УДК 681.3.06: 519.248.681

КІЛЬКІСНА ОЦІНКА БЕЗПЕЧНОЇ ЕКСПЛУАТАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ

Володимир Ахрамович, Вадим Ахрамович, Сергій Чупрун, Роман Придибайло.

В основі інформаційної безпеки лежить діяльність із захисту інформації — забезпечення її конфіденційності, доступності та цілісності, а також недопущення будь-якої компрометації в критичній ситуації. Правильне її забезпечення відповідає за безпеку інформаційної інфраструктури підприємства, безпеку всіх її даних та їх конфіденційність.

Зараз інформаційна безпека у тренді, однак, завжди потрібно пам'ятати, що це не набір дорогих технічних засобів, а безперервний процес, який повинен постійно вдосконалюватися, реагуючи на появу нових загроз та техніки атак. Збитки від цих загроз можуть істотно перевищити вартість впровадження захисних заходів, і очевидно, що ці ризики необхідно знижувати якомога ефективніше.

В статті розроблено моделі кількісної оцінити коефіцієнт готовності до безпечної експлуатації інформаційних систем. Для цього виконано:

–моделювання коефіцієнт готовності до безпечної експлуатації з урахуванням впливу одномоментної появи в системі кількох однотипних вразливостей;

–моделювання коефіцієнт готовності до безпечної експлуатації з урахуванням ймовірність наявності в системі одночасно r не усунених вразливостей (реальних загроз вразливостей);

–моделювання коефіцієнт готовності до безпечної експлуатації сукупності комп'ютерів, наприклад, комп'ютерних мереж, де одночасно може усуватися кілька вразливостей.

–моделювання коефіцієнт готовності до безпечної експлуатації якщо система захисту, використовується для нівелювання вразливості, готова до безпечної експлуатації.

Для графічної інтерпретації залежностей представлені графічні матеріали для чого виконано моделювання в системі MatLab. Графічні матеріали наочно вказують на можливість отримання стану безпечної експлуатації інформаційних систем в залежності від інтенсивності припинення системою захисту спроб нелегальних проникнень до інформації, та інтенсивності таких спроб на вході в систему захисту.

Це дозволить для розробників інформаційних систем та обслуговуючого персоналу мати кількісні показники коефіцієнта готовності до безпечної експлуатації системи і прийняття рішень відносно можливих вразливостей.

Ключові слова: *коефіцієнт готовності до безпечної експлуатації; моделювання; графічна інтерпретація; інформаційні системи; параметри; спроби нелегальних проникнень до інформації.*

Вступ

Гострота проблеми забезпечення безпеки суб'єктів інформаційних відносин, захист їх законних інтересів при використанні інформаційних і керуючих систем інформації, що зберігається і обробляється в них, все більше зростає.

Цьому є низка причин:

По-перше, це розширення сфери застосування засобів обчислювальної техніки та зростання довіри до автоматизованих систем управління та обробки інформації.

По-друге, це доступність обчислювальної техніки, розвиток обчислювальної техніки, розвиток обчислювальних мереж та систем з віддаленим доступом.

По-третє, бурхливий розвиток та поширення комп'ютерних вірусів, здатних приховано існувати в системі та здійснювати потенційно несанкціоновані дії.

Системні адміністратори, керівники повинні знати сучасні загрози, пов'язані з ними ризики, розмір можливої шкоди, а також набір допустимих заходів для запобігання відбитку нападів.

При виборі підходу до вирішення проблеми комп'ютерної інформаційної безпеки слід завжди виходити з того, що захист інформації та обчислювальної системи не є самоціллю.

Кінцевою метою створення системи комп'ютерної безпеки є захист всіх категорій суб'єктів прямо чи опосередковано учасники процесів інформаційного взаємодії від завдання їм відчутного матеріально морального чи іншого шкоди внаслідок випадкових чи навмисних впливів на інформацію та систему її обробки та передачі.

Постановка проблеми

Необхідно кількісно оцінити коефіцієнт готовності до безпечної експлуатації інформаційних систем. Для цього необхідно:

виконати моделювання коефіцієнт готовності до безпечної експлуатації з урахуванням впливу одномоментної появи в системі кількох однотипних вразливостей;

виконати моделювання коефіцієнт готовності до безпечної експлуатації з урахуванням ймовірність наявності в системі одночасно r не усунених вразливостей (реальних загроз вразливостей);

– виконати моделювання коефіцієнт готовності до безпечної експлуатації сукупність комп'ютерів, наприклад, комп'ютерна мережа, де одночасно може усуватися кілька вразливостей. – виконати моделювання коефіцієнт готовності до безпечної експлуатації якщо система

захисту, яка використовується для нівелювання вразливості, готова до безпечної експлуатації.

Це дозволить для розробників інформаційних систем та обслуговуючого персоналу мати кількісні показники коефіцієнта готовності до безпечної експлуатації системи і прийняття рішень відносно можливих вразливостей.

Мета статті

Метою дослідження є розробка методики кількісної оцінки коефіцієнта готовності до безпечної експлуатації інформаційних систем. Ці. дослідження дозволять враховувати вказані показники при плануванні та реалізації систем захисту інформаційних систем.

Аналіз останніх досліджень і публікацій

В роботі [1] відмічається, що ландшафт загроз розподіленої відмови в обслуговуванні (DDoS) продовжує тримати суспільство в напрузі. Нові та старі групи DDoS-активістів зростають у всьому світі. Було відзначено щодо складності атак, коли деякі з них використовують спеціальні інструменти та складну архітектуру, а інші використовують базові, часто безкоштовні сервіси для запуску атак. Гнучкий, цілеспрямований захист є необхідністю для підприємств і постачальників послуг будь-яких форм і розмірів.

В роботі [2] розглядаються проблеми конфіденційності, пов'язані, зокрема, з роботою відносно великих даних. Розглянуто кілька класифікаційних схем таких викликів. Розрізняють три тенденції:
(1) повернення кінцевого користувача послуг обробки даних як центрального координаційного центру технологій, що зберігають конфіденційність, (2) оцифрування та автоматизація політик конфіденційності для сервісів великих даних та (3) розробка безпечних методів багатосторонніх обчислень та аналітики, що дозволяє як надійним, так і ненадійним партнерам працювати разом з великими даними, одночасно зберігаючи конфіденційність. Висновки та рекомендації зокрема, демонструють роль технологій, що зберігають конфіденційність, як особливо важливого прикладу технологій даних для штучного інтелекту, керованого даними. Відмічається, що Технології, що зберігають конфіденційність, є важливим елементом програми AI Innovation Ecosystem Enablers (Data for AI).

В роботах [3], [4], розглядаються системи захисту інформації та їх вплив на уразливості, безпеку інформаційних систем. Розглянуто приклади реалізації політик інформаційної безпеки, налаштування основних компонентів системи захисту.

В роботах [5], [9] розкриті питаня теорії та практики проектування систем захисту інформації та включає чітко систематизований матеріал з методології захисту інформації та методології проектування відповідних систем, прикладної теорії інформації, кібернетичної теорії моделювання систем захисту інформації.

В роботі [6] розглядаються актуальні питання щодо створення систем захисту інформації в умовах повної відкритості сучасних інформаційних технологій, викладено причини порушення безпеки комп'ютерних систем, наведено опис математичних моделей систем захисту інформації, а також розглянуто методи та засоби впровадження механізмів захисту у існуючі інформаційні системи з можливістю гнучкого управління безпекою в залежності від вимог, допустимого ризику та оптимальної витрати ресурсів.

В роботі [7] розглянуто основи сучасної теорії синтезу та аналізу політик інформаційної безпеки. Наведено нормативно-правову основу створення політик інформаційної безпеки, вимоги міжнародних стандартів, документи, що забезпечують реалізацію політики безпеки. Розглянуто приклади реалізації політик інформаційної безпеки, налаштування основних компонентів системи захисту.

У роботі [8] класифіковано підхід до визначення якості систем захисту інформації, наведенопоказники оцінки якості та особливості розрахунку показників. Описано модифікацію алгоритму Балаша, що дозволяє мінімізувати обчислювальні витрати за рахунок

використання цілих змінних, операцій складання та віднімання та вибору кращого напрямку спуску по дереву рішень, властивого методам типу гілок та кордонів. Запропоновано методику оцінки обчислювальної складності алгоритму, використовує цю модифікацію.

У роботі [10] відображаються теоретичні основи системного аналізу у сфері інформаційної безпеки, застосування методологічних підходів до створення систем управління інформаційною безпекою, з особливостями створення систем управління інцидентами і управління ризиками інформаційної безпеки та їх впровадження; розкриття застосування методів в системному аналізі інформаційної безпеки: аналіз інформаційних систем, аналіз та синтез у дослідженні і проектуванні організацій, метод аналізу ієрархій і метод мережевого планування; порядок оцінки стану інформаційної безпеки організації: оцінка економічної безпеки підприємства, моніторинг і аудит інформаційної безпеки організації, SIEM в системі управління подіями.

Загальний недолік розглянутої літератури - відсутність кількісної оцінки коефіцієнта готовності до безпечної експлуатації.

Основна частина

Представляє інтерес кількісної оцінки коефіцієнта готовності до безпечної експлуатації. Очевидно, що в загальному випадку інтенсивність виникнення вразливості за деякий час буде знижуватися, оскільки в першу чергу порушником будуть виявлятися найпростіші недоліки функціональної реалізації захисту та помилки в програмному забезпеченні (збільшення складності виявлення вразливості природно призведе до зниження їх інтенсивності. Щодо параметра, а можемо сказати, що він ніяк не пов'язаний зі складністю виявлення вразливості порушником безпеки, визначається виключно типом уразливості (наприклад, помилки в системних драйверах і додатках вимагають різної трудомісткості виправлення), тобто для кожного типу вразливості можемо прийняти: a = const

З урахуванням того, що ймовірністю одномоментної появи в системі кількох однотипних вразливостей (не одночасної присутності, саме виникнення реальних загроз вразливостей) можемо знехтувати, процес виникнення та усунення в системі загрози вразливості може бути описаний схемою "загибелі та розмноження". Тоді для випадку одного обслуговуючого, наприклад, ПК шукана характеристика безпеки – коефіцієнт готовності (у даному випадку готовності до безпечної експлуатації щодо загрози вразливості) визначається так:

$$P_1 = 1 - \rho, \quad (1)$$

де $\rho = a / b$

де a- інтенсивності припинення системою захисту спроб нелегальних проникнень до інформації, b- інтенсивності таких спроб на вході в систему захисту. На рис 1-2 представлені графічні залежності вразливостей, в залежності від змінних параметрів, отримані в системі MatLab. a ймовірність наявності в системі одночасно r не усунених вразливостей (реальних загроз вразливостей) (рис. 3-8).

$$P_2 = \rho^r (1 - \rho) \quad (2)$$

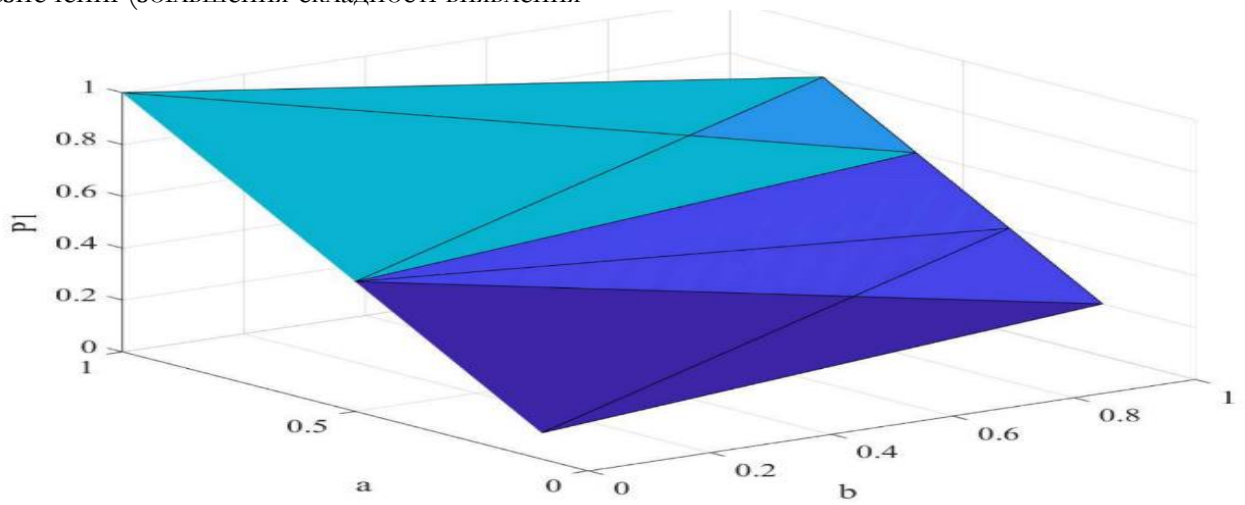

Рисунок 1 Коефіцієнт готовності до безпечної експлуатації при a=0,1-1; b=0,1-1

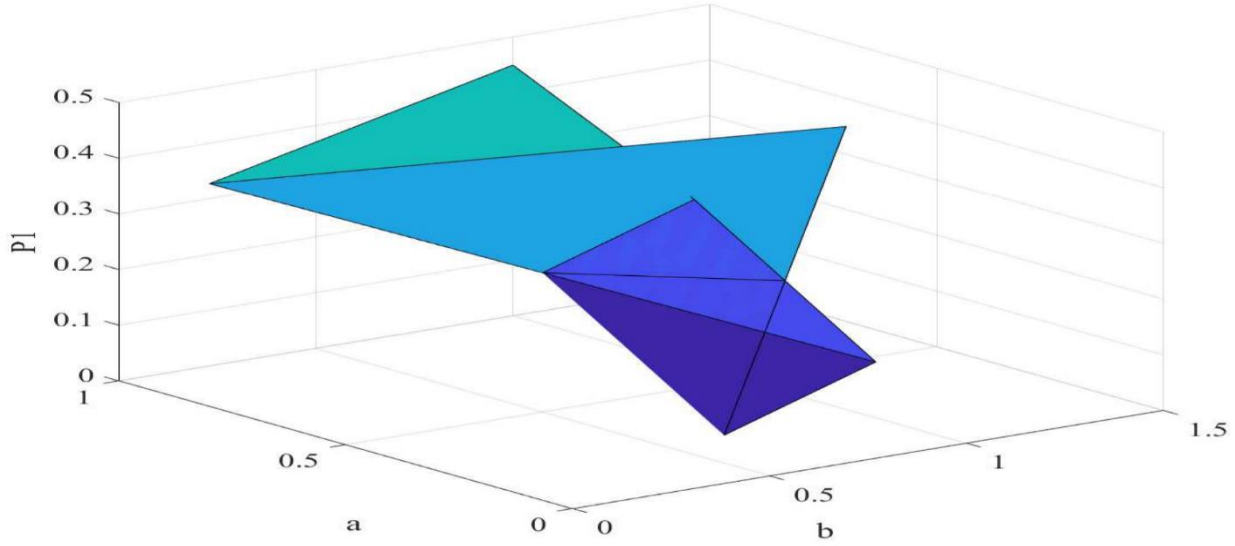

Рисунок 2 Коефіцієнт готовності до безпечної експлуатації при a=0,1-0,45; b=0,1-1

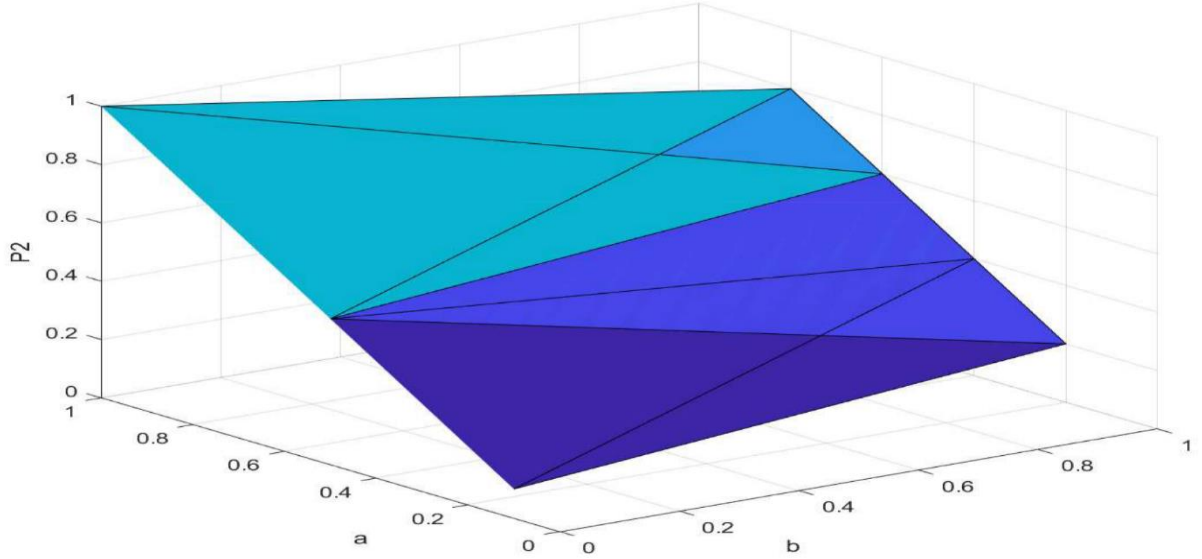

Рисунок 3 Коефіцієнт готовності до безпечної експлуатації при a=0,1-0,45; b=0,1-1; r=0,1-1

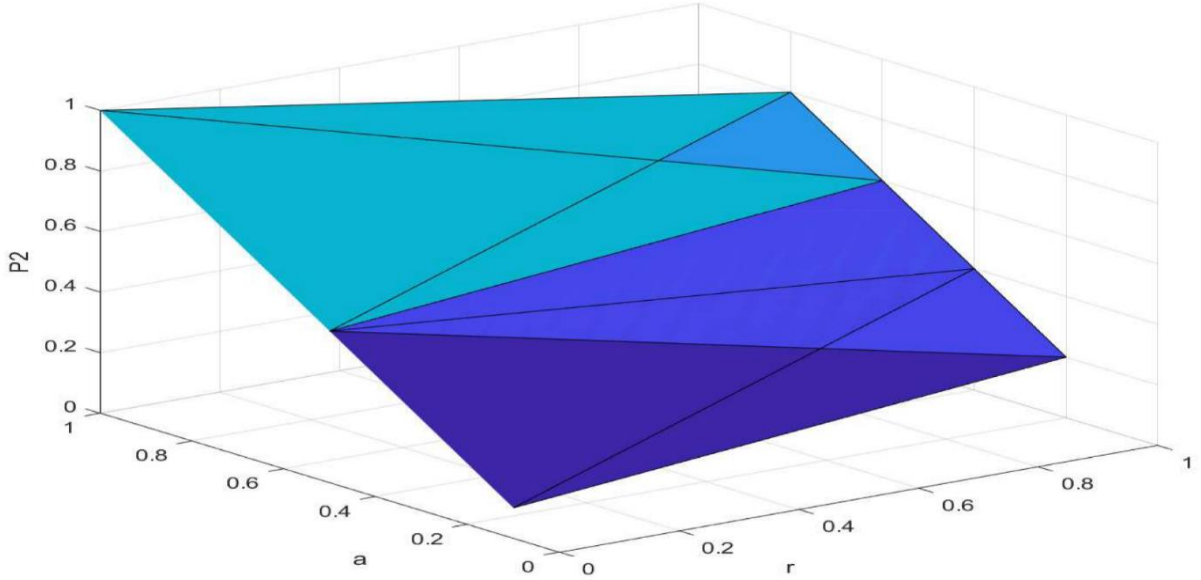

Рисунок 4 Коефіцієнт готовності до безпечної експлуатації при a=0,1-0,45; b=0,1-1; r=0,1-1

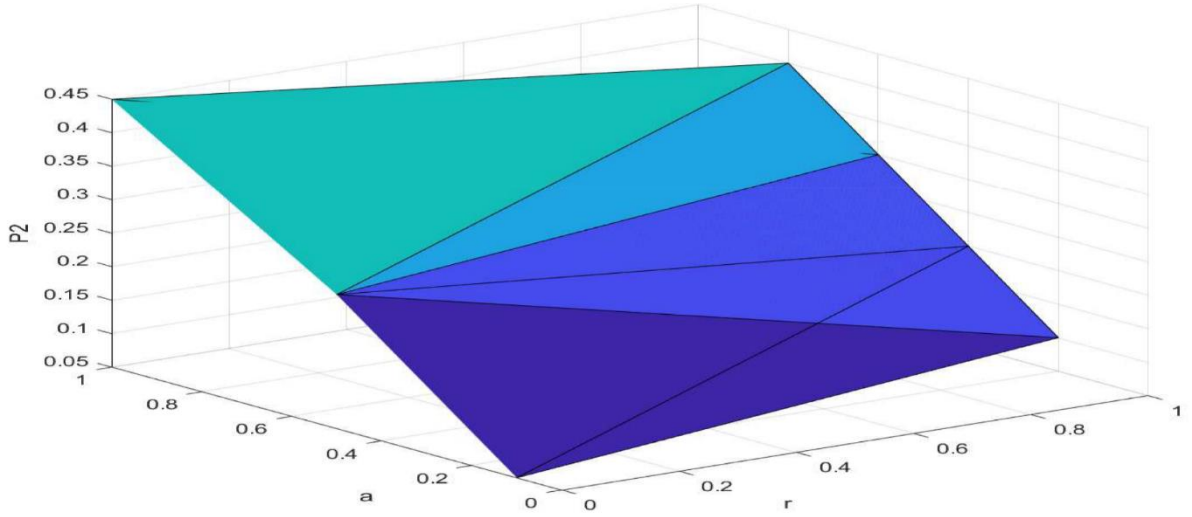

Рисунок 5 Коефіцієнт готовності до безпечної експлуатації при a=0,1-0,45; b=0,1-1; r=0,1-0,45

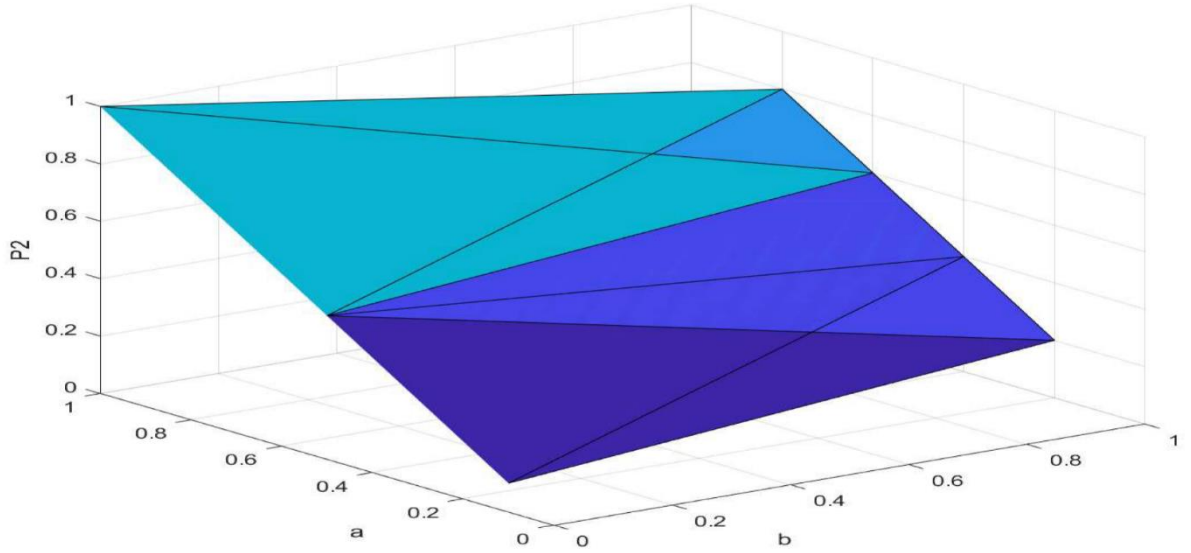

Рисунок 6 Коефіцієнт готовності до безпечної експлуатації при a=0,1-1; b=0,1-1; r=0,1-0,45

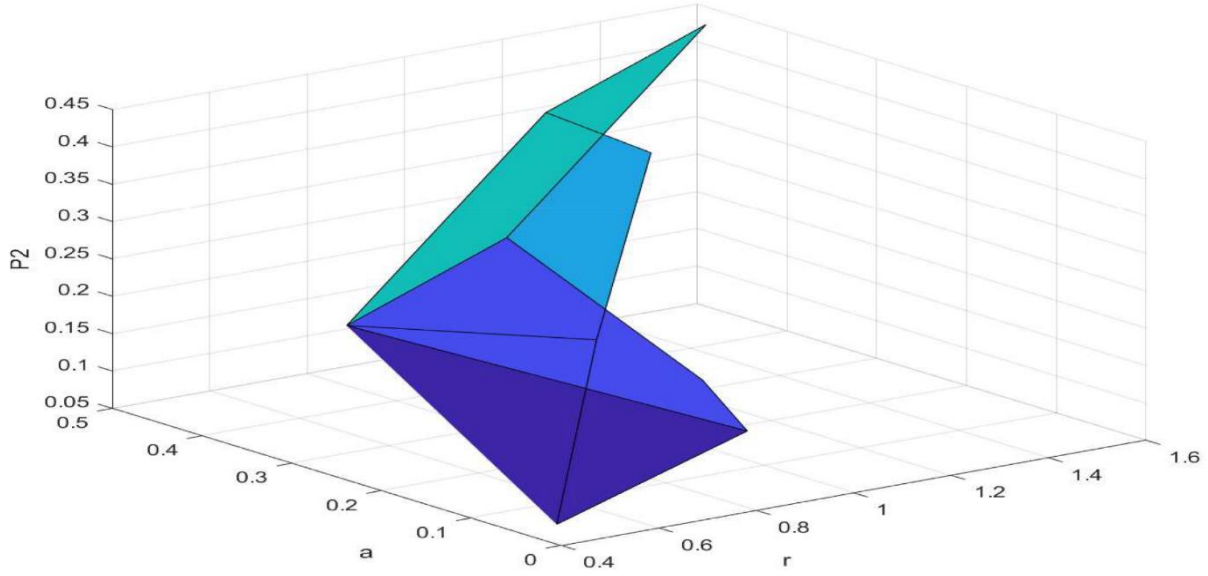

Рисунок 7 Коефіцієнт готовності до безпечної експлуатації при a=0,1-0,45; b=0,1-0,45; r=0,1-0,45

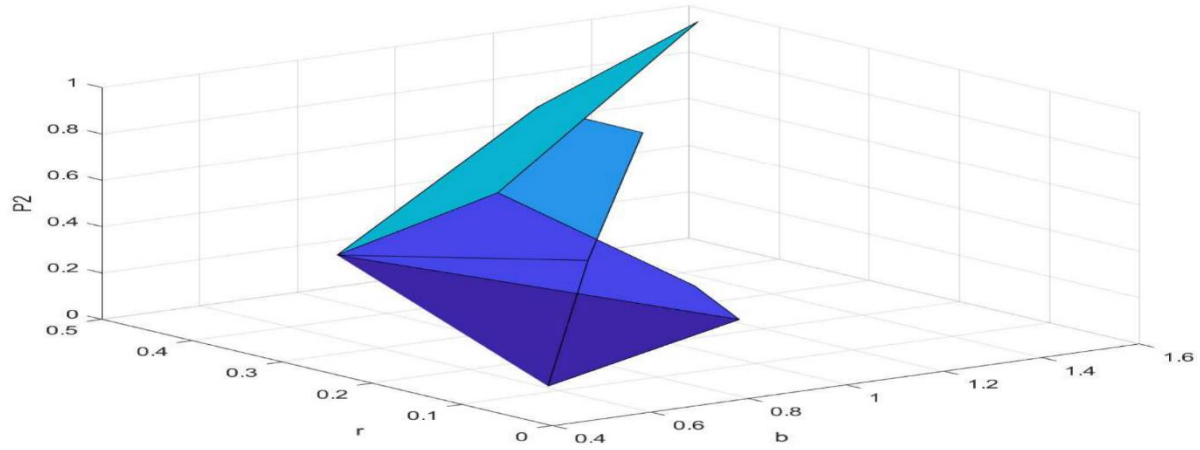

Рисунок 8 Коефіцієнт готовності до безпечної експлуатації при a=0,1-0,45; b=0,1-1; r=0,1-0,45

Якщо в якості системи розглядається сукупність комп'ютерів, наприклад, комп'ютерна мережа, одночасно може усуватися кілька вразливостей. Для такої моделі потрібна характеристика визначається так (рис. 9- 12):

$$P_3 = \frac{\rho^C}{C!} P_1 \quad (3)$$

Де С- кількість засобів обслуговування.

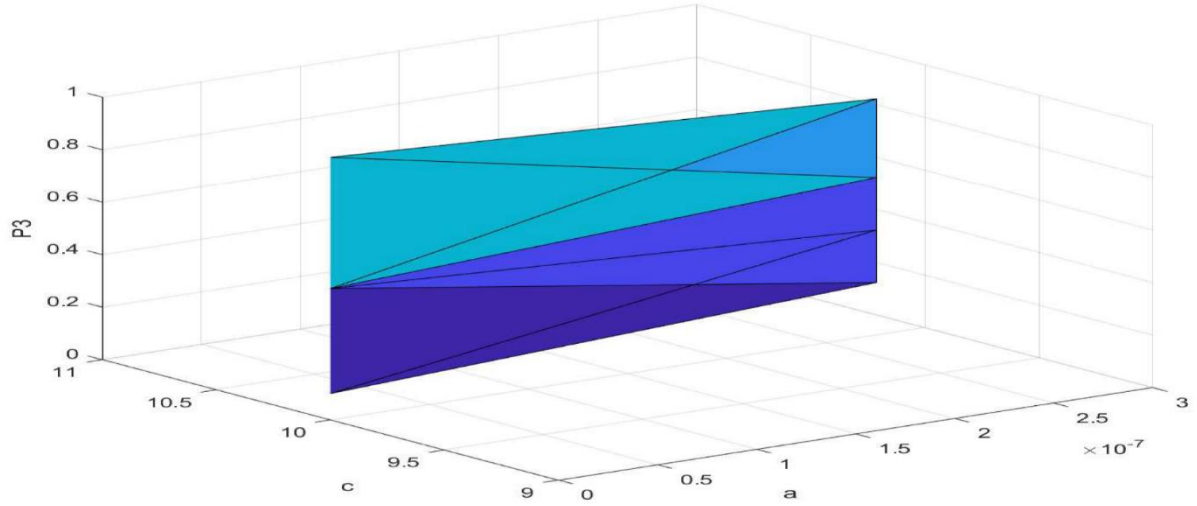

Рисунок 9 Коефіцієнт готовності до безпечної експлуатації при a=0,1-1; b=0,1-1; r=0,1-1; c=10

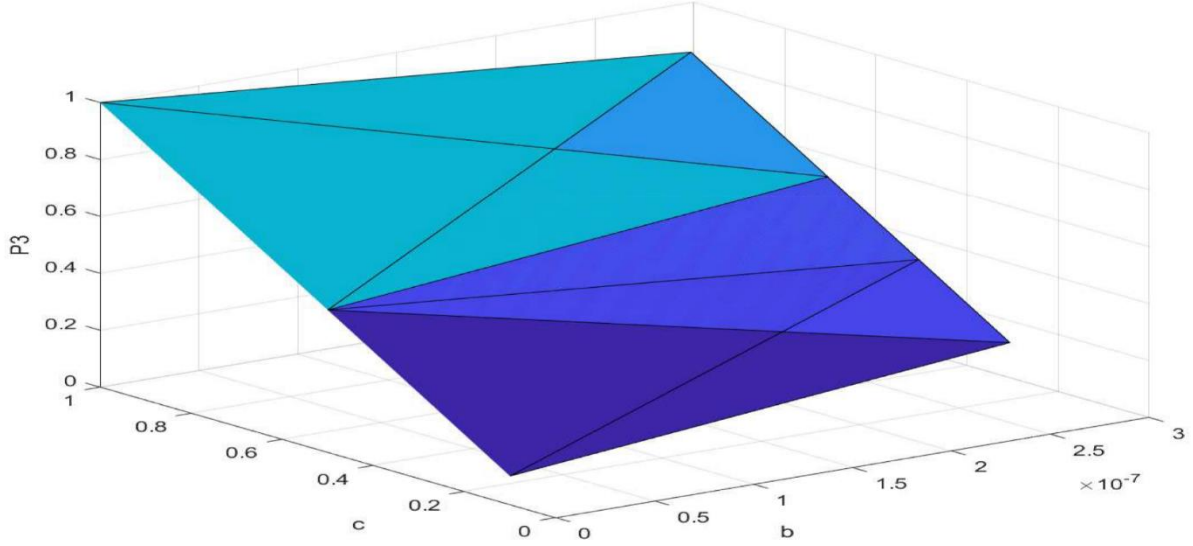

Рисунок 10 Коефіцієнт готовності до безпечної експлуатації при a=0,1-1; b=0,1-1; r=0,1-1; c=10

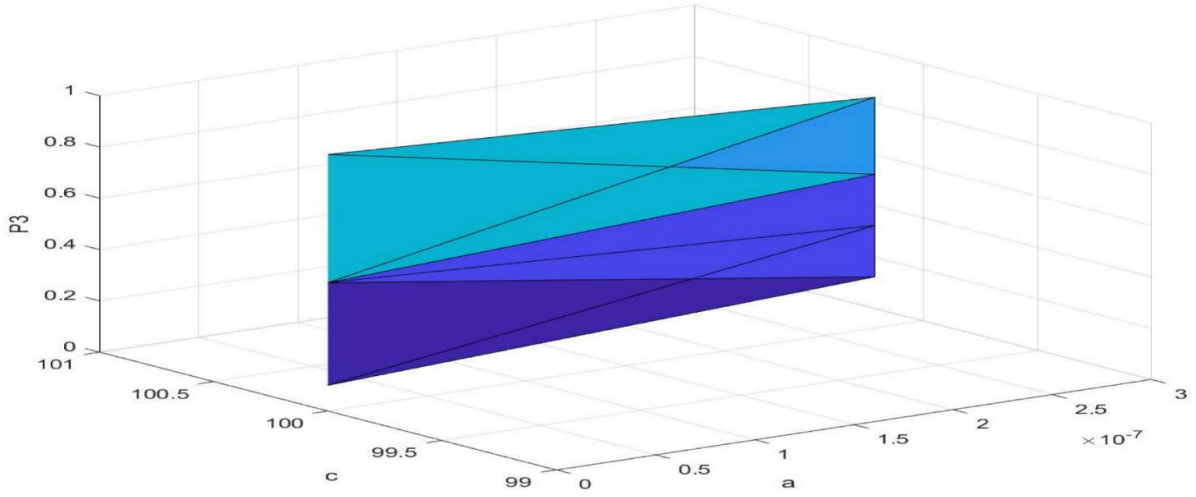

Рисунок 11 Коефіцієнт готовності до безпечної експлуатації при a=0,1-1; b=0,1-1; r=0,1-1; c=100

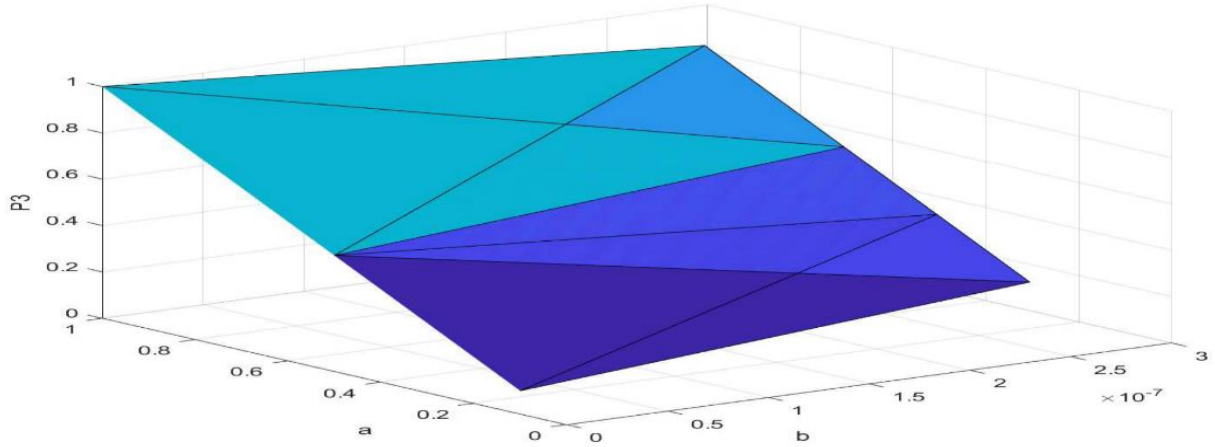

Рисунок 12 Коефіцієнт готовності до безпечної експлуатації при a=0,1-1; b=0,1-1; r=0,1-1; c=100

Якщо позначити ймовірність того, що система захисту, яка використовується для нівелювання вразливості, готова до безпечної експлуатації через $P4$, то ймовірність того, що захищена щодо загрози вразливості інформаційна система буде готова до безпечної експлуатації , може бути визначена таким чином (рис. 13-16):

$$P_4 = 1 - (1 - P_1)(1 - P_0) \qquad (4)$$

де - показник щодо загрози атаки при використанні системи захисту, при нівелюванні однієї з r вразливостей, які використовуються атакою.

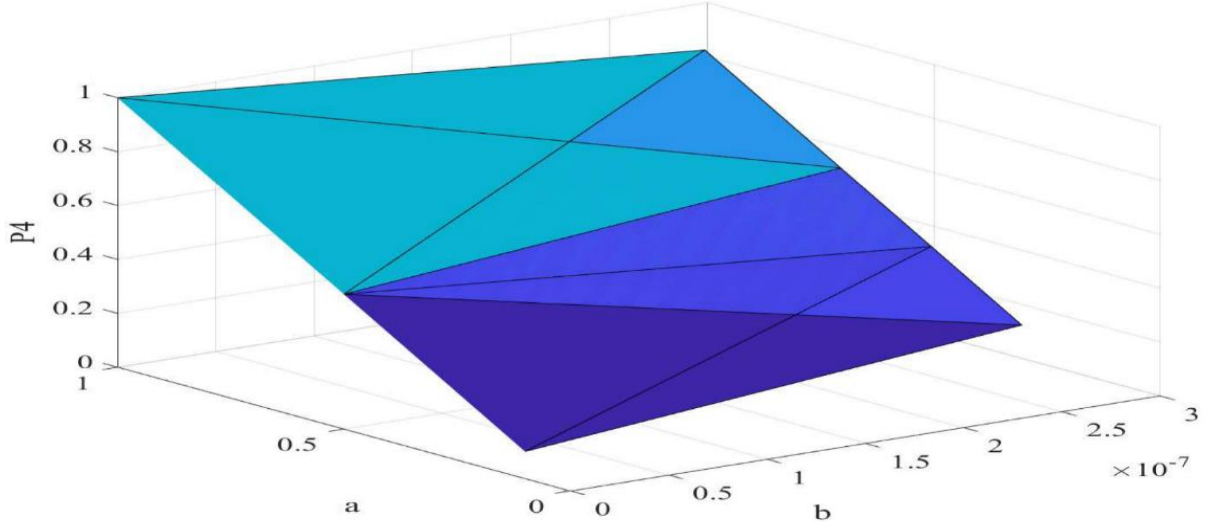

Рисунок 13 Коефіцієнт готовності до безпечної експлуатації при a=0,1-1; b=0,1-1; Po=0,1-1

Ймовірність того, що захищена інформаційна система готова до безпечної експлуатації, PP_0 щодо загрози атаки при використанні системи захисту, що нівелює одну з r вразливостей, яка використовуються атакою:

$$P_5 = 1-(1-P_0)\prod_r^R(1-P_4) \quad (5)$$

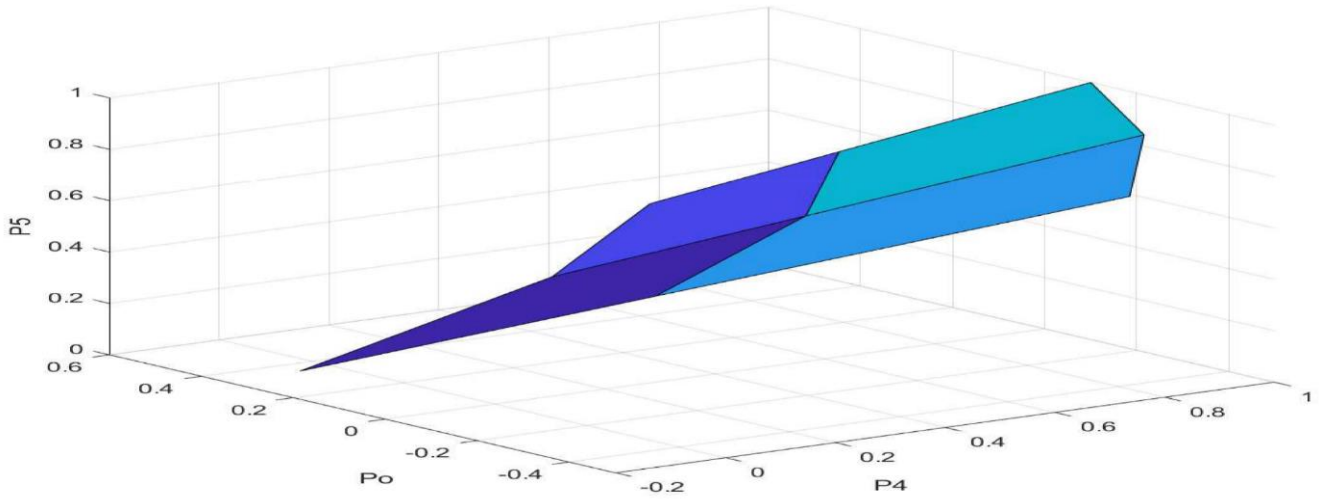

Рисунок 14 Коефіцієнт готовності до безпечної експлуатації при a=0,1-1; b=0,1-1; Po=0,1-1

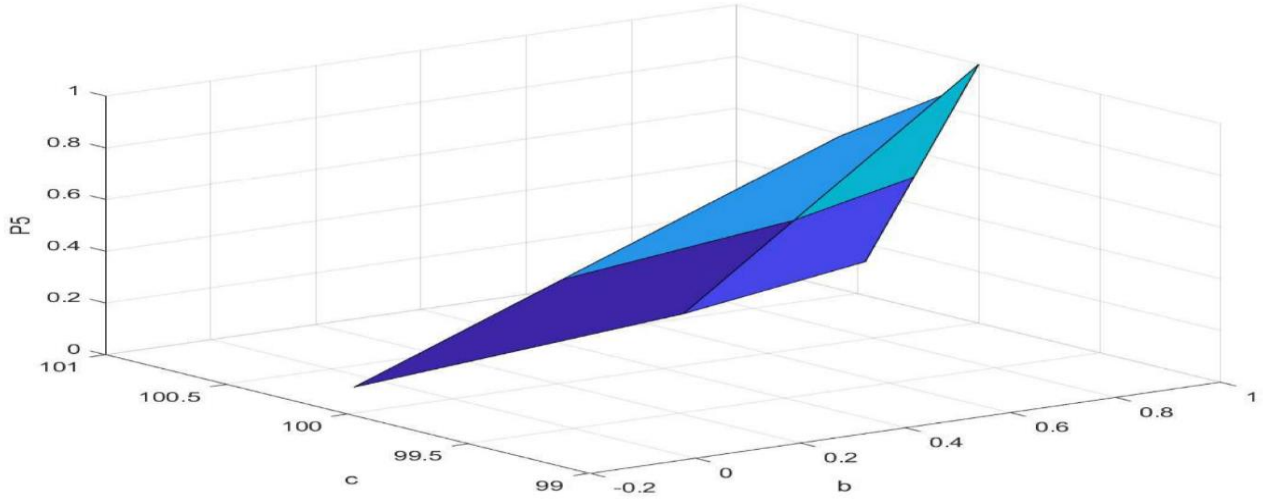

Рисунок 15 Коефіцієнт готовності до безпечної експлуатації при a=0,1-1; b=0,1-1; Po=0,1-1

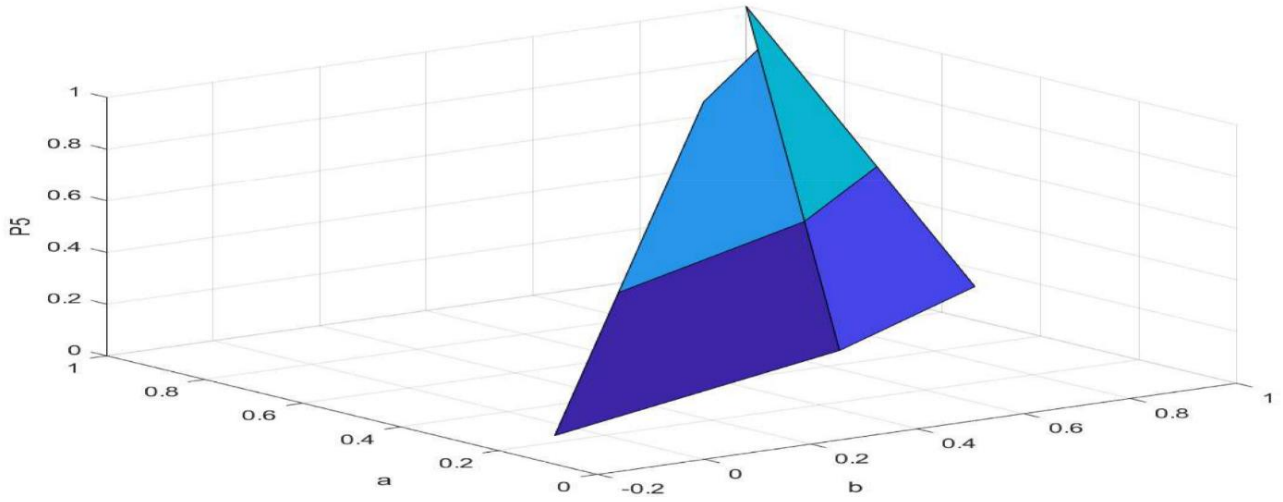

Рисунок 16 Коефіцієнт готовності до безпечної експлуатації при a=0,1-1; b=0,1-1; Po=0,1-1

Висновки

Проведено дослідження кількісного показника (коефіцієнт готовності до безпечної експлуатації) з урахуванням того, що ймовірністю одномоментної появи в системі кількох однотипних вразливостей (не одночасної присутності, саме виникнення реальних загроз вразливостей) можемо знехтувати, процес виникнення та усунення в системі загрози вразливості описаний схемою "загибелі та розмноження".

Перспектива досліджень вбачається в тому, що необхідно деталізувати уразливості та реакції на них системи захисту ввести вказані параметри в моделі коефіцієнта готовності до безпечної експлуатації.

Література

[1].Netscout. DDoS Threat Intelligence Report / Findings from 1st half 2023. Internet Traffic and Slipstreamed Threats. DOI:10.30534/ijatcse/ 2019/12812019. URL: https://www. netscout.com/threatreport/internet-traffic-slipstreamed-threats/

[2].Timan, T., Mann, Z. (2021). Data Protection in the Era of Artificial Intelligence: Trends, Existing Solutions and Recommendations for Privacy-Preserving Technologies. In: Curry, E., Metzger, A., Zillner, S., Pazzaglia, JC., García Robles, A. (eds) The Elements of Big Data Value. Springer, Cham. Pp. 153-175.https://doi.org/10.1007/ 978-3-030-68176-0_7

[3].Ахрамович В.М. Інформатика. Програмне забезпечення (навчальний посібник) Практикум: навч.-метод. посіб..- К.:ДП «Інформ.-аналіт. Агенство», 2013.-276с

[4].Ахрамович В.М. Інформатика. Програмне забезпечення (навчальний посібник) Навчальний посібник.- К.:ДП «Інформ.-аналіт. агенство», 2012.-375с

[5].Гарбарчук В., Зінович З., Свіц О. Кібернетичний підхід до проектування систем захисту інформації / Українська академія інформатики; Волинський держ. ун-т ім. Лесі Українки; Люблінський політехнічний ун-т. - К.; Луцьк; Люблін, 2003. - 658 с.

[6].Домарев В.В. Безпека інформаційних технологій. Методологія створення систем захисту. - Вид-во «ДіаСофт», 2002. - 693с.

[7].Козачок, В. А., Гайдур, Г. І., Гахов, С. О., Хмелевський, Р. М., Чумак, Н. С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів. Київ: ДУТ НННЗІ, 2020.167 с.

[8].Маслова Н.А. Побудова моделі захисту інформації із заданими характеристиками якості //Штучний інтелект. – Донецьк: ІІІІ, 2007. – №1. – С. 51-57.

[9].Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак – К.: Видавництво НА СБ України, 2020/ -256 с.

[10].Якименко, Ю. М., Савченко, В. А., Легомінова, С. В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с.

QUANTITATIVE ASSESSMENT OF SECURE OPERATION OF INFORMATION SYSTEMS

The basis of information security is the activity of protecting information — ensuring its confidentiality, availability and integrity, as well as preventing any compromise in a critical situation. Its correct provision is responsible for the security of the company's information infrastructure, the security of all its data and their confidentiality.

Currently, information security is in trend, however, it is always necessary to remember that it is not a set of expensive technical means, but a continuous process that must be constantly improved, responding to the emergence of new threats and attack techniques. The damage from these threats can significantly exceed the cost of implementing protective measures, and it is clear that these risks must be mitigated as effectively as possible.

The article developed a model for quantitatively assessing the coefficient of readiness for safe operation of information systems. To do this, the following was done:

- modeling the coefficient of readiness for safe operation, taking into account the impact of the simultaneous appearance in the system of several vulnerabilities of the same type;
- modeling the coefficient of readiness for safe operation, taking into account the probability of the presence of r unremedied vulnerabilities (real threats of vulnerabilities) in the system at the same time;
- modeling the readiness factor for the safe operation of a set of computers, for example, computer networks, where several vulnerabilities can be eliminated at the same time;
- modeling factor of readiness for safe operation if the protection system used for

vulnerability leveling is ready for safe operation.

For graphical interpretation of dependencies, graphic materials are presented, for which simulations were performed in the MatLab system. The graphic materials clearly indicate the possibility of obtaining a state of safe operation of information systems depending on the intensity of stopping attempts by the protection system of illegal access to information, and the intensity of such attempts at the entrance to the protection system.

This will allow developers of information systems and service personnel to have quantitative indicators of the coefficient of readiness for safe operation of the system and decision-making regarding possible vulnerabilities.

Keywords: coefficient of readiness for safe operation, modeling, graphical interpretation, information systems, parameters, attempts of illegal access to information.

Ахрамович Володимир Миколайович, д.т.н., професор, професор кафедри кібербезпека, Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут», м. Київ, Україна.

Akhramovych Volodymyr, Doctor of Technical Science, Professor, Professor, Department of Cybersecurity of the State non-commercial company state university «Kyiv aviation institute», Kyiv, Ukraine.

E-mail: 12z@ukr.net.

ORCID ID 0000-0002-0086-9131.

Чупрун Сергій, аспірант на кафедрі систем інформаційного та кібер- нетичного захисту, державного університету інформаційно - телекомунікаційних технологій, Київ, Україна.

Chuprun Sergii, postgraduate of the Department of Information and Cyber Defense Systems of the State University of information and telecommunication technologies, Kyiv, Ukraine.

E-mail: ua0988888424@gmail.com.

ORCID ID:0009-0007-7336-1068.

Придибайло Роман, аспірант на кафедрі систем інформаційного та кібернетичного захисту, Державного університету інформаційно-телекомунікаційних технологій, Київ, Україна

E-mail: drake0103@gmail.com.

ORCID ID:0009-0003-1747-7518.

Prydybailo Roman, postgraduate of the Department of Information and Cyber Defense Systems of the State University of information and telecommunication technologies, Kyiv, Ukraine.

E-mail: drake0103@gmail.com.

ORCID ID:0009-0003-1747-7518.

УДК 336.71:004.056

МЕТОД ПОБУДОВИ ПРОФІЛЮ КЛЮЧОВИХ ФАКТОРІВ РИЗИКУ КІБЕРБЕЗПЕКИ СУЧАСНИХ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Дмитро Палко, Лариса Мирутенко

Оцінка та аналіз ризиків кібербезпеки є фундаментальними аспектами формування надійної і ефективної СУІБ, особливо в умовах стрімкого розвитку технологій та зростання складності сучасних РІС. Традиційні методи оцінки ризиків, що засновані переважно на концептуальних підходах і класичних методах, мають ряд обмежень та є малоефективними в умовах сучасних масштабованих розподілених систем, оскільки не враховують динаміку середовища та не забезпечують ефективний аналіз взаємозв'язків між численними факторами ризику. В дослідженні запропоновано метод побудови профілю ключових факторів ризику сучасних розподілених інформаційних систем на основі урахування кореляційного аналізу та моделювання їх взаємозв'язків, що дозволяє підвищити ефективність процесу оцінки ризиків кібербезпеки в умовах динамічного середовища сучасних масштабованих розподілених інформаційних систем. На основі запропонованого методу здійснено розробку профілю ключових факторів ризику сучасних розподілених систем, проведено аналіз їх статистичної важливості та кореляції, а також визначено і структуровано основні заходи та контролі інформаційної безпеки, які демонструють найкращі показники ефективності в умовах розподіленості середовища, враховують як технологічні, так і організаційні аспекти, забезпечуючи системний підхід до управління ризиками ІБ, зменшення впливу загроз і підвищення стійкості розподілених систем до можливих атак. Запропонований підхід до оптимізації вибору вхідного набору ознак та виокремлення найбільш вагомих факторів ризику на основі спроектованого профілю ключових факторів ризику для сучасних РІС продемонстрував тотожний результат по числовому показнику кількості відібраних для аналізу метрик у порівнянні з факторним аналізом за допомогою методу головних компонент (PCA) – 42 метрики у порівнянні із 40 для PCA, але при цьому забезпечив покращення загальних показників точності класифікації для проєктованих моделей оцінки ризику кібербезпеки в РІС на 4% у порівнянні з контрольною моделлю на основі PCA, що підтверджує його ефективність у контексті адаптивного аналізу ризиків у розподілених середовищах.

Ключові слова: *інформаційна безпека, ризик інформаційної безпеки, фактори ризику, оцінка ризиків, управління ризиками, розподілена інформаційна система, нейронна мережа.*