УДК 004.056:004.738.5(045) **doi: 10.26906/SUNZ.2018.4.091**

Г. В. Шуклін, О. В. Барабаш

Державний університет телекомунікацій, Київ, Україна

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ КЕРУВАННЯ ПРОЦЕСАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ ДЕРЖАВНОГО РЕГУЛЮВАННЯ КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ ФОНДОВОГО РИНКУ

В роботі застосовано математичну теорію керування системами диференціальних рівнянь з запізненням, для моделювання процесами регулювання кібернетичної безпеки з боку держави на фондовому ринку. Розглянуті умови стійкості інформаційної безпеки держави на прикладі кібернетичного простору фондового ринку. Запропоновано алгоритм побудови функції керування процесом виявлення кількості кібернетичних атак на електронний торгівельний майданчик на фондовому ринку, який розглядається, як динамічна система, яка описується системами диференціальних рівнянь з запізненням. Запропонована структурна схема системи захисту інформації з введенням інфраструктурного сервісу та аналізатора атак. Встановлено, що системи з запізненням породжують нову інформацію, яку необхідно використовувати при модернізації системи захисту.

Ключові слова: кібернетичний простір, фондовий ринок, керування процесами інформаційною безпекою, державне регулювання кібернетичною безпекою, функція керування, запізнення, час квантування.

Вступ

Постановка завдання. Забезпечення інформаційної безпеки в кібернетичному просторі є однією з основних завдань держави на теперішній час. Так як держава інтегрує велику кількість інституцій, які забезпечують її існування, то задача керування і регулювання інформаційною безпекою їх є однією з найважливіших, особливо в умовах євроінтеграції.

Однією з таких інституцій, яка є складовою макроекономічної системи держави є фондовий ринок (ФР). Стійке функціонування ФР, а саме, здійснення відкритих торгів на електронних майданчиках, які забезпечують надходження податків до бюджету, приток інвестицій та регулювання цінової політики в державі, залежить від забезпечення захищеності інформації і персональних даних учасників ФР від стороннього впливу.

Учасники ФР здійснюють торги на електронних майданчиках у віддалених доступах, та здійснюють розрахунки в режимі онлайн. Для успішних виконань дій в процесі роботи ФР, інформаційно – телекомунікаційні ресурси останнього мають бути стійко захищені.

27 червня 2017 року Інтерфакс-Україна процитувало повідомлення біржі ПФТС, в якому визначалось, що Український фондовий ринок фактично припинив роботу в очікуванні відновлення роботи основних інститутів депозитарно-клірингової системи - Національного депозитарію України (НДУ) і Розрахункового центру з обслуговування договорів на фінансових ринках (РЦ, обидва - Київ), які 27 червня стали жертвою масштабної вірусної кібератаки."Початок торгів на Фондовій біржі ПФТС відкладено до відновлення роботи клірингово-розрахункової інфраструктури ринку цінних паперів України". Цю атаку було здійснено за допомогою віруса Petya.A. Крім того, в повідомлені визналось, що хакерські атаки були націлені на об'єкти критичної інформаційної інфраструктури енергогенеруючих і енергопостачальних компаній, об'єктів транспорту, ряду банківських установ, телекомунікаційних компаній. Вірус атакував і Кабінет міністрів України [1].

Злочинники намагаються здійснювати атаки на вказані об’єкти через відповідні професійні мережі в режимі онлайн. Ці мережі, якими користуються Учасники ФР, виконують не тільки функції отримання необхідної інформації та здійснення платежів за біржовими контрактами, але ще є засобами керування кібербезпекою, та зоною інформаційної протидії. Такі ресурси є інструментом інформаційного впливу, метою яких є маніпулювання думкою гравця, або групи гравців при створені торговельних стратегій для формування портфелів інвесторів. Все це призводить до інформаційних війн, наслідком яких може бути дестабілізація ринку(«обвал ринку»). Історії відомі декілька таких обвалів, які закінчилися втратами мільярдів доларів і масовою загибеллю матеріальних благ: обвал на Уолл-Стріт в 1929 році, обвал 1973-1974 роки, Чорний понеділок 1987 рік, Бум доткомів в 2000 році і обвал 2008 року.

Злочинники активно використовують інформаційні технології та маскуються таким чином, що виявлення їх намірів є однією з нелегких задач сучасності. Тому, актуальною є задача підвищення якості захисту і створення оптимального процесу управління та регулювання інформаційною безпекою з боку держави .

Одним з ефективних підходів для розв’язування зазначеної вище задачі є застосування декомпозиції. Принцип декомпозиції полягає у тому, що для розв’язання задачі виконується розбиття її на ряд окремих простіших задач, які мають певну ієрархічну будову на відповідному рівні. Такий підхід, дає змогу мінімізувати ризик захищеності [4]. Саме формулюванню і розв’язуванню такого класу задач присвячена ця робота.

Мета роботи. Метою даної роботи є розробка методики синтезу динамічної моделі керування процесом інформаційної безпеки фондового ринку з використанням математичної теорії керування системами диференціальних рівнянь з запізненням.

Аналіз останніх досліджень показав, що існує достатня кількість публікацій, присвячена побудові математичних моделей оцінки ефективності систем захисту інформації [6-12] . Однак кожна з моделей має свої недоліки і тому існують обмеження її використання.

Однією з таких обмежень є те, що складністю врахування показників надійності захисту інформаційних систем пов'язана з постійною появою нових факторів, які впливають на її захищеність. Також встановлено, що сучасна методологічна база оцінювання ефективності системи захисту інформації характеризується певним ступенем суб'єктивізму процедур оцінювання [7]. Проблемним залишається питання вибору відповідних показників при оцінці рівня захищеності інформаційної системи з урахуванням наявності часу запізнення.

Основний результат

В роботі [16] побудовано алгоритм побудови функції керування системою диференціальних систем з запізненням, яка має наступний вид

$$\dot{x}(t) = Ax(t-\tau) + bu(t),\ t \geq t_0,\ \tau > 0. \quad (1)$$

Було зазначено, що система (1) відносно керована, якщо для довільної неперервно-диференційованої функції $\varphi(t)$, часу $t_0 - \tau \leq t \leq \tau_0$, що визначає початкові умови, та кінцевого стану x_1 та моментів часу t_0, t_1 існує управління $u_0(t)$, $t_0 \leq t \leq \tau_1$ таке, що система (1) має розв'язок $x_0(t)$, який задовольняє граничним умовам

$$x_0(t) = \varphi(t),\ t_0 - \tau \leq t \leq \tau_0,\ x_0(t_1) = x_1.$$

При конструюванні функції управління системою (1) було введено матричну функцію, яка отримала назву запізнюючого експоненціалу і яка має такий вигляд:

$$e_\tau^{At} = \begin{cases} \theta, & -\infty < t < -\tau; \\ I, & -\tau \leq t < 0; \\ I + A\cdot\dfrac{t}{1!} + A^2\cdot\dfrac{(t-\tau)^2}{2!} + \cdots + A^k\cdot\dfrac{(t-(k-1)\tau)^k}{k!}, & (k-1)\tau \leq t < k\tau, \end{cases} \quad (2)$$

де θ – нульова матриця, I – одинична матриця.

За допомогою функції (2) розв'язок системи (1) було представлено у вигляді

$$x(t) = e_\tau^{At}\varphi(t_0 - \tau) + \int_{t_0-\tau}^{t_0} e_\tau^{A(t-\tau-s)}\varphi'(s)\,ds + \int_{t_0}^{t} e_\tau^{A(t-\tau-s)}bu(s)\,ds, \quad (3)$$

з початковими умовами $x_0(t) = \varphi(t)$, $t_0 - \tau \leq t \leq \tau_0$ [17].

Функція керування, яка входить в третій доданок представлення (3), має такий вигляд:

$$u(s) = b^T e_\tau^{A^T(t-\tau-s)}\left(\int_{t_0}^{t_1} e_\tau^{A(t_1-\tau-\varepsilon)}bb^T e_\tau^{A^T(t_1-\tau-\varepsilon)}d\varepsilon\right)^{-1}\times \times\left(x_1 - e_\tau^{At_1}\varphi(t_0-\tau) - \int_{t_0-\tau}^{t_0} e_\tau^{A(t-\tau-s)}\varphi'(s)\,ds\right). \quad (4)$$

В наших дослідженнях керування інформаційною безпекою в системі державного регулювання кібернетичною безпекою фондового ринку в якості математичної моделі будемо використовувати представлення (3) і (4).

Здійснюючи постійний моніторинг інформаційно-телекомунікаційних систем, які забезпечують функціонування ФР, необхідно виділяти, як окрему множину, сценаріїв атак, та їх кількість $x(t)$, які здійснюються в момент часу t. Початкова функція $\varphi(t)$ формується постійно на відрізку часу $[t_0 - \tau; t_0]$, яка визначає кількість атак протягом часу τ, який назвемо часом квантування. При цьому, система державного регулювання кібернетичною безпекою повинна здійснити відповідні заходи, при яких $x_1 = 0$. В цьому випадку керуюча функція $u(s)$ здійснює стабілізацію функціонування інформаційних систем і відбиває атаки. Кількість майбутніх можливих атак на проміжку $[t_0;\ t_0 + \tau]$, визначається розв'язком представленням (3), яке в свою чергу є початковою функцією для прогнозування кількості атак на проміжку часу $[t_0 + \tau;\ t_0 + 2\tau]$.

Матриця $A = \|a_{ij}\|_{n\times m}$, яка входить в представлення (3) уявляє собою степінь незахищеності інформаційної системи, на яку здійснюється атака і є стохастичною. Елементи цієї матриці a_{ij} – це ймовірність незахищеності i-го об'єкта, $i = \overline{1,n}$ від j-го сценарію атаки, $j = \overline{1,m}$.

Вектор – стовпчик b визначає степінь захищеності i-го об'єкту від всіх можливих сценаріїв атак. Ми будемо припускати, що $m = n$. Якщо рівність не виконується, то відповідна прямокутна матриця доповнюється до квадратної нулями.

Виходячи з вищесказаного, за допомогою представлення (3) і структурі функції керування (4), ми можемо прогнозувати кількість можливих атак і при цьому, аналізуючи їх сценарії, своєчасно їх відбивати. При цьому, побудувавши фазові портрети на інтервалах часів квантування, ми можемо аналізувати стійкість системи захисту.

На рис. 1 представлена залежність кількості атак від часу квантування, які спостерігались протягом години на українській біржі під час електронних торгів.

Крива, яка зображена на цьому рисунку є початковою функцією $\varphi(t)$, при $0 \leq t \leq 1$.

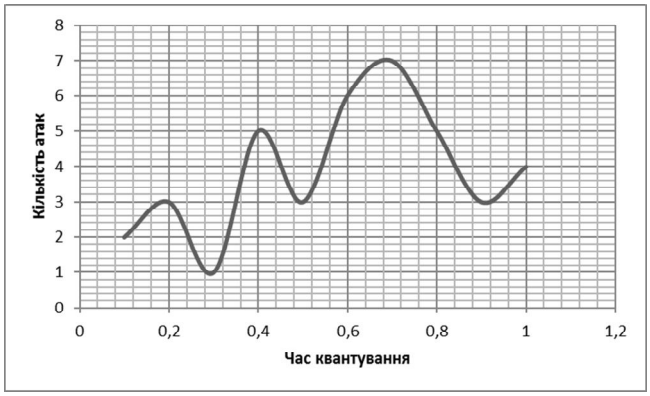

Рис. 1. Залежність кількості кібератак протягом однієї години на Українській фондовій біржі

Степінь незахищеності інформаційної системи при цьому була 0,01, а степінь захищеності була 0,99. Тому (1) в цьому випадку перетворюється в одномірну, тобто в наступне диференціальне рівняння

$$x(t) = 0.01x(t-1) + 0.99u(t), \quad 1 \le t \le 2. \qquad (5)$$

Задача керуючої функції полягає в тому, щоб протягом наступного часу система продовжувала працювати в стаціонарному режимі, а атаки були відбиті. Інакше кажучи, $x_1(t) = 0$, тобто функція (4) здійснює стабілізацію динамічної системи, яка описується рівнянням (5).

На рис. 2 побудовано фазову траєкторію, яка відображає процес стабілізації даного динамічного об'єкту, яка здійснювалась за допомогою керуючої функції (4), яка мала такий вигляд

$$u(t) = (1307s + 2668.1) / (-6).$$

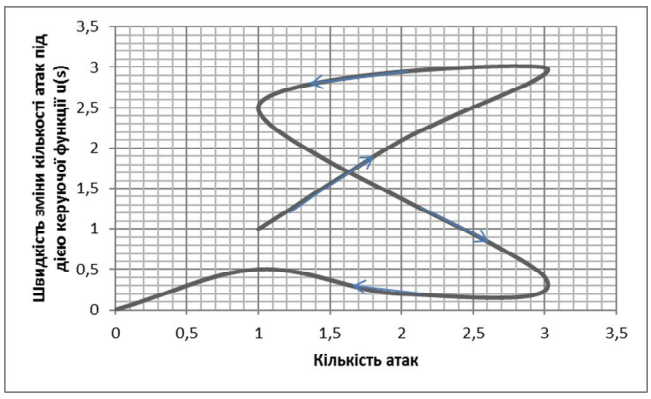

Рис. 2. Фазова траєкторія стабілізації динамічної системи захисту інформації

Схема керування процесом забезпечення інформаційної безпеки на фондовому ринку представлено на рис. 3.

З практичної точки зору, керування – це інфраструктурний сервіс (рис. 3). Між електронним торгівельним майданчиком і інтернет-мережею повинно існувати інформаційно-телекомунікаційна система (інфраструктурний сервіс), яка приймає на себе атаки, які фіксуються програмами-тестерами і подають інформацію в аналізатор сценарію атак і одночасно після їх відбиття за допомогою функції керування $u(s)$, дає дозвіл електронному майданчику на проведення торгів.

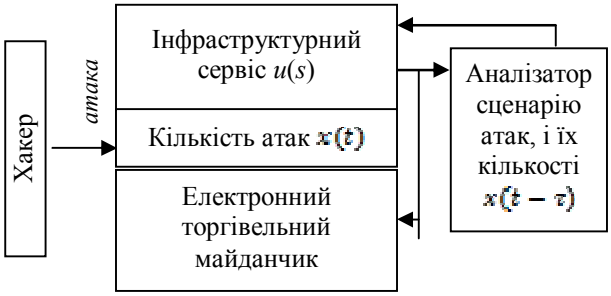

Рис. 3. Керування процесом захисту інформації

Цей процес відбувається неперервно. Аналізатор сценарію атак – це каркас в якому створюється база знань про сценарії атак і здійснюється формування нових функцій для протидії для інфраструктурного сервісу.

Висновки

Виходячи з вищевикладеного, можна зробити висновок, що однією із складових стабілізації фондового ринку в є інформаційна безпека на торгах, тому ефективність торгів залежить від вміння системи захисту виявити і відбити атаку в поточний момент часу. За допомогою математичної теорії керування можна будувати моделі державного регулювання кібернетичною безпекою фондового ринку. Створення систем захисту, як буфера між інтернет – мережою і інформаційною системою дає можливість не тільки виявляти атаки, але аналізуючи їх сценарії, постійно модернізувати існуючі засоби захисту.

Розглядаючи динаміку атак, як динамічну систему з запізненням, ми постійно маємо можливість прогнозувати їх кількість, будуючи закон розподілу ймовірностей їх за допомогою систем диференціальних рівнянь з запізненням і водночас отримувати нову інформацію про розвиток новітніх сценаріїв кібернетичних атак.

Система захисту повинна бути керованою. Завжди необхідно володіти інформацією про те, що відбувається в інформаційній системі, а ще краще, отримати прогноз розвитку ситуації.

СПИСОК ЛІТЕРАТУРИ

1. Електронний ресурс: https:// biz.nv.ua/ukr/finance.
2. Г.В. Шуклін. Моделювання інвестиційних рішень на фондовому ринку.//Г.В. Шуклін. Моделювання та інформаційні системи в економіці. Збірник наукових праць. Випуск 79, 2009 р. с. 62-69.
3. Борсуковський Ю.В. Базові напрямки забезпечення кібербезпеки державного та приватного секторів / Ю.В. Борсуковський, В.Л. Бурячок, В.Ю. Борсуковська // Сучасний захист інформації. - №2(30), 2017.- с.85-89.
4. Проект Концепції інформаційної безпеки України : [Електронний ресурс] / Офіційний сайт Міністерства інформаційної політики України. – Режим доступу: http://www.mip.gov.ua/documents/30.html (дата звернення 25.07.2018). - Назва з екрану.
5. Юдін О.К. Інформаційна безпека держави : навч. посіб./ О.К. Юдін, В.М. Богуш. – Харків: Консум, 2004. – 508 с.
6. Тюлюпа С.В. Проектирование систем поддержки принятия решений в процессе восстановления и обеспечения комплексной защиты информационных систем / С.В. Тюлюпа // Сучасний захист інформації. - №4, 2012. – с.69-74.
7. Грищук Р.В. Диференціально-ігровий метод оцінювання ефективності систем захисту інформації / Р.В.Грищук // Сучасний захист інформації. - №1,2012. – С 40-44.
8. Хорошко В.О. Оцінка захищеності інформаційних систем / В.О.Хорошко, Ю.Є. Хохлачова. // Сучасний захист інформації, № 4,2012.- С. 50-89.
9. Грищук Р.В. Використання диференціальних ігор для оптимізації управління в системах захисту інформації / Грищук Р.В., Хорошко В.О., Хохлачова Ю.Є. // Сучасний захист інформації №2,2012.- с 21-26.

10. Ahentstvo z rozvytku infrastruktury fondovoho rynku Ukrayiny.Vlasnyky krupnykh paketiv aktsiy PrAT «Fondova birzha PFTS». (2010). Retrieved from: URL:http://smida.gov.ua/db/owners/21672206/2010/2.
11. Хорошко В.О. Алгоритм виявлення атак для засобів моніторингу інформації / В.О. Хорошко, О.М. Чернишев // Сучасний захист інформації. - №1, 2012. – с. 49-56.
12. Невойт Я.В. Влияние генетических алгоритмов на эффективность решения задач по информационной безопасности / Невойт Я.В., Хорошко В.А.// Сучасний захист інформації №2,2012.- с 58-64.
13. Д.Я.Хусаінов. Керування в системах з чистим запізненням.// Д.Я. Хусаінов, Г.В. Шуклін. Вісник Київського Університету, випуск №1, 2002р. С. 267-276.
14. Грищук Р.В. Основи кібернетичної безпеки: монографія / Р.В. Грищук, Ю.Г. Даник; під заг. Ред. проф. Ю.Г. Даника.- Житомир: ЖВІ ім. С.П.Корольова, 2016.- 636 с.
15. Доктрина інформаційної безпеки України (затверджена указом Президента України №47/2017 від 25 лютого 2017 року) : [Електронний ресурс] / Офіційне представництво Президента України. – режим доступу: http://www.president.gov.ua/documents/472017-21374 (дата звернення 25.07.2018). - Назва з екрану.
16. Д.Я. Хусаінов. Про один алгоритм керування в системах з чистим запізненням.// Д.Я. Хусаінов, Г.В. Шуклін. Вісник Київського Університету, випуск №2, 2002р. С. 262-267.
17. Д.Я. Хусаинов.Об относительной управляемости в системах с чистым запаздыванием.// Д.Я. Хусаинов, Г.В. Шуклин. Прикладная механика, Том 41, № 2, 2005 г, с. 118-130.
18. В.В. Глушак. Синтез структури системи захисту інформації з використанням позиційної гри захисника та зловмисника. // В.В. Глушак, О. М. Новіков, Системні дослідження та інформаційні технології, №2, 2013 р. с. 89-100.
19. Р.В. Грищук. Неперервна дискретна диференціально-ігрова модель процесу нападу на інформацію. // Р.В. Грищук, Вісник ЖДТУ, №4 (51), 2009 р. с. 135-141.
20. В.И. Зубов. Лекции по теории управления.-М.: Наука, 1975. – 496 с.

Рецензент: д-р техн. наук, проф. Г. А. Кучук,
Національний технічний університет "Харківський політехнічний інститут", Харків
Received (Надійшла) 28.06.2018
Accepted for publication (Прийнята до друку) 22.08.2018

Математическое моделирование управления процессами информационной безопасности в системе государственного регулирования кибернетической безопасностью фондового рынка

Г. В. Шуклин, О. В. Барабаш

В работе использована математическая теория управления системами дифференциальных уравнений с запаздыванием для моделирования процессами регулирования кибернетической безопасности со стороны государства на фондовом рынке. Рассмотрены условия устойчивости информационной безопасности государства на примере кибернетического пространства фондового рынка. Предложен алгоритм построения функции управления процессом выявления количества кибернетических атак на электронную торговую платформу на фондовом рынке, который рассматривается, как динамическая система, которая описывается системами дифференциальных уравнений с запаздыванием. Предложена структурная схема системы защиты информации с введением инфраструктурного сервиса и анализатора атак. Установлено, что системы с запаздыванием порождают новую информацию, которую необходимо использовать при модернизации системы защиты.

Ключевые слова: кибернетическое пространство, фондовый рынок, управление процессами информационной безопасности, государственное регулирование кибернетической безопасностью, функция управления, запаздывание, время квантования.

Mathematical modeling of the control of information security processes in the state regulation of the cybernetic security of the stock market

G. Shuklin, O. Barabash

In the work the mathematical theory of control of systems of late differential equations is used, for modeling the processes of regulation of cybernetic security by the state in the stock market. Conditions of stability of state information security are considered on the example of the cyberspace of the stock market. An algorithm for constructing a control function for detecting the number of cybernetic attacks on an electronic trading platform on the stock market is proposed, which is considered as a dynamic system described by systems of late differential equations. A structural scheme of the information security system with introduction of infrastructure service and attack analyzer is proposed. It has been established that latent systems generate new information that should be used when upgrading the security system. A comparative analysis of the existing mathematical approaches to ensuring the effectiveness of the information security system is carried out. Consider integration of the newest managerial technology in system of state regulation of cyber security of stock market, especially integration of aimed and processing state regulation of cyber security, which continue application managing technologies for this. In case of mathematical model proposed systems of differential equations with downtime. With help of methods of their calculation is show phase pictures, which give possibilities to analyze concrete systems of information security in cyber space and build managerial systems for futher improving and developing of relevant technology. In the work proposed the conceptual subjection of the national monopolies of the cyber security regulation of the stock market, which goes into the general system of the economy of state regulation of cyber security of stock market. Shown the directions of inporting of system of state regulation of cyber security. The form of forecasting of cyber attack on electronic trade systems of stock market with help of forerunner is proposed.

Keywords: cybernetic space, stock market, information security processes management, state regulation of cybernetic security, control function, delay, quantization time.