УДК 004.056.53
DOI https://doi.org/10.32782/IT/2024-4-1

Валентина АБЛАМСЬКА
викладач кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе, 210, м. Київ, Україна, 02121
ORCID:*0000-0003-0768-4102*

Наталія ДЯЧЕНКО
кандидат наук з державного управління,доцент кафедри кібербезпеки, інформаційних технологій та економіки, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе, 210, м. Київ, Україна, 02121
ORCID: *0000-0002-4306-7665*

Валентин ГАЛУНЬКО
доктор філософії з галузі права, доцент кафедри адміністративного права, інтелектуальної власності та цивільно-правових дисциплін, Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія», Харківське шосе, 210, Київ, Україна, 02121,
ORCID: *0000-0002-8133-6766*

Бібліографічний опис статті: Абламська, В., Дяченко, Н., Галунько, В. (2024). Математичне моделювання вразливості інформаційної системи та прогнозування можливостей її захисту. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 4, 3–8, doi: https://doi.org/10.32782/IT/2024-4-1

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ВРАЗЛИВОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ ТА ПРОГНОЗУВАННЯ МОЖЛИВОСТЕЙ ЇЇ ЗАХИСТУ

Проблематику статті присвячено дослідженню застосування математичних моделей для аналізу та вдосконалення роботи систем кібербезпеки та захисту інформації. Актуальність роботи зумовлена сучасними викликами цифрової епохи, коли інформаційні системи стають об'єктами численних новітніх атак (електронний скіммінг, фішинг, шкідливе програмне забезпечення (Malware), атаки типу DDoS та міжсайтовий скриптинг (XSS), спрямованих на викрадення, знищення, пошкодження або компрометацію даних. Особливу увагу приділено використанню диференціальних рівнянь та систем диференціальних рівнянь до моделювання роботи системи захисту, що дозволяє проаналізувати взаємодію атакуючих суб'єктів (зловмисників) та захисних систем, враховуючи нерівномірність кількості атак та динамічний характер загроз.

Наукова стаття обґрунтовує доцільність застосування диференціальних рівнянь для опису динамічних змін у системах кібербезпеки. Зокрема, запропоновано методику аналізу обсягу та інтенсивності атак за певний період часу (для короткотермінового прогнозу, який є залежним від початкових показників системи) для визначення продуктивності системи захисту даних. В даному контексті розглянуто застосовність диференціальних рівнянь та систем диференціальних рівнянь для оцінки ефективності поточних заходів кіберзахисту, що дозволяє прогнозувати при зміні потенційних інцидентів рівень забезпечення оперативної реакції на загрози.

Метою роботи *є огляд і оцінка місця диференціальних рівнянь та систем диференціальних рівнянь в моделюванні роботи системи захисту інформації.*

Методологія. *В рамках дослідження проведено моделювання реагування системи захисту інформації на несанкціонований вплив ззовні на об'єкти збереження інформації. Продемонстровано можливості та роль математичного моделювання у визначенні необхідного обсягу ресурсів, їх потенціалу для забезпечення стабільної роботи інформаційних систем. Розроблені підходи дозволяють адаптувати методи протидії до характеру та кількості загроз, включаючи застосування різноманітних програмних засобів, оптимізацію кількості інструментів чи методів для підвищення якісних характеристик систем.*

Наукова новизна *цього дослідження полягає у використанні математичного методу диференціальних рівнянь для оцінки ефективності системи захисту інформації та короткострокове прогнозування на основі отриманих результатів.*

Висновки. *Отримані результати мають практичне призначення (для діагностики спроможності системи кібербезпеки запобіганню несанкціонованого впливу) і можуть бути використані для подальшої розробки нових алгоритмів забезпечення кібербезпеки, оптимізації роботи захисних систем та підвищення їх ефективності в умовах постійно змінюваного кіберландшафту.*

Ключові слова: *кібербезпека, математична модель, диференціальні рівняння, системи диференціальних рівнянь, атака, протидія, прогноз.*

Valentyna ABLAMSKA
Lecturer at the Department of Cybersecurity, Information Technology and Economics, Kyiv University of Intellectual Property and Law of the National University «Odessa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121
***ORCID:** 0000-0003-0768-4102*

Natalia DIACHENKO
Candidate of Public Administration Sciences, Associate Professor at the Department of Cybersecurity, Information Technology and Economics, Kyiv University of Intellectual Property and Law of the National University «Odessa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121
***ORCID:** 0000-0002-4306-7665*
***Scopus-Author ID:** 57216565101*

Valentyn HALUNKO
PhD in law, Associate Professor at the Department of Administrative Law, Intellectual Property and Civil-Law Disciplines, Kyiv University of Intellectual Property and Law of the National University «Odessa Law Academy», 210, Kharkivske highway, Kyiv, Ukraine, 02121, valentinvalentin0987@gmail.com
***ORCID:** 0000-0002-8133-6766*

To cite this article: Ablamska, V., Diachenko, N., Halunko, V. (2024). Matematychne modeliuvannia vrazlyvosti informatsiinoi systemy ta prohnozuvannia mozhlyvostei yii zakhystu [Mathematical modeling of the vulnerability of the information system and forecasting the possibilities of its protection]. Information Technology: Computer Science, Software Engineering and Cyber Security, 4, 3–8, doi: https://doi.org/10.32782/IT/2024-4-1

MATHEMATICAL MODELING OF THE VULNERABILITY OF THE INFORMATION SYSTEM AND FORECASTING OF ITS PROTECTION POSSIBILITIES

The issue of the article is devoted to the study of the application of mathematical models for the analysis and improvement of the work of cyber security and information protection systems. The relevance of the work is determined by the modern challenges of the digital age, when information systems become the objects of numerous modern attacks (electronic skimming, phishing, malicious software (Malware), DDoS attacks and cross-site scripting (XSS), aimed at theft, destruction, damage or compromise data. Special attention is paid to the use of differential equations and systems of differential equations to model the operation of the protection system, which allows analyzing the interaction of attacking subjects (criminals) and protective systems, taking into account the uneven number of attacks and the dynamic nature of threats.

The scientific article substantiates the feasibility of using differential equations to describe dynamic changes in cyber security systems. In particular, a technique for analyzing the volume and intensity of attacks for a certain period of time (for a short-term forecast that is dependent on the initial indicators of the system) is proposed to determine the performance of the data protection system.In this context, the applicability of differential equations and systems of differential equations for evaluating the effectiveness of current cyber protection measures is considered, which allows predicting the level of ensuring operational response to threats when potential incidents change.

***The objective** of the work is to review and evaluate the place of differential equations and systems of differential equations in modeling the operation of the information protection system.*

***Methodology.** As part of the study, a simulation of the response of the information protection system to unauthorized external influence on information storage facilities was carried out. The capabilities and role of mathematical modeling in determining the required amount of resources and their potential to ensure the stable operation of information systems are demonstrated. The developed approaches make it possible to adapt countermeasures to the nature and number of threats, including the use of various software tools, optimization of the number of tools or methods to improve the quality characteristics of systems.*

***The novelty** of this study is to use the mathematical method of differential equations to evaluate the effectiveness of the information protection system and short-term forecasting based on the obtained results.*

***The results.** The obtained results have a practical purpose (to diagnose the ability of the cyber security system to prevent unauthorized influence) and can be used for the further development of new algorithms for ensuring cyber security, optimizing the operation of protective systems and increasing their effectiveness in the conditions of a constantly changing cyber landscape.*

***Key words:** cyber security, mathematical model, differential equations, systems of differential equations, attack, countermeasure, forecast.*

Актуальність проблеми. Кіберзагрози стають дедалі складнішими та різноманітнішими, і важливо постійно вдосконалювати системи безпеки та навчання персоналу для запобігання таким атакам. Їх існує велика кількість: ФІШИНГ (спроби шахраїв отримати конфіденційну інформацію про логіни, паролі, номери кредитних карток через обман або підроблені веб-сайти, електронні листи або спам-повідомлення); MALWARE (віруси, трояни, руткіти, шифрувальне ПЗ, які призначені для шкоди комп'ютерам та мережам); DDoS – Distributed Denial of Service (атака, при якій зловмисники намагаються перевантажити сервер або мережу величезною кількістю запитів, що призводить до відмови в обслуговуванні); RANSOMWARE (тип шкідливого програмного забезпечення, яке блокує доступ до файлів або системи і вимагає викупу за їх відновлення); INSIDER THREATS (зловживання, вчинені співробітниками, партнерами або іншими особами, які мають доступ до внутрішніх систем організації); SNIFFING (спеціальне програмне забезпечення для прослуховування мережевого трафіку з метою перехоплення чутливої інформації.) та ін.

Комплексний підхід до захисту від цих загроз включає використання шифрування, багатофакторної автентифікації, антивірусних програм, а також регулярне оновлення програмного забезпечення.

Математика широко застосовується для моделювання процесів, аналізу та прогнозування майбутніх змін у різних галузях, у тому числі й в кібербезпеці. Використання математичних методів у виявленні аномальної поведінки, загроз та вразливостей у системах дозволяє здійснювати своєчасні заходи для запобігання кібератакам.

З розвитком технологій зростає ймовірність несанкціонованого доступу до важливих даних, їх змін або крадіжки. Відповідно, швидкий розвиток вимагає від спеціалістів з кібербезпеки розробки нових, складніших алгоритмів та методів захисту. У цій статті розглядається роль математичних методів в оцінці рівня кіберзагроз і можливості покращення ефективності систем захисту.

Сучасні організації стикаються з тим, що певні дані швидко трансформуються в інформацію, яка зберігається на фізичних носіях або в хмарних сховищах. Якщо ця інформація є власністю організації, вона може бути уразливою для кібератак, крадіжки або знищення. Оскільки конкуренція на ринку постійно зростає, доступ до чужих даних чи інноваційних технологій стає важливим фактором, що привертає все більше уваги. Тому необхідно проводити систематичний моніторинг та збір даних про несанкціоновані дії в інформаційних системах організацій, аналізувати їх і прогнозувати можливі загрози. Завдяки цьому можна розробити відповідні заходи для зниження ризиків і покращення безпеки.

Аналіз останніх досліджень і публікацій. У сучасному цифровому світі кібербезпека стала критично важливою сферою досліджень, що охоплює широкий спектр тем, від аналізу загроз до розробки стратегій захисту. Існує декілька ключових напрямків досліджень у галузі кібербезпеки, які висвітлено у сучасних публікаціях.

Важливу роль відіграє забезпечення кібербезпеки, включаючи професійні та керовані послуги, а також продукти, що охоплюють функції ідентифікації, виявлення, захисту та реагування, підкреслює важливість адаптації кіберрішень до унікальних вимог організацій з урахуванням їхнього ландшафту ризиків і стратегій безпеки (IT Ukraine Association, IEEE ICT Conference, 2025).

В сучасних дослідженнях щодо захищеності даних приділяється особлива увага на необхідність підвищення обізнаності користувачів з основних принципів кібергігієни для зниження ризиків кіберзагроз, доцільність самоосвіти у галузі кібергігієни та кібербезпеки кожного користувача, що є все більш актуальним в сучасному технологічному середовищі (Федушко С., 2023).

Важливим є і аналіз сучасних загроз, такі як розширені стійкі загрози (APT), атаки програм-вимагачів, вразливості Інтернету речей (IoT) та соціальні інженерні експлойти. Тому також важливою є необхідність багаторівневого підходу до кібербезпеки, що включає надійні заходи безпеки, комплексне навчання співробітників та регулярні аудити безпеки (29th International Conference on Telecommunications (ICT), 2023).

Важливим напрямком дослідження проблем кіберзахисту є створення законодавчих актів та організаційних заходів, спрямованих на забезпечення колективної кібербезпеки, а також ознайомлення з досвідом передових практик у сфері кібербезпеки в країнах, що входять до десятки найуспішніших у цій сфері (United Nations Development Program).

В сучасних публікаціях наголошується важливість постійного ознайомлення з актуальною інформацію про останні кіберінциденти, вразливості та тенденції у сфері кібербезпеки,

постійних адаптацій систем захисту до нових загроз у кіберпросторі (Рада національної безпеки і оборони України, 2024; Український фонд безпеки, 2024).

Мета дослідження. Метою даного дослідження є: проведення аналізу сучасних математичних моделей, застосовуваних для оцінки ефективності систем кібербезпеки; дослідження застосовності диференційних рівнянь та систем диференційних рівнянь для моделювання динаміки кібератак та ефективності протидії загрозам у нерівномірних умовах атак; оцінка ролі диференціальних рівнянь у побудові динамічних моделей кіберзахисту, зокрема для прогнозування розвитку загроз і реакції системи; надання рекомендацій щодо вдосконалення системи протидії кібератакам шляхом впровадження комплексного підходу до управління ризиками.

Виклад основного матеріалу дослідження. У сучасному світі цифрові технології стали невід'ємною частиною соціальних, економічних і технічних систем. Однак зростання кількості кіберзагроз створює нові виклики для забезпечення інформаційної безпеки. Відомо, що традиційні методи аналізу не завжди дозволяють оперативно адаптувати системи захисту до умов нерівномірного розподілу атак.

У цьому дослідженні основна увага приділяється побудові моделі на застосуванні диференціальних рівнянь та систем диференціальних рівнянь, які описують зміну кількості атак та реакцію захисних механізмів.

Також представлено теоретичне обґрунтування обраного підходу, описано моделі та методи, використані для дослідження, а також наведено результати моделювання та їх інтерпретацію.

Застосування диференційних рівнянь чи систем диференційних рівнянь розглянемо в ситуації «атака-протидія», коли несанкціонований вплив виступає в якості атаки, а знешкодження атак – система протидії. Головне припущення, що лежить в основі моделі, полягає в тому, що система кібербезпеки активно обробляє атаки аж до певної межі.

Розглянемо можливі три різні випадки наступних взаємодій.

Випадок перший. При невеликому збільшенню кількості атак протидія повністю їх знищує. Тобто не дає інцидентам знищити певні ресурси чи їх пошкодити.

Випадок другий. При збільшенні кількості атак в залежності від зовнішніх умов і випадкових причин протидія може знищити ці атаки, а може і не впоратися з великою кількістю несанкціонованих дій, які створять нестабільну ситуацію.

Випадок третій. Відповідає катастрофі. Атаки діють дуже швидко, їх кількість занадто велика і ресурси зазнають втрат або взагалі знищуються (зникають). Захист не може знищити атаки, яких занадто багато, він не може використати для своєї роботи більше інструментів ніж він має в своєму арсеналі (чи є недостатня кількість фахівців), не в змозі відслідкувати і знищити всі інциденти.

Припустимо, що атаки і протидія характеризуються кількістю P і щільністю E, відповідно. У випадку, що атаки постійно існують, процес еволюції можна описати рівнянням

$$\frac{dP}{dt} = a - bP, \tag{1}$$

де a – збільшення атак за одиницю часу,

b – коефіцієнт знищення відомих атак без перенапруження системи протидії. При початковій умові, за одиницю часу $t = 0$: $P(t = 0) = P_0$ рівняння (1) має вигляд

$$P_t = \frac{a}{b} + \left(P_0 - \frac{a}{b}\right)e^{-bt},$$

якщо з часом відомі атаки знищуються без перенапруження системи.

Можна припустити, що атаки і протидія знаходяться в постійній взаємодії, і процес взаємодії є замкнутим. Цей процес взаємодії можна описати наступним рівнянням

$$\frac{dP}{dt} = a - bP - f(,P), \tag{2}$$

де функція $f(,P) \geq 0$ – описує відслідковування і знищення атаки.

Приймемо за g(ε) величину, коли система протидії не знаходить атак, $ah(E,P)$ – за функцію, коли атаки впливають на систему безпеки.

Тоді відслідковування і знищення атаки можна подати формулами

$$f(,P) = cP \;\; ma \;\; h(E,P) = dP,$$

де c і d – деякі коефіцієнти (кількість атак).

При відсутності атак поведінку протидії можна описати рівнянням

g()=$r\left(1 - \frac{}{K}\right)$, де r – постійний коефіцієнт, а K – відповідає найбільшому значенню, коли $\frac{d}{dt} = 0$. Тоді отримаємо систему рівнянь:

$$\frac{dP}{dt} = a - bP - cP,$$

$$\frac{d}{dt} = r\left(1 - \frac{}{K}\right) - dP \tag{3}$$

Якщо спробуємо перейти до безрозмірних даних, отримаємо

$$P = \frac{by}{d}, = \frac{bv}{c}, \tau = bt, \alpha = \frac{ad}{b^2}, u_0 = \frac{r}{b}, p = \frac{r}{cK},$$

Звідси, модель «атака-протидія» набуває виду

$$\frac{du}{dt} = \alpha - u - uv, \quad \frac{dv}{dt} = v(u_0 - u) - pv^2. \qquad (4)$$

В системі (4) параметр α – це потужність атак, u_0 – гранично допустима кількість атак (якщо $u > u_0$), $\frac{dv}{dt} < 0$ – система протидії «зависає», або взагалі не може протидіяти), p – коефіцієнт концентрації інцидентів на систему.

Для успішного знищення популяції атак потрібно дослідити значення рівноваги в системі диференціальних рівнянь.

Рівновагу для успішного знищення атак $\frac{du}{dt} = 0$, $\frac{dv}{dt} = 0$, можна знайти з таких рівнянь:

$$a - u(1 + t) = 0, \; -v(u - u_0) - pv^2 = 0.$$

Тоді для *Випадку 1* положення рівноваги матиме вигляд*:*

$$A_1 = (\alpha, 0),$$

для *Випадку 2* положення рівноваги матиме вигляд*:*

$$A_2 = \left(\frac{u_0 + p + Q}{2}, \frac{u_0 - p - Q}{2p} \right),$$

для *Випадку 3* положення рівноваги матиме вигляд*:*

$$A_3 = \left(\frac{u_0 + p - Q}{2}, \frac{u_0 - p + Q}{2p} \right),$$

де $Q = \sqrt{(u_0 + p)^2 - 4\alpha p}$.

Для *Випадку 2* і *Випадку 3* положення рівноваги існує, коли $\left[\left(u + p \right)^2 - 4\alpha p \right] > 0$.

Наступна функція описує процес завантаженості системи атаками:

$$f(, P) = \frac{\left(\frac{cP}{d} \right)}{A + P}. \qquad (5)$$

Якщо врахувати цю функцію та безрозмірний вигляд, то система рівнянь (4) перепишеться

$$\frac{du}{dt} = \alpha - u - \frac{uv}{\lambda + u}, \quad \frac{dv}{dt} = v(u_0 - u) - pv^2, \quad (6)$$

де $\lambda = A\left(\frac{d}{b} \right) > 0$ – це ступінь захисту системи протидії, чим більше його значення, тим менш вразлива система безпеки і захисту. Параметр λ – характеризує надійність системи безпеки. Тобто, чим більший параметр λ, тим більший захист може надати система протидії.

Висновки і перспективи подальших досліджень. Зроблено висновок, що застосування математичних моделей є ефективним підходом для вдосконалення систем протидії сучасним кіберзагрозам, зокрема в контексті забезпечення цілісності, конфіденційності та доступності інформаційних ресурсів.

Дослідження за допомогою диференціальних рівнянь аналізу у сфері кібербезпеки підкреслюють необхідність комплексного підходу до захисту інформаційних систем, що включає постійний моніторинг нових загроз та адаптація до них елементів ефективної стратегії кібербезпеки.

Отримані результати можуть слугувати основою для подальших досліджень у галузі математичного моделювання кібербезпеки, а також для вдосконалення методів і засобів захисту інформації.

У подальшій перспективі автори планують дослідити модель, що перебуває під дією атак у стані катастрофи (*Випадок 3* положення рівноваги).

ЛІТЕРАТУРА:

1. Огляд ринку кібербезпеки в Україні. IT Ukraine Association, IEEE ICT Conference, 2025. 43 с. URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf.

2. Федушко С. Сучасні підходи до дослідження кібербезпеки та кібергігієни. Науковий вісник Хмельницького національного університету. Хмельницький: «ХНУ», 2023. С. 210–213. URL: https://journals.khnu.km.ua/vestnik/?p =18284

3. The New Frontier of Cybersecurity: Emerging Threats and Innovations. 29th International Conference on Telecommunications (ICT). 2023. URL: https://arxiv.org/abs/2311.02630

4. Analytical materials on cybersecurity. United Nations Development Program. URL: https://www.undp.org/ukraine/publications/analytical-materials-cybersecurity

5. Огляд подій у сфері кібербезпеки, січень 2024. Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua /files/2024/NATIONAL_CYBER_SCC/Cyber%20digest/Cyber%20digest_Jan_2024_UA.pdf

6. Огляд подій у сфері кібербезпеки, квітень 2024. Український фонд безпеки. URL: https://ufss.com.ua/wp-content/uploads/2024/05/Cyber-digest_Apr_2024_UA.pdf

REFERENCES:

1. Ohlyad rynkhu kiberbezpeky v Ukrayini (2025). [Overview of the cyber security market in Ukraine]. IT Ukraine Association. IEEE ICT Conference. Vol. 43, Retrieved from: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf [in Ukrainian].

2. Fedushko S. (2023). Suchasni pidhody do doslidzhennya kiberbezpeky ta kiberhiyieny [Modern approaches to cyber security and cyber hygiene research] Naukovyi visnyk Khmelnyts'koho natsional'noho universytetu [Scientific Bulletin of the Khmelnytskyi National University]. 210–213. Retrieved from: ttps://journals.khnu.km.ua/vestnik/?p=18284 [in Ukrainian].

3. The New Frontier of Cybersecurity: Emerging Threats and Innovations. (2023). 29th International Conference on Telecommunications (ICT). Retrieved from: https://arxiv.org/abs/2311.02630 [in USA].

4. Analytical materials on cybersecurity. United Nations Development Program. Retrieved from: https://www.undp.org/ukraine/publications/analytical-materials-cybersecurity

5. Ohlyad podiy u sferi kiberbezpeky, sichen 2024 [Overview of events in the field of cyber security, January 2024]. Rada natsional'noyi bezpeky i oborony Ukrayiny [National Security and Defense Council of Ukraine]. Retrieved from: https://www.rnbo.gov.uafiles/2024/NATIONAL_CYBER_SCC/Cyber%20digest/Cyber%20digest_Jan_2024_UA.pdf [in Ukrainian].

6. Ohlyad podiy u sferi kiberbezpeky, kviten 2024. [Overview of events in the field of cyber security, April 2024]. Rada natsional'noyi bezpeky i oborony Ukrayiny [National Security and Defense Council of Ukraine]. Retrieved from: https://ufss.com.ua/wp-content/uploads/2024/05/Cyber-digest_Apr_2024_UA.pdf [in Ukrainian].