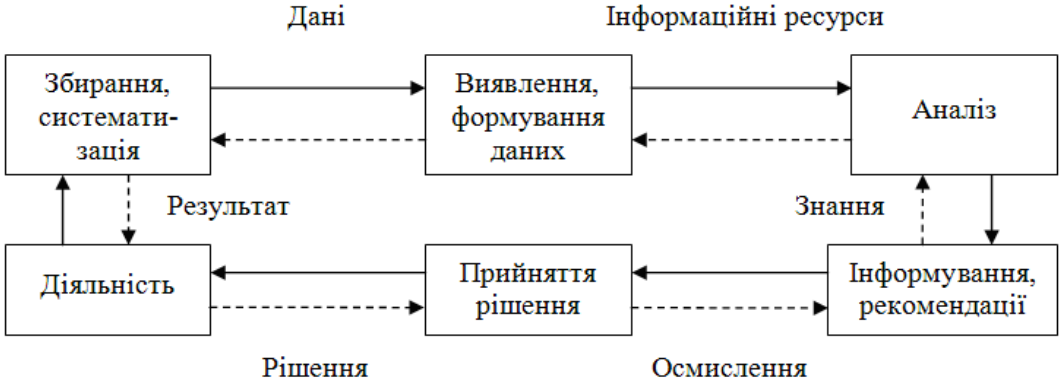

Рис. 1. Цикл перетворення даних у знання та рішення

Не всі цикли управління є чисто послідовними. Наприклад, у циклах Бойда є взаємодія несуміжних процесів циклу. При цьому ніде не враховується зворотний вплив суміжних процесів. Вдосконалення моделі полягає у тому, що в математичній моделі передбачається двостороння взаємодія між суміжними процесами. Генеровані процесом елементи інформації, знання чи рішення можуть повертатись до попереднього процесу для уточнення або доповнення. Ці «зворотні» взаємодії показані на рис. 1 пунктиром.

Математична модель циклічної системи управління пропонується у такому загальному вигляді наступного відображення.

$$\Phi(x,y,z,v,w)=\begin{cases} x_{n+1}=x_n-k_{xy}px_n^2+k_{yx}qy_n^2+x_{in} \\ y_{n+1}=y_n+k_{xy}px_n^2-\left(k_{yx}+k_{yz}\right)qy_n^2+k_{zy}rz_n^2 \\ \dots \\ w_{n+1}=w_n+k_{vw}sv_n^2-\left(k_{wv}+k_{out}\right)tw_n^2 \end{cases} \quad (1)$$

де x, y, …, w являються динамічними змінними; k_{ij}, p, q, r, s, ..., t є перехідні та, відповідно, розподільні коефіцієнти, які за Герегою мають чітке тлумачення у залежності від фізичної чи інформаційної природи системи; x_{in} – кількісна характеристика інформаційного вхідного потоку даних щодо середовища. При цьому, $\{k_{ij}\}$ и $\{p, q, r, s,..., t\} \in (0,1)$, $\{x, y, ..., w\} \in R$, $x_{in}= const \in R^+$.

У попередній роботі автора показано, що «наявність у системі двох груп коефіцієнтів (k_{ij} и p, q, r, s, ..., t) має конкретну фізичну інтерпретацію: коефіцієнти k_{ij} описують відносну величину редукції і консолідації інформації та задають долю інформаційного потоку, який переходить з одного етапу на сусідній. Частина інформаційного потоку повертається на попередній етап обробки для виправлення неточностей, врахування зауважень тощо. Коефіцієнти p, q, r, s ..., t описують розподіл елементів інформаційного потоку за їх видами. Перехід між етапами обробки визначається добутком коефіцієнтів обох груп [16]».

Аналіз моделі проводився при наступних умовах. На початку моделювання на всіх етапах обробки інформації руху нема і здійснюється включення вхідного потоку заданої інтенсивності. Для відображення рівнянь руху чисельно вирішувалась система рівнянь (1) при початкових умовах: x_0=0; y_0=0; ...; w_0=0. Приклад графіку рівнянь руху

у вигляді проекцій на площину 0_{yz} при певних значеннях коефіцієнтів системи рівнянь (1) [16], інтенсивності вхідного потоку x_{in} = 4,94 показано на рис. 2. Графік відтворює у часі значення змінної y_n другого рівняння системи (1).

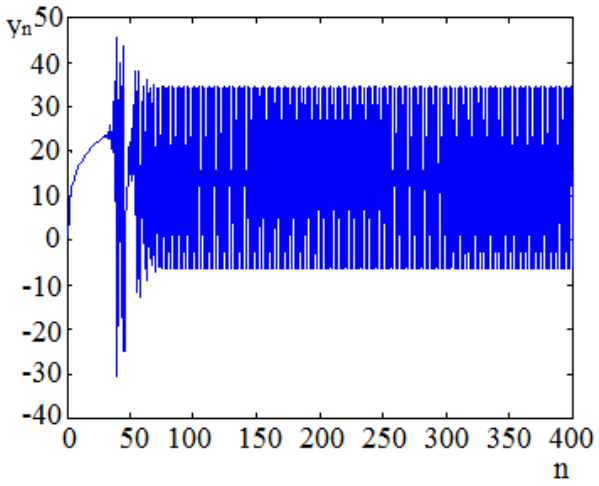

Рис. 2. Графік рівняння руху в проекції на площину 0_{xt}

На графіку виділяються три характерні ділянки: початкова, турбулентна і усталена (при заданих значеннях параметрів – квазіперіодична). Початкова ділянка відрізняється плавним зростанням величини інтенсивності потоку від нуля до максимального значення. Потік не може вирости миттєво і наростає плавно.

Турбулентна ділянка характеризується хаотичними коливаннями, викиди досягають великих значень і при збільшенні інтенсивності вхідного потоку прямують до нескінченності. Сингулярності у даній моделі, за певних параметрах виникають при $x_{in} > 4{,}94$. Причиною виникнення коливань і турбулентності являються зворотні зв'язки між етапами обробки інформації та перехідні процеси при включенні потоку. Наявність інерційних ефектів сприяє виникненню коливань.

Якщо сингулярність не досягається, то поступово хаотичні коливання затухають і замінюються стаціонарними квазіперіодичними коливаннями. В усталеній ділянці, в залежності від величин параметрів системи, відбуваються біфуркації подвоєння періоду Фейгенбаума. Періодичні коливання змінюються на квазіперіодичні, а потім – динамічним хаосом [17]. Коливання являються повздовжніми. З результатів моделювання витікає, що в стаціонарному режимі всі змінні коливаються з однаковою частотою і фазою, представляючи собою єдину хвилю. Турбулентну і стаціонарну ділянки наглядно видно на фазовому портреті системи у перехідному і стаціонарному режимах. На рис. 3 представлена проекція багатомірного фазового портрета на трьохмірний простір 0_{xyt}. Останнє дозволяє прослідкувати еволюцію траєкторії до атрактору.

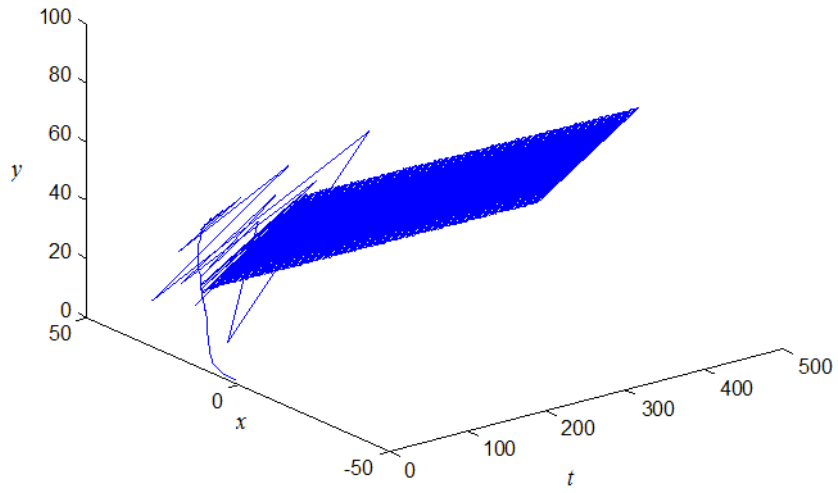

Рис. 3. Перехідний процес і атрактор системи (1)

У турбулентному режимі спостерігаються хаотичні траєкторії. У стаціонарному режимі маємо атрактор у вигляді тонкого сильно витягнутого еліпсоїдного тора.

Таким чином, турбулентність і сингулярність динамічних систем типу (1), для яких характерна наявність позитивних зворотних зв'язків, визначаються природними властивостями цих систем. Турбулентність виникає як при включенні вхідного інформаційного потоку, так і при його виключенні.

Тривіальний метод зменшення турбулентності у моделі динаміки узагальненого циклічного інформаційного процесу

Постає питання, чи можна у рамках даної моделі змінити якісний характер турбулентності або усунути саму турбулентність. Це можливо двома способами: за допомогою управління вхідним потоком у зоні перехідного процесу; та обмеженням інтенсивності вхідного потоку не досягаючи біфуркацій. Розглянемо перший спосіб.

У даному випадку ми доводимо саму можливість зменшення розмаху турбулентності у моделі динаміки циклічного інформаційного процесу. Задача полягає у тому, щоб безпечно провести систему через ділянку турбулентності, виключивши попадання траєкторії в окіл, де можливі сингулярності. Таку задачу можна вирішити синергетичними методами управління складними системами, що описані Колесниковим [18]. Проте у даній роботі розглянемо тривіальний метод. Із фізичних міркувань слідує, що причиною турбулентності може бути велика швидкість перехідного процесу у ті моменти, коли виникають умови для коливань. Моменти поблизу біфуркації являються такими умовами. По інерції траєкторії можуть вибігати на великі відхилення. Щоб зменшити ці явища, досить уповільнити перехідні процеси в районі біфуркацій. В моделі вхідний потік включається стрибком, що зумовлює велику початкову швидкість перехідного процесу. У найпростішому випадку розглянемо управління вхідним потоком за допомогою функції, вираженою у неперервній та дискретній формах:

$$U(t)=1-e^{-\lambda t}, t>0; U_n=1-e^{-\lambda n}, n>0, \qquad (2)$$

де λ – управляючий параметр.

Змінюючи управляючий параметр, можна регулювати швидкість за рахунок тривалості перехідного процесу. При цьому, перше рівняння системи (1) набуває такого вигляду

$$x_{n+1} = x_n - k_{xy} p x_n^2 + k_{yx} q y_n^2 + x_{in}\left(1 - e^{-\lambda n}\right), \qquad (3)$$

На рис. 4 показана часова діаграма змінної $y(t)$ при експоненціальному управлінні вхідним потоком згідно з виразом (3) і величиною $\lambda = 0{,}003$.

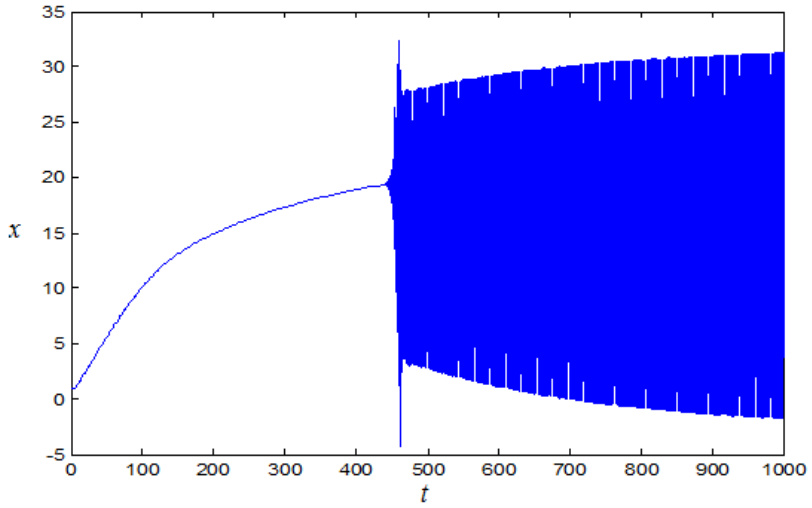

Рис. 4. Рівняння руху системи (1) при експоненціальному управлінні вхідним потоком

Управління вхідним потоком, як і управління параметрами системи (1) не змінює якісний характер турбулентності, який визначається властивостями системи (1), але дозволяє зменшити величину викидів та сингулярності. Сингулярність є природною властивістю такого роду систем. Внутрішньо системними засобами повністю позбутись сингулярності не можливо. До того ж, практична реалізація такого управління здається не здійсненною. Мова йдеться про управління «усталеним розвитком» інформаційних технологій (ІТ) шляхом уповільнення його початкової прискореної стадії, яка згідно із Законом Мура, ще не закінчилась. Уповільнення усталеного розвитку ІТ могло б дати можливість випереджаючого його розвиток засобів забезпечення кібербезпеки.

Тому є сенс звернутись до другого способу зменшення інтенсивності вхідного потоку позасистемними засобами. Позасистемні засоби мають впливати на параметри вхідного потоку утримуючи його в рамках до біфуркаційного (до турбулентного) режиму роботи системи (1).

Логіко-лінгвістична модель позасистемного впливу на динаміку узагальненого циклічного інформаційного процесу

Розглянемо логіко-лінгвістичну модель гіперболічного зростання кількості інцидентів КБ. Причинами гіперболічного зростання кількості інцидентів КБ на сучасному етапі являється зростання степені вразливості інформації та відповідних систем і ресурсів. Це пояснюється комплексом основних факторів. З одного боку, бурхливо розвиваються інформаційні технології, комунікаційні мережі, швидкими темпами зростають валові обсяги інформації в глобальних і місцевих інформаційних мережах, а також пропускна здатність інформаційно-комунікаційних мереж. Це різко розширює поле деструктивної діяльності. З іншого боку, «відбувається зосередження у єдиних базах даних великих обсягів інформації різного призначення, розвиток систем колективного користування, що приводить до розширення кола користувачів, які мають до обчислювальним ресурсам і даних, широке впровадження режимів розділення часу і реального часу, висока степінь автоматизації обміну інформації між ЕОТ [13]». Крім того, на зростання кількості інцидентів КБ впливають розвиток технологій кібератак,

недостатність ресурсів, що виділяються на КБ, легкість і малі витрати реалізації атак, не досконаліть задіяних засобів і заходів забезпечення КБ. Недостатність задіяних засобів і заходів забезпечення КБ мають внутрішньо та зовнішньо системні причини і фактори. До внутрішньо системних причин відносяться:

- поки що відсутні розробки превентивних методів забезпечення КБ, які мають протистояти всім загрозам, що виникли і що можуть виникнути у майбутньому;
- не розроблені операційні системи, що мали б високий стандартний рівень інформаційної захищеності;
- комунікаційні мережі залишаються не довіреною ланкою інформаційно-комунікаційних систем;
- є певне об'єктивне протиріччя між багатофункціональністю, масштабованістю, гнучкістю інформаційних систем та їх захищеністю. Засоби захисту знижують продуктивність систем, зменшують зручність їх використання. Є широкий діапазон у виборі величини витрат на захист: від захисту будь-якою ціною, навіть ціною людського життя; до оптимального відношення між витратами і можливим ризиком.

У череді не вирішуваних проблем КБ є такі:

- проблема керівника. Керівник відповідає за стан безпеки своєї організації, установи, підприємства. Але керівник організації не має права суміщати свою посаду із посадою керівника служби безпеки, Це часто порушується, особливо, у невеликих фірмах, організаціях, підприємствах;
- проблема системного адміністратора. Не можливо при розмежуванні прав доступу суттєво обмежити права доступу системного адміністратора до системи. Інакше він не зможе повністю відповідати за правильну роботу комп'ютерної системи. Необхідно удосконалювати підбір кадрів, мотивації і методи контролю;
- проблема головного криптографа. Цю проблему іноді формулюють так: «Головний криптограф ні за яких умов не повинен пересікати лінію фронту». У будь-якій системі захисту є частина ядра захисту чи персоналу, якому доводиться довіряти безумовно, не маючи можливості її абсолютного контролю. Звідси неможливість досягнення абсолютного захисту, абсолютної безпеки;
- соціально-психологічна проблема. Знаходячись на перехідному періоді переходу від індустріального суспільства до високотехнологічного суспільства ми маємо ситуацію відставання соціально-психологічного розвитку від високих темпів технологічного розвитку, а також посилення «цифрової нерівності». Члени суспільства з «індустріальною» психологією і менталітетом, опинившись у високотехнологічному інтелектуальному середовищі повільно адаптуються до його вимог і умов існування. Звідси походить девіантна, з точки зору нового суспільства, поведінка як мас, так і еліти. В результаті ті прошарки суспільства, з якого рекрутуються хакери та інші зловмисники, часто не усвідомлюють свої дії як злочинні;
- стратегічна проблема. Стратегії КБ і військові оборонні стратегії все більше стають схожими. На сьогодні сфера КБ, по її значимості для стану та розвитку людства і особливостях ситуації, що склалася у сучасному світі, в значній мірі можна віднести до військової сфери. Стратегія КБ базується на інтелекті та психології й пов'язана з усіма проблемами впливу одного розуму на інший. Сфера КБ вимагає застосування нешаблонних і ефективних управлінських рішень. В програми навчання менеджменту включається вивчення військової стратегії. Ймовірно, що у віддаленому майбутньому, буде комплементація політичних, ділових та етичних стандартів поведінки і ера інформаційних та корпоративних воєн відійде у минуле, тоді будуть створені умови для чесного законного застосування принципів і методик конкуренції та КБ;
- поки що має місце різне відношення до кіберзлокинців і кіберпорушників на територіях різних країн. З позицій місця, на яке направлена кібератака, кіберпорушник є злочинцем. З позицій місця, з якого кібератака здійснюється, кіберпорушник може

бути героєм. Інакше кажучи, поки відсутній єдиний міжнародний підхід до проблеми відповідальності за порушення КБ;

- нерозуміння керівництвом, користувачами і пересічним громадянинм важливості дотримання заходів КБ;
- не розвиненість правових і юридичних норм, невідповідність цих норм новим умовам функціонування постіндустріального високотехнологічного суспільства, та елементарна комп'ютерна неграмотність персоналу правоохоронних органів.

Мають також місце наступні тенденції розвитку сфери безпеки, які заслуговують підвищеної уваги. Це тенденції інтеграції та конвергенції різних видів безпеки в межах одного об'єкта: інформаційної, фізичної та економічної безпеки, охорони та відео спостереження; кібернетичної та національної безпеки й енергетичної та економічної безпеки. Переваги конвергенції та уніфікації практично доведені в багатьох сферах. Важливо вияснити умови, за яких можлива конвергенція в сфері безпеки.

«Наприклад, в сфері телекомунікації вона стала можлива за таких умов: цифровізація і наступна комп'ютеризація телекомунікаційних систем передачі сигналів різної природи (телеграфних, телефонних, телевізійних тощо); ієрархічна блочно-модульна архітектура систем на базі семирівневої моделі взаємодії систем, яка дозволила легко замінювати та удосконалювати будь-які модулі незалежно від інших; вирішальна умова, універсальний пакетний спосіб передачі і розподілу сигналів; винайдення функціонально повної системи функціональних елементів (функцій), із яких можна будувати функціональні схеми будь-якої складності [19]».

«У сфері безпеки друга та третя умови виконується легко. Перша умова набирає широти свого впровадження – розповсюджуються цифрові камери відео спостереження, роботизація у виробничій, енергетичній, побутовій сферах, інтелектуалізація управління, автоматичне розпізнавання образів та аналізу критичних ситуацій, тощо. Що стосується четвертої умови, тут ще потрібні теоретичні і практичні дослідження. Одна з ідей, яка може привести до замкнутої функціонально повної системи елементів безпеки, це впровадження техніки (технології) визначення ідентичності [19]».

Ще одна тенденція полягає в усвідомленні соціальної природи КБ. Є «взаємозалежність інформації та безпеки як стійкості та соціальної упорядкованості, безпеки суб'єкта в умовах наростання інтенсивності інформаційних потоків та особливостей соціальних практик забезпечення інформаційної безпеки; ролі кіберпростору у забезпеченні безпеки суб'єкта та аналізом основних груп загроз в Інтернеті [20]».

Сукупність розглянутих проблем та причин недостатності засовів забезпечення КБ дозволяє дійти до висновку, що на даному етапі суттєве значення мають позасистемні, зовнішні засоби забезпечення КБ. Враховуючи соціальну природу КБ, може бути ефективним розвиток соціальних аспектів теорії і технології КБ, підкріплений поглибленням інтеграції видів безпеки та організаційними й технічними заходами контролю за допомогою категорії й технологій визначення ідентичності.

Категорія технологій визначення ідентичності та управління визначенням ідентичності

Дана категорія ІБ введена Рекомендаціями МСЕ X.1250 – X.1279, Y.2720 – Y.2739 і пропонується автором для тотального впровадження в телекомунікаційних мережах України та кіберпросторі. Суть застосування технології викладена автором в [21].

«У мережному середовищі менеджмент визначення ідентичності (MBI – identify management) має забезпечувати можливості, які забезпечують гарантування безпечного обміну інформацією між об'єктами. Обмін інформацією засновується на розробленій

політиці та довірі, що встановлюється між цими об'єктами у середовищі з участю багатьох постачальників послуг. МВІ надає можливості захисту конфіденційності інформації об'єктів та забезпечує, щоб у телекомунікаціях розповсюджувалась лише авторизована інформація. Ідентичність – це інформація щодо об'єкта, якої досить для ідентифікації цього об'єкта у тому чи іншому контексті. Менеджмент визначенням ідентичності – МВІ – це набір функцій та можливостей (наприклад, адміністрування, управління та технічне обслуговування, виявлення, обмін повідомленнями, співставлення та ув'язування, забезпечення реалізації політики, автентифікація та затвердження), які використовуються для: гарантування інформації, що підтверджує ідентичність (наприклад, ідентифікаторів, реєстраційних даних, атрибутів); гарантування ідентичності об'єкта; забезпечення комерційних застосувань та застосувань безпеки [21]».

Багато сучасних інформаційних послуг, таких як електронна торгівля, електронній уряд, вимагають від телекомунікаційного середовища посиленої спостережності. Необхідне забезпечення визначення ідентичності всіх об'єктів та їх інформаційних потоків, на всіх рівнях та на всіх компонентах телекомунікаційної мережі при максимальному сприянні вільному, але контрольованому обертанні інформації. Поряд з іншими механізмами захисту, міжмережними екранами, системами виявлення вторгнень, захистом від вірусів, МВІ відіграє важливу роль у захисті інфраструктури, послуг та застосування телекомунікацій від кіберзлочинності, таких як шахрайство та крадіжка даних ідентичності. Трансакції у телекомунікаціях будуть захищеними та надійними.

Корисним ефектом визначення ідентичності є те, що вона частково відтворює властивості безпосередніх контактів між людьми. Люди безпосередньо сприймають (за допомогою усіх органів почуттів) один одного і мають можливість пізнавати фізичні, психологічні та індивідуальні особливості, притаманні кожній стороні. Співрозмовники у процесі контактів мають змогу скласти більш-менш об'єктивне враження про те, що становить собою партнер по спілкуванню, проникнути в його внутрішній світ, зрозуміти мотиви поведінки, звички, оцінити ставлення до фактів дійсності. Бажано, щоб телекомунікації надавали хоча б частину цих можливостей.

З теоретичної точки зору, технологія визначення ідентичності є елементом функціонально повного набору технологій КБ. У сфері КБ принцип функціональної повноти повинен поєднуватись із принципом безперервності захисту (принципом «кругової оборони»). Захищеність об'єкта визначається рівнем захищеності найслабшої ланки. Системи контролю доступу, як правило, є лише на вході у систему, або при доступах до ресурсу і не контролюють подальші дії суб'єкта. Технологія визначення ідентичності застосовується для кожної транзакції, замикаючи функціональну повноту технологій захисту. А у розподілених системах КБ технологія визначення ідентичності є не замінимою. Універсальна техніка визначення ідентичності значно полегшує вирішення проблем КБ. У повсякденному житті є стійка тенденція до зменшення анонімності. Повсюдно встановлюється камери спостереження, вживлюються чіпи для автоматичної ідентифікації тощо. Заборона анонімності не означає обмеження нашої свободи. Ми діємо там, де нам потрібно та дозволено і робимо те законне, що є нашим інтересом. Але робимо це відкрито, так як це роблять інші люди.

Висновки

Проведене математичного моделювання перехідних процесів забезпечення КБ показало, що в них можуть виникати стаціонарні квазіперіодичні коливання, біфуркації, а в перехідний період можливі турбулентність і сингулярність. Запропоновано метод управління перехідним процесом, який підвищує стійкість інформаційної системи, знижує ризик впливу сингулярностей і в середньому вдвічі

знижує величину викидів у зоні турбулентності. Отримано висновок, щодо необхідності застосування позасистемних заходів захисту. Логіко-лінгвістична модель перехідних процесів забезпечення КБ дала можливість виробити позасистемні засоби захисту шляхом застосування технік і технологій, які замикають систему захисту до функціонально повної. Доведена ефективність категорії і технології визначення ідентичності. Напрямок подальшої роботи полягає у виконанні повної програми досліджень нелінійних турбулентних властивостей системи забезпечення КБ.

Список літератури

1. Бурячок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В.Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С. В. Толюпа за заг. ред. д-ра техн. наук, професора В.Б. Толубка. – К.: ДУТ, 2015. – 288 с.
2. Обзор кибербезопасности / Рекомендация МСЭ-Т X.1205 // Безопасность электросвязи. – Женева: 2008. – 56 с.
3. Котенко, И.В. Аналитические модели распространения сетевых червей / И.В. Котенко, В.В. Воронцов // Труды СПИИРАН. Вып. 4. – СПб.: Наука. – 2007. – С. 208-224.
4. Захарченко, А.А. Черводинамика: причины и следствия / А.А. Захарченко // Защита информации. Конфидент. – 2004. – № 2. – С. 50–55.
5. Кононович, І. В. Динаміка кількості інцидентів інформаційної безпеки / І. В. Кононович // Інформатика та математичні методи в моделюванні. – 2014. – Т. 3. – № 3. – С. 35-43.
6. 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. – Том 20, № 1. – С. 83 - 91.
7. The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world. – November 2011. – 43 p.
8. Кононович, І. В. Інформаційні революції. Ієрархічна класифікація інформації / І.В. Кононович // Цифрові технології: Збірник / Кол. Авт: – Вип. 8. Одес. нац. академія зв'язку. – Одеса, 2010. – С. 88 - 96.
9. ДСТУ ISO 9001:2009 Системи менеджменту якості. Вимоги [Аналог ISO 9001:2008]. – 32 с.
10. Ивлев, А.А. Основы теории Джона Бойда. Принципы, применение и реализация / А.А. Ивлев [Электронный ресурс]. – 2009. – 21 с. Режим доступа: http://www.milresource.ru/Boyd.html.
11. Кононович, В.Г. Технічна експлуатація систем захисту інформації. Частина 4 – Інформаційна безпека комунікаційних мереж та. Реагування на атаки: навч. посібник / В.Г. Кононович, С.В. Гладиш; За ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2009. – 208 с.
12. Милованов, В.П. Неравновесные социально-экономические системы: синергетика и самоорганизация // В.П. Милованов. – М.: Эдиториал УРСС, 2001. – 264 с.
13. Кузнецов, Н.А. Информационная безопасность системы организационного управления. Теоретические основы : в 2 т. / Н.А. Кузнецов, В.В. Кульба, Е.А. Микрин и др.; [отв. ред. Н.А. Кузнецов, В.В. Кульба] ; Ин-т проблем передачи информ. РАН. – М.: Наука, 2006. – Т.1 – 495 с.
14. Бондаренко, М.Ф. Підготовка професіоналів у галузі інформації для державної служби України / М.Ф. Бондаренко, С.І. Маторін, К.А. Соловйова // Навчання державних службовців [Електронний ресурс]. – 7 с. Режим доступу: http://nadoest.com/navchannya-derjavnih-slujbovciv-m-bondarenko.
15. Кононович, В.Г. Нелінійні моделі циклічного управління кібербезпекою / В.Г. Кононович, І.В. Кононович, А.І. Міхова // «ІНФОРМАЦІЙНІ УПРАВЛЯЮЧІ СИСТЕМИ ТА ТЕХНОЛОГІЇ» (ІУСТ – ОДЕСА – 2015) [Електронний ресурс]. Матеріали Міжнародної науково-практичної конференції, 22 – 24 вересня 2015 р., Одеса / відп. ред. В.В. Вичужанін. –, 2015. (– 336 .с). – С. 171 – 173.
16. Герега, О.М. Гіпотеза і формальна модель сингулярної динаміки інцидентів кібернетичної безпеки / О.М. Герега, С.О. Гнатюк, В.Г. Кононович, І.В Кононович // Інформатика та математичні методи в моделюванні. – Одеса, 2016. – Т. 6. – № 1. – С. 35-43.
17. Табор, М. Хаос и интегрируемость в нелинейных системах / М. Табор // М.: Эдиториал УРСС. – 2001. – 320 с.
18. Колесников, А.А. Синергетического управления сложными системами: Теория системного синтеза / А.А. Колесников. – М.: КомКнига, 2006. – 240 с.

19. Кононович, В.Г. Метастратегія інформації та управління захистом інформації / В.Г. Кононович // Перспективні напрями захисту інформації : матеріали першої всеукраїнської наук.-пр. конф. м. Одеса 7 – 9 вересня 2015 р. – Одеса: ОНАЗ, 2015. – С. 49-53.
20. Владимирова, Т.В. Социальная природа информационной безопасности [Текст] : монография / Т.В. Владимирова // АНО содействия развитию соврем. отечеств. науки. Изд. Дом «Науч. обозрение». – 2014. – 239 с.
21. Кононович, В.Г. Визначення ідентичності об'єктів у системі соціальної та інформаційної безпеки / В. Г. Кононович, І. В. Кононович, С.В. Стайкуца, О.О. Цвілій // Сучасний захист інформації. – 2015. – № 1. – С. 19-27.

МЕТОДЫ УМЕНЬШЕНИЯ ТУРБУЛЕНТНЫХ И СИНГУЛЯРНЫХ ЯВЛЕНИЙ В МОДЕЛИ ДИНАМИКИ ИНЦИДЕНТОВ КИБЕРБЕЗОПАСНОСТИ

И.В. Кононович

Одесская национальная академия пищевых технологий,
ул. Канатная, 112, м. Одесса, 65039, Украина; e-mail: kononovich@mail.ru

Рассматриваются пути решения проблемы гиперболичного роста количества инцидентов кибербезопасности. Процесс роста количества инцидентов кибербезопасности представлен в виде переходного процесса, который описывается математической моделью циклической многоэтапной обработки информационных потоков с положительными обратными связями. В модели могут возникать регулярные, квазипериодические колебания и динамический хаос. В переходный период возможны турбулентность и сингулярность. Предложен метод управления переходным процессом, который повышает стойкость системы, снижает риск возникновения сингулярности и уменьшает, в среднем вдвое, выбросы в зоне турбулентности. Как дополнение к математической модели, представлена логико-лингвистическая модель процессов роста количества инцидентов. Поясняются внутренне внешне системные причины недостаточности использованных сегодня средств обеспечения кибербезопасности. Для кардинального решения проблемы инцидентов кибербезопасности предложены внесистемные меры, которые обеспечивают функциональную полноту средств контроля доступов. Одним из таких средств является технология определения идентичности.
Ключевые слова: кибернетическая безопасность, модель динамической системы, турбулентность, сингулярность, управление безопасностью, социальная природа кибербезопасности.

METHOD TO REDUCE TURBULENCE AND SINGULAR EFFECTS IN DYNAMICS MODELS INCIDENTS CIBERSECURITY

I.V. Kononovich

Odessa National Academy of Food Technologies,
112, Kanatnaja str, Odessa, 65039, Ukraine; e-mail: kononovich@mail.ru

Discusses ways solving the problem of hyperbolic growth in the number of incidents of cybersecurity. The process of growth in the number of incidents of cyber security presented in the form of the transition process, which is described by a mathematical model of a multi-stage cyclic processing of information flows from the positive feedback. In the model, there may be regular, quasi-periodic oscillations and dynamic chaos. During the transition period may be turbulence and singularity. A method for management transition process, which increases the stability of the system, reduces the risk of singularity and reduces, on average twice the emissions in the zone of turbulence. As an addition to the mathematical model presented logical-linguistic model of growth the number of incidents. Describes the internal and external system causes of insufficiency of cybersecurity tools. For a radical solution to the problem of cybersecurity incidents out of system proposed measures, which provide functional completeness access controls. One such tool is the technology determining the identity.
Keywords: cyber security model dynamic systems, turbulence, singularity, bifurcation, safety management, social nature of cybersecurity.