DOI 10.31891/2307-5732-2020-289-5-280-285
УДК 004.49

В. П. ПАЮК, О. В. ГЕЙДАРОВА, В. Д. КОСЕНКОВ, О. С. САВЕНКО
Хмельницький національний університет

ЗАСТОСУВАННЯ БАГАТОФАКТОРНОГО АНАЛІЗУ З МЕТОЮ ВИЯВЛЕННЯ НЕЗАДОКУМЕНТОВАНИХ ЗАКЛАДОК ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

В роботі здійснено дослідження стратегій з виявлення в програмному забезпеченні незадокументованих закладок, які можуть бути самостійними об'єктами або частиною певного зловмисного програмного забезпечення. Місцем дослідження вибрано локальні комп'ютерні мережі. Досліджено застосування методів багатофакторного аналізу з метою виявлення незадокументованих закладок програмного забезпечення. Це дозволило застосувати результати до незадокументованих закладок програмного забезпечення, які є частинами певного зловмисного програмного забезпечення, отримані для нього шляхом використання розподіленої багаторівневої системи виявлення. В економічних дослідженнях для співставлення об'єктів, що характеризуються великою кількістю ознак, застосовують таксономічний показник рівня розвитку. У розглядуваному випадку це може бути показник наявності незадокументованих закладок програмного забезпечення в локальній мережі. В основу покладений таксонометричний метод обробки статистичних даних спостережень, який використовується в економічних дослідженнях. В розглянутому випадку в якості об'єктів виступають комп'ютерні мережі, а ознаками можуть бути наявність модулів програмного забезпечення, які не відповідають призначенню процесу; наявність елементів операційних систем, які відкриті процесом, що не відповідають призначенню процесу; висока інтенсивність операцій введення-виведення зі сторони певного процесу тощо. Результат покращення результатів виявлення було підтверджено проведеним протягом тривалого часу експерименту з виявлення незадокументованих закладок програмного забезпечення.

Ключові слова: незадокументовані закладки, програмне забезпечення, багатофакторний аналіз, зловмисне програмне забезпечення, локальна комп'ютерна мережа.

V. PAIUK , O. HEIDAROVA, V. KOSENKOV, O. SAVENKO
Khmelnytskyi National University

APPLICATION OF MULTIFACTOR ANALYSIS FOR THE PURPOSE OF DETECTING IMPLANT IN THE SOFTWARE IN LOCAL COMPUTER NETWORKS

The paper investigates strategies for detecting undocumented bookmarks in software, which may be independent objects or part of certain malicious software. Local computer networks were chosen as the place of research. The difficulty of detecting such a secretly included in the software functional object, which under certain conditions is able to provide unauthorized software influence, due to the possibility of its absence for a long time. Such an object can be part of a software package that performs tasks, replace completely certain parts of the software package, replace a certain required program. As a rule, such undocumented software bookmarks allow to store the software functions declared by the manufacturer and are realized by a part of functions which are a part of a software complex. *The application of multifactor analysis methods to detect undocumented software bookmarks has been studied. This allowed the results to be applied to undocumented software bookmarks that are part of certain malware obtained for it by using a distributed multi-level detection system. In economic research, a taxonomic indicator of the level of development is used to compare objects that are characterized by a large number of features. In this case, it may be an indicator of the presence of undocumented software bookmarks on the local network. It is based on the taxonomic method of processing statistical data of observations, which is used in economic research. In this case, the objects are computer networks, and the signs may be: the presence of software modules that do not meet the purpose of the process; the presence of elements of operating systems that are open to the process, which do not meet the purpose of the process; high intensity of input-output operations from a certain process, etc. The result of improved detection results was confirmed by a long-term experiment to detect undocumented software bookmarks.*

Keywords: implant, software, multifactor analysis, malicious software, local computer network.

Вступ. Постановка задачі

Застосування сучасних інформаційних технологій в різних сферах зростає. Це породжує активність зловмисників з метою отримати вигоду за рахунок недоліків в їх захисті. Актуальними для отримання вигоди з погляду зловмисників є організації та підприємства, в яких функціонують інформаційні технології. Одним із способів доступу зловмисників до інформаційних систем підприємств є використання незадокументованих можливостей в програмному та апаратному забезпеченні персональних комп'ютерів і периферійному обладнанні, які дозволяють здійснювати прихований несанкціонований доступ до ресурсів системи, як правило, за допомогою локальної мережі. Основне призначення незадокументованих програмних закладок – забезпечити несанкціонований доступ до конфіденційної інформації. Для виявлення таких дій і несанкціонованої активності в комп'ютерних мережах використовується багато засобів і методів [1], але можуть бути застосовні приманки [2–13].

В якості об'єкту дослідження розглядатимемо незадокументовані закладки програмного забезпечення [14], яке використовується в локальних комп'ютерних мережах підприємств (організацій). Виявлення такого таємно внесеного в програмне забезпечення функціонального об'єкту, який за певних умов здатний забезпечити несанкціонований програмний вплив [15], пов'язане з можливістю відсутності його прояву протягом тривалого часу. Такий об'єкт може бути частиною програмного комплексу, який виконує поставлені завдання, замінювати повністю певні частини програмного комплексу, замінювати

певну потрібну програму. Як правило, такі незадокументовані закладки програмного забезпечення дозволяють зберігати заявлені виробником функції програмного забезпечення і реалізуються частиною функцій, які входять до програмного комплексу.

Одним із завдань, які потребують вирішення, є розробка математичного забезпечення для методів виявлення незадокументованих закладок програмного забезпечення в локальних комп'ютерних мережах.

Основна частина

В роботі [1] наведено підхід до проведення багатофакторного аналізу з метою виявлення не задокументованих закладок програмного забезпечення (НЗПЗ) в локальній комп'ютерній мережі. В основу покладений аксонометричний метод обробки статистичних даних спостережень, який використовується в економічних дослідженнях [16, 17]. В нашому випадку в якості об'єктів виступають комп'ютерні мережі, а ознаками можуть бути [18]: наявність модулів програмного забезпечення (ПЗ), які не відповідають призначенню процесу; наявність елементів операційних систем, які відкриті процесом, що не відповідають призначенню процесу; висока інтенсивність операцій введення – виведення зі сторони певного процесу тощо (наведено 11 ознак, хоча їх кількість може бути більшою).

$$X = \begin{bmatrix} x_{11} & x_{21} & \dots & x_{1k} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2k} & \dots & x_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ x_{i1} & x_{i2} & \dots & x_{ik} & \dots & x_{in} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ x_{\omega 1} & x_{\omega 2} & \dots & x_{\omega k} & \dots & x_{\omega n} \end{bmatrix}, \quad (1)$$

де x_{ik} - кількість проявів k-тої ознаки у i-того об'єкту за період спостереження; n - кількість ознак; ω - кількість об'єктів.

Наведено, як проводиться ізотонічне та ізоморфічне (структурне) упорядкування об'єктів, метод Чекановського для дослідження підмножин на однорідність.

В економічних дослідженнях для співставлення об'єктів, що характеризуються великою кількістю ознак, застосовують таксономічний показник рівня розвитку [16]. У нашому випадку це може бути показник наявності НЗПЗ в локальній мережі. І це буде подальшим розвитком досліджень, які викладені в роботі [1].

Першим етапом є стандартизація ознак в матриці (1) і її перетворення в матрицю Z.

Найпростішим прийомом є ділення кожного значення елементу стовпця на суму елементів стовпця. Але більш поглиблений аналіз може передбачати введення ієрархії ознак за допомогою коефіцієнтів ієрархії, які дозволяють розрізняти ознаки за їх значущістю. Для цього можна застосовувати метод аналізу ієрархій [17–19]:

- експертом будується квадратна матриця $n \times n$ попарних порівнянь ознак, яка має властивість зворотної симетрії $a_{ji} = \frac{1}{a_{ij}}$;
- розраховуються власні вектори пріоритетів, для чого перемножуються усі елементи рядка і береться корінь n-ного ступеня з результату, а потім отримане число ділиться на суму таких чисел стовпця і отримуються оцінки вектора пріоритетів $(x_1, x_2, \cdots, x_n)$;
- матриця $n \times n$ перемножується на стовпчик вектора пріоритетів і отримується стовпець з $(y_1, y_2, \cdots, y_n)$, який показує ступінь важливості кожної ознаки.

Тоді до переходу від матриці X до матриці Z треба результати спостережень в матриці (1) помножити на коефіцієнти відповідно $y_к$.

В роботі [16] пропонується перехід до матриці Z у такій послідовності:

$$Z_{ik} = \frac{X_{ik} - \overline{X}_k}{S_k}, \quad (2)$$

де

$$\overline{X}_k = \frac{1}{\omega} \sum_{i=1}^{\omega} X_{ik}, \quad (3)$$

$$S_k = \left[\frac{1}{\omega} \sum_{i=1}^{\omega} \left(X_{ik} - \overline{X}_k \right)^2 \right]^{\frac{1}{2}}. \quad (4)$$

$k = 1,2, \cdots, n$; X_{ik} - значення ознаки k для одиниці i; $\overline{X}_k$ - середньоарифметичне значення ознаки k; S_k - стандартне відхилення ознаки k; Z_{ik} – стандартизоване значення ознаки k для одиниці i.

Далі формується так званий еталон розвитку, який представляє точку P_0 з координатами $Z_{01}, Z_{02}, \dots, Z_{0k}, \dots, Z_{0n}$. Ці координати представляють еталони або допустимі значення ознак.

Тоді відстань між точками-одиницями матриці Z та точкою P_0 визначається за формулою:

$$C_{i0} = \left[\sum_{k=1}^{n} \left(Z_{ik} - Z_{0k} \right)^2 \right]^{\frac{1}{2}} \quad (i = 1, \ldots, \omega). \tag{5}$$

За цими відстанями розраховується показник наявності НЗПЗ:

$$d_i^* = \frac{C_{i0}}{C_0}, \tag{6}$$

де

$$C_0 = \overline{C}_0 + 2S_0, \tag{7}$$

$$\overline{C}_0 = \frac{1}{\omega} \sum_{i=1}^{\omega} C_{i0}, \tag{8}$$

$$S_0 = \left[\frac{1}{\omega} \sum_{k=1}^{n} \left(C_{i0} - Z_{0k} \right)^2 \right]. \tag{9}$$

Показник d_i^* може знаходитися в межах 0….1. Чим ближче цей показник до нуля, тим більша ймовірність відсутності НЗПЗ у об'єкту.

Показник d_i^* служить для статичної характеристики множини об'єктів. Для більш глибокого аналізу необхідно розглянути динамічну характеристику одного об'єкту, а потім – множини об'єктів.

Тоді за результатами спостережень за декілька періодів часу формується матриця спостережень X для одного об'єкту:

$$X = \begin{bmatrix} x_{11} & x_{21} & \ldots & x_{1k} & \ldots & x_{1n} \\ x_{21} & x_{22} & \ldots & x_{2k} & \ldots & x_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ x_{i1} & x_{i2} & \ldots & x_{ik} & \ldots & x_{in} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ x_{t1} & x_{t2} & \ldots & x_{tk} & \ldots & x_{tn} \end{bmatrix}, \tag{10}$$

де x_{ik} - значення ознаки k в період i.

Далі, як було показано вище, відбувається процес стандартизації (матриця Z), будується еталон P_0.

Таксономічний показник d_i^* визначається формулою (6), де

$$C_{i0} = \left[\sum_{k=1}^{n} \left(Z_{ik} - Z_{0k} \right)^2 \right]^{\frac{1}{2}} \quad \left(i = 1, \ldots, t \right), \tag{11}$$

$$C_0 = \overline{C}_0 + 2S_0, \tag{12}$$

$$\overline{C}_0 = \frac{1}{t} \sum_{i=1}^{t} C_{i0}, \tag{13}$$

$$S_0 = \left[\frac{1}{t} \sum_{k=1}^{t} \left(C_{i0} - C_0 \right)^2 \right]^{\frac{1}{2}}. \tag{14}$$

Отже, тепер показник d_i^* описує динаміку змін наборів, що досліджуються, однак для одного об'єкту.

Тепер можна перейти до динамічної характеристики множини об'єктів. Якщо позначити матрицю спостережень об'єкту j символом X_j, то сукупна матриця для ω об'єктів залишиться у вигляді блочної матриці:

$$X_0 = [X_1, X_2, \ldots, X_j, \ldots, X_\omega]. \tag{15}$$

Враховуючи, що в мережі всі об'єкти однотипні – це комп'ютери, то еталон P_0 може залишитися з попереднього аналізу.

Узагальнений показник d_i^* визначається формулою (6), де:

$$C_{i0} = \left[\sum_{i=1}^{\omega} \sum_{k=1}^{n} \left(Z_{ik} - Z_{0k} \right)^2 \right]^{\frac{1}{2}} \quad \left(i = 1, \ldots, t \right). \tag{16}$$

C_0, $\overline{C}_0$, S_0 визначаються формулами (12), (13), (14).

Тут n – кількість ознак; ω - кількість об'єктів; Z_{ik} - стандартизоване значення ознаки k в період t.

Обчислений показник d_i^* описує процес з динамічною характеристикою усіх об'єктів. Але згідно [16] тут не враховуються напрями змін окремих складових на загальну величину показника. Тому, в роботі [16] пропонується заміна відстані C_{i0} на $C_{i0,j}$:

$$C_{i0,j} = \left[\sum_{k=1}^{n} \left(Z_{ik} - Z_{0k,j} \right)^2 \right]^{\frac{1}{2}}. \tag{17}$$

де $i = 1, 2, \ldots, t$: $j = 1, 2, \ldots, \omega$; $Z_{0k,j}$ - координати еталону розвитку об'єкту j.

Тоді залежність (16) для квадрату відстані для сукупного показника та квадратом відстані для індивідуальних показників можна записати у вигляді:

$$C_{i0}^2 = \sum_{j=1}^{\omega} C_{i0,j}^2 \ . \tag{18}$$

З урахуванням $C_{i0} = C_0 \cdot d_i^*$ та $C_{i0,j} = C_{0,j} \cdot d_{i,j}$ залежність між сукупним та індивідуальними показниками залишиться:

$$d_i^* = \frac{\sum_{j=1}^{\omega} C_{0,j}^2 \cdot d_{i,j}^*}{C_0^2}. \tag{19}$$

Отримана формула дозволяє оцінити вплив індивідуальних таксономічних показників об'єктів $d_{i,j}^*$ на загальний таксономічний показник множини об`єктів d_i^*. Тут, як і раніше, цей показник знаходиться в інтервалі (0,1).

Результат показника відносимо до одного із п'яти інтервалів, які дозволяють оцінити рівень можливої присутності НЗПЗ.

Експериментальні дослідження

Проведення експериментів було здійснено з використанням розподіленої багаторівневої системи виявлення ЗПЗ [20]. НЗПЗ було розроблено як складову кожної з типових бот-мереж. Тоді, метою експериментів була перевірка застосування методу виявлення бот-мереж, роботи класифікатору в структурі розподіленої системи та визначення залежності відсотку виявлених вузлів бот-мережі від їх представлення векторами, в складі яких були НЗПЗ. В результаті проведення експерименту отримано віднесення до потрібного підкласу та класу отриманих на основі моніторингу векторів з точністю до 66% для класифікатору без введених векторів 28 штучно згенерованих бот-мереж та 88% для класифікатору, в який попередньо було додано вектори шляхом здійснення його навчання, зберігаючи в ньому шаблони попередніх наповнень. Відсоток ознак, які були використані РБС для виявлення бот-мереж і пов'язані з проявами НЗПЗ, становить приблизно 27% від загальної кількості виявлених. Інтенсивність проявів від НЗПЗ суттєво нижче від типових проявів бот-мереж. Таким чином, НЗПЗ в складі бот-мереж можуть бути виявлені розподіленими багаторівневими системами [20] і напрям таких досліджень є перспективним.

Висновки

Незадокументовані закладки програмного забезпечення, яке використовується в локальних комп'ютерних мережах, можуть завдати значної шкоди користувачам персональних комп'ютерів, а особливо підприємствам, які експлуатують комп'ютерні мережі та використовують спеціалізоване програмне забезпечення.

Запропонований підхід до виявлення незадокументованих закладок програмного забезпечення дозволяє оцінити ступінь їх присутності. Це дало можливість за рахунок застосування багатофакторного аналізу з метою виявлення незадокументованих закладок програмного забезпечення в локальній комп'ютерній мережі покращити ефективність виявлення НЗПЗ на 4%.

Напрямком подальших досліджень є розробка методів виявлення НЗПЗ для застосування їх в розподіленій системі корпоративної мережі.

Література

1. Савенко О. С. Дослідження методів антивірусного діагностування комп'ютерних мереж / О. С. Савенко, С. М. Лисенко // Вісник Хмельницького національного університету. Технічні науки. – 2007. – № 2, т. 2. – С. 120–126.

2. Data Collection and Data Analysis in Honeypots and Honeynets. Pavol Sokol, Patrik Pekarčík, Tomáš Bajtoš. URL: http://spi.unob.cz/papers/2015/2015-19.pdf [Access 18.04.2020].

3. Study of Internet Threats and Attach Methods Using Honeypots and Honeynets. Tomas Sochor, Matej Zuzcak - Springer International Publishing Switzerland 2014, A. Kwiecie´n, P. Gaj, and P. Stera (Eds.): CN 2014, CCIS 431, pp. 118–127, 2014.

4. Sochor Tomas. Attractiveness Study of Honeypots and Honeynets in Internet Threat Detection. Tomas Sochor, Matey Zuzcak – Springer International Publishing Switzerland 2015, P. Gaj at al. (Eds.): CN 2015, CCIS 522, pp. 69–81, 2015. DOI: 10.1007/978-3-319-19419-6 7.

5. A Survey on Honeypot Software and Data Analysis. Marcin Nawrocki, Matthias Wählisch, Thomas C. Schmidt, Christian Keil, Jochen Schönfelder. arXiv:1608.06249v1 [cs.CR] 22 Aug 2016. URL: https://arxiv.org/abs/1608.06249 [Access 26.03.2020]

6. Composite Hybrid Techniques for Defending Against Targeted Attacks. S. Sidiroglou, A.D. Keromytis. Part of the Advanced in Information Security book series (ADIS, volume 27), 2007, 213-229 pp.

7. Shadow Honeypots. K.G. Anagnostakis, S. Sidiroglou, M. Polychronakis, A.D. Keromytis, P. Markatos. International Journal of Computer and Network Security, Vol. 2, No. 9, September 2010, 16 p.

8. POSTER: Dragging Attackers to Honeypots for Effective Analysis of Cyber Threats. Martin Husak, Jan Vykopal. URL: https://is.muni.cz/repo/1188174/POSTER-Dragging_Attackers_to_Honeypots_for_Effective_Analysis_of_Cyber_Threats.pdf [Access 30.05.2020]

9. Effective Proactive and Reactive Defense Strategies against Malicious Attacks in a Virtualized Honeynet. Frank Yeong-Sung Lin, Yu-Shun Wang, Ming-Yang Huang. Journal of Applied Mathematics, Vol. 2013, Article ID 518213, 11 pages. URL: https://www.hindawi.com/journals/jam/2013/518213/ [Access 10.04.2020]

10. Automatic Identification of Honeypot Server Using Machine Learning Techniques. Cheng Huang, Jiaxuan Han, Xing Zhang, Jiayong Liu. Hindawi, Security and Communication Networks Volume 2019, Article ID 2627608, 8 pages.

11. Survey of Attach Projection, Prediction, and Forecasting in Cyber Security. Martin Husak, Jana Komarkova, Elias Bou-Harb, Pavel Celeda. IEEE Communication Survays & Tutorials – September 2018, URL: https://www.researchgate.net/publication/327449459_Survey_of_Attack_Projection_Prediction_and_Forecasting_in_Cyber_Security [Access 12.05.2020]

12. Honeypots and Routers: Collecting Internet Attacks. Mohssen Mohammed, Habib-ur Rehman – CRC Press, Taylor & Francis Group LLC, 2016. 197p.

13. Honeypots. A new Paradigm to Information Security. R.C. Joshi, Anjali Sardana - Science Publishers, P.O. Box 699, Enfield, NH 03748, USA, 2011. 323 p.

14. Савенко О.С. Моделі незадокументованих закладок програмного забезпечення в локальних комп'ютерних мережах / О. С. Савенко, В. П. Паюк, Б. О. Савенко, А.С. Каштальян // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2019. – № 2. – С. 84–90.

15. Савенко О.С. Дослідження та аналіз блокування процесів в комп'ютерній системі / О.С. Савенко, Ю.П. Кльоц, С.В. Мостовий // Вісник Хмельницького національного університету. – 2007. – № 3, Том 1. – С. 248–251.

16. Плюта В. Сравнительный многомерный анализ в экономических исследованиях: методы таксономии и факторного анализа / Плюта В. ; пер. с пол. – М. : Статистика,1980. – 151 с., ил.

17. Игумнов Б.Н. Кибернетические основы построения экономических систем для предприятий : уч. пособие / Игумнов Б.Н., Завгородняя Т.П. – Хмельницкий : ТУП, 2000. – 344 с.

18. Саати Г. Аналитическое планирование. Организация систем / Саати Г., Керно К. ; пер.с англ. – М. : Радио и свіязь, 1991. – 224 с.

19. Андрейчиков А.В. Анализ, синтез, планирование решений в экономике : уч. пособие / Андрейчиков А.В., Андрейчикова О.Н. – М. : Финансы и статистика, 2001. – 368 с.

20. Савенко О.С. Оцінки ефективності та достовірності розподілених систем виявлення зловмисного програмного забезпечення в комп'ютерних системах локальних мережах / О.С. Савенко, А.О. Нічепорук, В.П. Паюк // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – 2019. – № 36. – С. 134–139.

References

1. Savenko O.S. Research of methods of antiviral diagnostics of computer networks / O.S. Savenko, S.M. Lysenko // Herald of Khmelnytskyi National University. Technical sciences. – 2007. – Issue 2, vol. 2. – P. 120–126.

2. Data Collection and Data Analysis in Honeypots and Honeynets. Pavol Sokol, Patrik Pekarčík, Tomáš Bajtoš. URL: http://spi.unob.cz/papers/2015/2015-19.pdf [Access 18.04.2020].

3. Study of Internet Threats and Attach Methods Using Honeypots and Honeynets. Tomas Sochor, Matej Zuzcak - Springer International Publishing Switzerland 2014, A. Kwiecie´n, P. Gaj, and P. Stera (Eds.): CN 2014, CCIS 431, pp. 118–127, 2014.

4. Sochor Tomas. Attractiveness Study of Honeypots and Honeynets in Internet Threat Detection. Tomas Sochor, Matey Zuzcak – Springer International Publishing Switzerland 2015, P. Gaj at al. (Eds.): CN 2015, CCIS 522, pp. 69–81, 2015. DOI: 10.1007/978-3-319-19419-6 7.

5. A Survey on Honeypot Software and Data Analysis. Marcin Nawrocki, Matthias Wählisch, Thomas C. Schmidt, Christian Keil, Jochen Schönfelder. arXiv:1608.06249v1 [cs.CR] 22 Aug 2016. URL: https://arxiv.org/abs/1608.06249 [Access 26.03.2020]

6. Composite Hybrid Techniques for Defending Against Targeted Attacks. S. Sidiroglou, A.D. Keromytis. Part of the Advanced in Information Security book series (ADIS, volume 27), 2007, 213-229 pp.

7. Shadow Honeypots. K.G. Anagnostakis, S. Sidiroglou, M. Polychronakis, A.D. Keromytis, P. Markatos. International Journal of Computer and Network Security, Vol. 2, No. 9, September 2010, 16 p.

8. POSTER: Dragging Attackers to Honeypots for Effective Analysis of Cyber Threats. Martin Husak, Jan Vykopal. URL: https://is.muni.cz/repo/1188174/POSTER-Dragging_Attackers_to_Honeypots_for_Effective_Analysis_of_Cyber_Threats.pdf [Access 30.05.2020]

9. Effective Proactive and Reactive Defense Strategies against Malicious Attacks in a Virtualized Honeynet. Frank Yeong-Sung Lin, Yu-Shun Wang, Ming-Yang Huang. Journal of Applied Mathematics, Vol. 2013, Article ID 518213, 11 pages. URL: https://www.hindawi.com/journals/jam/2013/518213/ [Access 10.04.2020]

10. Automatic Identification of Honeypot Server Using Machine Learning Techniques. Cheng Huang, Jiaxuan Han, Xing Zhang, Jiayong Liu. Hindawi, Security and Communication Networks Volume 2019, Article ID 2627608, 8 pages.

11. Survey of Attach Projection, Prediction, and Forecasting in Cyber Security. Martin Husak, Jana Komarkova, Elias Bou-Harb, Pavel Celeda. IEEE Communication Survays & Tutorials – September 2018, URL: https://www.researchgate.net/publication/327449459_Survey_of_Attack_Projection_Prediction_and_Forecasting_in_Cyber_Security [Access 12.05.2020]

12. Honeypots and Routers: Collecting Internet Attacks. Mohssen Mohammed, Habib-ur Rehman – CRC Press, Taylor & Francis Group LLC, 2016. 197p.

13. Honeypots. A new Paradigm to Information Security. R.C. Joshi, Anjali Sardana - Science Publishers, P.O. Box 699, Enfield, NH 03748, USA, 2011. 323 p.

14. Savenko O.S., Payuk V.P., Savenko B.O., Kashtalyan A.S. Models of undocumented software bookmarks in local computer networks. Measuring and computing equipment in technological processes. 2019. № 2. P. 84–90.

15. Savenko O.S., Klots Y.P, Mostoviy S.V. Research and analysis of process blocking in a computer system // Herald of Khmelnytskyi National University. 2007. Issue 3, Volume 1. – P. 248-251.

16. Pluta V. Comparative multidimensional analysis in economic research: methods of taxonomy and factor analysis / Per. s pol. - M.: Statistics, 1980. – 151 p.

17. Igumnov B.N., Zavgorodnyaya T.P. Cybernetic bases of construction of economic systems for the enterprises. Khmelnitsky: TUP, 2000. 344p.

18. Saati G., Kerno K. Analytical planning. Organization of systems: Translated from English. M.: Radio and communication, 1991. 224 p.

19. Andreychikov A.V., Andreychikova O.N. Analysis, synthesis, planning solutions in economics. M.: Finance and Statistics, 2001. 368 p.

20. Savenko O.S., Nicheporuk A.O., Paiuk V.P. Estimates of efficiency and reliability of distributed malware detection systems in computer systems of local networks // Computer-integrated technologies: education, science, production, № 36, 2019. P. 134–139.

Надійшла / Paper received : 16.10.2020 Надрукована/Printed :27.11.2020