CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

DOI 10.20535/2411-1031.2024.12.2.315745
УДК 621.391:004.056.5

ВОЛОДИМИР АХРАМОВИЧ
ВАДИМ АХРАМОВИЧ

КІЛЬКІСНА ОЦІНКА ЙМОВІРНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ЗАХИСТУ БЕЗ ПРОТИПРАВНИХ ДІЙ

Анотація. Інформаційна безпека (англ. Information Security, а також – англ. InfoSec) – практика запобігання несанкціонованому доступу, використанню, розкриттю, спотворенню, змінам, дослідженням, запису чи видаленню інформації. Основне завдання інформаційної безпеки – збалансований захист конфіденційності, цілісності та доступності даних, з урахуванням доцільності застосування та без будь–якої шкоди продуктивності організації.

В статті отримані рівні безпеки (threat) T від k-ї загрози для властивостей інформації, що циркулює в ІТС від параметрів: c – оцінка впливу k-ї загрози на конфіденційність інформації, i, a та s, – оцінки впливу k-ї загрози на цілісність, доступність та спостережність інформації відповідно, ваговий коефіцієнт p визначає частку появи даної загрози відносно усієї сукупності загроз та може обчислюватися на основі аналізу статистики функціонування ІТС або з використанням відомих методик прогнозування.

Оцінено кількісно, імовірність того, що за час від початку функціонування системи захисту не відбудеться жодного протиправного доступу до інформації, при параметрах a – інтенсивності припинення системою захисту спроб нелегальних проникнень до інформації, b – інтенсивності таких спроб на вході в систему захисту; t – кількість діб функціонування системи

Для графічної інтерпретації залежностей представлені графічні матеріали для чого виконано моделювання в системі MatLab. Графічні матеріали наочно вказують на можливість отримання стану функціонування системи захисту без протиправних дій в залежності від впливу загроз на конфіденційність, цілісність, доступність інформації, та протиправного доступу до інформації в залежності від параметрів інтенсивності припинення системою захисту спроб нелегальних проникнень до інформації, та інтенсивності таких спроб на вході в систему захисту.

Це дозволить, на відміну від аналогів, для розробників інформаційних систем та обслуговуючого персоналу мати кількісні показники, що не відбудеться жодного протиправного доступу до інформації і прийняття рішень відносно можливих вразливостей.

Ключові слова: рівні безпеки, протиправний доступу до інформації, параметри, ймовірність, модель, залежність, графічна інтерпретація.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Необхідно отримати рівні безпеки T від k-ї загрози для властивостей інформації що циркулює в ІТС від параметрів: c – оцінки впливу k-ї загрози на конфіденційність інформації, i, a та s, – оцінки впливу k-ї загрози на цілісність, доступність та спостережність інформації відповідно, вагового коефіцієнта p, який визначає частку появи даної загрози відносно усієї сукупності загроз.

Оцінити імовірність того, що за час від початку функціонування системи захисту не відбудеться жодного протиправного доступу до інформації, при параметрах a – інтенсивності

припинення системою захисту спроб нелегальних проникнень до інформації, b – інтенсивності таких спроб на вході в систему захисту, t – кількості діб функціонування системи.

Отримати кількісні показники вказаних величин та графічно інтерпретувати вказані моделі.

Аналіз останніх досліджень і публікацій. У статті [1] проаналізовано та структуровано літературу з моделювання надійності програмно-апаратних засобів протягом останніх 10 років. В результаті дослідження охоплено загалом близько 1000 наукових праць. З них було відібрано понад 500 базових досліджень, проте результати, отримані під час їх дослідження, показують високу різнорідність робіт. Було виявлено, що найбільш поширена модель оцінки надійності – це модель зростання надійності програмно–апаратних засобів. Крім того, було встановлено, що все більше зустрічається в літературі моделювання на основі статичних та архітектурних характеристик, а також моделей на основі штучного інтелекту та автоматичних методах навчання. Недоліком являється відсутність кількісного аналізу рівнів безпеки, та що від початку функціонування системи захисту не відбудеться жодного протиправного доступу до інформації від визначених параметрів.

У статті [2] проведено порівняння ефективності застосування аспектно-орієнтованого підходу з об’єктноорієнтованим за рядом метрик. Показано, що використання цієї технології покращує надійність програмного забезпечення за рахунок меншої складності проекту.

Стаття [3] присвячена сучасним досягненням в галузі технічної діагностики і метрології. Розглядається можливість використання спеціальних методів оцінки технічного стану цифрових пристроїв (енергостатичний, енергодинамічний, електромагнітний) як окремо, так і комплексно. Це незначно збільшує середній час відновлення, але суттєво впливає на досягнення необхідного значення комплексного показника надійності виробу – його коефіцієнта готовностію

В роботах [4], [5] розглянута динамічна модель соціальної мережі, наведено методику розрахунку показника інформаційної безпеки в соціальних мережах з урахуванням тривалості шляху між клієнтами та взаємовпливу на основі нелінійних диференціальних рівнянь.

В роботі [6] наведено опис основних аспектів сучасного середовища кібербезпеки. Визначена фундаментальна термінологія та концепції, що використовуються в спільноті кібербезпеки, а також описуються основні кроки для включення ризиків кібербезпеки в загальний процес управління ризиками, що є центральною відповідальністю ДП. Перераховані деякі з основних джерел інформації, керівництва та стандарти, на які системний інженер може і повинен спиратися. Узагальнені основні аспекти включення засобів контролю безпеки до архітектури та дизайну системи з метою досягнення прийнятного рівня ризику безпеці. Розглянуті підходи поширено на множину сервісно-орієнтованих, мережевих і розподілених систем.

У статті [7] представлено дослідження, і якому в основному використовувався кількісний підхід. Вихідні дані зібрані за допомогою анкет на різноманітній виборці з 374 осіб, включаючно із студентами та співробітниками. Крім того, було використано якісний метод для отримання даних про готовність організації до запобігання загрозам кібербезпеці від ключових інформаторів, включаючи системних адміністраторів та персонал топ–менеджменту. Програмне забезпечення Statistical Package for the Social Sciences (SPSS) проаналізувало кількісні дані за допомогою описового аналізу. Результати дослідження підкреслюють нагальну потребу в розробці ефективних механізмів кібербезпеки в освітньому секторі на прикладі системи управління студентською інформацією Католицького університету Руаха.

В роботі [8] визначена система показників фінансової безпеки і сектору державних фінансів України, формалізовані розрахунки, розроблена інформаційна база та обґрунтовані їхні порогові значення. Досліджені питання фінансової безпеки трансформаційних процесів у національній економіці, виклики й загрози стабільності фінансової системи, а також безпекові

аспекти бюджетної політики, зокрема її особливості в умовах існуючих зовнішніх і внутрішніх ризиків.

У статті [9] розглянуто основні наукові засади та визначено основні наукові підходи до методології дослідження систем економічної безпеки підприємств (системний, структурний, функціональний, процесний, комплексний, організаційно-науковий, ресурсно–функціональний). Установлено, що інтеграція цих підходів дає змогу глибше зрозуміти механізми функціонування і розбудови економічної безпеки підприємств на різних рівнях. Охарактеризовано специфічні наукові підходи (захисний, конкурентний, гармонізаційний, конвергентний, динамічний, адаптаційний, діяльнісний, реактивно-ситуативний, стійкісний), притаманні розбудові методологічних засад безпекології.

В роботі [10] наведений підхід до оцінки ризиків задля визначення найкращого співвідношення витрат і вигод. Одним із способів досягти цього є моделювання загроз; однак моделювання загроз зазвичай не використовується в корпоративній сфері IT-ризиків. Крім того, існуючі методи моделювання загроз мають недоліки. У цьому документі представлено підхід, заснований на метамоделі, під назвою Yet Another Cybersecurity Risk Assessment Framework (Yacraf). Yacraf має на меті забезпечити комплексну оцінку ризиків для організацій з більшою підтримкою прийняття рішень. Документ містить формалізацію розрахунку ризиків, а також приклад, що показує, як організація може використовувати та отримувати вигоду від Yacraf.

Метою статті є дослідження впливу параметрів системи ІТС на кількісні показники рівнів безпеки, протиправного доступу до інформації.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Визначення рівня безпеки (threat) T від k-ї загрози для властивостей інформації, що циркулює в ІТС, здійснюємо за залежністю (1):

$$T = \frac{s + i + c + a}{4} p, \tag{1}$$

де: c – оцінка впливу k її загрози на конфіденційність інформації;

i, a та s – оцінки впливу k-ї загрози на цілісність, доступність та спостережність інформації відповідно;

p – ваговий коефіцієнт, який визначає частку появи даної загрози відносно усієї сукупності загроз та може обчислюватися на основі аналізу статистики функціонування ІТС або з використанням відомих методик прогнозування.

Проведено моделювання залежності (1) в системі MatLab з метою отримання наочних графічних залежностей кількісного показника рівня безпеки від складових (рис. 1-5)

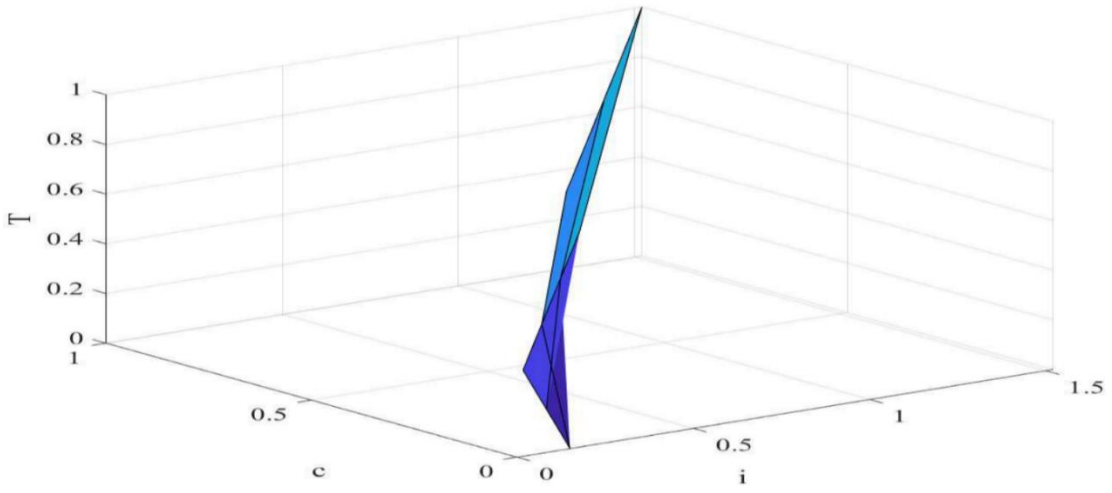

Рисунок 1 – Значення показника рівня безпеки при величинах складових
$s = [0,1]$, $i = [0,1]$, $a = [0,1]$, $c = [0,1]$, $p = [0,1]$

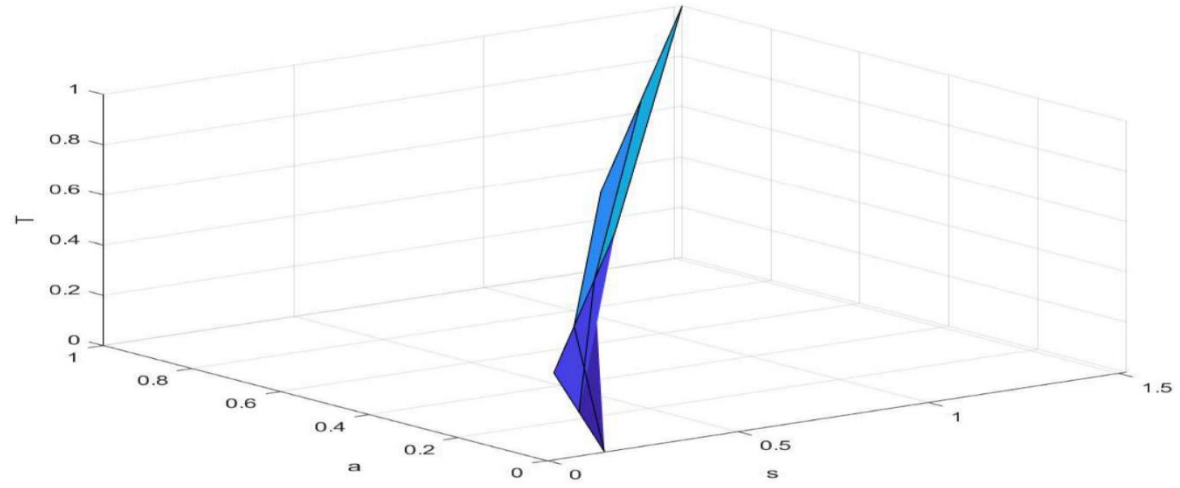

Рисунок.2 – Значення показника рівня безпеки при величинах складових
$s = [0,1]$, $i = [0,1]$, $a = [0,1]$, $c = [0,1]$, $p = [0,1]$

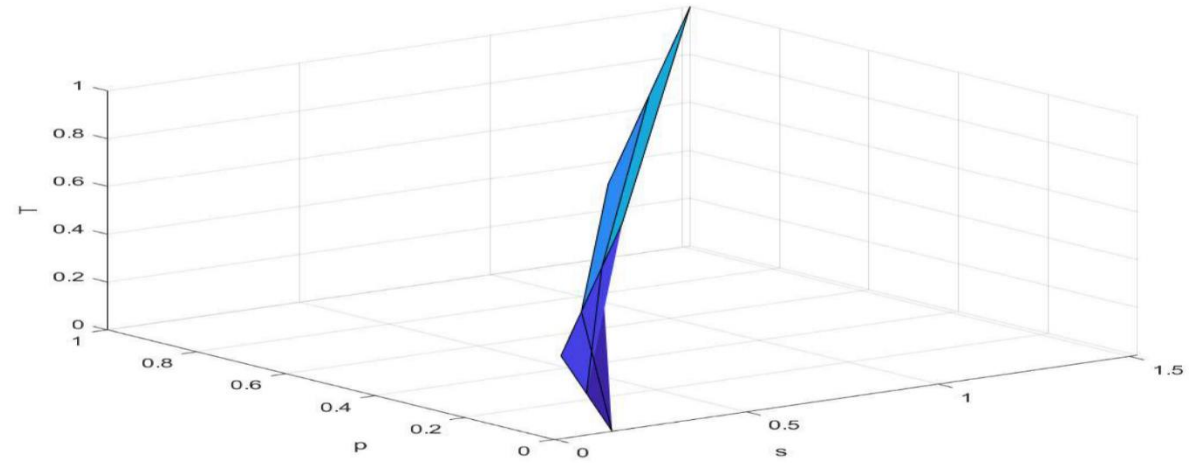

Рисунок 3 – Значення показника рівня безпеки при величинах складових
$s = [0,1]$, $i = [0,1]$, $a = [0,1]$, $c = [0,1]$, $p = [0,1]$

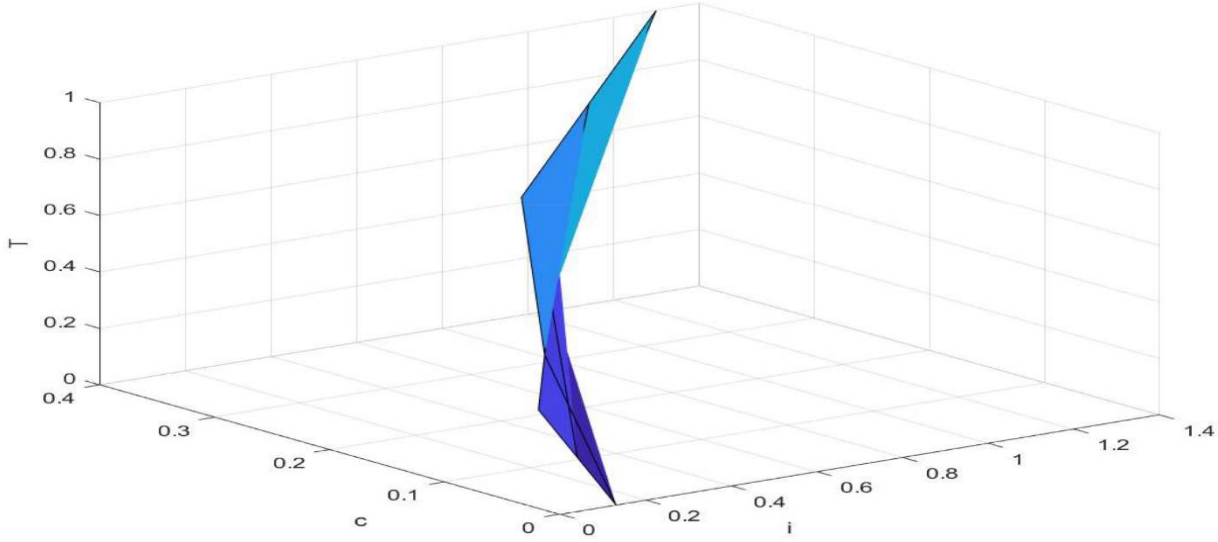

Рисунок 4 – Значення показника рівня безпеки при значеннях складових
$s = [0,1]$, $i = [0,1]$, $a = [0,1]$, $p = [0,1]$, $c = [0,0,4]$

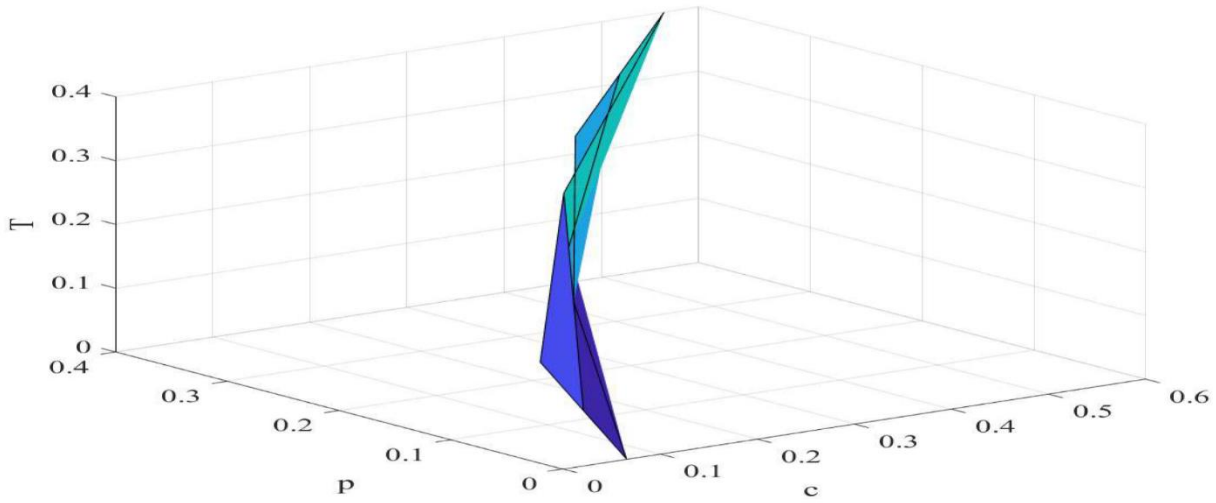

Рисунок 5 – Значення показника рівня безпеки при значеннях складових
$s = [0,1]$, $i = [0,1]$, $a = [0,1]$, $c = [0,0,4]$, $p = [0,0,4]$

Представляє інтерес оцінити кількісно імовірність того, що за час від початку функціонування системи захисту не відбудеться жодного протиправного доступу до інформації. Можна записати вираз визначення такого показника в залежності від: a – інтенсивності припинення системою захисту спроб нелегальних проникнень до інформації, b – інтенсивності таких спроб на вході в систему захисту; t – кількість діб дослідження.

$$P(t) = \frac{1}{2}\left[\left(1+\sqrt{\frac{a}{b}}\right)e^{-\left(a-\sqrt{ab}\right)t} + \left(1-\sqrt{\frac{a}{b}}\right)e^{-\left(a+\sqrt{ab}\right)t}\right], \quad (2)$$

Моделювання вказаної залежності в системі MatLab у залежності від кількісних значень вихідних показників представлено на рис. 6-14.

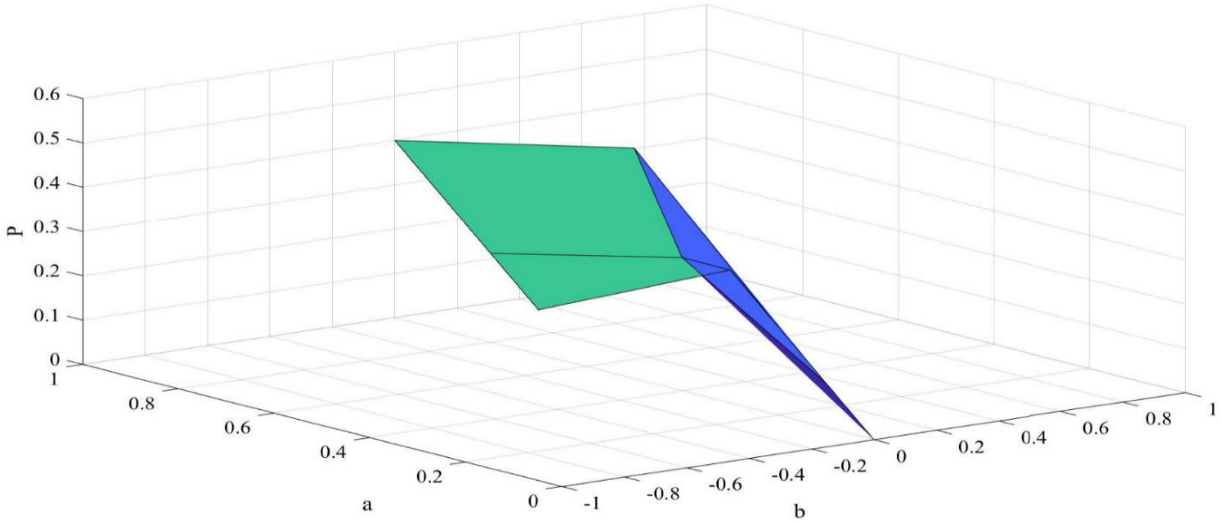

Рисунок 6 – Залежність того, що не відбудеться жодного протиправного доступу до інформації при $a = [0,1]$, $b = [0,1]$, $t = [1,16]$

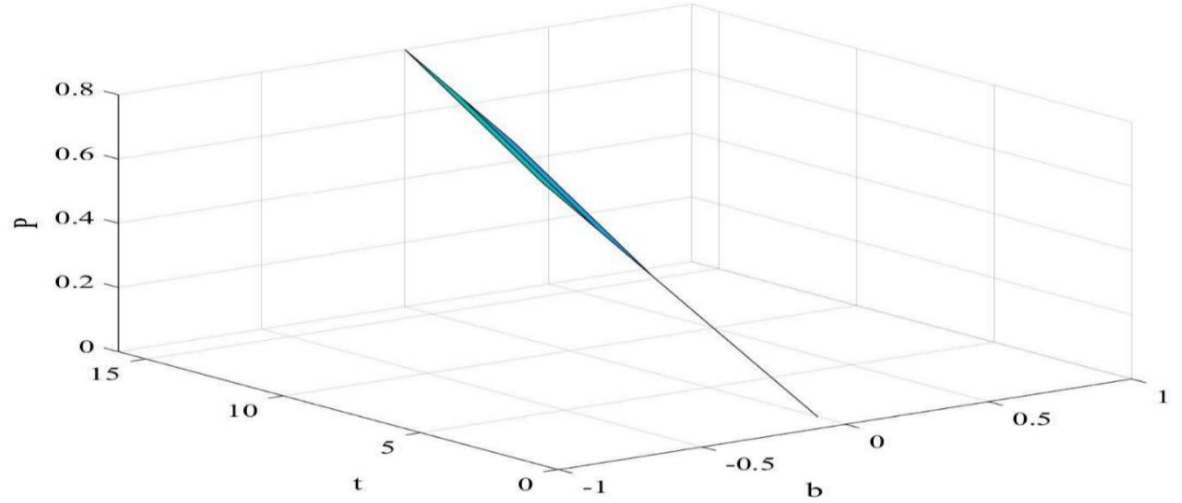

Рисунок 7 – Залежність того, що не відбудеться жодного протиправного доступу до інформації при $a = [0,1], b = [0,1], t = [1,16]$

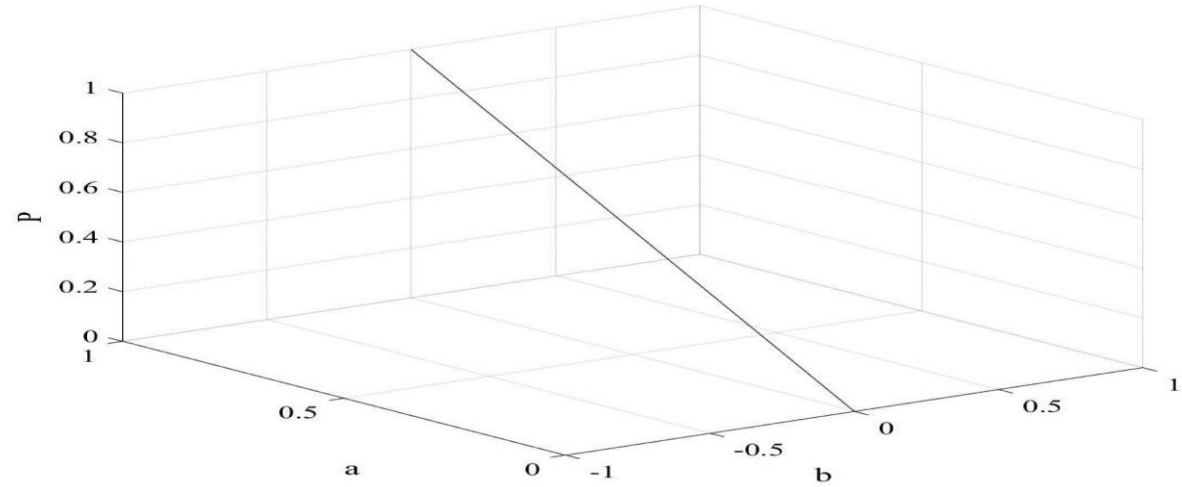

Рисунок 8 – Залежність того, що не відбудеться жодного протиправного доступу до інформації при $a = [0,1], b = [0,1], t = [1,16]$

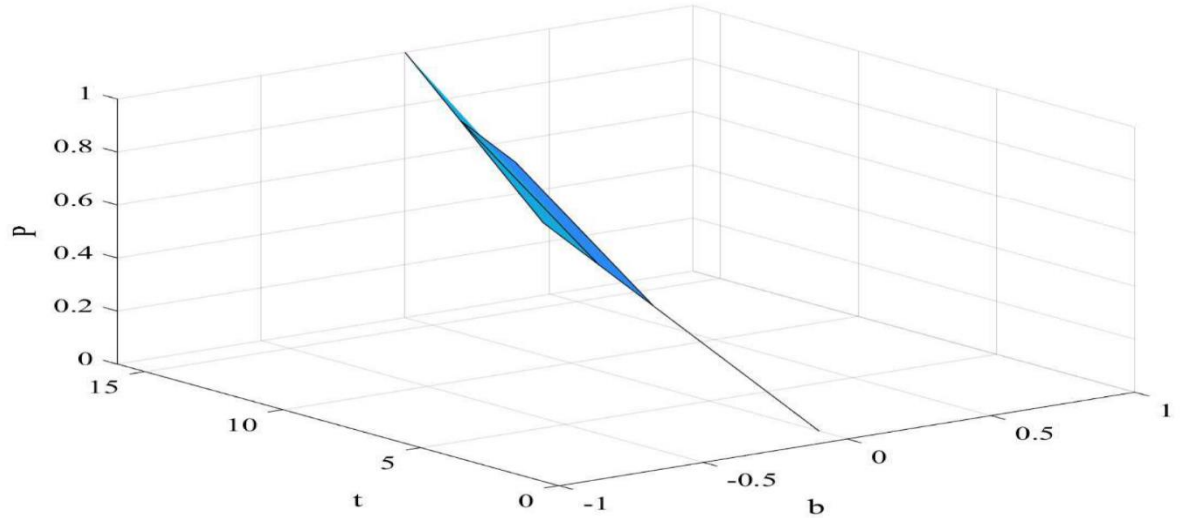

Рисунок 9. – Залежність того, що не відбудеться жодного протиправного доступу до інформації при значеннях вихідних показників $a = [0,0,8], b = [0,1], t = [1,16]$

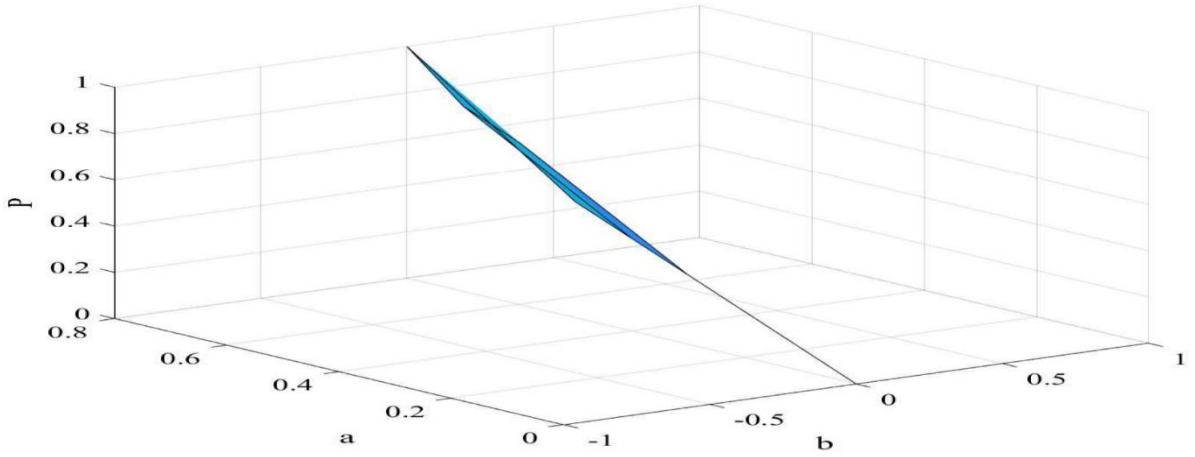

Рисунок 10 – Залежність того, що не відбудеться жодного протиправного доступу до інформації при значеннях вихідних показників $a = [0,1]$, $b = [0,1]$, $t = [1,16]$

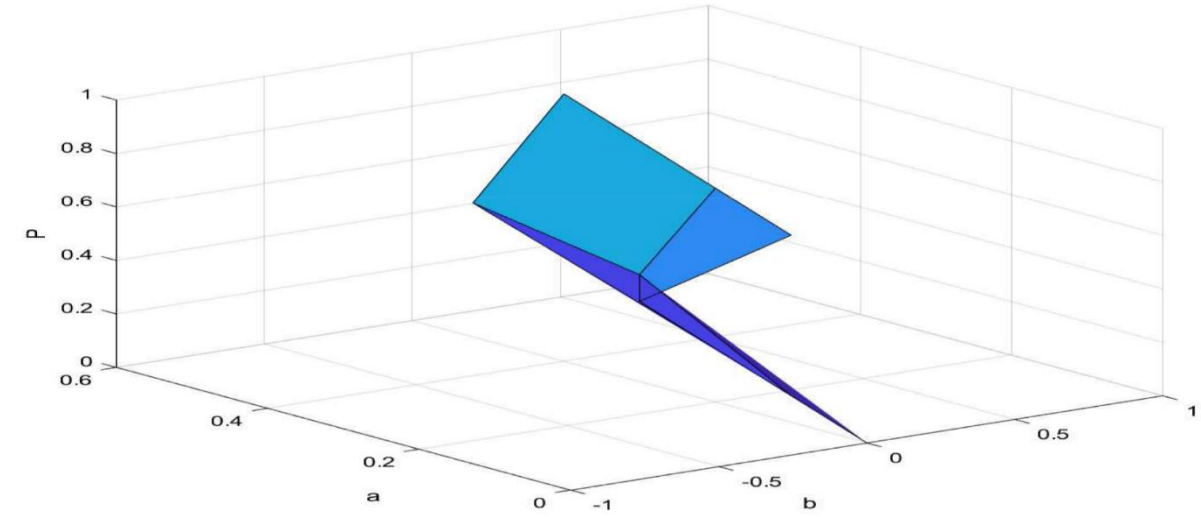

Рисунок 11 – Залежність того, що не відбудеться жодного протиправного доступу до інформації при значеннях вихідних показників $a = [0,\ 0,6]$, $b = [0,1]$, $t = [1,16]$

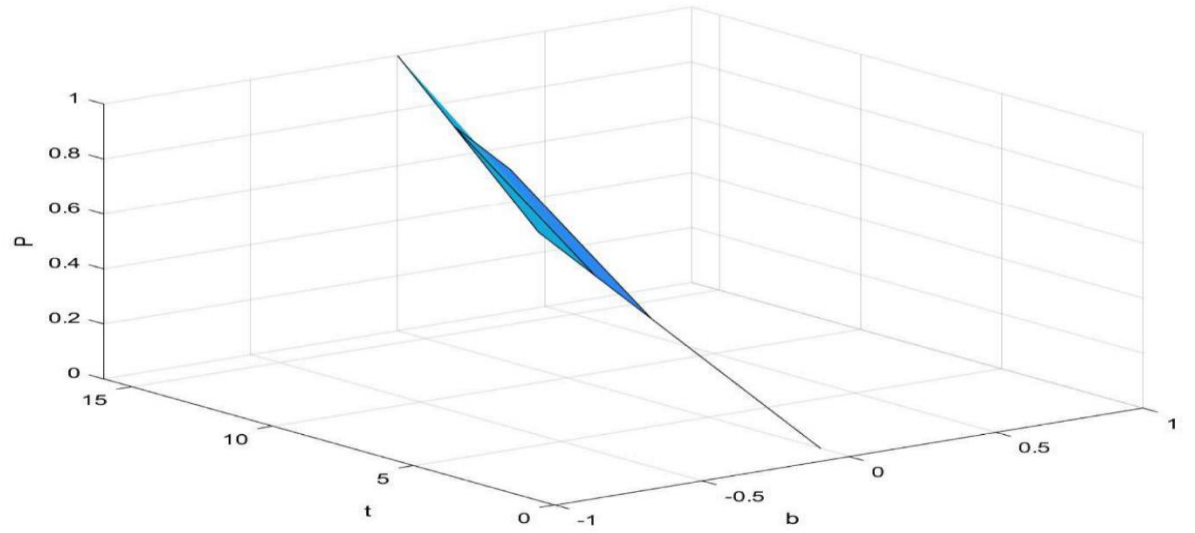

Рисунок 12 – Залежність того, що не відбудеться жодного протиправного доступу до інформації при значеннях вихідних показників $a = [0,1]$, $b = [0,0,8]$, $t = [1,16]$

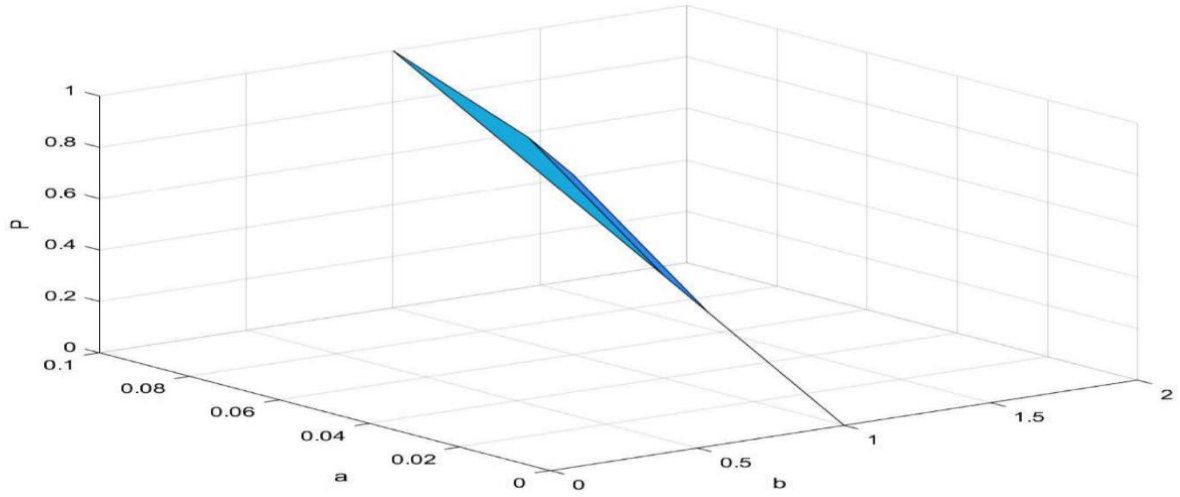

Рисунок 13 – Залежність того, що не відбудеться жодного протиправного доступу до інформації при значеннях вихідних показників $a = [0,1]$, $b = [0,1]$, $t = [1,16]$

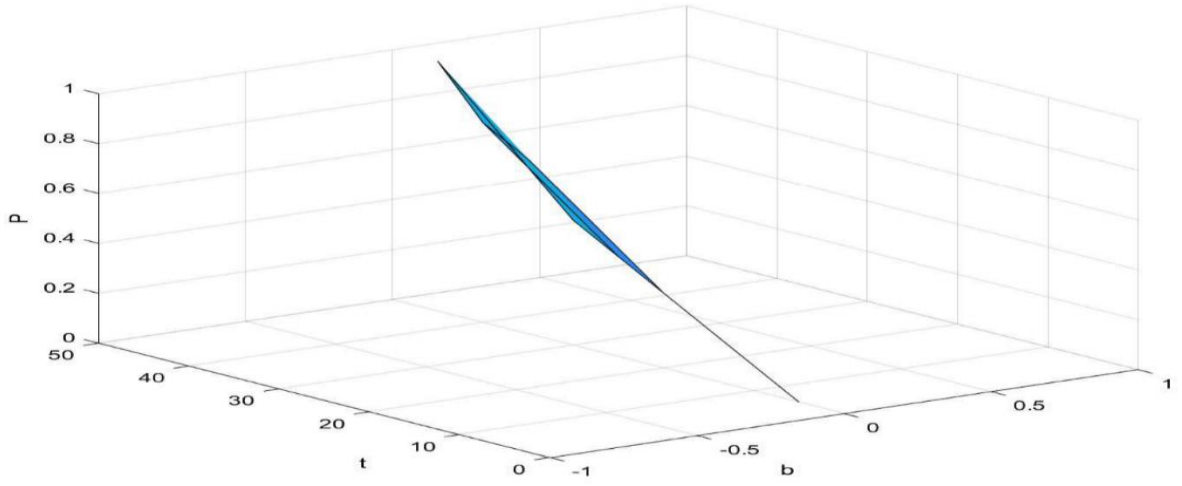

Рисунок 14 – Залежність того, що не відбудеться жодного протиправного доступу до інформації при значеннях вихідних показників $a = [0,1]$, $b = [0,1]$, $t = [5,45]$

Висновки та перспективи подальших досліджень. Залежність (1) показує можливість визначення рівня безпеки (threat) T від k-ї загрози для властивостей інформації, що циркулює в ІТС.

Шляхом графічного моделювання в системі Matlab 2022b (рис. 1-5) було доведено можливість забезпечення потрібного рівня безпеки при різних значеннях параметрів ІТС.

Особливості запропонованого методу і отриманих результатів полягають в одержанні кількісних показників рівня безпеки від специфічних параметрів ІТС, в тому числі, від параметрів: оцінка впливу k-ї загрози на конфіденційність інформації та цілісність, доступність та спостережність інформації відповідно, ваговий коефіцієнт p визначає частоту появи даної загрози відносно усієї сукупності загроз.

Подальший розвиток даного дослідження полягає у використані і виявленні нових факторів та параметрів.

Залежність (2) показує можливість визначення коли не відбудеться жодного протиправного доступу до інформації.

Шляхом моделювання в системі Matlab 2022b (рис. 6-14) було доведено можливість забезпечення коли не відбудеться жодного протиправного доступу до інформації ІТС.

Було встановлено, що система захисту інформації є нелінійною, що витікає з зовнішнього вигляду отриманих фігур.

Особливості запропонованого методу і отриманих результатів полягають в одержанні кількісних показників коли не відбудеться жодного протиправного доступу до інформації при значеннях вихідних показників ІТС, в тому числі, від параметрів: інтенсивності припинення системою захисту спроб нелегальних проникнень до інформації, інтенсивності таких спроб на вході в систему захисту; t – кількості діб дослідження.

Таким чином проведено оцінювання кількісно, рівня безпеки від оцінки впливу k-ї загрози на конфіденційність інформації, та цілісність, доступність та спостережність інформації відповідно, вагового коефіцієнта p який визначає частку появи даної загрози відносно усієї сукупності загроз.

А також, проведено оцінювання кількісно імовірності того, що за час від початку функціонування системи захисту не відбудеться жодного протиправного доступу до інформації, в залежності від: інтенсивності припинення системою захисту спроб нелегальних проникнень до інформації, інтенсивності таких спроб на вході в систему захисту; кількості діб дослідження. Мета, яка ставилась перед науковим дослідженням, була досягнута.

Подальший розвиток даного дослідження полягає у використані і виявленні нових факторів та параметрів, які впливають на рівень безпеки та що за час від початку функціонування системи захисту не відбудеться жодного протиправного доступу до інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] F.F. Hidalgo, C. Calero, and M.A. Moraga, “A Systematic Mapping Study of Software Reliability Modeling”, *Information and Software Technology*, vol. 56 (8), pp/ 839-849, 2024. doi: https://doi.org/10.1016/j.infsof.2014.03.006.

[2] В.С. Яковина, Д.В. Федасюк, та Н.М. Мамроха, “Аналіз використання аспектно-орієнтованого програмування як засобу підвищення надійності програмного забезпечення”, *Інженерія програмного забезпечення*, № 2, с. 24-29, 2010. [Електронний ресурс]. Доступно: https://jrnl.nau.edu.ua/index.php/IPZ/article/view/3533. Дата звернення: Лип. 19, 2024.

[3] Є. Рижов, Л. Сакович, С. Глухов, та Ю. Настишин, “Оцінка впливу діагностичного забезпечення на надійність радіоелектронних систем”, *Військово–технічний збірник*, № 24, с. 3-8, 2021. doi: https://doi.org/10.33577/2312-4458.24.2021.3-8.

[4] V. Akhramovych, Y. Pepa, A. Zahynei1, V. Akhramovych, T. Dzyuba, and I. Danylov, “Method for calculating the information security indicator in social media with considerationof the path durationbetween clients”, *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska* (*IAPGOS*), vol. 14, no. 1, pp. 71-77, 2024. doi: http://doi.org/10.35784/iapgos.5720.2024.03.31.

[5] R. Khrashchevskyi, V. Klobukov, V. Kozlovskyi, V. Akhramovych, and S. Lazarenko, “Method of calculating information protection from mutual influence of users in social networks”, *Inter. Jour. of Comp. Net. and Inf. Sec.* (*IJCNIS*), vol. 15, no. 5, pp. 27-40, 2023. doi: https://doi.org/10.5815/ijcnis.2023.05.03.

[6] J.M. Borky, T.H. Bradley, “Protecting Information with Cybersecurity”, in *Effective Model-Based Systems Engineering*. NY, USA: Springer International Publishing AG, 2019, pp. 345-404. doi: https://doi.org/10.1007/978-3-319-95669-5_10.

[7] F.R. Kifaru, K.D. Kavuta, and A.A. Semlambo, “Assessment of the impacts of cyber security on student information management systems: a case of Ruaha Catholic University”, *The Journal of Informatics*, vol. 3, iss. 1 pp. 51-67, 2023. doi: https://doi.org/10.59645/tji.v3i1.127.

[8] О.С. Власюк, *Теорія і практика економічної безпеки в системі науки та економіки*. Київ, Україна: Нац. Ін-т проблем міжнар. безпеки при Раді нац. безпеки і оборони України, 2008.

[9] О.М. Правдивець, "Наукові підходи до дослідження системи економічної безпеки підприємства", *Регіональна економіка*, №4 (110). с. 74-90. 2023. doi: https://doi.org/10.36818/1562-0905-2023-4-8.

[10] M. Ekstedt, Z. Afzal1, P. Mukherjee, S. Hacks, and R. Lagerström, "Yet another cybersecurity risk assessment framework", *International Journal of Information Security*, vol. 22, pp.1713-1729, 2023. doi: https://doi.org/10.1007/s10207-023-00713-y.

Стаття надійшла до редакції 15.11.2024.

REFERENCE

[1] F.F. Hidalgo, C. Calero, and M.A. Moraga, "A Systematic Mapping Study of Software Reliability Modeling", *Information and Software Technology*, vol. 56 (8), pp/ 839-849, 2024. doi: https://doi.org/10.1016/j.infsof.2014.03.006.

[2] V.S. Yakovina, D.V. Fedasiuk, and N.M Mamroha, "Analysis of the use of aspect-oriented programming as a means of increasing the reliability of software", *Software engineering*, no. 2, pp. 24-29, 2010. [Online]. Available: https://jrnl.nau.edu.ua/index.php/IPZ/article/view/3533. Accessed on: July 19, 2024.

[3] E. Ryzhov, L. Sakovich, S. Glukhov, and Yu. Nastyshyn, "Assessment of the impact of diagnostic support on the reliability of radio electronic systems", *Military and technical collection*, no. 24, pp. 3-8, 2021. doi: https://doi.org/10.33577/2312-4458.24.2021.3-8.

[4] V. Akhramovych, Y. Pepa, A. Zahynei1, V. Akhramovych, T. Dzyuba, and I. Danylov, "Method for calculating the information security indicator in social media with considerationof the path durationbetween clients", *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska* (*IAPGOS*), vol. 14, no. 1, pp. 71-77, 2024. doi: http://doi.org/10.35784/iapgos.5720.2024.03.31.

[5] R. Khrashchevskyi, V. Klobukov, V. Kozlovskyi, V. Akhramovych, and S. Lazarenko, "Method of calculating information protection from mutual influence of users in social networks", *Inter. Jour. of Comp. Net. and Inf. Sec.* (*IJCNIS*), vol. 15, no. 5, pp. 27-40, 2023. doi: https://doi.org/10.5815/ijcnis.2023.05.03.

[6] J.M. Borky, T.H. Bradley, "Protecting Information with Cybersecurity", in *Effective Model-Based Systems Engineering*. NY, USA: Springer International Publishing AG, 2019, pp. 345-404. doi: https://doi.org/10.1007/978-3-319-95669-5_10.

[7] F.R. Kifaru, K.D. Kavuta, and A.A. Semlambo, "Assessment of the impacts of cyber security on student information management systems: a case of Ruaha Catholic University", *The Journal of Informatics*, vol. 3, iss. 1 pp. 51-67, 2023. doi: https://doi.org/10.59645/tji.v3i1.127.

[8] O.S. Vlasyuk, *Theory and practice of economic security in the system of science and economics*. Kyiv, Ukraine: National Institute of International Security Problems at the Council of National security and defense of Ukraine, 2008.

[9] O.M. Pravdyvets, "Scientific approaches to the study of the economic security system of the enterprise", *Regional economy*, no. 4 (110). pp. 74-90. 2023. doi: https://doi.org/ 10.36818/1562-0905-2023-4-8.

[10] M. Ekstedt, Z. Afzal1, P. Mukherjee, S. Hacks, and R. Lagerström, "Yet another cybersecurity risk assessment framework", *International Journal of Information Security*, vol. 22, pp.1713-1729, 2023. doi: https://doi.org/10.1007/s10207-023-00713-y.

VOLODYMYR AKHRAMOVYCH,
VADYM AKHRAMOVYCH

QUANTITATIVE ASSESSMENT OF THE PROBABILITY OF PROTECTIVE SYSTEM FUNCTIONING WITHOUT UNLAWFUL ACTIONS

Information security, also known as InfoSec, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, or destruction of information. The primary goal of information security is to achieve a balanced protection of data confidentiality, integrity, and availability, while considering the expediency of application and without any harm to the organization's productivity.

In this paper, the security levels (threats) T of the k-th threat to the properties of information circulating in the information and telecommunications system (ITS) are obtained from the parameters: c – assessment of the impact of the k–th threat on the confidentiality of information, i, a and s – assessments of the impact of the k-th threat on the integrity, availability, and observations of information, respectively. The weight coefficient p determines the share of the occurrence of this threat relative to the entire set of threats and can be calculated based on the analysis of ITS operation statistics or using known forecasting methods.

The probability of no unauthorized access to information during the operation of the protection system has been quantitatively assessed. The assessment is based on the parameters: a – the intensity of the protection system's suppression of attempts to illegally access information, b – the intensity of such attempts at the input to the protection system, t – the number of days of the system's operation.

For graphical interpretation of the dependencies, graphical materials are presented. For this purpose, modeling was performed in the MatLab system. The graphical materials clearly indicate the possibility of obtaining a state of operation of the protection system without unauthorized actions depending on the influence of threats to confidentiality, integrity, availability of information, and unauthorized access to information depending on the parameters of the intensity of suppression by the protection system of attempts to illegally access information, and the intensity of such attempts at the input to the protection system.

This will, unlike analogues, allow developers of information systems and service personnel to have quantitative indicators of the probability of no unauthorized access to information and to make decisions regarding possible vulnerabilities.

Keywords: security levels; unauthorized access to information, parameters, probability, model, dependency, graphical interpretation.

Ахрамович Володимир Миколайович, д.т.н., проф., професор кафедри Систем інформаційного та кібернетичного захисту, Державнийо університет інформаційно-комунікаційних технологій, Київ, Україна. ORCID 0000-0002-0086-9131, 12z@ukr.net.

Ахрамович Вадим Володимирович, завідувач комп'ютерним центром, Національна академія статистики, обліку та аудиту, Київ, Україна. ORCID 0009-0003-2787-8745, 12zstzi@gmail.com.

Akhramovych Volodymyr, doctor of technical sciences, professor, professor at the academic department of information and cyber defense systems, State university of telecommunications, Kyiv, Ukraine.

Akhramovych Vadym, head of the computing center, National academy of statistics, accounting and auditing, Kyiv, Ukraine.