УДК 004.056 DOI:10.31673/2412-4338.2021.023543

Гребенніков А.Б., Шуклін Г.В. *Державний університет телекомунікацій, Київ*

АНАЛІЗ СТІЙКОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПРИЙНЯТТІ УПРАВЛІНСЬКИХ РІШЕНЬ НА ПІДПРИЄМСТВІ В УМОВАХ ДЕСТАБІЛІЗУЮЧОГО ІНФОРМАЦІЙНОГО ВПЛИВУ

Анотація. *В статті проведено моделювання системи захисту інформації при прийнятті управлінських рішень на підприємстві в умовах дестабілізуючих інформаційних впливів. В основі моделювання розглядається модель ФітцХью-Нагумо, яка моделює релаксаційні коливання та спайкові послідовності в неавтономній моделі нейронної збудженості. Метою дослідження є побудова математичної моделі системи захисту інформації при прийнятті управлінських рішень на підприємстві в умовах дестабілізуючих інформаційних впливів і за допомогою якої здійснити якісний аналіз станів системи захисту інформації. На основі проведених в роботі досліджень було побудовано математичну модель системи захисту інформації при прийнятті управлінських рішень на підприємстві в умовах дестабілізуючих інформаційних впливів, яка дає можливість виявляти точки біфуркації, які визначають як стійкі стани системи захисту так і не стійкі, які характеризують уразливість системи захисту інформації при прийнятті управлінських рішень на підприємстві. Встановлено, що відгук на дестабілізуючий інформаційний вплив на прийняття управлінських рішень на підприємстві характеризується довірою посадової особи. Завдяки встановленому взаємозв'язку між інтенсивністю впливу і довірою, вдалося побудувати математичну модель системи захисту інформації при прийнятті управлінських рішень на підприємстві, що дає можливість здійснювати якісний аналіз системи захисту інформації на основі точок біфуркацій, які характеризують стійкі та нестійкі стани системи захисту. Отримані аналітичні залежності обчислення точок біфуркацій, які залежать від параметрів, які характеризують захист конфіденційної інформації, цілісність інформації та умови неможливості блокування доступу до інформації. Дана модель дає можливість здійснювати якісний аналіз системи інформаційного захисту на підприємстві, що в свою чергу дає можливість виявляти вразливі місця системи інформаційного захисту на підприємстві в цілому.*

Ключові слова: *точки біфуркації, довіра, релаксаційні коливання, впливові імпульси, управлінські рішення.*

Hrebennikov A.B, Shuklin G. V. *State University of Telecommunications, Kyiv*

ANALYSIS OF STABILITY OF SYSTEM OF DEFENCE OF INFORMATION AT ACCEPTANCE OF ADMINISTRATIVE DECISIONS ON ENTERPRISE IN THE CONDITIONS OF DESTABILIZING INFORMATIVE INFLUENCE

Abstract. *In the article the design of the system of defence of information is conducted at the acceptance of administrative decisions on an enterprise in the conditions of destabilizing informative influences. In basis a design is examined model of FitzHue-Nagumo, that designs relaxation vibrations and to the spike of sequence in the non-autonomous model of neuron excited.The aim of the study is construction of mathematical model of the system of defence of information at the acceptance of administrative decisions on an enterprise in the conditions of destabilizing informative influences and by means of that to carry out the quality analysis of the states of the system of defence of information. On the basis of studies undertaken an in-process the mathematical model of the system of defence of information was built at the acceptance of administrative decisions on an enterprise in the conditions of destabilizing informative influences, that gives an opportunity to find out the points of bifurcation, that determine as the proof states of the system of defence are so not proof that characterize vulnerability of the system of defence of information at the acceptance of administrative decisions on an enterprise. It is set that a review on destabilizing informative influence on the acceptance of administrative decisions on an enterprise is characterized the trust of public servant. Due to the set*

intercommunication between intensity of influence and trust, it was succeeded to build the mathematical model of the system of defence of information at the acceptance of administrative decisions on an enterprise, that gives an opportunity to carry out the quality analysis of the system of defence of information on the basis of points of bifurcations, that characterize the proof and unsteady states of the system of defence. Got analytical dependences of calculation of points of bifurcations, that depend on parameters that characterize defence of confidential information, integrity of information and condition of impossibility of blocking of access to information.

Keywords: *bifurcation, relaxation vibration, informative influences, trust, influential impulses, managerial decisions.*

Гребенников А.Б., Шуклин Г.В. *Государственный университет телекоммуникаций, Киев*

АНАЛИЗ УСТОЙЧИВОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПРИНЯТИИ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ НА ПРЕДПРИЯТИИ В УСЛОВИЯХ ДЕСТАБИЛИЗИРУЮЩЕГО ИНФОРМАЦИОННОГО ВЛИЯНИЯ

Аннотация. *В статье проведено моделирование системы защиты информации при принятии управленческих решений на предприятии в условиях дестабилизирующих информационных влияний. В основе моделирования рассматривается модель ФитцХью-Нагумо, которая моделирует релаксационные колебания и спайковые последовательности в неавтономной модели нейронной возбудимости. Целью исследования является построение математической модели системы защиты информации при принятии управленческих решений на предприятии в условиях дестабилизирующих информационных влияний и с помощью которой осуществить качественный анализ состояний системы защиты информации. На основе проведенных в работе исследований была построена математическая модель системы защиты информации при принятии управленческих решений на предприятии в условиях дестабилизирующих информационных влияний, которая даёт возможность выявлять точки бифуркации, которые определяют как устойчивые состояния системы защиты так и не устойчивые, которые характеризуют уязвимость системы защиты информации при принятии управленческих решений на предприятии. Установлено, что отклик на дестабилизирующее информационное влияние на принятие управленческих решений на предприятии характеризуется доверием должностного лица. Благодаря установленной взаимосвязи между интенсивностью влияния и доверием, удалось построить математическую модель системы защиты информации при принятии управленческих решений на предприятии, что даёт возможность осуществлять качественный анализ системы защиты информации на основе точек бифуркаций, которые характеризуют устойчивые и не устойчивые состояния системы защиты. Получены аналитические зависимости определения точек бифуркаций, которые зависят от параметров, которые характеризуют защиту конфиденциальной информации, целостность информации и условия невозможности блокирования доступа к информации.*

Ключевые слова: *точки бифуркации, доверие, релаксационные колебания, информационное влияние, время запаздывания, влияющие импульсы, управленческое решение.*

Вступ

При дослідженні стійкості системи захисту інформації при прийнятті управлінських рішень одним з основних показників є відгук (довіра) особи, яка приймає управлінські рішення (посадова особа) на зовнішній дестабілізуючий інформативний вплив (ЗДІВ). Основною задачею даних досліджень є реакція посадової особи в прийняті управлінських рішень в залежності від параметрів, які характеризують довіру. Крім того, цікавим є дослідження умов, при яких виникає миттєва довіра на ЗДІВ у вигляді послідовності коротких дій при прийнятті управлінських рішень. При цьому припускається, що довіра протягом деякого проміжку часу є постійною. Сама довіра, як показник, який характеризує захист

конфіденційної інформації, якою володіє посадова особа, характеризується коливальними процесами, так як в залежності від інформації, яка надходить зовні, потребує ретельного аналізу. В таких умовах задача виникнення таких коливань довіри зводиться до дослідження біфуркацій, які визначають втрату стійкості системи захисту інформації при прийнятті управлінських рішень. При проведенні ряду досліджень, було підмічено, що довіра повільно змінюється з часом. В цьому випадку для розуміння виникнення коротких дій при прийнятті управлінських рішень необхідно залучити теорію динамічних біфуркацій, тобто біфуркацій, які виникають при повільній зміні довіри.

В даній роботі застосовується модель ФітцХью-Нагумо з нелінійним відновленням, яка моделює релаксаційні коливання та спайкові послідовності в неавтономній моделі нейронної збудженості [1]. В моделюванні системи захисту інформації при прийнятті управлінських рішень на підприємстві при умові, що довіра повільно зростає з часом за лінійним законом дана модель достатньо точно відображає якісний аналіз системи захисту інформації. В цій моделі вводиться функція керування системою захисту інформації при прийнятті управлінських рішень, за допомогою якої відбувається стабілізація системи захисту інформації при спробі вивести її з під контролю (стану рівноваги) в прийнятті управлінських рішень.

Постановка проблеми. Для забезпечення системи захисту інформації при прийнятті управлінських рішень на підприємстві необхідно в першу чергу визначити час, протягом якого в період отримання інформації посадовою особою зі збоку ЗДІВ, відбуваються послідовні короткі дії, які в подальшому будуть основою для прийняття остаточних управлінських рішень, що в свою чергу забезпечить напрям розвитку підприємства. Отже, при врахуванні локальних властивостей системи інформаційного захисту при прийнятті управлінських рішень на підприємстві, необхідно враховувати нелокальні коливання, які виникають за рахунок ЗДІВ, що характеризуються динамікою швидких параметрів.

Аналіз останніх досліджень і публікацій.

В роботах [2,3] здійснено моделювання процесу розповсюдження інформаційної загрози за допомогою диференціальних рівнянь відкритого типу в припущенні наявності зовнішнього інформаційного каналу та внутрішнього. Аналізуються інтегральна та миттєва ефективності витрат на розповсюдження інформаційної загрози. Однак в роботах запропоновані математичні моделі не дають змогу здійснити якісний аналіз системи інформаційного захисту при прийнятті управлінських рішень. В роботі [4] представлено графічно імітація ознак, які дають максимальний внесок в розпізнавання хибної інформації. Дане графічне представлення уявляє собою релаксаційні коливання процесів приховування інформації, нав`язування інформації, та природної суперечності. Однак в роботі не здійснено математичного моделювання даної імітації та не представлені якісні (фазові) портрети даної динаміки. В роботі [5] представлені технологічні аспекти інформаційного протиборства на сучасному етапі, які складаються з трьох складових: складова, в якій формулюються цілі та задачі, складова, яка уявляє етап планування, та складова етапу реалізації. Також представлена життєздатна модель інформаційного протиборства, а також проаналізована інформаційна атака Джонсона. Дане представлення є підґрунтям для математичного моделювання інформаційно-аналітичних впливів, що в подальшому дає можливість проведення якісного аналізу в аспекті інформаційного протиборства. В роботі [6] сформульовані рекомендації, яких необхідно дотримуватись, щоб забезпечити мінімум впливу соціального фактору на інформаційну безпеку підприємства. Було здійснено аналіз стійкості до впливу соціальних чинників, але запропонований математичний апарат не дає можливість дати якісну оцінку цьому. В роботі [7] представлено схему взаємодії процесу керування інформаційною безпекою з іншими процесами керування підприємством. Дана схема дає можливість в подальшому

створювати математичні моделі керування захистом інформації при прийнятті управлінських рішень на підприємстві та виявляти слабкі місця системи інформаційного захисту підприємства. В роботі [8] запропоновано підхід щодо оцінки ентропії системи забезпечення інформаційної безпеки підприємства. Однак, розрахунок ентропії в складних системах має враховувати не тільки потік та виробництво ентропії, а і ймовірність успішної реалізації зняття конфіденційної інформації в умовах дестабілізуючого інформаційного впливу. В роботі [9] проаналізовано технологію інформаційно-психологічного впливу, яка здійснюється за допомогою розповсюдження спеціальних мемів. Дана структурна модель мема, але не здійснено математичного моделювання даного динамічного процесу. В роботі [10] представлено методику формування комплексного підходу для забезпечення інформаційної безпеки кредитно-фінансової сфери. Здійснено математичне моделювання рівня комплексної безпеки об`єктів інформатизації кредитно-фінансової сфери з використанням теорії ймовірності з метою отримання функціональної залежності для знаходження чисельного значення коефіцієнта уразливості, який характеризує комплексну безпеку об`єкту кредитно-фінансової сфери. Даний підхід можна застосовувати при визначенні параметрів, які характеризують систему інформаційного захисту при прийнятті управлінських рішень на підприємстві. Однак, недоліком даного підходу є те, що ймовірності, які визначають появу загрози не визначаються оперативно, а задаються на основі минулих спостережень. В роботі [11] запропоновано модель інтегрованої системи менеджменту інформаційної безпеки підприємства, яка враховує динамічну природу зміни показника ефективності. Однак математичне представлення даної моделі не дає можливість здійснити якісний аналіз забезпечення системи інформаційного захисту підприємства при прийнятті управлінських рішень.

Метою статті є побудова математичної моделі системи захисту інформації при прийнятті управлінських рішень на підприємстві в умовах дестабілізуючих інформаційних впливів і за допомогою якої здійснити якісний аналіз станів системи захисту інформації.

Основна частина.

Модель ФітцХью-Нагумо з нелінійним відновленням уявляє собою наступну систему рівнянь

$$\begin{cases} \dfrac{dx}{dt} = f(x) - u + \Xi(t) \\ \dfrac{du}{dt} = \varepsilon\big(g(x) - u\big) \end{cases}, \qquad (1)$$

де $f(x) = x - \dfrac{1}{3}x^3$ і $\begin{cases} g(x) = kx, & x \le 0, k \in [0;1] \\ g(x) = \lambda x, & x > 0, \quad \lambda \in [0;1] \end{cases}$. Параметри k, λ - параметри, які задають нелінійне відновлення. Параметр k уявляє собою ймовірність того, що відбудеться успішне зняття конфіденційної інформації за рахунок дестабілізуючого інформаційного впливу. Параметр λ уявляє собою ймовірність того, що відбудеться пошкодження конфіденційної інформації за рахунок дестабілізуючого інформаційного впливу Змінна x описує динаміку дестабілізуючого інформаційного впливу (ЗДІВ), тобто інтенсивність впливу, а u - сукупність дій, які забезпечують всю систему захисту інформації підприємства. Параметр $\varepsilon > 0$ визначає швидкість зміни дестабілізуючого інформаційного впливу, а параметри k і λ характеризують нелінійну залежність інтенсивності дестабілізуючого інформаційного впливу при прийнятті управлінських рішень від якості системи захисту інформації, $\Xi(t)$ - довіра. При аналізі стійкості системи захисту інформації, припускається, що довіра зростає повільно, тобто

$$\Xi(t) = \begin{cases} \Xi_0 + e^{-\mu t}, & 0 \le t \le T \\ \Xi_0, & t > T \end{cases}, \tag{2}$$

де $\Xi_0 = \Xi(0) = (1-k_0)(1-\lambda_0)(1-\mu)$, $0 < \mu < 1$, k_0 - середнє значення ймовірності того, що відбудеться успішне зняття конфіденційної інформації за рахунок дестабілізуючого інформаційного впливу, λ_0 - середнє значення ймовірності того, що відбудеться пошкодження конфіденційної інформації за рахунок дестабілізуючого інформаційного впливу, T - час, протягом якого відбувається дестабілізуючий інформаційний вплив. Параметр μ уявляє собою ймовірність того, що відбудеться блокування конфіденційної інформації за рахунок дестабілізуючого інформаційного впливу. При аналізі системи захисту інформації при прийнятті управлінських рішень на підприємстві параметри k, λ і μ змінюються місцями і в результаті відбувається дослідження трьох систем виду (1) – (2). В даній роботі розглядається дослідження однієї системи, а дві інші досліджуються аналогічно.

Ввівши нові змінні $X_1 = x$, $X_2 = \frac{dX_1}{dt}$, $X_3 = \Xi_0 - \frac{\mu}{\varepsilon} + e^{-\mu t}$, аналог системи (1) з урахуванням (2) прийме вид

$$\begin{cases} \frac{dX_1}{dt} = X_2 \\ \frac{dX_2}{dt} = \left(1 - X_1^2 - \varepsilon\right)X_2 - \varepsilon\left(g(X_1) - f(X_1) - X_3\right). \\ \frac{dX_3}{dt} = -\mu e^{-\mu t} \end{cases} \tag{3}$$

Так як $\mu < 1$, то змінна X_3 змінюється з часом повільніше ніж змінні X_1 і X_2, а значить, система містить одну повільну змінну і дві швидкі. Отже, дослідження динаміки довіри при прийнятті управлінських рішень на підприємстві та динаміки дестабілізуючого інформаційного впливу при цьому, зводиться спочатку до роздільного дослідження першого рівняння системи (3) та другого та третього рівнянь системи (3). Спираючись на повільні та швидкі динаміки можна отримати розбиття на траєкторії фазового простору системи (3).

При проведенні досліджень, були обчислені середні значення параметрів k_0, λ_0 і ε які входять в систему (3), а параметр $L(\mu) = \Xi_0 - \frac{\mu}{\varepsilon}$ є контрольним. Після підстановки середніх значень параметрів $k_0 = 0{,}5, \lambda_0 = 0{,}2$ і $\varepsilon = 0{,}34$ в (3) з урахуванням вилучення третього рівняння цієї системи отримаємо

$$\begin{cases} \frac{dX_1}{dt} = X_2 \\ \frac{dX_2}{dt} = \left(1 - X_1^2 - 0{,}34\right)X_2 - 0{,}34\left(0{,}5X_1 - X_1 + \frac{1}{3}X_1^3 - X_3\right) \end{cases}, \text{ при } X_1 \le 0 \tag{4}$$

$$\begin{cases} \frac{dX_1}{dt} = X_2 \\ \frac{dX_2}{dt} = \left(1 - X_1^2 - 0{,}34\right)X_2 - 0{,}34\left(0{,}2X_1 - X_1 + \frac{1}{3}X_1^3 - X_3\right) \end{cases}, \text{ при } X_1 > 0. \tag{5}$$

При цьому $L(\mu) = 0{,}4(1-\mu) - \frac{\mu}{0{,}34}$, або $L(\mu) = 0{,}4 - 3{,}34\mu$. Стійкість системи захисту інформації визначається такими значеннями змінних X_1 і X_2, при яких параметр $L(\mu)$ не перевищує заданого порогового значення. Для побудови діаграми біфуркацій необхідно визначити умови стійкості системи захисту інформації. Для цього в першу чергу необхідно праву частину другого рівняння систем (4) і (5) прирівняти до 0. В результаті отримаємо

$$\begin{cases} \left(1 - X_1^2 - 0{,}34\right)X_2 - 0{,}34\left(-0{,}5X_1 + \frac{1}{3}X_1^3 - X_3\right) = 0,\ X_1 \le 0 \\ \left(1 - X_1^2 - 0{,}34\right)X_2 - 0{,}34\left(-0{,}8 + \frac{1}{3}X_1^3 - X_3\right) = 0,\ X_1 > 0 \end{cases},$$

звідки

$$X_2 = \begin{cases} \frac{0{,}11X_1^3 - 0{,}17X_1 - 0{,}34X_3}{1 - X_1^2 - 0{,}34},\ X_1 \le 0 \\ \frac{0{,}11X_1^3 - 0{,}272X_1 - 0{,}34X_3}{1 - X_1^2 - 0{,}34},\ X_1 > 0 \end{cases}. \qquad (6)$$

Так як $X_3 = \Xi_0 - \frac{\mu}{\varepsilon} + e^{-\mu t}$, а при заданих числових значеннях $X_3 = 0{,}4(1-\mu) - \frac{\mu}{0{,}34} + e^{-\mu t}$, то (6) прийме вид

$$X_2 = \begin{cases} \frac{0{,}11X_1^3 - 0{,}17X_1 - 0{,}136 + 1{,}34\mu - 0{,}34e^{-\mu t}}{1 - X_1^2 - 0{,}34},\ X_1 \le 0 \\ \frac{0{,}11X_1^3 - 0{,}272X_1 - 0{,}136 + 1{,}34\mu - 0{,}34e^{-\mu t}}{1 - X_1^2 - 0{,}34},\ X_1 > 0 \end{cases}. \qquad (7)$$

З системи (7) отримаємо умови для стійкості системи захисту інформації, а саме

$$\begin{cases} 0{,}11X_1^3 - 0{,}17X_1 - 0{,}136 + 1{,}34\mu - 0{,}34e^{-\mu t} = 0,\ X_1 \le 0 \\ 0{,}11X_1^3 - 0{,}272X_1 - 0{,}136 + 1{,}34\mu - 0{,}34e^{-\mu t} = 0,\ X_1 > 0 \end{cases}. \qquad (8)$$

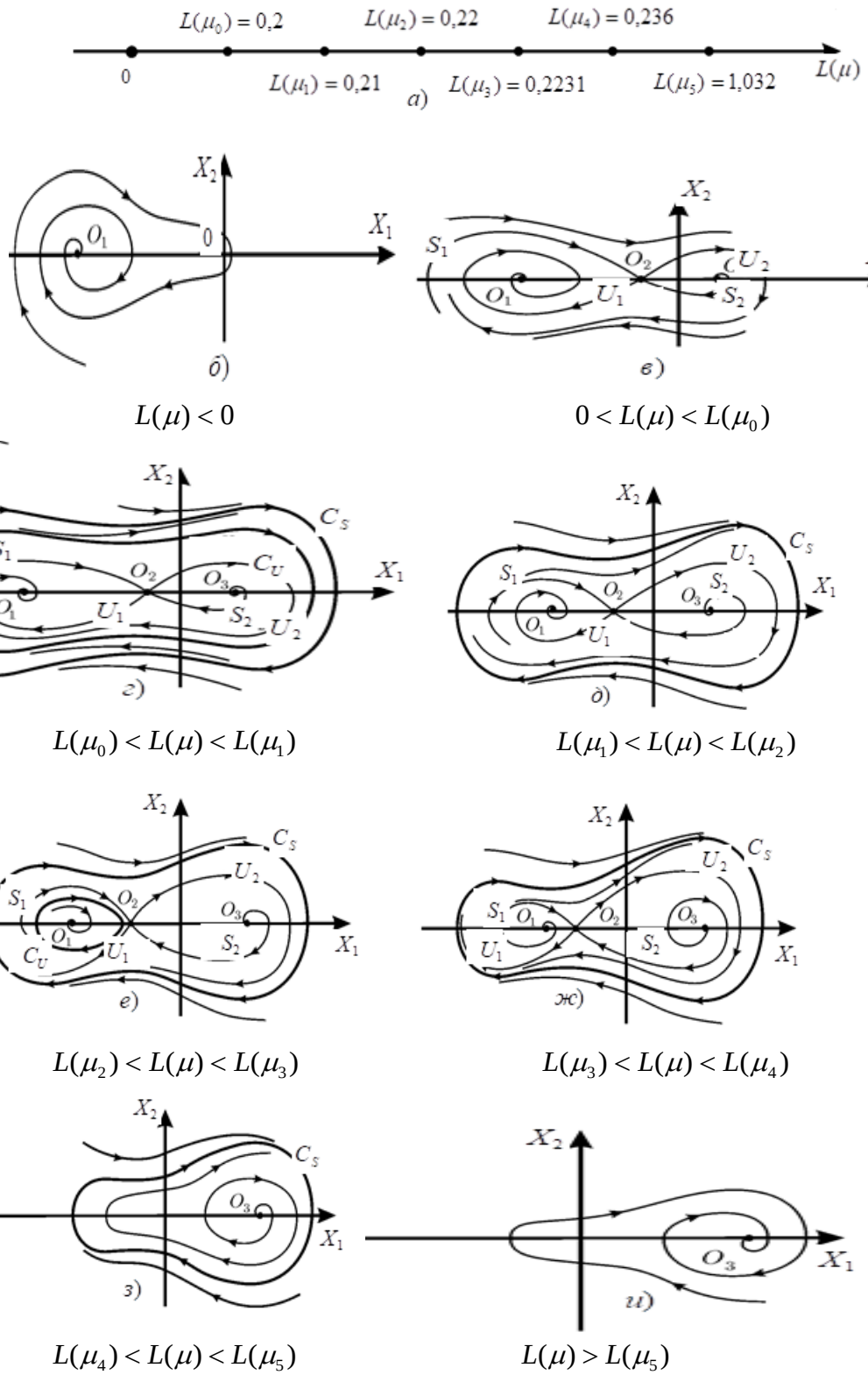
Так як рівняння (8) можуть мати не більше трьох коренів, то в залежності від значень параметра $L(\mu)$ системи (4) і (5) можуть мати від одного до трьох станів рівноваги (три стани стійкості системи захисту інформації) (рис.1).

З рисунку 1 видно, що при $0 < L(\mu) < L(\mu_4)$ системи (4) і (5) мають три стани рівноваги: $O_1(X_1 = l_1, 0)$, $O_2(X_1 = l_2, 0)$ і $O_3(X_1 = l_3, 0)$, де

$$l_1 = \sqrt{(1-k)}\sin\left(\varphi_1 - \frac{\pi}{3}\right),\ l_2 = \sqrt{1-\lambda}\sin\left(\varphi_2 - \frac{2}{3}\pi\right),\ l_3 = \sqrt{(1-k)(1-\lambda)}sh\varphi_3, \qquad (9)$$

де $\varphi_1 = \arcsin\frac{L(\mu)}{\sqrt[3]{(1-k)^2}}$, $\varphi_2 = \ln\left(\sqrt{\frac{(L(\mu))^2}{(1-\lambda)^3} - 1} - \frac{L(\mu)}{\sqrt[3]{(1-\lambda)^2}}\right)$,

$$\varphi_3 = \ln\left(\sqrt{\frac{(L(\mu))^2}{((1-\lambda)(1-k))^3} - 1} - \frac{L(\mu)}{\sqrt[3]{((1-\lambda)(1-k))^2}}\right).$$



$L(\mu) < 0$ $\qquad$ $0 < L(\mu) < L(\mu_0)$

$L(\mu_0) < L(\mu) < L(\mu_1)$ $\qquad$ $L(\mu_1) < L(\mu) < L(\mu_2)$

$L(\mu_2) < L(\mu) < L(\mu_3)$ $\qquad$ $L(\mu_3) < L(\mu) < L(\mu_4)$

$L(\mu_4) < L(\mu) < L(\mu_5)$ $\qquad$ $L(\mu) > L(\mu_5)$

Рис. 1. Якісний вид діаграми біфуркацій систем рівнянь (4) і (5) для параметрів $k_0 = 0{,}5, \lambda_0 = 0{,}2$ і $\varepsilon = 0{,}34$.

Точки O_1 і O_3 є або вузлами або фокусами, а точка O_2 є сідлом. В залежності від значення $L(\mu)$ точки O_1 і O_3 можуть характеризувати як стійкий стан (система захисту інформації повністю відповідає всім нормам), а можуть характеризувати не стійкий стан (система захисту інформації не повністю відповідає всім нормам). При $L(\mu) = 0$ відбувається біфуркація точок

O_2 і O_3, а при $L(\mu) = L(\mu_4)$ відбувається стійкість станів O_1 і O_2. Якщо $L(\mu) = L(\mu_0)$, то цикли C_S і C_U співпадають та зникають і утворюють двократний граничний цикл. При $L(\mu) = L(\mu_1)$ виникає інша біфуркація в циклі C_U при спаданні значення $L(\mu)$. Цикл C_S виникає при $L(\mu) = L(\mu_5)$, при цьому

$$L(\mu_5) = 5\sqrt{1-\varepsilon}(5{,}94k\lambda - \varepsilon).$$

Висновки

Встановлено, що відгук на дестабілізуючий інформаційний вплив при прийняття управлінських рішень на підприємстві характеризується довірою посадової особи. Завдяки встановленому взаємозв'язку між інтенсивністю впливу і довірою, вдалося побудувати математичну модель системи захисту інформації при прийнятті управлінських рішень на підприємстві, що дає можливість здійснювати якісний аналіз системи захисту інформації на основі точок біфуркацій, які характеризують стійкі та нестійкі стани системи захисту. Отримані аналітичні залежності обчислення точок біфуркацій, які залежать від параметрів, які характеризують захист конфіденційної інформації, цілісність інформації та умови неможливості блокування доступу до інформації. Дана модель дає можливість здійснювати якісний аналіз системи інформаційного захисту на підприємстві, що в свою чергу дає можливість виявляти вразливі місця системи інформаційного захисту на підприємстві в цілому.

Список використаної літератури

1. Кириллов С.Ю. Релаксационные колебания и спайковые последовательности в неавтономной модели нейронной возбудимости / С.Ю. Кириллов, В.И. Некоркин // Известия вузов. Радиофизика Том LVI, №1– 2013. –С. 39-54.

2. Михайлов А.П. Модели информационной борьбы / А.П. Михайлов, Н.А. Маревцева // Математическое моделирование, том 23, №10. 2011. – С.- 19-32.

3. Михайлов А.П. Модель информационного противоборства в социуме при периодическом дестабилизирующем воздействии / А.П. Михайлов, А.П. Петров, О.Г. Прончева, Н.А. Маревцева // Математическое моделирование, том 29, №2. 2017– С.- 23-32.

4. Комарова Л.О. Інформаційно-аналітична діяльність як шлях забезпечення безпеки прийняття управлінських рішень у кризових ситуаціях / Л.О. Комарова // Сучасний захист інформації, №2. – 2016. С.- 10-16.

5. Гізун А.І. Аналіз сучасних теорій інформаційно-психологічних впливів в аспекті інформаційного протиборства / А.І. Гізун, В.С. Гріга // Ukrainian Scientific Journal of Information Security, vol. 22, issue 3. – 2016. P.-272-282.

6. Курченко О.А. Розробка моделі паніки інформаційної безпеки підприємства / О.А. Курченко, Ю.О. Ковтун // Сучасний захист інформації, №4. – 2017. С.- 30-36.

7. Кузнецов А.В. Взаимосвязь процесса управления событиями с другими процессами управления предприятия / А.В. Кузнецов // Вопросы кибербезопасности, №5(24) – 2017. С.- 17-22.

8. Лифшиц И.И. К вопросу оценивания энтропии системы обеспечения информационной безопасности / И.И. Лифшиц, А.В. Неклюдов // Вопросы кибербезопасности, №5(24) – 2017. – С.30-41.

9. Лужецький В.А. Концептуальна модель системи інформаційного впливу / В.А. Лужецький, А.В. Дудатьєв // Ukrainian Scientific Journal of Information Security, vol. 23, issue 1. – 2017. P.-45-49.

10. Козьминых С.И. Математическое моделирование обеспечения комплексной безопасности объектов информатизации кредитно-финансовой сферы / С.И. Козьминых // Вопросы кибербезопасности №1(25). – 2018. С.-54-63.

11. Лившиц И.И. Модель интегрированной системы менеджмента для обеспечения безопасности сложных объектов / И.И. Лившиц, Р.Р. Фактиева // Вопросы кибербезопасности №1(25). – 2018. С.-64-71.

References

1. S.Yu. Kirillov and V.I. Nekorkin. Relaxation oscillations and spike sequences in the nonautonomous neuron-excitability model // Izvestia. Vuzov. Radiophysics. Vol. LVI, №1. 2013. P. 39-54.

2. A.P. Mikhailov. Model of information Struggle / A.P. Mikhailov, N.A. Marevtseva // Mathematical modeling, Vol. 23, №10. 2011. P.19-32.

3. A.P. Mikhailov A model of information warfare in a society under periodic destabilizing effect / A.P. Mikhailov, A.P. Petrov, O.G. Proncheva, N.A. Marevtseva // Mathematical modeling. Vol. 29, №2. 2017. P.23-32.

4. L.O. Komarova. Information and analytical activity as a way to ensure safety in making management decisions in crisis situation / L.O. Komarova // Modern information security, №2. 2016. P.10-16.

5. Gizun A. Analysis of modern information-psychological influence theories in aspect of information confrontation / A. Gizun, V. Griga // Ukrainian Scientific Journal of Information Security, vol. 22, issue 3. 2016. P.272-282.

6. O.Kurchenko. Development of a model of the information security of the company / O. Kurchenko, U. Kovtun // Modern information security, №4. 2017. P.30-36.

7. A. Kuznetcov. The relationship of the event management process with other management processes of the enterprise / A. Kuznetcov // Cybersecurity issues, №5(24).2017. P.17-22.

8. Livshitz I.I. Assessment of entropy of information security systems / I.I. Livshitz, A.V. Neklydov // Cybersecurity issues, №5(24). 2017. P.30-41.

9. Luzhetskyi V. Conceptual model of information impact system / Luzhetskyi V., A. Dudatyev // Ukrainian Scientific Journal of Information Security, vol. 23, issue 1. 2017. P.45-49.

10. Kozminykh S.I. Mathematical modeling of credit and finance complex security solutions / S.I. Kozminykh // Cybersecurity issues №1(25). 2018. P.54-63.

11. Livshitz I.I. The integrity management system for security ensuring for complex facilities / I.I. Livshitz, R. Фактieva // Cybersecurity issues №1(25). 2018. P.64-71.