РОЗДІЛ ІІ. ІНФОРМАЦІЙНО-КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ

УДК 004.056
DOI: 10.25140/2411-5363-2020-2(20)-109-115

Марина Синенко, Юлія Ткач

МАТЕМАТИЧНА МОДЕЛЬ МЕТОДІВ АКТИВНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Актуальність теми дослідження. *Бурхливий розвиток ІТ-технологій та інтенсивна інформатизація всіх сфер суспільства веде до появи нових інформаційних загроз, тому інформаційна безпека є однією з найбільш важливих завдань ІТ-індустрії. Важливим елементом у процесі розроблення нових методів захисту інформації є їх апробація за допомогою математичних моделей.*

Постановка проблеми. *Перспективним напрямом у сфері захисту інформації є розробка активних методів забезпечення захисту, серед яких можна виділити, наприклад, упереджуючий удар, контратаку, дезінформування. Побудова математичних моделей таких методів є важливим етапом на шляху вироблення концепції активного захисту.*

Аналіз останніх досліджень і публікацій. *У сучасних дослідженнях значне місце посідають математичні моделі інформаційної безпеки, зокрема, з використанням марківських процесів, які дозволяють розв'язати широкий спектр прикладних задач, а саме, виявлення кібератак, виявлення вторгнення в комп'ютерні системи. За допомогою математичних моделей розв'язують задачі оптимізації та підвищення надійності захисту інформаційних систем.*

Виділення недосліджених частин загальної проблеми. *Нині в роботах вітчизняних та закордонних учених недостатньо уваги приділяється розробці математичних моделям методів активного захисту інформації, що не дозволяє повною мірою продемонструвати ефективність цих методів.*

Постановка завдання. *Мета статті полягає в розробці та аналізі математичної моделі методів активного захисту інформаційних систем.*

Виклад основного матеріалу. *З використанням ймовірнісного формалізму «розорення гравців» побудована та досліджена математична модель для методу активного захисту інформації. На основі побудованої моделі розроблені рекомендації щодо значення параметрів моделі для забезпечення надійності захисту.*

Висновки відповідно до статті. *У роботі досліджена математична модель методів активного захисту інформації з використанням формалізму «розорення гравців», знайдені оцінки для параметрів системи захисту, які забезпечують певну його надійність.*

Ключові слова: *ймовірність; математична модель; методи активного захисту інформації.*
Рис.: 3. Табл.: 1. Бібл.: 9.

Актуальність теми дослідження. Бурхливий розвиток ІТ-технологій та інтенсивна інформатизація усіх сфер суспільства веде до появи нових інформаційних загроз, тому нині інформаційна безпека є однією з найбільш важливих задач ІТ-індустрії. Створення надійних систем захисту інформації експериментальним шляхом здебільшого вимагає значних матеріальних та часових затрат, тому важливим елементом розробки методів захисту інформаційних систем є їх апробація з використанням математичного моделювання. Оскільки інформаційні загрози мають переважно ймовірнісний характер, то при моделюванні засобів захисту інформаційних систем (ІС) доцільно використовувати математичний апарат теорії ймовірності, зокрема, випадкових процесів.

Постановка проблеми. На сьогодні загальноприйняті підходи захисту інформаційних систем (ЗІС) ставлять за мету нейтралізацію або мінімізацію наслідків інформаційних вторгнень (атак). Такі методи прийнято називати пасивними методами захисту. Однак перспективним напрямом у сфері захисту інформації є розробка активних методів забезпечення ЗІ, серед яких можна виділити, наприклад, упереджуючий удар, контратаку, дезінформування. Розробка математичних моделей активних методів захисту інформації є важливим етапом на шляху вироблення певної концепції таких підходів.

Аналіз останніх досліджень та публікацій. У сучасних дослідженнях значне місце посідають математичні моделі інформаційної безпеки з використанням марківських процесів, оскільки спектр прикладних задач, які можна розв'язати в такий спосіб, досить широкий. Так, у роботах [1-3] вивчається виявлення кібератак, у роботах [4; 5] досліджується виявлення вторгнення в комп'ютерні системи. У роботах, присвячених криптозахисту, ви-

користовують моделі з прихованим марківським процесом [6]. За допомогою математичних моделей розв'язують задачі оптимізації та підвищення надійності захисту інформаційних систем [7]. Питання активного захисту інформації розглядались у роботах [8; 9].

Виділення недосліджених частин загальної проблеми. Нині в роботах вітчизняних та зарубіжних вчених недостатньо уваги приділяється розробці математичних моделям методів активного захисту інформації, що не дозволяє повною мірою продемонструвати ефективність цих методів.

Мета статті. Мета статті полягає в розробці та аналізі математичної моделі методів активного захисту інформаційних систем.

Виклад основного матеріалу. Нехай задачі активного захисту інформаційних систем вирішуються програмно-апаратними засобами, які будемо називати серверами активного захисту (САЗ). Будемо вважати, що разом із засобами пасивного захисту такі сервери можуть виконувати такі функції: ідентифікація атакуючої системи з використанням засобів комп'ютерної розвідки, вибір видів та засобів реалізації інформаційних атак, розкриття засобів захисту суперника.

Розглянемо математичну модель протидії серверів активного захисту сторін A та B, використовуючи формалізм «задачі про розорення гравців» [9].

Будемо припускати, що до початку протидії сторона A мала в наявності n, а сторона B відповідно m захисних ресурсів (САЗ). Результатом кожної атаки, які будемо вважати незалежними, є захват одного із САЗ суперника, причому захоплений сервер також може бути використаний для нанесення збитків його попередньому власнику. Атаки можуть продовжуватись до повної втрати САЗ однією зі сторін протиборства.

Позначимо p та q ймовірності успішних атак сторін A та B відповідно. Нехай щодо p і q виконуються такі умови:

$$0 < p < 1;\ 0 < q < 1;\ p + q = 1.$$

Виконання строгих нерівностей для p і q означає припущення про відсутність нічиїх при атаках на ІС.

Для аналізу ефективності застосування засобів активного захисту при заданих значеннях параметрів p, q, m, n обчислимо ймовірність поразки, наприклад, сторони A. Під поразкою будемо розуміти, що сторона втрачає всі наявні в неї САЗ.

Позначимо ймовірності поразки сторін A та B відповідно P_n, Q_m. (Тут індекси n та m вказують на наявність у сторін САЗ, що діють у їхніх інтересах перед початком протидії.) Нехай перед початком деякої атаки сторона A мала в наявності r серверів активного захисту, діючих у її інтересах, тоді отримати поразку сторона A може двома способами: або наступна атака буде успішною, а всі інші сторона A програє, або вона програє як наступну атаку, так і все протистояння. Тоді, використовуючи формулу повної ймовірності, маємо:

$$P_r = pP_{r+1} + qP_{r-1} \Leftrightarrow pP_{r+1} - P_r + qP_{r-1} = 0. \quad (1)$$

Рівняння (1) є лінійним однорідним різницевим рівнянням другого порядку. Щоб знайти загальний розв'язок (1), запишемо його характеристичне рівняння:

$$p\lambda^2 - \lambda + q = 0, \quad (2)$$

корені якого $\lambda_1 = 1;\ \lambda_2 = {}^{q}/_{p}$. У припущенні, що $p \neq q$, загальний розв'язок різницевого рівняння (1) має вигляд:

$$P_r = C_1 + C_2\left(\frac{q}{p}\right)^r. \quad (3)$$

Для визначення констант C_1, C_2 розглянемо граничні умови: $P_0 = 1, P_{n+m} = 0$, які є цілком природніми, оскільки відсутність ресурсів для захисту у сторони A означає її цілковиту поразку (достовірна подія), аналогічно, якщо сторона A зосередить у собі всі засоби захисту, то це унеможливить її поразку (неможлива подія). Таким чином, маємо:

$$\begin{cases} P_0 = & C_1 + C_2 = 1; \\ P_{n+m} = & C_1 + \left(\frac{q}{p}\right)^{n+m} = 0. \end{cases} \quad (4)$$

Звідки отримуємо

$$C_1 = -\frac{\left(\frac{q}{p}\right)^{n+m}}{1-\left(\frac{q}{p}\right)^{n+m}};\ C_2 = \frac{1}{1-\left(\frac{q}{p}\right)^{n+m}},$$

і, відповідно,

$$P_r = \frac{\left(\frac{q}{p}\right)^{n+m} - \left(\frac{q}{p}\right)^{r}}{\left(\frac{q}{p}\right)^{n+m} - 1}. \quad (5)$$

Тоді

$$P_n = \frac{1-\left(\frac{p}{q}\right)^{m}}{1-\left(\frac{p}{q}\right)^{n+m}}\ ; \quad (6)$$

$$Q_m = 1 - P_n = \frac{1-\left(\frac{q}{p}\right)^{n}}{1-\left(\frac{q}{p}\right)^{n+m}}. \quad (7)$$

У випадку, коли $p = q = 0{,}5$, загальний розв'язок рівняння (1) записується у вигляді:

$$P_r = C_1 + C_2 r. \quad (8)$$

З урахуванням початкових умов маємо: $P_r = 1 - \frac{r}{n+m}$, і, відповідно,

$$P_n = 1 - \frac{n}{n+m} = \frac{m}{n+m}. \quad (9)$$

Проаналізуємо отримані вирази для ймовірностей поразки сторін. Слід зазначити, що при $p = q = 0{,}5$ перевага тієї чи іншої сторони при активному захисті ІС повністю визначається перевагами в технічному оснащенні.

Для надійності роботи систем захисту інформації важливо підібрати параметри системи таким чином, щоб ймовірність поразки не перевищувала деякого наперед заданого значення α. Наприклад, при $p = q$, щоб виконувалась нерівність $P_n \le \alpha$, число САЗ повинно задовольняти нерівність:

$$n \ge \left[\frac{(1-\alpha)m}{\alpha}\right] + 1,$$

($[x]$ означає цілу частину числа).

Нехай $p \ne q$. Графіки залежності ймовірності P_n від величини $u = \frac{p}{q}, u \ne 1$ при різних, але фіксованих m та n наведені на рис. 1. Перший графік відповідає випадку $n = 4; m = n$, другий – $n = 4; m = 2n$.

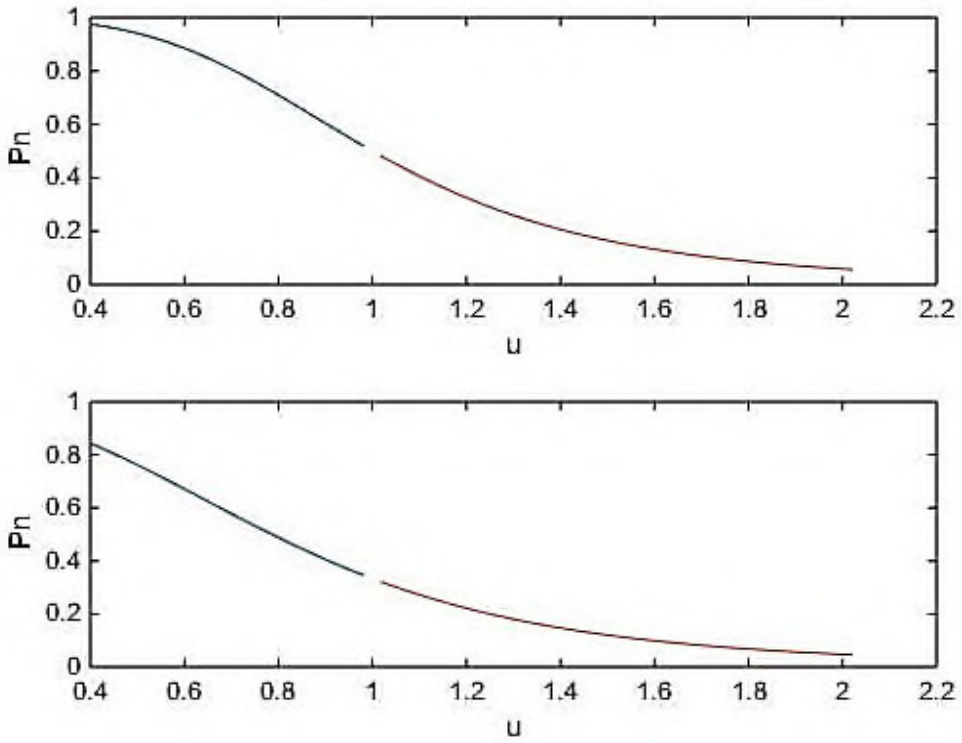

Рис. 1. Графік залежності ймовірності поразки P_n від величини $u = {}^{p}/_{q}, n = m = 4,\ n = 4; m = 2n$

Розглянемо детальніше випадок $p > q$. Зазначимо, що $P_n \sim \left(\frac{q}{p}\right)^n$, якщо $m \sim \infty$. Це означає, що при $p > q$ сторона A може отримати перемогу, навіть якщо кількість САЗ противника значно перевищує ресурси сторони A, $m \gg n$. (Графіки залежностей P_n від величини $u = \frac{p}{q}$ при $p > q$ і $m > n$ наведений на рис. 2).

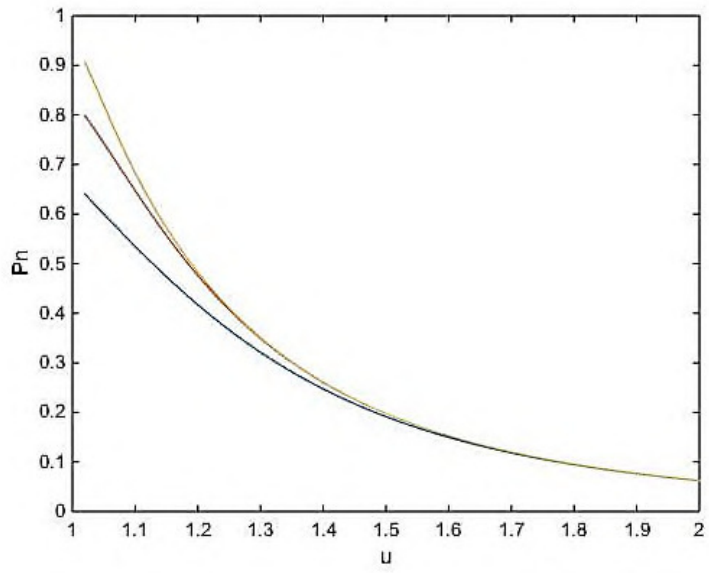

Рис. 2. Графік залежності ймовірності поразки P_n від величини $u = \frac{p}{q}, p > q, n = 4, \frac{m}{n} = k$ для $k = 2; 5; 20$

Нехай $\frac{m}{n} = k, k > 1$, що означає перевагу в технічній оснащеності сторони B порівняно з A у k разів. Визначимо, за яких p у такій ситуації буде виконуватись нерівність $P_n \leq \alpha$.

$$P_n = \frac{1 - \left(\frac{p}{q}\right)^m}{1 - \left(\frac{p}{q}\right)^{n+m}} = \frac{1 - \left(\frac{p}{q}\right)^{kn}}{1 - \left(\frac{p}{q}\right)^{(k+1)n}}.$$

Позначивши $x = \left(\frac{p}{q}\right)^n$, маємо:

$$P_n \leq \alpha \Leftrightarrow \frac{1 - x^k}{1 - x^{k+1}} \leq \alpha \Leftrightarrow \frac{\alpha x^{k+1} - x^k + 1 - \alpha}{1 - x^{k+1}} \leq 0. \quad (10)$$

Оскільки у даних припущеннях $1 - x^{k+1} < 0$, то нерівність (10) рівносильна нерівності:

$$\alpha x^{k+1} - x^k + 1 - \alpha \geq 0 \Leftrightarrow x^k(\alpha x - 1) \geq \alpha - 1. \quad (11)$$

Права частина нерівності (11) від'ємна, тому (11) гарантовано буде виконуватись за умови $\alpha x - 1 \geq 0$. З останньої нерівності маємо:

$$\frac{p}{q} \geq \sqrt[n]{\alpha^{-1}} \Leftrightarrow p \geq \frac{1}{1 + \sqrt[n]{\alpha}}.$$

Отже, треба відзначити, що при великих значеннях p перевага в технічній оснащеності сторони B нівелюється. Деякі значення ймовірності p при заданих значеннях n і α наведені в таблиці.

Таблиця 1

Значення ймовірності p залежно від α та n.

	$n = 4$					$n = 8$				
α	0,1	0,2	0,3	0,4	0,5	0,1	0,2	0,3	0,4	0,5
p	0,640	0,599	0,57	0,557	0,543	0,572	0,550	0,538	0,529	0,522

Якщо $p < q$ (рис. 3), то ймовірність поразки сторони A можна намагатись зменшити за рахунок збільшення n, але в цьому випадку можливості A обмежені, оскільки при $n \sim \infty$,

$$P_n \sim 1 - \left(\frac{p}{q}\right)^m.$$

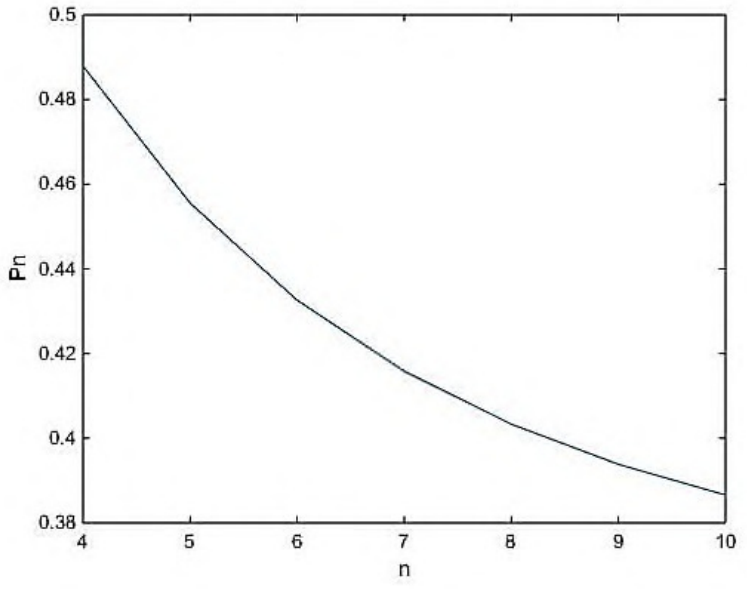

Рис. 3. Графік залежності ймовірності P_n від n, у випадку $p < q$

Висновки відповідно до статті. У роботі досліджена математична модель методів активного захисту інформації з використанням формалізму «розорення гравців», знайдені оцінки для параметрів системи захисту, які забезпечують певну його надійність. Отримані наступні результати: якщо ймовірності успішної атаки кожної з протидіючих сторін рівні ($p = q = 0{,}5$), то переваги сторін повністю визначаються їх технічною оснащеністю; якщо $p > q$, то сторона A може отримати перемогу, навіть у випадку, коли протидіюча сторона значно переважає у технічному оснащенні; якщо $p < q$, то сторона A може збільшити ймовірність перемоги за рахунок технічного оснащення, але в цьому випадку її можливості суттєво обмежені. Розглянута математична модель допускає подальший розвиток, якщо припустити, що одна із протидіючих сторін може «навчатися» у процесі протидії і, відповідно, збільшувати ймовірність успіху.

Список використаних джерел

1. Ye N. et al. Robustness of the Markov-Chain Model for Cyber-Attack Detection. *IEEE Transactions on Reliability*. 2004. Vol. 53:1. P. 116-123.

2. Fava D. et al. Projecting Cyberattacks through Variable-Length Markov Models. *IEEE Transactions on Information Forensics and Security*. 2008. Vol. 3:3. P. 359-369.

3. Pietre-Cambacedes L., Bouissou M. Beyond Attack Trees: Dynamic Security Modeling with Boolean Logic Driven Markov Processes (BDMP). *Proceedings of the 2010 European Dependable Computing Conference*, IEEE Computer Society, 2010. P. 199-208.

4. Kovalev S. M., Sukhanov A. V. Anomaly detection based on Markov chain model with production rules. *Software and Systems*. 2014. Vol. 107:3. P. 40–43.

5. Austin T. H. et al. Exploring Hidden Markov Models for Virus Analysis: a Semantic Approach. *Proceedings of the 2013 46th Hawaii International Conference on System Sciences*, IEEE Computer Society. 2013. P. 5039-5048.

6. Математические модели распространения вирусов в компьютерных сетях различной структуры / Далингер Я. М. и др. *Информатика и системы управления*. 2011. № 4. С. 3–11.

7. Щеглов К. А., Щеглов А. Ю. Марковские модели угрозы безопасности информационной системы. *Известия высших учебных заведений. Приборостроение*. 2015. № 58:12. С. 957–965.

8. Тутубалин П. И., Моисеев В. С. Вероятностные модели обеспечения информационной безопасности автоматизированных систем обработки информации и управления : монография. Казань : Изд. РИЦ «Школа», 2008. 144 с.

9. Гнеденко Б. В. Курс теории вероятностей. Москва : Наука. 1988. 488 с.

References

1. Ye, N. et al. (2004). Robustness of the Markov-Chain Model for Cyber-Attack Detection. *IEEE Transactions on Reliability*, 53:1, 116-123.

2. Fava, D. et al. (2008). Projecting Cyberattacks through Variable-Length Markov Models. *IEEE Transactions on Information Forensics and Security*, 3:3, 359-369.

3. Pietre-Cambacedes L., Bouissou M. (2010). Beyond Attack Trees: Dynamic Security Modeling with Boolean Logic Driven Markov Processes (BDMP). *Proceedings of the 2010 European Dependable Computing Conference*, IEEE Computer Society, P. 199-208.

4. Kovalev, S. M., Sukhanov, A. V. (2014). Anomaly detection based on Markov chain model with production rules", *Software and Systems*, 107:3, 40–43.

5. Austin, T. H. et al. (2013). Exploring Hidden Markov Models for Virus Analysis: a Semantic Approach. *Proceedings of the 2013 46th Hawaii International Conference on System Sciences*. IEEE Computer Society (pp. 5039-5048).

6. Dalinger, Ya. M. et al. (2011). Matematicheskie modeli rasprostraneniia vyrusov v kompiuternykh setiakh razlichnoi struktury [The mathematical models of the spreading of viruses in computer networks with the diferent structures]. *Informatika i sistemy upravlenyia – Information Science and Control Systems*, 4, 3-11 [in Russian].

7. Shcheglov, K. A., Shcheglov, A. Yu. (2015). Markovskie modeli uhrozy bezopasnosti informatsionnoi sistemy [Markov models for informational system security threat]. *Izvestiia Vysshykh Uchebnykh Zavedeniy. Priborostroenie – News of higher educational institutions. Instrumentation*, 58:12, 957-965.

8. Tutubalin, P. I., Moiseev, V. S. (2008). *Veroiatnostnye modeli obespecheniia informatsionnoi bezopasnosti avtomatizirovannykh sistem obrabotki informatsii i upravleniia [Probabilistic Models for Ensuring Information Security of Automated Information Processing and Control Systems]*. Kazan: Publishing House RITS «Schol» [in Russian].

9. Gnedenko, B. V. (1988). *Kurs teoryy veroiatnostei [Probability Theory]*. Moscow: Science [in Russian].

UDC 004.056

Maryna Synenko, Yuliia Tkach

MATHEMATICAL MODEL OF ACTIVE INFORMATION PROTECTION METHODS

Urgency of the research. *Rapid development of IT-technologies and intensive informing of all spheres of society leads to emergence of new information threats, which is why information security is one of the most important tasks of the IT-industry. An important element in the process of developing new methods of information security is their testing through mathematical modeling.*

Target setting *A promising area in the field of information security is the development of active security methods, which include, for example, pre-emptive strike, counterattack, misinformation. The construction of mathematical models of such methods is an important step in the development of the concept of active protection.*

Actual scientific researches and issues analysis. *In modern studies, mathematical models of information security take a significant role, in particular, using Markov processes, which allow to solve a wide range of applied problems, namely, detection of cyberattacks, detection of invasion of computer systems. Mathematical models solve the problems of optimizing and improving the security of information systems.*

Uninvestigated parts of general matters defining. *Currently, in the works of domestic and foreign scientists, insufficient attention is paid to the development of mathematical models of active information protection methods, which does not allow to fully demonstrate these methods effectiveness.*

The research objective.*The purpose of the article is to develop and analyze a mathematical model of active methods of information systems protection.*

The statement of basic materials. *Using the probable formalism of "player ruin", a mathematical model for the method of active protection of information was constructed and investigated. Based on the model built, recommendations for the value of model parameters were developed to provide security protection.*

Conclusions.*The mathematical model of the active methods of information protection using the "player ruin" formalism is investigated, the estimates for the parameters of the security system providing its certain reliability are found.*

Keywords: *probability; mathematical model; methods of active protection of information.*

Fig.: 3. Table: 1. References: 9.

Синенко Марина Анатоліївна – кандидат фізико-математичних наук, доцент, доцент кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Synenko Maryna – PhD of Physical and Mathematical Sciences, Associate Professor, Associate Professor of the Department of Cybernetic Protection and Mathematical Modeling, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: mara.a.snnk@gmail.com
ORCID: https://orcid.org/0000-0002-8961-533X
Scopus ID: 6504542623

Ткач Юлія Миколаївна – доктор педагогічних наук, доцент, завідувач, професор кафедри кібербезпеки та математичного моделювання, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
Tkach Yulia – Doctor of Pedagogical Sciences, Associate Professor, Head, Professor, Department of Cybersecurity and Mathematical Modeling, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
E-mail: tkachym79@gmail.com
ORCID: http:/orcid.org/0000-0002-8565-0525

Синенко М., Ткач Ю. Математична модель методів активного захисту інформації. *Технічні науки та технології.* 2020. № 2 (20). С. 109-115.