Methods of information systems protection

УДК 004. 056:004.738.5(045) **doi: 10.20998/2522-9052.2018.3.19**

Г. В. Шуклін, О. В. Барабаш

Державний університет телекомунікацій, Київ, Україна

МОДЕЛЬ РОЗРАХУНКУ ІНТЕНСИВНОСТІ КІБЕРНЕТИЧНИХ АТАК В СИСТЕМІ ЕЛЕКТРОННИХ ТОРГІВ НА ФОНДОВОМУ РИНКУ

Метою статті є адаптація існуючих математичних моделей інтнсивності кібернетичних атак для використання в системі інформаційної безпеки і фізичного захисту електронних торгівельних майданчиків на фондовому ринку до сучасних умов, а також умов прогнозування. **Результати.** Виявлено, що моделювання залежності потоку зовнішніх кібернетичних атак на електронні торгівельні майданчики фондового ринку, може розглядатись як послідовність почергових стрибків і падінь, що свідчить про коливальну природу процесу потоку атак. Обгрунтовано, що система кібернетичного захисту електронних торгівельних майданчиків фондових ринків характеризується часом запізнення. Це створює передумови для порушення стійкості коливань. Результати досліджень носять прикладний характер і можуть бути використані для проведення експериментів і прогнозування значень параметрів, які характеризують кібернетичні загрози, що направлені на електронні торгівельні майданчики фондових ринків з метою їх запобігання та превентивного забезпечення інформаційної безпеки сучасних технологій електронних торгів і взаєморозрахунків. Залежності, які виявлені в процесі моделювання, адаптовані до умов здійснення електронних торгів і взаєморозрахунків на фондових ринках і враховують фактори протидії кібернетичним загрозам, які пов'язані з часом запізнення. Вперше показано, що існує можливість будувати залежності інтенсивності кібернетичних атак за допомогою лінійних диференціальних рівнянь з запізненням, направлених на інформаційно-телекомунікаційні засоби інформаційної безпеки кібернетичного простору фондового ринку. Новий підхід дає можливість здійснювати порушення стійкості коливального процесу «хижак – жертва» завдяки регулюванню часу запізнення і при цьому визначати параметри, які впливають на запас стійкості. Отримані результати дають можливість будувати функціональну залежність інтенсивності кібернетичних атак від часу. Це дає можливість своєчасно здійснювати необхідні дії по інформаційному захисту кібернетичного простору фондового ринку.

Ключові слова: кібернетична атака; кібернетичний простір; час запізнення; інтенсивність атак; фондовий ринок.

Вступ

Постановка завдання. Фондовий ринок є однією з складових економіки держави і відіграє суттєву роль в залучені інвестицій. Створення віртуальних валют і електронних торгівельних майданчиків призвело до зацікавленості кібернетичних злодіїв атакувати інформаційно-телекомунікаційні системи фондового ринку з метою присвоєння активів і коштів третіх осіб, що є учасниками ринку. Тому задача моделювання інтенсивності потоків кібернетичних атак на кібернетичний простір фондового ринку є актуальною і потребує ретельного аналізу.

Формальна постановка завдання полягає в наступному. Необхідно, проаналізувавши існуючі функціональні залежності атак (сигнальних потоків), побудувати диференціальне рівняння, яке моделює їх динаміку і враховує існуючі недоліки цих залежностей.

Аналіз літератури. Аналіз робіт, на які спирається наші дослідження дає можливість стверджувати, що моделювання змін з часом кількості кібернетичних атак при розгляданні задач інформаційної безпеки, суттєво залежить від специфіки об'єкта, кібернетичний простір якого захищається [1-7]. Однак, в багатьох випадках, в прикладній інформатиці для моделювання потоку кібернетичних атак , таких як «програмні віруси», до недавнього часу була математична модель, яка здійснювала опис процесу зміни інтенсивності $x(t)$ на основі аналітичної залежності Ферхюльста [1]:

$$x_i(t) = \frac{K_i}{1 + \frac{K_i - x_i^0}{x_i^0} e^{-r_i^m (t - t_0)}}, \qquad (1)$$

де K_i – рівень насиченості інтенсивності кібернетичних атак,

r_i^m – параметр крутизни початкового зростання інтенсивності кібернетичних атак,

t_0 – початковий момент часу,

x_i^0 – початкове значення кібернетичних атак.

В роботі [1] моделювання процесів інтенсивності кібернетичних атак, які направлені на атомні електростанції, запропоновано використання рівняння Хатчисона, як модифікацію моделей, які раніше були використані. В це рівняння входить час запізнення τ кількості атак на об'єкт, що захищається, і має такий вигляд

$$\frac{dx(t)}{dt} = r_i^m \left(1 - \frac{x(t-\tau)}{K_i}\right) x(t). \qquad (2)$$

Якщо в формулі (1), початковий моменту часу t_0 замінити на час запізнення τ, то моделі (1) і (2) можна використовувати для оцінки ефективності

системи фізичного захисту інформаційних систем, які посилюють моделі диференціально-ігрового підходу, які запропоновані в [2], так як вони враховують реальні умови їх роботи, з урахуванням запізнення технологічно важливих подій [1].

Основний матеріал

При аналізі статистики кібернетичних атак на електронні торгівельні майданчики фондового ринку було встановлено, що інтенсивність таких атак можна описати лінійним диференціальним рівнянням з запізненням, яке має такий вигляд:

$$\frac{dx(t)}{dt} = rx(t) + \frac{r}{K}x_0 x(t-\tau), \qquad (3)$$

де r – параметр крутизни початкового зростання кількості атак,

K – насиченість кібернетичних атак,

x_0 – початкове значення кібернетичних атак.

При аналізі атак протягом 2018 року, було встановлено, що для Українського фондового ринку r приймало значення приблизно 2, а насиченість кібернетичних атак $K = 10$.

В роботі [12] було запропоновано метод розв'язування рівняння (3) і його розв'язок $x_\tau(t)$, який задовольняє одиничним початковим умовам, має таке представлення

$$x_\tau(t) = \begin{cases} 1 + \left\{e^{rt}\left[\frac{1}{r}\right] - \frac{1}{r}\right\}(r + \frac{r}{K}), & 0 \le t < \tau; \\ 1 + \left\{e^{rt}\left[\frac{1}{r}\right] - \frac{1}{r}\right\}(r + \frac{r}{K}) + \\ \quad + \left\{e^{r(t-\tau)}\left[\frac{(t-\tau)}{1!r} - \frac{1}{r^2}\right] + \frac{1}{r^2}\right\} \times \\ \quad \times \frac{r}{K}(r + \frac{r}{K}), & \tau \le t < 2\tau; \\ \ldots \\ 1 + \left\{e^{rt}\left[\frac{1}{r}\right] - \frac{1}{r}\right\}(r + \frac{r}{K}) + \\ \quad + \left\{e^{r(t-\tau)}\left[\frac{(t-\tau)}{1!r} - \frac{1}{r^2}\right] + \frac{1}{r^2}\right\} \times \\ \quad \times \frac{r}{K}(r + \frac{r}{K}) + \ldots + \\ \quad + \left\{e^{r(t-n\tau)}\left[\begin{array}{c} \frac{(t-n\tau)^n}{n!r} - \\ -\frac{(t-n\tau)^{n-1}}{(n-1)!r^2} + \\ +\ldots + (-1)^n \frac{1}{r^{n+1}} \end{array}\right] + \right. \\ \quad \left. + (-1)^{n+1}\frac{1}{r^{n+1}}\right\} \times \\ \quad \times \frac{r}{K}^n (r + \frac{r}{K}), & (n-1) \le t < n\tau. \end{cases}$$

Останнє представлення дає можливість отримувати розв'язок рівняння (3) на проміжках часу

$$[(n-1)\tau; n\tau).$$

Це означає, що маючи інформацію про інтенсивність атак за попередній проміжок часу, ми можемо здійснити прогноз про очікувану інтенсивність загроз на наступний проміжок часу.

Ще варто відмітити, що інтенсивність кібернетичних атак мають і коливальну природу. Це означає, що крива $x_\tau(t)$, яка є розв'язком рівняння (3) має точки перегину.

Тобто, взявши другу похідну, ми можемо визначати період часу квантування, коли відбувається зміна знаку другої похідної функції $x_\tau(t)$. Це дає можливість вибрати час запізнення τ таким чином, щоб здійснювалось порушення стійкості коливань інтенсивності кібернетичних атак.

Порушення стійкості призведе до можливості створювати відповідні дії для забезпечення більш стійкої системи захисту електронних торгівельних майданчиків.

На рис. 1 зображено фазову траєкторію розв'язку рівняння (3) інтенсивності кібернетичних атак на електронний торгівельний майданчик Української фондової біржі, які спостерігались протягом 2018 року.

Рисунок показує, що завдяки стабільній системі захисту інформаційно-телекомунікаційної системи Української фондової біржі, була порушена стійкість коливань інтенсивності кібернетичних атак на електронний торгівельний майданчик, однак все одне інтенсивність атак була достатньо високою.

В результаті проведених якісних і кількісних експериментів виявлено, що інтенсивність кібернетичних атак на кібернетичний інформаційний простір фондового ринку України достатньо великий, що свідчить про присутність суб'єктів, які зацікавлені в організації загроз інформаційній безпеці електронних торгівельних майданчиків.

Функціональна залежність $x_\tau(t)$, яка є розв'язком рівняння (3) враховує не тільки існуючі загрози інформаційній безпеці кібернетичного простору фондового ринку, але дає інформацію про можливість прогнозу моменту часу з якого інтенсивність загроз може збільшуватись або зменшуватись. Це є важливим, так як, можна наперед володіти інформацією про те, коли можна мати додатковий час на вдосконалення інформаційно-телекомунікаційної системи захисту електронних торгівельних майданчиків для протидії зовнішнім загрозам.

Висновки

Запропоновано підхід до розв'язування завдання вибору адекватної моделі функціональної залежності інтенсивності кібернетичних атак на інформаційно-телекомунікаційні системи інформаційної безпеки фондового ринку.

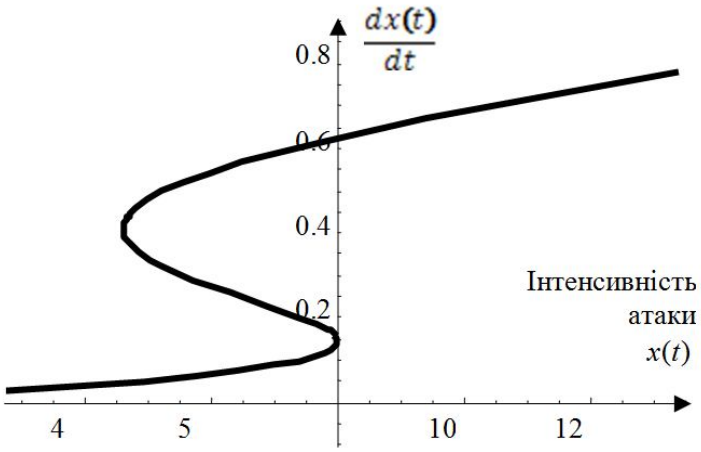

Рис. 1. Фазова траєкторія розв'язку рівняння (3) інтенсивності кібернетичних атак

Рекомендовані в використанні функціональні залежності вперше адаптовані до умов здійснення торгів і взаєморозрахунків на електронних майданчиках фондового ринку.

Враховуються фактори протидії загрозам, які пов'язані з часом запізнення.

Визначені нові шляхи вдосконалення існуючих математичних моделей для їх практичного застосування в забезпеченні інформаційної безпеки фондового ринку. Наукова новизна полягає в можливості будувати функціональні залежності інтенсивності кібернетичних атак , направлених на електронні торгівельні майданчики фондового ринку з урахуванням запізнення, яке в свою чергу, впливає на порушення стійкості коливань інтенсивності атак.

СПИСОК ЛІТЕРАТУРИ

1. Погосов А. Ю. Модели прикладной информатики учёта кинетики кибернетических угроз в системе физической защиты АЭС / А. Ю. Погосов, О. В. Деревянко // Радіоелектроніка, інформатика, управління. – 2017. – № 2. – С. 53-60.
2. Грищук Р. В. Диференціально-ігровий метод оцінювання ефективності систем захисту інформації / Р. В. Грищук // Сучасний захист інформації. – 2012. – № 1. – С/ 40-44.
3. Грищук Р. В. Використання диференціальних ігор для оптимізації управління в системах захисту інформації / Р. В. Грищук, В. О. Хорошко, Ю. Є. Хохлачова // Сучасний захист інформації. – 2012. – № 2. – С. 21-26.
4. Хорошко В. О. Алгоритм виявлення атак для засобів моніторингу інформації / В. О. Хорошко, О. М. Чернишев // Сучасний захист інформації. – 2012. – № 1. – С. 49-56.
5. Грищук Р.В. Постановка проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах / Р. В. Грищук, К. В. Молодецька – Гринчук // Сучасний захист інформації. – 2018. – № 1 (33). – С. 43-53.
6. 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.
7. Борсуковський В. Ю. Прикладні аспекти захисту інформації в сучасних умовах / Ю. В. Борсуковський, В. Ю. Борсуковська // Сучасний захист інформації. – 2018. – № 2. – С. 6-11.
8. The Open Group Releases Maturity Model for Information Security Management, SAN FRANCISCO. April 11, 2011. [Електронний ресурс]. – Режим доступу: http://www.opengroup.org/.
9. Computer security resoursce center [Електронний ресурс]/ – Режим доступу: http://csrc.nist.gov/Publications.
10. The Community Cyber Security Maturity Model [Електронний ресурс]/ – Режим доступу: http://pdfs.semanticscholar.org/c76f/bfde67b7afcbae58ee7f2323fa9746d32f80.pdf.
11. Zybin S. The one method to decision making support for formation of complex security information programs / S. Zybin // Сучасний захист інформації. – 2017. – № 1. – P. 73-78.
12. Khusainov D. Ya. On a Representation of Solutions of Linear Delay Systems / D. Ya. Khusainov, A.F. Ivanov, G.V. Shuklin // Differential Equations. – 2005. – Vol. 41, №7. – P. 1054-1058.

REFERENCES

1. Pogosov, O.Yu. and Derevianko, O.V. (2017), "Modeli prikladnoy informatiki uchota kinetiki kiberneticheskih ugroz v sistemi fizicheskoy zashity AES", *Radioelectronics, computer science, control*, No. 2, pp. 53-60.
2. Grishuk, R. (2012), "Differential-game method for evaluating the effectiveness of information security systems", *Modern information security*, No. 1, pp. 40-44.
3. Grishuk, R., Horoshko, V. and Hohlachova, Yu. (2012), "Use of differential games to optimize control in information security systems", *Modern information security*, No. 2, pp. 21-26.
4. Horoshko, V. and Chernishev, O. (2012), "An algorithm for detecting attacks for information monitoring tools", *Modern information security*, No. 1, pp. 49-56.
5. Grishuk, R.V. and Molodetska, K.V. (2018), "Resolving the problem of providing information security of state in social networking services", *Modern information security*, No. 1 (33), pp. 43-53.

6. Grishuk, R.V. and Danik, Yu.H. (2016), *Fundamental cyber security*, Zhytomyr Military Institute the name of S.P. Korolev, Zhytomyr, 636 p.
7. Borsukovskii, Y. and Borsukovska, V. (2018), "Applied aspects of protection of information in modern conditions", *Modern information security*, No. 2, pp. 6-11.
8. *The Open Group Releases Maturity Model for Information Security Management*, San Francisco, April 11, 2011, available at: http://www.opengroup.org/ (last accessed on May 30, 2018).
9. *Computer security resoursce center*, available at: http://csrc.nist.gov/Publications (last accessed on May 30, 2018).
10. Gregory B. White (2007), *The Community Cyber Security Maturity Model*, available at: http://pdfs.semanticscholar.org/c76f/bfde67b7afcbae58ee7f2323fa9746d32f80.pdf (last accessed on May 30, 2018).
11. Zybin, S. (2017), "The one method to decision making support for formation of complex security information programs", *Modern information security*, No. 1, pp. 73-78.
12. Khusainov, D.Ya., Ivanov, A.F. and Shuklin G.V. (2005), "On a Representation of Solutions of Linear Delay Systems", *Differential Equations*, Vol. 41, No. 7, pp. 1054-1058.

Надійшла (received) 14.06.2018
Прийнята до друку (accepted for publication) 15.08.2018

Модель расчёта интенсивности кибернетических атак в системе электронных торгов на фондовом рынке

Г. В. Шуклин, О. В. Барабаш

Целью статьи является адаптация существующих математических моделей интенсивности кибернетических атак для использования их в системе информационной безопасности и физической защиты электронных торговых площадок на фондовом рынке в современных условиях, а также условий возможных прогнозов. **Результаты.** Установлено, что моделирование зависимости потока внешних кибернетических атак на электронные торговые площадки фондового рынка, можно рассматривать как последовательность поочерёдных скачков и падений, что свидетельствует о колебательной природе процесса потока атак. Обосновано, что система кибернетической безопасности электронных торговых платформ фондовых рынков характеризуется временем запаздывания. Это создаёт предпосылки для нарушения устойчивости колебаний. Результаты исследований носят прикладной характер и могут быть использованы для проведения экспериментов и прогнозирования значений параметров, которые характеризуют кибернетические атаки, которые направлены на электронные торговые площадки фондовых рынков с целью их устранения и превентивного обеспечения информационной безопасности современных технологий электронных торгов и взаиморасчётов. Зависимости, которые выявлены в процессе моделирования, адаптированы к условиям осуществления электронных торгов и взаиморасчётов на фондовых рынках и учитывают факторы противоборства кібернетическим атакам, которые связаны со временем запаздывания. Впервые показано, что существует возможность строить зависимости интенсивности кибернетических атак при помощи линейных дифференциальных уравнений с запаздыванием, направленных на информационно-телекомуникационные средства информационной безопасности кибернетического пространства фондового рынка. Новый подход даёт возможность влиять на нарушение устойчивости колебательного процесса «хищник – жертва» посредством регулирования временем запаздывания и при этом определять параметры, которые вплияют на запас устойчивости. Полученные результаты дают возможность строить функциональную зависимость интенсивности кибернетических атак от времени. Это даёт возможность своевременно осуществлять необходимые действия, направленные на информационную защиту кибернетического простораства фондового рынка.

Ключевые слова: кибернетическая атака; кибернетическое пространство; время запаздывания; интенсивность атак; фондовый рынок.

Model of cybernetic attacks intensity calculation in the electronic trading system on the stock market

G. Shuklin, O. Barabash

The purpose of the article is to adapt existing mathematical models of intensive cybernetic attacks for use in the information security system and physical protection of electronic trading platforms in the stock market in modern conditions, as well as conditions for possible forecasts. **Results.** It is established that the modeling of the dependence of the flow of external cybernetic attacks on the electronic trading platforms of the stock market can be regarded as a sequence of alternating jumps and falls, which indicates the vibrational nature of the process of attack flow. It is substantiated that the system of cybernetic security of electronic trading platforms of stock markets is characterized by delay time. This creates the prerequisites for disturbing the stability of oscillations. The results of the research are of an applied nature and can be used to conduct experiments and predict the values of the parameters that characterize cyber attacks that are aimed at the electronic trading platforms of stock markets in order to eliminate them and prevent the information security of modern electronic trading technologies and mutual settlements. The dependencies, which are revealed in the modeling process, are adapted to the conditions of electronic trading and mutual settlements in stock markets and take into account the factors of confrontation to cybernetic attacks that are associated with the delay time. It is shown for the first time that it is possible to construct the dependences of the intensity of cybernetic attacks using linear differential equations with delay directed at information and telecommunication means of information security of the cybernetic space of the stock market. The new approach makes it possible to influence the instability of the predator-prey oscillatory process by adjusting the delay time and at the same time to determine the parameters that affect the stability margin. The results obtained make it possible to construct a functional dependence of the intensity of cybernetic attacks on time. This makes it possible to timely implement the necessary actions aimed at information protection of the cybernetic space of the stock market.

Keywords: cybernetic attack; cybernetic space; delay time; intensity of attacks; stock market.