DOI 10.31891/2307-5732-2025-347-55
УДК 004.056:004.942

МАЛИЦЬКИЙ ТАРАС
Хмельницький національний університет
e-mail: tarasmalitskyi@gmail.com
ЧЕШУН ВІКТОР
Хмельницький національний університет
https://orcid.org/0000-0002-3935-2068
e-mail: cheshunvn@khmnu.edu.ua
ОЛЕКСЮК ДМИТРО
Хмельницький фаховий економіко-технологічний коледж УЕП
https://orcid.org/0009-0006-3735-1930
e-mail: oleksuk.dima@gmail.com
ЧЕШУН ДМИТРО
Хмельницький фаховий економіко-технологічний коледж УЕП
e-mail: dmitry_95@ukr.net

МАТЕМАТИЧНА МОДЕЛЬ МЕТОДУ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ КОРПОРАТИВНОЇ МЕРЕЖІ ІЗ ЗАСТОСУВАННЯМ ІМОВІРНІСНИХ КРИТЕРІЇВ ДОВІРИ

Стаття присвячена презентації математичної моделі методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу із застосуванням імовірнісних критеріїв довіри. За результатами аналізу покладених на метод завдань, концептуально математичну модель методу захисту інформаційних ресурсів корпоративної мережі класифіковано як ймовірнісну статистичну модель систем управління доступом на основі концепції (критеріїв) довіри. Математична модель методу базується на аналізі взаємодії між різними суб'єктами (користувачами) та об'єктами (інформаційними ресурсами) в інформаційному середовищі корпоративної мережі та дає інструментарій для визначення ступеня довіри до суб'єктів інформаційних відносин в корпоративній мережі з точки зору інформаційної безпеки. Принципи застосування моделі продемонстровано структурно-логічною схемою взаємозв'язку елементів математичної моделі в реалізації методу.

Ключові слова: захист інформації, контроль доступу, корпоративна мережа, критерії довіри.

MALYTSKYI TARAS, CHESHUN VIKTOR
Khmelnytsky National University
OLEKSIUK DMYTRO, CHESHUN DMYTRO
Khmelnytskyi Vocational Economic and Technological College of the UEE

MATHEMATICAL MODEL OF THE METHOD OF PROTECTING CORPORATE NETWORK INFORMATION RESOURCES USING PROBABILITY TRUST CRITERIA

Abstract. The article is devoted to the presentation of a mathematical model of the method of protecting information resources of the corporate network from unauthorized access using probabilistic trust criteria. According to the results of the analysis of the tasks assigned to the method, the conceptual mathematical model of the method of protecting information resources of the corporate network is classified as a probabilistic statistical model of access control systems based on the concept (criteria) of trust. The mathematical model of the method is focused on the statistical analysis of the interaction between various subjects (users) and objects (information resources) in the information environment of the corporate network and provides a toolkit for determining the degree of trust in subjects of information relations in the corporate network from the point of view of information security.

Plural of objects and subjects of information relations are identified in the model. A binary access matrix was selected as the main element for managing access to information resources of the corporate network, the rules for its formation are detailed. A formula for calculating the probabilistic criterion of trust in the user based on statistical data about his actions in the network is also proposed. The principles of using the data of the vector of trust criteria and the vector of limit restrictions for making changes to the user's access rights are defined. The change of access rights is implemented in real time through the adjustment of the access matrix taking into account the decrease in the criterion of trust in the user according to the statistics of his work.

The principles of applying the model are demonstrated by the structural and logical diagram of the relationship between the elements of the mathematical model in the implementation of the method.

Keywords: information protection, access control, corporate network, trust criteria.

Вступ

Поширення цифрових технологій та нарощування їх можливостей супроводжується одночасним збільшенням кількості кіберзагроз. За таких умов ключовим аспектом сучасного бізнесу стає безпека корпоративних мереж як основної інфраструктури для забезпечення зв'язку і ефективної взаємодії між всіма рівнями організації, а також головного сховища комерційної та конфіденційної інформації.

Забезпечення ефективної безпеки корпоративних мереж вимагає комплексного підходу, який охоплює технологічні інновації та докладний аналіз потенційних загроз [1]. Технологічні інновації включають організаційні та програмно-апаратні заходи безпеки, такі як міжмережеві екрани, антивірусне програмне забезпечення, шифрування даних, аутентифікація та авторизація, навчання персоналу, регулярні оновлення та патчі, резервне копіювання та відновлення даних, а також моніторинг та аналіз активності мережі.

Одним із головних аспектів інформаційної безпеки корпоративних мереж є саме постійний моніторинг та аналіз активності мережі для блокування потенційно можливих шкідливих дій з інформаційними ресурсами [2]. Систематичний моніторинг мережі та виявлення загроз дозволяють не лише своєчасно реагувати на кібератаки та аномальну активність, але і запобігати можливим інцидентам кібербезпеки.

Постановка задачі

Ефективність заходів і засобів захисту інформаційних ресурсів корпоративних мереж полягає не тільки в можливості якнайшвидшого виявлення і блокування шкідливої активності користувачів, але й в прогнозуванні та попередженні можливих зловмисних дій. При цьому будь-яка оцінка потребує використання певних критеріїв.

В галузі інформаційної безпеки існує досить велика кількість національних і міжнародних стандартів, що пропонують різні підходи до вибору і застосування критеріїв оцінки безпеки інформаційних систем різних класів. До таких стандартів можна віднести: «Критерії оцінки довірених комп'ютерних систем Міністерства оборони» (TCSEC) [3,4], розроблені у США; Європейські стандарти під назвою «Критерії оцінки безпеки ІТ» (ITSEC) [5,6]; «Федеральні критерії» (FC) Германії [7,8]; «Канадські критерії безпеки комп'ютерних систем CTCPEC» [5,9]; «Загальні критерії оцінки безпеки інформаційних технологій» [10,11]; серії міжнародних стандартів ISO/IEC [12] тощо.

Міжнародні стандарти стали важливим еталоном оцінки безпеки інформаційних технологій та забезпечили загальноприйняті критерії для оцінки рівня захищеності ІТ-продуктів [13], але не надали універсальних критеріїв для всіх завдань кібербезпеки, що зумовило появу нових об’єктно-орієнтованих рішень.

В роботі [14] пропонується методика оцінювання ефективності системи інформаційної безпеки міністерства оборони та ЗСУ, яка ґрунтується на удосконаленій системі критеріїв та показників оцінювання ефективності функціонування системи забезпечення інформаційної безпеки. Автори методики оцінки захищеності інформаційних систем [15] пропонують здійснювати оцінку через розрахунок зв'язків, показників категорій та узагальненого показника, що беруть участь у оцінці, для надання рекомендацій щодо підвищення безпеки інформаційної системи.

Одним із перспективних напрямків оцінки захисту інформаційних ресурсів від несанкціонованого доступу, що активно розвивається, є використання в оцінці критеріїв довіри. Для прикладу, механізм оцінки аудиту SOC 2 [16] дозволяє виміряти ефективність функціонування системи безпеки компанії, спираючись на основні стандартів та Критеріїв довірених сервісів. Ці критерії дозволяють компанії визначити ступінь вірогідності, що процеси і системи відповідають встановленим нормам безпеки, конфіденційності, обробки, конфігурації та доступності даних.

Проведені дослідження свідчать про можливість застосування імовірнісних оцінок критеріїв довіри для захисту від несанкціонованого доступу інформаційних ресурсів корпоративної мережі. Для реалізації і апробації відповідної технології першочергово набуває актуальності задача вибору елементів математичної моделі.

Основна частина

Типовими сторонами, що вступають у взаємодію при реалізації систем управління доступом, є користувачі та інформаційні ресурси, ідентифіковані в Законі України «Про інформацію» [17] як суб'єкти і об'єкти інформаційних відносин. Для ідентифікації в математичній моделі суб'єктів і об'єктів інформаційних використано теорію множин:

$$\text{SUBJECTS}: \{\text{Subject}_1, \text{Subject}_2, \ \dots\ , \text{Subject}_i, \ \dots\ , \text{Subject}_k\}, \tag{1}$$

$$\text{OBJECTS}: \{\text{Object}_1, \text{Object}_2, \ \dots\ , \text{Object}_j, \ \dots\ , \text{Object}_n\}, \tag{2}$$

де SUBJECTS – множина, що відображує всіх користувачів корпоративної мережі $\text{Subject}_i \in \text{SUBJECTS}$, якими можуть бути як звичайні користувачі мережі з різними посадовими обов’язками (керівництво, посадові особи, оператори тощо), так і адміністратори цієї мережі; OBJECTS – множина, що відображує облікові об’єкти інформаційної взаємодії інформаційні ресурси корпоративної мережі $\text{Object}_j \in \text{OBJECTS}$, якими можуть бути бази даних, програмне забезпечення, файлові елементи, накопичувачі даних тощо.

Для відображення взаємодії об’єктів і суб’єктів інформаційних відносин найбільш інформативною і зручною в подальшій обробці є матрична форма представлення даних. З урахуванням приналежності математичної моделі методу до підкласу моделей систем управління доступом прийнято рішення обрати типовий для систем контролю доступу варіант представлення є даних у матричній формі – матрицю доступу [18]. Для зручності математичної обробки в моделі використано матрицю прав доступу булевого типу, в якій кожен елемент $AR_{ij} \in \text{MatrixOfAccessRights}$ є бінарним однорозрядним числом, що визначається за правилом:

$$AR_{ij} = \begin{cases} 0, \ \text{якщо суб'єкт } \text{Subject}_i \in \text{SUBJECTS не має прав доступу до ресурсу } Object_j \in \text{OBJECTS}, \\ 1, \ \text{якщо суб'єкт } \text{Subject}_i \in \text{SUBJECTS має права доступу до ресурсу } Object_j \in \text{OBJECTS}. \end{cases} \tag{3}$$

В узагальненому представлені матриця прав доступу множини користувачів корпоративної мережі SUBJECTS до множини облікованих інформаційних ресурсів корпоративної мережі OBJECTS має формат:

$$\text{MatrixOfAccessRights} = \begin{vmatrix} AR_{1,1} & AR_{1,2} & \dots & AR_{1,|\text{OBJECTS}|} \\ AR_{2,1} & AR_{2,2} & \cdots & AR_{2,|\text{OBJECTS}|} \\ \vdots & \vdots & & \vdots \\ AR_{|\text{SUBJECTS}|,1} & AR_{|\text{SUBJECTS}|,2} & \cdots & AR_{|\text{SUBJECTS}|,|\text{OBJECTS}|} \end{vmatrix} \tag{4}$$

Наступний заявлений компонент моделі – матриця фіксації санкціонованих (дозволених) дій

користувачів $\text{Subject}_i \in \text{SUBJECTS}$ корпоративної мережі в полі інформаційних ресурсів $\text{Object}_j \in \text{OBJECTS}$, яка в моделі ідентифікується як матриця санкціонованих дій MatrixOfAuthorizedActions з узагальненим представленням:

$$\text{MatrixOfAuthorizedActions} = \begin{vmatrix} AA_{1,1} & AA_{1,2} & \dots & AA_{1,|\text{OBJECTS}|} \\ AA_{2,1} & AA_{2,2} & \cdots & AA_{2,|\text{OBJECTS}|} \\ \vdots & \vdots & & \vdots \\ AA_{|\text{SUBJECTS}|,1} & AA_{|\text{SUBJECTS}|,2} & \cdots & AA_{|\text{SUBJECTS}|,|\text{OBJECTS}|} \end{vmatrix} \quad (5)$$

Кожен елемент матриці санкціонованих дій $AA_{ij} \in \text{MatrixOfAuthorizedActions}$, фактично, відіграє роль лічильника санкціонованих дій користувачів $\text{Subject}_i \in \text{SUBJECTS}$ корпоративної мережі в полі інформаційних ресурсів $\text{Object}_j \in \text{OBJECTS}$ (дій, які не порушують прав доступу користувачів до інформаційних ресурсів мережі).

Для фіксації спроб (вдалих або невдалих) здійснення несанкціонованих (заборонених) дій користувачів $\text{Subject}_i \in \text{SUBJECTS}$ корпоративної мережі в полі інформаційних ресурсів $\text{Object}_j \in \text{OBJECTS}$ в моделі використовується матриця заборонених дій MatrixOfProhibitedActions з узагальненим представленням:

$$\text{MatrixOfProhibitedActions} = \begin{vmatrix} PA_{1,1} & PA_{1,2} & \dots & PA_{1,|\text{OBJECTS}|} \\ PA_{2,1} & PA_{2,2} & \cdots & PA_{2,|\text{OBJECTS}|} \\ \vdots & \vdots & & \vdots \\ PA_{|\text{SUBJECTS}|,1} & PA_{|\text{SUBJECTS}|,2} & \cdots & PA_{|\text{SUBJECTS}|,|\text{OBJECTS}|} \end{vmatrix} \quad (6)$$

Кожен елемент матриці заборонених дій $PA_{ij} \in \text{MatrixOfProhibitedActions}$ є лічильником спроб доступу до інформаційного ресурсу $\text{Object}_j \in \text{OBJECTS}$, які порушують надані користувачу $\text{Subject}_i \in \text{SUBJECTS}$ права.

Матриці санкціонованих дій MatrixOfAuthorizedActions і заборонених дій MatrixOfProhibitedActions відображають задекларовану в концептуальних положеннях методу приналежність математичної моделі до різновидів статистичних моделей, оскільки вони мають використовуватись для аналізу випадкових процесів та подій у корпоративній мережі, пов'язаних з поведінкою користувачів $\text{Subject}_i \in \text{SUBJECTS}$, яку апріорно неможливо передбачити. В даній інтерпретації математичної моделі як лічильники накопичення будуть працювати лише елементи $AA_{ij} \in \text{MatrixOfAuthorizedActions}$, для яких $AR_{ij}=1$, тобто, робота користувача з ресурсами, до яких йому надано права доступу. Як лічильники накопичення заборонених дій будуть працювати елементи $PA_{ij} \in \text{MatrixOfProhibitedActions}$, для яких $AR_{ij}=0$, тобто, дії користувача з ресурсами, до яких йому заборонено доступ.

Наступним кроком деталізуємо в математичній моделі задекларовану в ймовірнісну статистичну складову, якою передбачається використання ймовірнісні підходів прогнозування-попередження зловмисних дій та статистичних методів аналізу поведінки користувачів. Перехід від статистичних даних до імовірнісних оцінок будемо виконувати традиційними для таких задач способами через розрахунок $\text{Subject}_i \in \text{SUBJECTS}$ співвідношення санкціонованих дій кожного користувача $\text{Subject}_i \in \text{SUBJECTS}$ до його загальної активності:

$$P(\text{AuthorizedActions})_i = \sum_{\forall(AA_{ij}+PA_{ij})>0}^{j=0}{}^{|OBJECTS|} \frac{AA_{ij}}{AA_{ij}+PA_{ij}}, \quad (7)$$

де $P(\text{AuthorizedActions})_i$ – статистична імовірність роботи користувача $\text{Subject}_i \in \text{SUBJECTS}$ без несанкціонованих дій в полі OBJECTS інформаційних ресурсів корпоративної мережі. Обмеження $\forall(AA_{ij}+PA_{ij})>0$ в формулу (7) введене через можливу нульову статистичну активність користувачів, які з різних причин ще не працювали в мережі (новозарахованих користувачів тощо), що враховується при обчисленні статистичної імовірності санкціонованих дій $P(\text{AuthorizedActions})_i$ для уникнення ситуації з діленням на нуль.

Статистична імовірність коректності дій користувача $\text{Subject}_i \in \text{SUBJECTS}$ в полі OBJECTS інформаційних ресурсів корпоративної мережі передбачається до використання як основний критерій довіри для захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу. Для більш наочного представлення розраховувані за формулою (7) значення групуються у вигляді вектора критеріїв довіри VectorOfTrustCriteria:

$$\text{VectorOfTrustCriteria} = \begin{vmatrix} P(\text{AuthorizedActions})_1 \\ P(\text{AuthorizedActions})_2 \\ \vdots \\ P(\text{AuthorizedActions})_{|\text{SUBJECTS}|} \end{vmatrix}. \quad (8)$$

Обмеження для блокування прав доступу користувачів $\text{Subject}_i \in \text{SUBJECTS}$ за критерієм довіри до кожного облікованого інформаційного ресурсу $\text{Object}_j \in \text{OBJECTS}$ в моделі представлені як вектор граничних обмежень VectorOfBoundaryConstraints:

$$\text{VectorOfBoundaryConstraints} = \begin{vmatrix} BC_1 \\ BC_2 \\ \vdots \\ BC_{|\text{OBJECTS}|} \end{vmatrix}, \quad (9)$$

де BC_j – рівень обмеження довірчого допуску користувачів $\text{Subject}_i \in \text{SUBJECTS}$ до ресурсу $\text{Object}_j \in \text{OBJECTS}$.

На рисунку 1 представлена структурно-логічна схема взаємозв'язку елементів математичної моделі в реалізації захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу на основі імовірнісних оцінок критеріїв довіри.

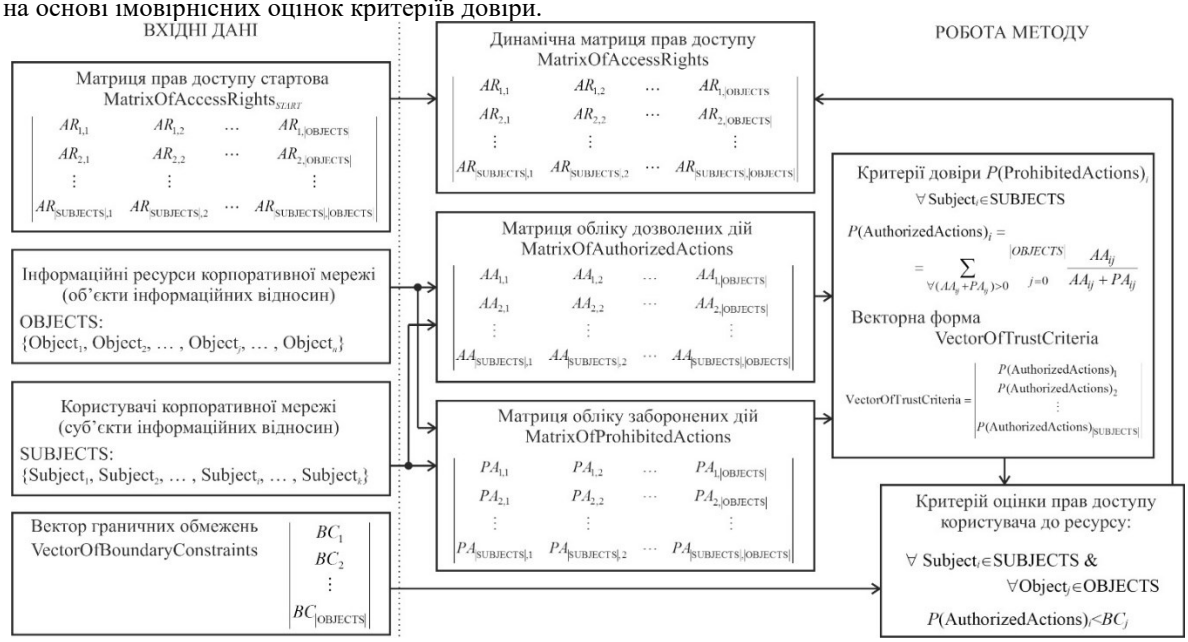

Рис. 1 – Структурно-логічна схема взаємозв'язку складових математичної моделі в реалізації методу

Основою для корегування прав доступу є рівень обмеження довірчого допуску $BC_j \in \text{VectorOfBoundaryConstraints}$ користувачів SUBJECTS до ресурсу $\text{Object}_j \in \text{OBJECTS}$ і значення імовірнісної критерія оцінки довіри $P(\text{AuthorizedActions})_i$ до користувача $\text{Subject}_i \in \text{SUBJECTS}$. Після зменшення рівня довіри до користувача нижче за рівень обмеження довірчого допуску $P(\text{AuthorizedActions})_i < BC_j$, доступ до ресурсу $\text{Object}_j \in \text{OBJECTS}$ користувачу $\text{Subject}_i \in \text{SUBJECTS}$ автоматично блокується до прийняття рішення щодо подальших заходів комісією (експертами) з розслідування інцидентів інформаційної безпеки

Висновки

В статті презентовано математичну модель методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу із застосуванням імовірнісних критеріїв довіри. Математична модель методу базується на аналізі взаємодії між різними суб'єктами (користувачами) та об'єктами (інформаційними ресурсами) в інформаційному середовищі корпоративної мережі та дає інструментарій для визначення ступеня довіри до суб'єктів інформаційних відносин в корпоративній мережі з точки зору інформаційної безпеки. В якості критерію довіри до суб'єктів взаємодії в інформаційному просторі корпоративної мережі використовується імовірнісний показник, що формується на основі накопичуваної статистики попередньої діяльності кожного суб'єкта із урахуванням зафіксованих випадків шкідливої активності відносно загального показника активності.

Математичну модель методу захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу ідентифіковано як ймовірнісну статистичну модель систем управління доступом на основі концепції (критеріїв) довіри.

Література

1. Карпович І.М., Гладка О.М., Наконечна Ю.А. Аналіз ризиків безпеки інформаційної системи ІТ-підприємства. *Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки.* 2020. Том 31 (70) № 5. С. 69-74.

2. Храпкін О.М. Захист інформаційно-комунікаційної мережі установи від несанкціонованого доступу. *Системи озброєння і військова техніка*. 2020. № 3(63). С.45-53.

3. Livshitz I.I., Neklyudov A.V., Lontsikh P.A. Evaluation of IT security – genesis and its state-of-art. *International Conference Information Technologies in Business and Industry* 2018. IOP Publishing. 2018. С. 1-7.

4. Lawrence C. Miller and Peter H. Gregory. Evaluation Criteria of Systems Security Controls. *CISSP Articles*. 2018. URL: https://www.dummies.com/article/academics-the-arts/study-skills-test-

prep/cissp/evaluation-criteria-systems-security-controls-254878/ (дата звернення: 30.11.2023).

5. Abhi G. CISSP Concepts – Trusted Computing Base/ TCEC, ITSEC and Common Criteria. *Cyber Management Alliance Articles.* Jan 28, 2020. URL: https://www.cm-alliance.com/cissp/trusted-computing-base/-tcec-itsec-and-common-criteria (дата звернення: 30.11.2023).

6. Randal Allen. Evolved Artificial Intelligence for Stochastic Clustering Unsupervised Learning. *Interservice/Industry Training, Simulation, and Education Conference.* 2020. Paper № 20258. 8 p.

7. Donald P. Kommersю The Basic Law: A Fifty Year Assessment. *German Law Journal.* 2019. Volume 20, Issue 4. P. 571-582.

8. Турчак А. Основні складові інформаційної безпеки держави. *Аспекти публічного управління.* Том 7, № 5. 2019. С. 44-56.

9. The Canadian Trusted Computer Product Evaluation Criteria 3rd Ed. CTCPEC Version 3.0e. Publisher: Communications Security Establishment, 1993. Last modified: April 15, 2022. 208 p.

10. Defining Security Requirements with the Common Criteria: Applications, Adoptions, and Challenges / Nan Sun et al. *Computer Science - Cryptography and Security*. 2022. V.1. P. 44756-44777.

11. A survey on common criteria (CC) evaluating schemes for security assessment of IT products / Chang-Tsun Li et al. PeerJ Comput Sci. 2021. №7. 22p.

12. Standards. URL:https://www.iso.org/standards.html (дата звернення: 30.11.2023).

13. Дикий О. В., Флюнт М. О. Стандарти інформаційної безпеки: компаративне дослідження. *Право та державне управління.* 2019. № 2 (35), том 1. С. 80-87.

14. Петренко К.М. Удосконалена методика оцінювання ефективності системи забезпечення інформаційної безпеки Міністерства оборони та збройних сил України. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2022. № 3 (45). С. 97-100.

15. Батечко С.В., Лебедєва О.Ю., Зоріло В.В. Методика оцінки захищеності інформаційних систем. *Інформатика та математичні методи в моделюванні*. 2021. Том 11, № 3. С. 173-180.

16. Kim Koch. How to Comply with Trust Services Criteria for SOC 2 Examinations. *Moss Adams.* 2022. URL: https://www.mossadams.com/articles/2021/07/soc-2-trust-services-criteria (дата звернення: 5.12.2023).

17. Про інформацію : Закон України від 2.10.1992р. № № 2657-XII : Редакція від 27.07.2023р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#doc_info (дата звернення: 11.10.2023).

18. Марченко П. А. Методи розмежування доступу в розподілених системах кешування даних. Магістерська дисертація. Київ: НТУ УКРАЇНИ «КПІ ім. І. Сікорського», 2018. 91 с.

References

1. Karpovych I.M., Hladka O.M., Nakonechna Yu.A. Analiz ryzykiv bezpeky informatsiinoi systemy IT-pidpryiemstva. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: tekhnichni nauky*. 2020. Tom 31 (70) № 5. C. 69-74.

2. Khrapkin O.M. Zakhyst informatsiino-komunikatsiinoi merezhi ustanovy vid nesanktsionovanoho dostupu. *Systemy ozbroiennia i viiskova tekhnika*. 2020. № 3(63). S.45-53.

3. Livshitz I.I., Neklyudov A.V., Lontsikh P.A. Evaluation of IT security – genesis and its state-of-art. International *Conference Information Technologies in Business and Industry* 2018. IOP Publishing. 2018. C. 1-7.

4. Lawrence C. Miller and Peter H. Gregory. Evaluation Criteria of Systems Security Controls. *CISSP Articles*. 2018. URL: https://www.dummies.com/article/academics-the-arts/study-skills-test-prep/cissp/evaluation-criteria-systems-security-controls-254878/ (date of access: 30.09.2023).

5. Abhi G. CISSP Concepts – Trusted Computing Base/ TCEC, ITSEC and Common Criteria. *Cyber Management Alliance Articles*. Jan 28, 2020. URL: https://www.cm-alliance.com/cissp/trusted-computing-base/-tcec-itsec-and-common-criteria (date of access: 30.09.2023).

6. Randal Allen. Evolved Artificial Intelligence for Stochastic Clustering Unsupervised Learning. *Interservice/Industry Training, Simulation, and Education Conference*. 2020. Paper № 20258. 8 p.

7. Donald P. Kommersю The Basic Law: A Fifty Year Assessment. *German Law Journal*. 2019. Volume 20, Issue 4. P. 571-582.

8. Turchak A. Osnovni skladovi informatsiinoi bezpeky derzhavy. *Aspekty publichnoho upravlinnia*. Tom 7, № 5. 2019. S. 44-56.

9. The Canadian Trusted Computer Product Evaluation Criteria 3rd Ed. CTCPEC Version 3.0e. Publisher: Communications Security Establishment, 1993. Last modified: April 15, 2022. 208 p.

10. Defining Security Requirements with the Common Criteria: Applications, Adoptions, and Challenges / Nan Sun et al. *Computer Science - Cryptography and Security*. 2022. V.1. P. 44756-44777.

11. A survey on common criteria (CC) evaluating schemes for security assessment of IT products / Chang-Tsun Li et al. *PeerJ Comput Sci*. 2021. №7. 22p.

12. Standards. URL:https://www.iso.org/standards.html (date of access: 30.11.2023).

13. Dykyi O. V., Fliunt M. O. Standarty informatsiinoi bezpeky: komparatyvne doslidzhennia. *Pravo ta derzhavne upravlinnia.* 2019. № 2 (35), tom 1. S. 80-87.

14. Petrenko K.M. Udoskonalena metodyka otsiniuvannia efektyvnosti systemy zabezpechennia informatsiinoi bezpeky Ministerstva oborony ta zbroinykh syl Ukrainy. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony.* 2022. № 3 (45). S. 97-100.

15. Batechko S.V., Lebedieva O.Iu., Zorilo V.V. Metodyka otsinky zakhyshchenosti informatsiinykh system. *Informatyka ta matematychni metody v modeliuvanni*. 2021. Tom 11, № 3. S. 173-180.

16. Kim Koch. How to Comply with Trust Services Criteria for SOC 2 Examinations. *Moss Adams*. 2022. URL: https://www.mossadams.com/articles/2021/07/soc-2-trust-services-criteria (date of access: 5.12.2023).

17. Marchenko P. A. Metody rozmezhuvannia dostupu v rozpodilenykh systemakh keshuvannia danykh. Mahisterska dysertatsiia. Kyiv: NTU UKRAINY «KPI im. I. Sikorskoho», 2018. 91 s.

18. Pro informatsiiu : Zakon Ukrainy vid 2.10.1992r. № № 2657-XII : Redaktsiia vid 27.07.2023r. URL: https://zakon.rada.gov.ua/laws/show/2657-12#doc_info (date of access: 11.10.2023).