УДК 004.056 DOI: 10.31673/2412-4338-2018-0-2-110-116

Шуклін Г. В., **Барабаш О. В.** *Державний університет телекомунікацій, Київ*

МЕТОД ПОБУДОВИ СТАБІЛІЗАЦІЙНОЇ ФУНКЦІЇ КЕРУВАННЯ КІБЕРБЕЗПЕКОЮ НА ОСНОВІ МАТЕМАТИЧНОЇ МОДЕЛІ КОЛИВАНЬ ПІД ДІЄЮ СИЛ ІЗ ЗАПІЗНЕННЯМ

Досліджуються системи керування кібербезпекою, які містять запізнення – окремий вид адаптивних систем. Проаналізовані причини, які сприяють наявності запізнення в системах захисту інформації при кібернетичних атаках. Запропоновано математичну модель кількісної оцінки ефективності системи захисту інформації, на прикладі коливань, які виникають під дією сили з запізненням. На прикладі атак на брандмауер показана методика керування кібербезпекою.

Ключові слова: *кібернетичний простір, атаки, час запізнення, функція керування, брандмауер,стійкість коливань,інтенсивність атак, довірені процеси.*

Shuklin H. V., Barabash O. V. *State University of Telecommunications, Kyiv*

METHOD FOR CONSTRUCTING A STABILIZATION FUNCTION FOR MANAGING CYBERSECURITY ON THE BASIS OF THE MATHEMATICAL MODEL OF OSCILLATIONS UNDER THE ACTION OF FORCES WITH A DELAY

The article studies cyber security management systems, in which there is a downtime - a separate type of adaptive systems. Made the analysis of the reasons that influence the appearance of delay (downtime) in information security systems in cybernetic attacks. A mathematical model of a quantitative evaluation of the effectiveness of the information protection system is proposed, for example of oscillations that arise under the action of a force with delay. Cybernetic attacks are considered as continuous messages in the form of difference starting counting points, and have the following principles: sequential coding, regeneration, robustness, uncertainty. The firewall attack simulator shows the cyber security management technique. Making an evaluation of effectiveness of data security system must be counted delay (downtime), which attacks were in previous period of time and which managing security features were used. Existing of security windows give a possibility to get new information about disadvantages, which are in security system and in time eliminate them.

Work in Internet now a days practical unbelievable without using firewall, which secures computer from outside attack and restrict application work according to task inserted by user his rules. Manufacturers of malicious programs, in turn apply different methods of struggle with firewall. Theme of the article is review of the most widespread methods to fight with firewall. For each method given technology of secure and methods of checking firewalls. 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.

Keywords: *cyber space, attacks, time delay, control function, firewall, oscillatory stability, intensity of attacks, trusted processes.*

Шуклин Г. В., Барабаш О. В. *Государственный университет телекоммуникаций, Киев*

МЕТОД ПОСТРОЕНИЯ СТАБИЛИЗАЦИОННОЙ ФУНКЦИИ УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ НА ОСНОВЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ КОЛЕБАНИЙ ПОД ВОЗДЕЙСТВИЕМ СИЛ С ЗАПАЗДЫВАНИЕМ

Исследуются системы управления кибернетической безопасностью, в которых присутствует запаздывание – отдельный тип адаптивных систем. Проведен анализ причин, влияющих на появление запаздывания в системах защиты информации при кибернетических атаках. Предложена

математическая модель количественной оценки эффективности системы защиты информации на примере колебаний, которые возникают под действием силы с запаздыванием. На примере атак на брандмауэр показана методика управления кибернетической безопасностью.

Ключевые слова: *кибернетическое пространство, атаки, время запаздывания, функция управления, брандмауэр, устойчивость колебаний, интенсивность атак, доверительные процессы.*

Вступ і постановка завдання. Аналізуючи загрози, які виникають в кібернетичному просторі, можна зробити висновок, що найчастіше вони є наслідком наявності вразливих зон в системі захисту інформаційних систем (таких, наприклад, як можливість доступу третіх осіб до критично важливого устаткування або помилки в програмному забезпеченні).

Інтервал часу від моменту, коли з'являється можливість використовувати слабку зону, і до моменту, коли недолік ліквідується, називають ***вікном безпеки***, яке асоціюється з даною вразливою зоною, або часом запізнення . Поки існує *вікно безпеки*, то можливі успішні атаки на інформаційні системи.

Для багатьох зон час запізнення має достатню тривалість (декілька днів, іноді – тижнів), так як за цей час повинні відбутися наступні події:

– виявлення засобів причин виникнення недоліків;

– повинні бути випущені відповідні латки;

– латки повинні бути встановленні в інформаційній системі яку захищають.

Так як час запізнення постійно існує і засоби їх використання з'являються постійно, то відстеження таких вікон повинно здійснюватись постійно. Інакше кажучи, керування інформаційною системою безпеки необхідно постійно здійснювати з урахуванням наявності вікон безпеки. Тому побудова відповідної функції керування, яка б постійно здійснювала стабілізацію інформаційної системи, тобто запобігала появленню або мінімізувала час запізнення, є актуальним завданням в здійсненні заходів щодо забезпечення безпеки інформаційним системам.

Аналіз останніх досліджень і публікацій показав, що існує достатня кількість наукових праць, присвячених побудові математичних моделей оцінки ефективності систем захисту інформації [1-8] . Однак кожна з моделей має свої недоліки і тому існують обмеження їх використання. Одним з таких обмежень є те, що складність врахування показників надійності захисту інформаційних систем пов'язана з постійною появою нових факторів, які впливають на їх захищеність. Також встановлено, що сучасна методологічна база оцінювання ефективності системи захисту інформації характеризується певним ступенем суб'єктивізму процедур оцінювання [2]. Проблемним залишається питання вибору відповідних показників при оцінці рівня захищеності інформаційної системи з урахуванням наявності часу запізнення.

Метою статті є побудова математичної моделі кількісної оцінки ефективності системи захисту інформації при керуванні кібербезпекою з урахуванням наявності вікон безпеки.

Викладення основного матеріалу дослідження. Кількісною характеристикою інтенсивності кібернетичних атак будемо вважати деяку функцію $x(t)$, яка залежить від часу t. Інтенсивність атак будемо розглядати як деякі коливання протягом певного періоду часу. Однак варто розуміти, що безпека інформаційної системи в поточний момент часу залежить від ефективності її захищеності за період часу, попередній поточному. Тому джерелом коливання атак будемо вважати деяку силу з запізненням.

Розглянемо диференціальне рівняння з запізненням

$$\ddot{x}(t)+x(t-2\tau)=u(t-\tau)\,,\ \ t\geq 0, \qquad (1)$$

яке моделює малі коливання під дією сили $u(t-\tau)$ з запізненням. Здійснивши заміну $\dot{x}(t)=y(t-\tau)$, приведемо рівняння (1) до системи:

$$\dot{x}(t)=y(t-\tau)\,,\quad \dot{y}(t)=-x(t-\tau)+u(t)\,. \qquad (2)$$

Початкові умови $x(t) \equiv \varphi(t)$, $\dot{x}(t) \equiv \dot{\varphi}(t)$ $-2\tau \le t \le 0$ для розв'язання рівняння (1) перейдуть в початкові умови

$$x(t) \equiv \varphi(t), \quad y(t) \equiv \dot{\varphi}(t-\tau), \ -\tau \le t \le 0$$

для розв'язування системи (2). Запишемо (2) в векторно-матричній формі

$$\dot{z}(t) = Az(t-\tau) + bu(t), \tag{3}$$

де $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $b = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $z(t) = \begin{bmatrix} x(t) \\ y(t) \end{bmatrix}$.

Нехай ставиться задача переводу початкового положення $x(t) \equiv \varphi(t), -\tau \le t \le 0$; $y(t) \equiv \dot{\varphi}(t-\tau)$, $-\tau \le t \le 0$ в початок координат, тобто $x(t_1) = 0, y(t_1) = 0$, або задача частинної стабілізації. В цьому випадку функція керування має вид:

$$u(s) = b^T e_\tau^{A^T(t_1-\tau-s)} \left[\int_0^{t_1} e^{A(t_1-\tau-\zeta)} b b^T e^{A^T(t_1-\tau-\zeta)} d\zeta \right]^{-1} \xi, \tag{4}$$

де $\xi = -e_\tau^{At_1} \begin{pmatrix} \phi(-\tau) \\ \phi'(-2\tau) \end{pmatrix} - \int_{-\tau}^{0} e^{A(t_1-\tau-\zeta)} \begin{pmatrix} \phi'(\zeta) \\ \phi''(\zeta-\tau) \end{pmatrix} d\zeta$, $0 \le s \le t_1$.

Нехай для спрощення $\varphi(t) \equiv 1$, $-2\tau \le t \le 0$ і $t_1 = 3\tau$. Тоді, враховуючи структуру вектора b і матриці e_τ^{At} [10], отримуємо:

$$u(s) = \begin{cases} l_1(2\tau - s) + l_2\left[1 - \dfrac{(s-\tau)^2}{2!}\right], & 0 \le s < \tau \\ l_1(2\tau - s) + l_2, & \tau < s \le 2\tau \\ l_2, & 2\tau < s \le 3\tau \end{cases} \tag{5}$$

де: $l_1 = -4\tau^4(-1+2\tau^2) - (2\tau^2 - \dfrac{5}{24}\tau^4)(3\tau - \dfrac{1}{6}\tau^3)$,

$$l_2 = -(2\tau^2 - \frac{5}{24}\tau^4)(-1+2\tau^2) - (3\tau - \frac{1}{2}\tau^2 + \frac{1}{20}\tau^5)(3\tau - \frac{1}{6}\tau^3).$$

На рис. 1 графічно показано дію стабілізації функцією керування (5), за допомогою якої відбувається відбиття атак. Інакше кажучи, відбувається порушення стійкості коливань інтенсивності атак, що описується рівнянням (1). Це дає час на прийняття захисних заходів щодо забезпечення інформаційної безпеки системи, на яку було здійснено атаку.

В табл. 1 представлено приклади атак, які здійснюються кіберзлочинцями, та методики захисту при атаках на брандмауер за час, протягом якого відбувається порушення стійкості інтенсивності атак під дією функції керування (права частина рівняння (1)). В таблиці показано приклади можливих атак і заходи, які необхідно застосовувати при керуванні кібернетичною безпекою.

На теперішній час поки ще не існує універсальних утиліт-тестів, які б могли реалізовувати імітацію всіх можливих методик обходу і нейтралізації брандмауерів. Однак, приведені приклади тестів (таблиця 1) можуть бути достатньо легко реалізовані вручну.

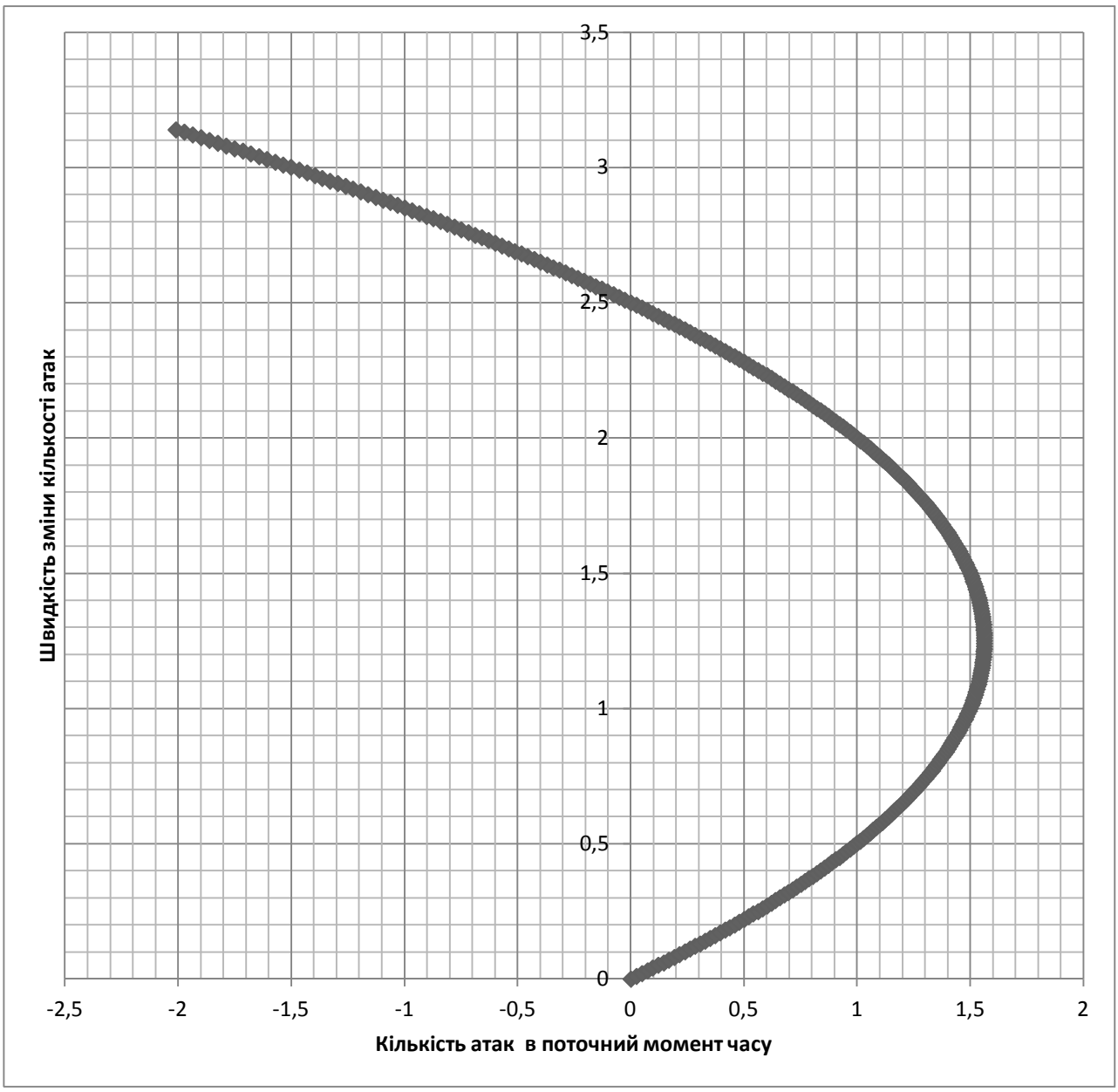

Рис. 1. Фазовий портрет стабілізації коливань під дією функції керування (5)

Приклади кібератак та методики захисту Табл. 1

Атаки	Методика захисту (керування $u(t-\tau)$)	Методика тестування
Доступ в мережу з використанням технології взаємодії двох або більше користувачів (RAW Socket)	Брандмауери дають можливість створювати окремі правила, що дозволяють або забороняють використовувати технологію RAW Socket. Якщо таку функцію не передбачено, то брандмауер повинен обмежити мережеву активність додатку згідно заданим правилам незалежно від методики обміну.	Програма-тестер здійснює спробу передачі інформації або прийому мережевих пакетів за допомогою RAW Socket, після чого вивчається реакція брандмауера на подібні операції.

Керування довіреним додатком	Брандмауер повинен контролювати запуск довіреного додатку особам, яким не довіряє, якщо мова йде про браузер. Брандмауери перевіряють, чи видно вікно додатку, що запущено користувачем. Обмін додатку з інтернетом, який не бачить користувач, є підозрою, а якщо цей додаток запущено додатком, що не є довірчим, то підозра ще сильніша.	Додаток-тестер запускає деяку довірену програму з параметрами. Як правило, запускається браузер, керування яким здійснюється за допомогою командної строки передачі повідомлень вікну браузера для імітації роботи користувача, при керуванні запущеної копії браузера за допомогою DDE (Dynamic Data Exchange — динамічний обмін даними). Деякі утиліти тестування створюють завдання за допомогою відповідних додаткових дій або функцій (в цьому випадку запуск довіреного додатку виконує сама система).
Створення в довірених процесах троянських потоків	Брандмауер повинен контролювати подібну операцію та або блокувати її, або вважати процес не довіреним з моменту влучення в нього іншого потоку. Важливо не тільки фіксувати факт створення потоку, але і здійснювати реєстрацію виконаної операції додатку для подальшого аналізу.	Створення в пам'яті імітації процесу троянського потоку, що здійснює обмін з Інтернетом, і спостерігання за реакцією брандмауера.
Впровадження сторонніх бібліотек елементів керування (DLL) в довірені процеси	Захист зводиться до контролю компонентів додатку, тобто до створення списку DLL, які використовує додаток і до видачі попереджень у випадку появи в пам'яті довіреного процесу нової DLL, яка відсутня в цьому списку. Для зменшення кількості хибних викликів може використовуватись перевірка цифрових підписів бібліотек (для виключення реакції на системні DLL) і інтеграція брандмауера з антивірусом для виявлення троянських бібліотек. Крім того, для деяких методик впровадження DLL необхідний запис в пам'ять процесу, що також може контролювати брандмауер.	Впровадження в пам'ять довіреного додатку зайвих DLL різними методами та спостерігання за реакцією брандмауера. В процесі тестування слід мати на увазі, що для зменшення кількості хибних викликів, розробники деяких брандмауерів не вважають сторонніми бібліотеки, які загружаються з робочої папки.
Модифікація машинного коду довірених процесів	Здійснюється блокування модифікації машинного коду довірених процесів або реєстрація цієї події, після чого, процес, який було модифіковано, вважається не довірчим. При виборі брандмауера варто приділяти увагу на те, яким чином здійснюється спостерігання за записом в пам'ять інших процесів.	Здійснюється запуск довіреного процесу і модифікується його машинний код. Здійснюється спостерігання за реакцією брандмауера.

На сайті [10] розміщено різноманітну кількість утиліт для тестування брандмауера. Велика кількість утиліт невеликі за розміром і містять короткий опис на англійській мові.

Наприклад, на сайті можна знайти наступні утиліти:

• Surfer – тест, який базується на керуванні браузера по DDE;

• Breakout – управління браузером за допомогою передачі його вікну повідомлень завдяки SendMessage;

• Ghost – обхід брандмауера за допомогою маніпуляцій з PID процесу тестер;

• PCAudit – реалізація DLL в пам'ять процесу Explorer.exe;

• WallBreaker – демонстрація різних методик запуску Internet Explorer з параметрами для передачі інформації.

Висновок. При оцінці ефективності системи захисту інформації слід враховувати запізнення, скажімо, які атаки відбувалися в попередній період часу і які засоби керування безпеки були при цьому здійснені. Наявність вікон безпеки дають можливість отримувати нову інформацію про недоліки, які присутні в системі захисту і своєчасно їх ліквідувати.

Також на прикладі атак на брандмауер, можна зробити висновок, що запущений брандмауер і правильно працюючий брандмауер не є одне й те саме. Тому слід періодично перевіряти правильність функціонування брандмауера, який використовується, за допомогою leak – тестів та сканування портів за межами, здійснювати аналіз його правил та налаштувань.

Список використаної літератури

1. Борсуковський Ю. В. Прикладні аспекти захисту інформації в сучасних умовах / Ю. В. Борсуковський, В. Ю. Борсуковська // Сучасний захист інформації. – 2018. – №2(34). – С.6-11.

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. Невойт Я. В. Влияние генетических алгоритмов на эффективность решения задач по информационной безопасности / Я. В. Невойт, В. А. Хорошко // Сучасний захист інформації. – 2012. – №2. – С. 58-64.

6. Толубко В. Б. Модель комбінованої системи управління мережі майбутнього / В. Б. Толубко, Л. Н. Беркман, С. І. Отрох, О. А. Кільменінов // Наукові записки Українського науково-дослідного інституту зв'язку. – 2018. – №1(49). – С. 5-11.

7. Дахно Н. Б. Аналіз захищеності інформації в інформаційно-комунікаційних системах і мережах, що моделюються інтегро-диференціальними рівняннями з малою не лінійністю на основі модифікованих градієнтних методів / Н. Б.Дахно, Т. В. Майсак, Г. В. Шевченко // Сучасний захист інформації. – 2017. – №1. – С. 115-119.

8. Хорошко В. О. Аналіз математичних моделей інформаційно-комунікаційних систем і мереж щодо захисту інформації на основі теорії варіаційно-градієнтних методів / В. О. Хорошко, Т. В. Майсак, Н. Б. Дахно // Моделювання та інформаційні методи в економіці. – 2015. – №91. – С. 246-255.

9. Шуклін Г. В. Про одну задачу стабілізації маятника з запізненням / Г. В. Шуклін // Вісник Київського Університету. – 2002. – №4. – С. 275-283.

10. http://firewallleaktester.com.

Reference (MLA)

1. Borsukovskii Y. V., and Borsukovska V. Y. "Applied Aspects of Protection of Information in Modern Conditions." *Sychasnyi Zakhyst Informatsii* 2(34) (2018): 6-11. Print.
2. Grishuk R.V. "Differential-Game Method For Evaluating The Effectiveness Of Information Security Systems." *Sychasnyi Zakhyst Informatsii* 1 (2012): 40-44. Print.
3. Grishuk R. V., Khoroshko V. O., and Hohlachova U. E. " Use of Differential Games to Optimize Control in Information Security Systems." *Sychasnyi Zakhyst Informatsii* 2 (2012): 21-26. Print.
4. Horoshko V.O., and Chernishev O. M., "An Algorithm for Detecting Attacks for Information Monitoring Tools." *Sychasnyi Zakhyst Informatsii* 1 (2012) : 49-56. Print.
5. Nevoyt Y. V., and Khoroshko V. O. " The Influence of Genetic Algorithms on the Effectiveness of Solving Information Security Problems." *Sychasnyi Zakhyst Informatsii* (2) (2012): 58-64. Print.
6. Tolubko V. B., Berkman L. N., Otroh S. I., and Kilmeninov O. A. "Model of the Combined System of Management of the Future Network." *Naukovi Zapysky Ukrayinskoho Naukovo-Doslidnoho Instytutu Zviazku* 1(49) (2018): 5-11. Print.
7. Dakhno N. B., Maisak T. V., and Shevchenko H. V. "Analysis of Information Security in Information and Communication Systems and Networks Modeled by Integrated Differential Equations with Low Non-Linearity Based on Modified Gradient Methods." *Sychasnyi Zakhyst Informatsii* (1) (2017): 115-119. Print.
8. Khoroshko V. O., Maisak T. V., and Dakhno N. B. "Analysis of Mathematical Models of Information and Communication Systems and Networks for the Protection of Information on the Basis of the Theory of Variational-Gradient Methods." *Modelling and Information Methods in Economic* 91 (2015): 246-255. Print.
9. Shuklin G.V. "About one problem of stabilization of the pendulum with delay." *Visnyk Kyivskoho Universytetu* (4) (2002): 275-283. Print.
10. http:// firewallleaktester.com. Web. 23 Feb. 2018

Автори статті

Шуклін Герман Вікторович – старший викладач кафедри вищої математики, Державний університет телекомунікацій, Київ. Тел.: +380 (97) 824 22 42. E-mail: mathacadem-kiev@ukr.net.

Барабаш Олег Володимирович – доктор технічних наук, професор, завідувач кафедри вищої математики, Державний університет телекомунікацій, Київ. Тел.: +380 (97) 911 08 54. E-mail: bar64@ukr.net.

Authors of the article

Shuklin Herman Viktorovich – senior lecturer of higher mathematics department, State University of Telecommunications, Kyiv. Tel: +380 (97) 824 22 42. E-mail: mathacadem-kiev@ukr.net.

Barabash Oleh Volodymyrovych – doctor of sciences (technical), professor, head of higher mathematics department, State University of Telecommunications, Kyiv. Tel: +380 (97) 911 08 54. E-mail: bar64@ukr.net.

Дата надходження
в редакцію: 15.03.2018 р.

Рецензент:
доктор технічних наук, професор М. К. Жердєв
Київський національний університет ім. Тараса Шевченка