КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.916
УДК 004.03

Лєнков Сергій Васильович
доктор технічних наук, професор
Військовий інститут Київського національного університету
імені Тараса Шевченка, Київ, Україна
ORCID ID: 0000-0001-7689-239X
lenkov_s@ukr.net

Джулій Володимир Миколайович
канд. техн. наук, доцент, доцент
Хмельницький національний університет, Хмельницький, Україна
ORCID ID: 0000-0003-1878-4301
dzhuliivm@khmnu.edu.ua

Муляр Ігор Володимирович
канд. техн. наук, доцент, доцент
Хмельницький національний університет, Хмельницький, Україна
ORCID ID: 0000-0002-6659-605X
muliariv@khmnu.edu.ua

Лєнков Євген Сергійович
канд. техн. наук, старший дослідник, провідний спеціаліст Міненерго України
Міненерго України, Київ, Україна
ORCID ID: 0000-0001-5819-2656
lenkov85es@gmail.com

Кольцов Руслан Юрійович
канд. техн. наук, доцент, доцент
Військовий інститут Київського національного університету
імені Тараса Шевченка, Київ, Україна
ORCID ID: 0000-0002-8441-9575
vsrus34@ukr.net

ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Анотація. У статті запропоновано алгоритми оцінки ефективності безпеки конфіденційних даних підприємства розподіленої інформаційної системи, заснованих на моделі визначення актуальних загроз безпеки конфіденційних даних в інформаційній розподіленій системі, на алгоритмах нечіткого виводу та теорії нечітких нейронних систем, на методі оцінки ефективності безпеки конфіденційних даних розподіленої інформаційної системи. На відміну від відомих підходів, використовуються достатні та необхідні показники, виключаються помилки експертів, збільшується виявлення кількості актуальних загроз безпеці конфіденційних даних підприємства, враховуються наступні фактори: ІТ-інфраструктура розподіленої інформаційної системи, можливості зловмисників та їх рівень мотивації в розподіленій інформаційній системи підприємства. Запропонований підхід щодо оцінки ефективності безпеки конфіденційних даних підприємства розподіленої інформаційної системи відрізняється від існуючих, в наступному: відсутність залучення висококваліфікованих фахівців в області безпеки інформації; процес автоматизований, має низьку обчислювальну складність; дозволяє визначати перелік актуальних загроз безпеки інформації в інформаційних системах різних класів та типів. Розроблені алгоритми оцінки ефективності безпеки інформації дозволять власникам розподілених інформаційних системах в режимі реального часу оцінювати ефективність системи захисту, знизити фінансові витрати на розробку системи захисту. Запропоновані в процесі дослідження алгоритми оцінки ефективності системи захисту конфіденційної інформації розподілених інформаційних систем дозволяють: мінімізувати проведення непотрібних та зайвих кроків

проведення оцінки системи захисту; враховувати всі аспекти процесу проведення оцінки ефективності системи захисту розподіленої інформаційної системи; враховувати під час проведення оцінки ефективності системи захисту вимоги у сфері забезпечення інформаційної безпеки; може бути адаптована під умови власників розподілених інформаційних систем.

Ключові слова: інформаційна безпека; вразливості; конфіденційні дані; безпечне функціонування; алгоритми; набір даних.

ВСТУП

Задача забезпечення безпеки конфіденційної інформації підприємства стає найактуальнішею, що обумовлено, зростанням комп'ютерних атак та витоків інформації, що відображаються у статистичних даних скоєння злочинів у сфері високих технологій, зростання кримінальної активності з використанням сучасних комунікаційних пристроїв та інтернет [3], [7], [9], [16]. Однією з найважливіших задач забезпечення безпеки конфіденційної інформації підприємства є оцінка ефективності системи захисту.

Існуючі методи моделювання актуальних загроз інформаційної безпеки та оцінки ефективності системи захисту інформації підприємства не можуть бути задіяні на всіх етапах життєвого циклу розподілених інформаційних систем — не враховують в комплексі наступні показники: IT-інфраструктуру розподілених інформаційних систем, актуальні загрози інформаційної безпеки, вимог безпеки конфіденційної інформації, перелік засобів захисту конфіденційної інформації та їх вартість як важливих показників при вирішенні даних задач [6], [12], [13]. Одночасно з цим, для розглянутих методів моделювання загроз інформаційної безпеки та проведення оцінки ефективності системи захисту розподілених інформаційних систем залишається мета — підвищення ефективності, з огляду на визначення кількості актуальних загроз інформаційної безпеки, виконання закладених вимог до безпеки інформації, зниження вартості витрат на проектування та створення системи захисту розподілених інформаційних систем, а також мінімізація помилок експертів. Для існуючих методів оцінки ефективності системи захисту залишається актуальною задача зменшення помилки середньоквадратичної роботи продукційних адаптивних нечітких нейронних систем.

На підставі проведеного дослідження можна зробити висновок про необхідність удосконалення оцінки ефективності системи захисту розподілених інформаційних систем [1], [2], [4], [11], [12], [17].

Одночасно, з розвитком та зростанням інформаційних технологій зростає і кількість засобів та методів порушень стану безпеки конфіденційної інформації підприємства. Протягом останніх років спостерігається різке зростання кількості витоків конфіденційної інформації (звіт експертно-аналітичного центру компаній SafeNet). Змінити ситуацію, до забезпечення інформаційної безпеки, можливо шляхом розробки нових підходів які можуть надати від сучасних загроз безпеці інформації надійний захист [1], [2], [8], [9], [15].

Для досягнення цілей забезпечення безпеки конфіденційної інформації необхідно: організувати ефективне створення системи захисту інформації, ефективне моделювання актуальних загроз інформаційної безпеки, визначення актуального порушника, а також надати можливість проводити якісну оцінку ефективності системи безпеки конфіденційних даних [5], [10], [19], [21].

Однією з найважливіших задач забезпечення безпеки конфіденційної інформації є оцінка ефективності системи захисту. У зв'язку з цим метою дослідження є підвищення якості оцінки ефективності систем захисту розподілених інформаційних систем за

рахунок визначення достатніх та необхідних показників оцінки з використанням перспективних інформаційних технологій, що дозволяють найбільш ефективно вирішувати наступні задачі: визначення параметрів роботи адаптивних продукційних нечітких нейронних систем, застосування технологій Data Science при обробці даних, алгоритмів нечіткого виведення [1], [2], [15].

Постановка проблеми. Розподілені інформаційні системи мають низку аспектів IT-інфраструктури, які необхідно враховувати при проведені оцінки загроз інформаційній безпеці, при формуванні показників оцінки ефективності системи безпеки, ключовими є: незахищені мережі передачі даних, обробка інформації у центрах обробки даних, географічна розподіленість інформаційної системи, клієнт-серверні додатки, хмарні інфраструктури. Необхідно приділяти особливу увагу категоріям зловмисників у розподілених інформаційних системах, якими є внутрішні, зовнішні групи порушників.

На підставі проведеного дослідження оцінки ефективності безпеки конфіденційних даних підприємства можна зробити висновок про необхідність удосконалення підходів щодо оцінки безпеки розподілених інформаційних систем.

Аналіз останніх досліджень і публікацій. З розвитком та зростанням інформаційних технологій зростає і складність архітектури інформаційних систем. Сучасні інформаційні системи є клієнт-серверні територіально-розподілені та багаткористувацької архітектури. Програмне забезпечення на базі відкритого програмного інтерфейсу надає можливості функціональних модифікацій з використанням поширених мов програмування (TypeScript (середовище розробки dotnet.core, платформа розробки Angular)) [6], [11], [22].

Інформаційні системи забезпечують принцип централізованого накопичення, зберігання, багаторазового використання даних. Для забезпечення інформаційної безпеки, економії ресурсів на автоматизованих робочих місцях користувачів зберігання інформації не здійснюється. Обробка даних здійснюється на серверній частини [6], [15], [18]. Для реалізації даного підходу можуть використовуватись технології термінального доступу. Дана технологія може бути реалізована в IT-інфраструктурі шляхом розгортання термінальної ферми Remote Desktop Services, в даному випадку робочі профілі співробітників зберігаються на серверах термінальної ферми, що полегшує організацію доступу користувачів до ресурсів інформаційної системи, найбільш ефективно забезпечує процеси безпеки даних. Також технологія забезпечує процеси при віддаленій роботі користувачів [13], [15], [18].

Для розподілених інформаційних систем характерне розміщення мережевого обладнання, робочих місць користувачів, серверних компонентів на всій території країни та за її межами. Такі системи мають складну архітектуру розташування компонентів і технологій обробки даних. Відповідно, при цьому, виникають складнощі із забезпеченням безпеки даних [4], [11], [12].

До складу розподіленої інформаційної системи входять наступні компоненти: сервери, включають спеціалізоване та прикладне програмне забезпечення, забезпечують представлення даних у виді, необхідному для автоматизованої обробки інформації, серверне обладнання; робоче місце користувачів: типові робочі місця користувача (стаціонарні персональні комп’ютери), мобільні робочі місця — мобільні телефони, планшети.

Для забезпечення захисту інформації, що передається по відкритих каналах зв’язку, використовується криптографічний захист між секціями інформаційними системами.

Розподілені інформаційні системи мають низку аспектів IT-інфраструктури, які необхідно враховувати при проведені оцінки загроз інформаційній безпеці, при формуванні показників оцінки ефективності системи інформаційної безпеки. Необхідно

приділяти особливу увагу категоріям зловмисників у розподілених інформаційних системах, якими є внутрішні, зовнішні групи порушників [1], [8], [10].

Комп'ютерна атака — несанкціонований цілеспрямований вплив на ресурс, інформацію автоматизованої системи, для отримання несанкціонованого доступу до даних із застосуванням програмно-апаратних, програмних засобів. Об'єкт атаки — елемент розподіленої інформаційної системи. На теперішній час існує множина моделей атак, засобів та методів моделювання атак. Порушник — особа, яка навмисно використовує вразливості нетехнічних та технічних заходів, засобів контролю, управління безпекою з метою компрометації чи захоплення мереж та систем, зниження доступності мережевих ресурсів, даних інформаційної системи для законних користувачів [17], [18], [21].

Основні моделі атак на розподілені інформаційні системи наведені на рис. 1.

Переваги та недоліки основних моделей атак на розподілені інформаційні системи наведені в табл. 1.

При реалізації оцінки ефективності системи захисту конфіденційних даних розподілених інформаційних систем необхідно враховувати моделі зловмисника та моделі загроз інформаційної безпеки, вектори атак в інформаційній системі.

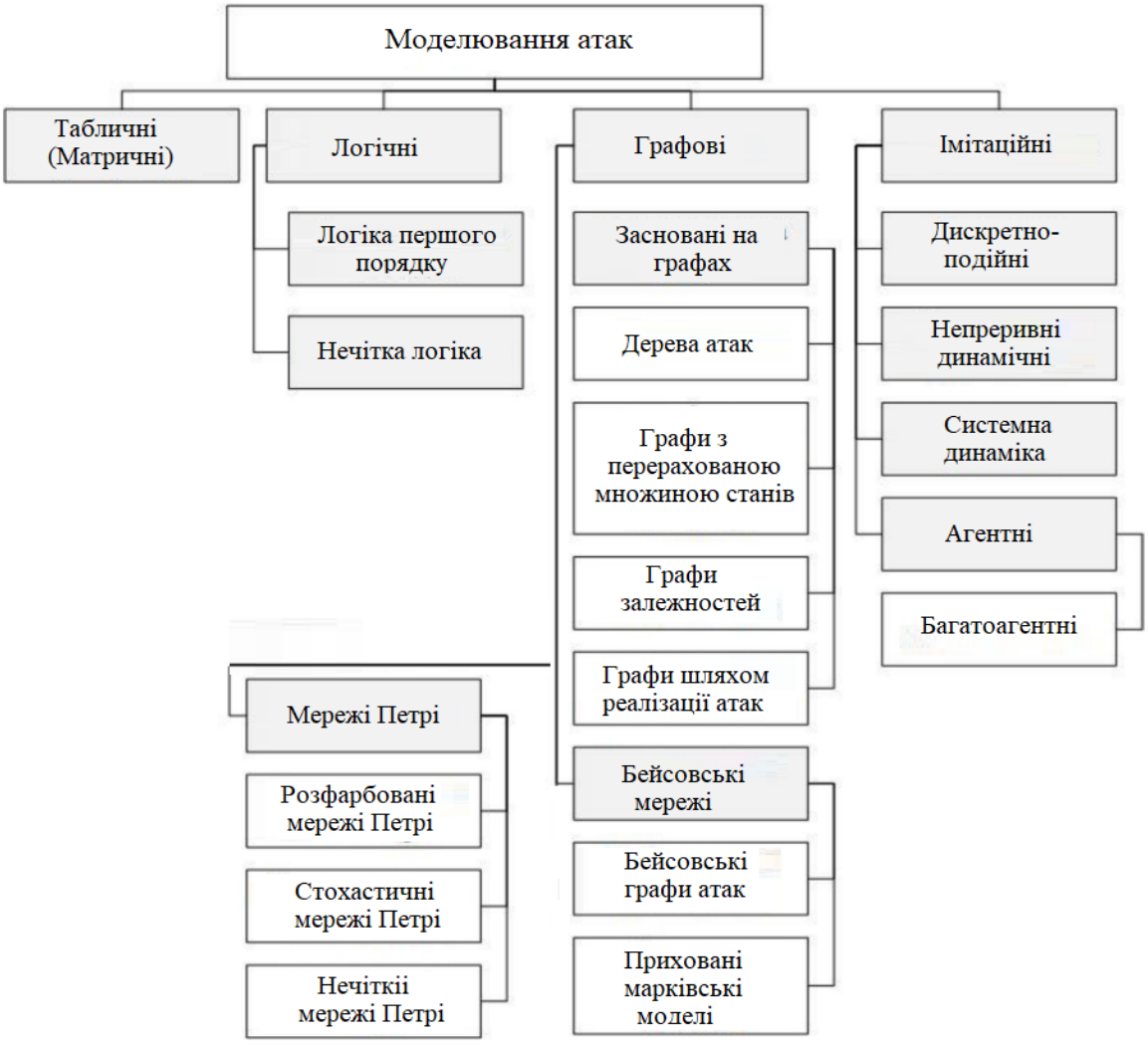

Рис. 1. Моделі атак на розподілені інформаційні системи

Таблиця 1

Переваги та недоліки основних моделей атак на розподілені системи

Модель	Переваги	Недоліки
Логічні	Обробка інцидентів та використання мов представлення знань про предметну область.	Потребує значних обчислювальних ресурсів
Графові на деревах атак	Наочність, масштабованість, адаптованість, універсальність	Складні при моделюванні циклічних атак.
Байєсівські графи	Масштабованість, адаптованість, універсальність, враховує невизначеності даних про атаки	Складні при моделюванні циклічних атак. Відсутність динамічного моделювання
Мережі Петрі	Зручність моделювання динаміч-них паралельних процесів, здатні відображати ймовірнісні процеси	Нездатність описувати пове-дінку порушника та цілі атаки
Імітаційні	Дозволяють моделювати поведінкові характеристики	Вимагають великих обчислювальних ресурсів

З проведеного аналізу досліджень можна дійти висновку про необхідність враховувати недоліки методів моделювання, зокрема загрозам безпеки інформації.

Аналіз досліджень оцінки ефективності системи захисту показав, що на теперішній час існують недоліки оцінки ефективності систем захисту, пов'язані з вибором показників оцінки, складне обчислювальне навантаження, недостатня ефективність в частині достовірної оцінки системи захисту, необхідність залучення висококваліфікованих фахівців у галузі інформаційної безпеки, недоліки експертних оцінок.

Існуючі підходи щодо оцінки ефективності системи захисту розподілених інформаційних систем недостатньо задовольняють показникам оцінки ефективності, не враховують достатні та необхідні показники оцінки ризиків реалізації загроз безпеці інформації, оцінки в частині виконання сукупності вимог безпеки даних, вартість фінансових витрат на створення системи захисту, IT-інфраструктуру розподілених систем.

Метою статті є проведення оцінки системи захисту, враховуючи всі аспекти процесу проведення оцінки ефективності системи захисту розподіленої інформаційної системи, вимоги у сфері забезпечення інформаційної безпеки, може бути адаптована під умови власників розподілених інформаційних систем.

АЛГОРИТМ ОЦІНКИ ЕФЕКТИВНОСТІ ЗАХИСТУ РОЗПОДІЛЕНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Проведення оцінки ефективності та оцінки відповідності систем захисту інформації ІС є обов'язковим для державних інформаційних систем, систем обробки персональних даних, критичних інфраструктур, автоматизованих систем управління технологічними процесами [4], [21].

Оцінка ефективності — ефективність системи захисту конфіденційних даних досягається шляхом розробки системи захисту, здатної максимально нейтралізувати актуальні загрози інформаційній безпеці, виконати вимоги до захисту інформації, які пред'являються інформаційній системі на підставі визначених вимог регуляторами у сфері забезпечення інформаційної безпеки даних, дозволяє, при цьому, максимально мінімізувати фінансові витрати на розробку системи захисту конфіденційних даних.

Алгоритм оцінки ефективності системи захисту розподілених інформаційних систем складається з наступних кроків:

1. Підготовка набору даних для оцінки ефективності систем захисту розподілених інформаційних систем, складається: відомості про IT-інфраструктуру розподіленої інформаційної системи; перелік актуальних загроз інформаційній безпеці у розподіленій інформаційній системі; перелік вимог щодо інформаційної безпеки; перелік засобів захисту інформації, що використовуються в розподіленій інформаційній системі; вартість створення системи захисту (вартість засобів захисту від виробників).
2. Аналіз, конвертація, форматування набору даних.
3. Формування бази правил для оцінки ефективності системи захисту розподілених інформаційних систем.
4. Проведення оцінки ефективності систем захисту розподілених інформаційних систем.
5. Оформлення результатів проведення оцінки ефективності систем захисту розподілених інформаційних систем. Внесення коригувань у проектні рішення, за потреби.

Алгоритм проведення оцінки ефективності та життєвого циклу розробки системи захисту представлені на рис. 2 та на рис. 3 відповідно.

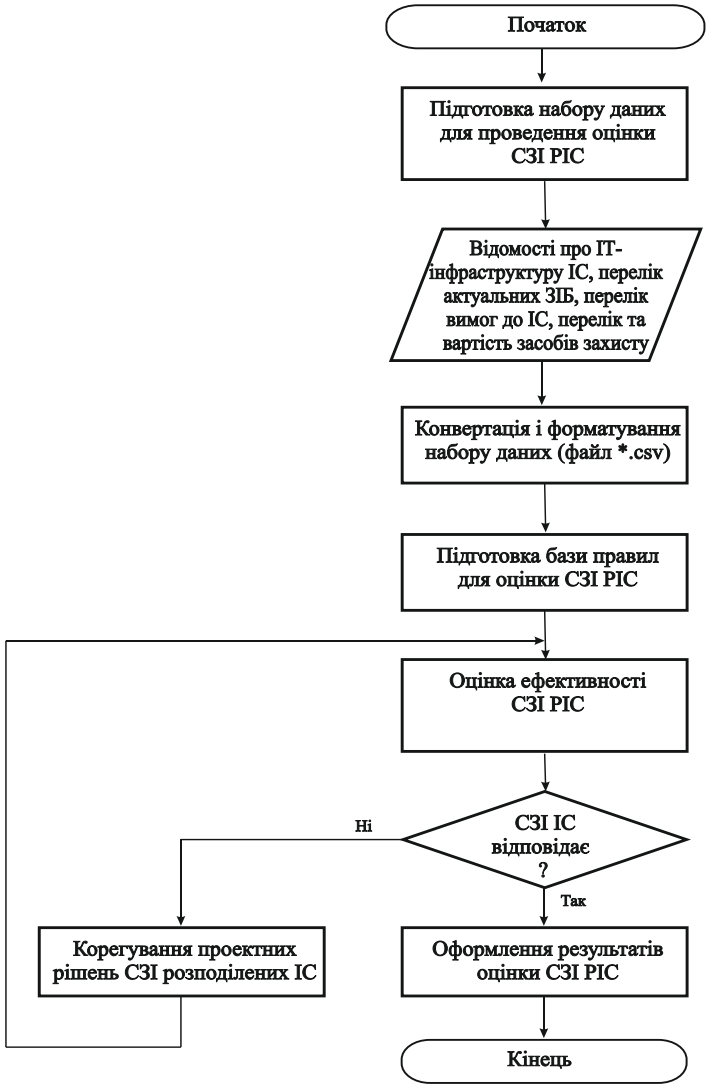

Рис. 2. Алгоритм оцінки ефективності захисту розподіленої інформаційної системи

№ 1 (29), 2025
ISSN 2663 - 4023

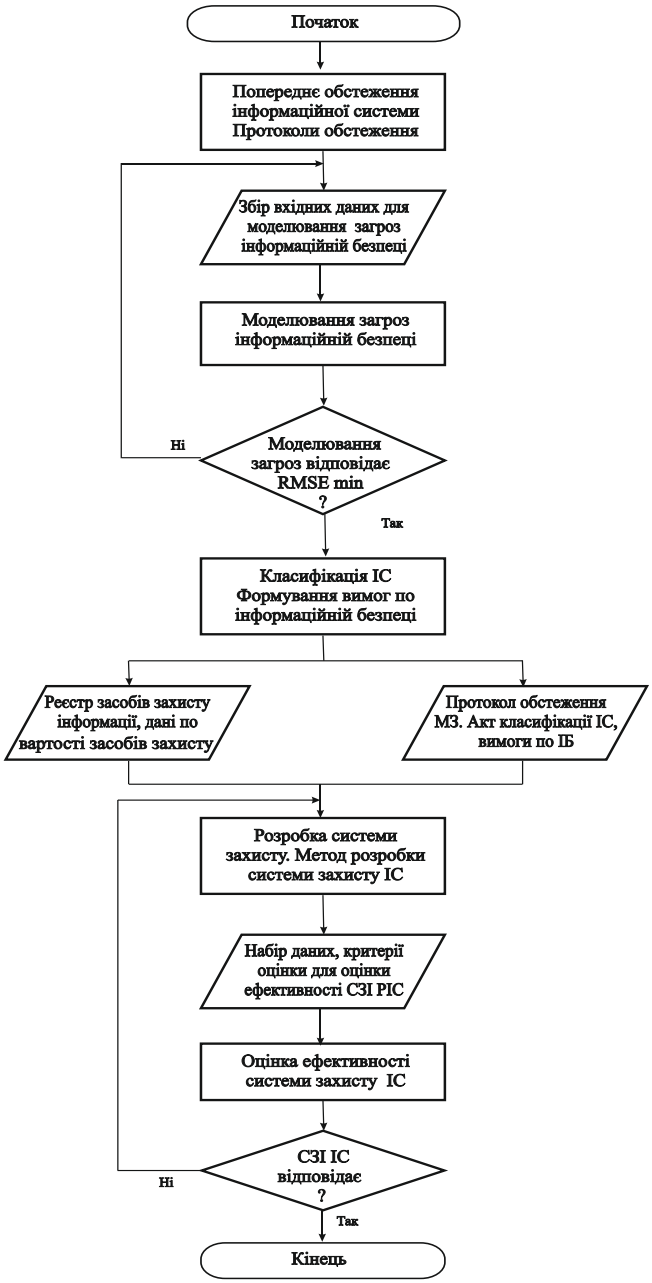

Рис. 3. Алгоритм життєвого циклу розробки системи захисту розподіленої інформаційної системи

Проведення оцінки ефективності системи захисту інформації необхідно виконати, відповідно до методичних рекомендацій, наступні кроки:

1. Провести обстеження розподіленої інформаційної системи, за результатами обстеження формується протокол, який включає опис IT-інфраструктури системи, а також відомі системи захисту інформації.
2. Визначити актуальні загрози інформаційній безпеці відповідно до методичних документів регуляторів. Визначити категорію значущості розподіленої системи, клас, тип, рівень захищеності. Актуальні загрози інформаційній безпеці.

3. Сформулювати, на підставі переліку актуальних загроз інформаційній безпеці, класифікації, та вимог до захисту інформації, перелік вимог.
4. Сформувати набір даних, що включає: IT-інфраструктуру розподіленої інформаційної системи, перелік актуальних загроз інформаційній безпеці в інформаційній системі, перелік вимог до захисту інформації, перелік використання засобів захисту інформації в системі захисту та їх вартість.
5. Врахувати та провести експертні оцінки відповідності розподіленої системи вимогам щодо захисту інформації.
6. На підставі розробленого методу оцінки ефективності системи захисту провести оцінку ефективності системи захисту розподіленої інформаційної системи [1], [2].
7. На підставі отриманих результатів оцінки ефективності системи захисту розподіленої інформаційної системи за необхідності впровести коригування до проектних рішень системи захисту інформації.

Структурна схема проведення оцінки ефективності системи захисту інформації розподіленої інформаційної системи наведена на рис. 4.

Процес проведення оцінки ефективності системи захисту складається з п’яти підсистем:

1. Підсистема обстеження розподіленої інформаційної системи.
2. Підсистема моделювання загроз інформаційній безпеці.
3. Підсистема формування вимог до системи щодо захисту інформації.
4. Підсистема оцінки ефективності системи захисту розподіленої інформаційної системи.
5. Підсистема коригування проектних рішень розробки системи захисту розподіленої інформаційної системи.

Запропоноване розбиття на підсистеми системи оцінки ефективності обумовлено незалежністю кожної з них, що, у свою чергу, дозволяє, у процесі проведення оцінки ефективності системи захисту вносити коригування без внесення змін до суміжних підсистем.

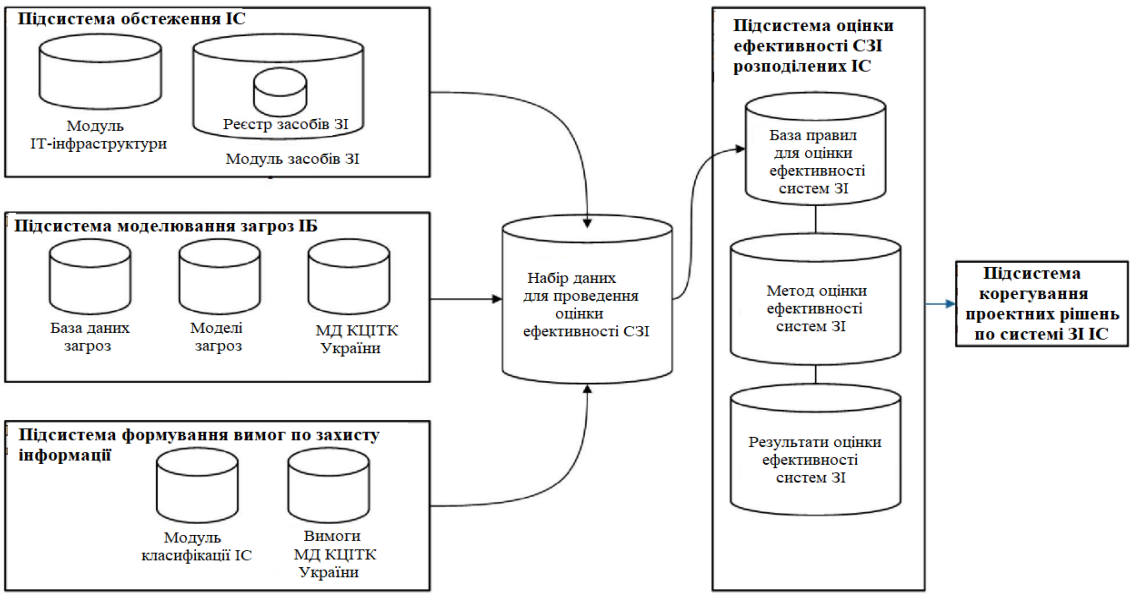

Рис. 4. Структурна схема оцінки ефективності системи захисту ІС

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

На підставі запропонованого методу оцінки ефективності системи захисту інформації розподілених інформаційних систем проведено оцінку ефективності системи [1], [2]. Система реалізована у форматі клієнт-серверної архітектури. Інформаційна система надає можливості модифікацій з урахуванням відкритого програмного інтерфейсу з використанням мов програмування (TypeScript, C# (середовище розробки dotnet.core, платформа розробки Angular)).

Система забезпечує принцип централізованого накопичення, зберігання, багаторазового використання даних. На робочих місцях користувачів зберігання даних не здійснюється. До складу інфраструктури інформаційної системи входять:

1. Сервери, включають: серверне обладнання; спеціалізоване та прикладне програмне забезпечення, забезпечують обробку інформації та представлення у вигляді, необхідному для подальшої автоматизованої обробки.
2. АРМ користувачів: типові робочі місця користувачів; АРМ керівника: використовується керівниками вищої ланки.

Серверні компоненти інформаційної системи розміщені в середовищі віртуалізації. Апаратно-програмний комплекс віртуаліза-ції системи складається з п’яти серверів віртуалізації на основі програмного забезпечення VMware, працює під управлінням сервера vCenter, мережі зберігання даних SAN.

У середовищі віртуалізації інформаційної системи розгорнуто віртуальні сервери: сервери програм; сервери OpenVPN для підключення віддалених користувачів із мережі Інтернет загального користування; сервери балансувальника навантаження Load Balancer; сервер СУБД; сервер для онлайн перегляду; термінальні сервери; сервери для веб-перегляду; менеджмент-сервер; сервери синхронізації для мобільного автоматизованого робочого місця.

Система зберігання даних, включає: повільне сховище — для Backup файлів віртуальних машин; швидкісні сховища — для зберігання файлів віртуальних машин.

Резервне копіювання даних інформаційної системи виконується з використанням можливостей Veeam Backup & Replication і MS SQL Server, не регламентовано час зберігання резервних копій.

Доступ до інформаційної системи для виконання функцій адміністрування IT-інфраструктури компонентів здійснюється з АРМ адміністратора, розташованих в межах контрольованої зони (периметра) системи. Контрольована зона інформаційної системи включає простори (приміщення, територія, будівлі), в яких розміщуються компоненти, виключено неконтрольоване перебування сторонніх транспортних засобів, відвідувачів. Інформаційний обмін даними між клієнтськими робочими місцями та серверами забезпечується з використанням організацій користувачів та ресурсів обчислювальних мереж, є можливість віддаленої роботи за межами локальної обчислювальної мережі з об’єктом інформатизації з використанням робочих місць.

До об’єктів захисту інформаційної системи відносяться: персональні дані, що обробляються в розподіленій інформаційній системі; технічні засоби, для обробки інформації (системи та засоби зв’язку передачі даних, машинні носії); прикладне та системне програмне забезпечення; засоби захисту інформації; засоби криптографічного захисту інформації; середовище функціонування системи криптографічного захисту інформації; інформація, що відноситься до криптографічного захисту інформації (персональні дані, аутентифікуючу та парольну інформацію); документи, журнали, видання, картотеки, технічні документи, кіно-, відео, фотоматеріали, робочі матеріали, в яких відображена інформація, що відноситься до інформаційної системи персональних

даних, їх криптографічний захист; носії інформації, що використовуються в розподіленій інформаційній системі у процесі криптографічного захисту даних, носії автентифікуючої, ключової, парольної інформації та порядок доступу до них; використовувані розподіленої інформаційної системи лінії (канали) зв'язку, включаючи кабельні системи; приміщення, в яких знаходяться ресурси розподіленої інформаційної системи, які мають відношення до криптографічного захисту інформації.

У розподіленій інформаційній системі обробляються наступні категорії інформації: службова інформація; персональні дані; технічні параметри розподіленої інформаційної системи, файли налаштувань та конфігураційні файли прикладного та системного програмного забезпечення, включаючи програмне забезпечення засобів системи. Відповідно до алгоритму запропонованого методу проведено дослідження інформаційної системи, за отриманими результатами запропоновано модель загроз безпеки даних, з використанням запропонованого методу визначення актуальних загроз інформаційній безпеці [1], [2].

За результатами дослідження інформаційної системи, визначення переліку актуальних загроз інформаційній безпеці та класифікації сформовано вимоги щодо захисту інформації.

В якості реалізації системи захисту інформаційної системи, наведено опис підсистеми реєстрації подій безпеки та захисту середовища віртуалізації. Підсистема захисту середовища віртуалізації забезпечує реалізацію наступних функцій: управління доступом суб'єктів доступу до об'єктів доступу у віртуальній інфраструктурі, також всередині віртуальних машин; аутентифікація та ідентифікація об'єктів доступу та суб'єктів доступу у віртуальній інфраструктурі, також адміністраторів управління засобами віртуалізації; реєстрація подій безпеки у віртуальній інфраструктурі; контроль цілісності віртуальної інфраструктури та її конфігурації; резервне копіювання даних, резервування каналів зв'язку всередині віртуальної інфраструктури, технічних засобів, програмного забезпечення віртуальної інфраструктури; керування переміщенням контейнерів (віртуальних машин) та даних, що оброблюються; сегментування віртуальної інфраструктури (розбиття віртуальної інфраструктури системи на сегменти) для подальшої обробки персональних даних групою користувачів або окремим користувачем; управління та реалізація антивірусним захистом у віртуальній інфраструктурі.

В якості підсистеми захисту середовища віртуалізації в інформаційній системі використовується сертифікований засіб захисту інформації — vGate. засіб захисту інформації vGate R2 забезпечує реалізацію функцій підсистеми захисту середовища віртуалізації, здійснює фільтрацію трафіку на рівні гіпервізора, дозволяє контролювати дії адміністраторів віртуальної інфраструктури та захист від специфічних загроз віртуалізації. До складу програмного забезпечення vGate входять консоль управління засобами захисту інформації, сервер авторизації, які встановлюються на автоматизованому робочому місці адміністратора по інформаційній безпеці. На рис. 5 представлена логічна схема підсистеми захисту середовища віртуалізації, реалізована із застосуванням засобу vGate R2.

Підсистема реєстрації подій безпеки забезпечує виконання наступних функцій: визначення подій безпеки та строків їх зберігання, що підлягають реєстрації; зберігання, збір, запис інформації про події безпеки протягом встановленого політикою безпеки часу зберігання; визначення змісту, складу інформації про події безпеки, що підлягають реєстрації; захист інформації щодо подій безпеки; перегляд, аналіз (моніторинг) результатів реєстрації подій безпеки та реагування на події безпеки. Засобами забезпечення відповідних функцій підсистеми реєстрації подій безпеки є журнали безпеки засіб безпеки інформації Dallas Lock 8.0-К, комплект програмного забезпечення

засіб захисту інформації ЕММ SafePhone, в якому міститься інформація про дії користувачів, починаючи з моменту входу користувача в операційну систему, про помилки, пов'язані з доступом до тих чи інших об'єктів, зокрема до тих додатків, доступ до яких заборонено. Засіб захисту інформації Dallas Lock 8.0-К містить наступні журнали: журнал управління обліковими записами; журнал входів; журнал ресурсів; журнал управління політиками; журнал друку; журнал пакетів міжмережевих екранів; журнал процесів; журнал з'єднань міжмережевих екранів; журнал контролю додатків; журнал трафіка; журнал подій операційної системи.

Рис. 5. Логічна схема підсистеми захисту середовища віртуалізації ІС

У кожному журналі фіксуються час, дата, операція, ім'я користувача, результат, інші параметри. Можливе, також, впорядкування (фільтрація) елементів списків журналу за необхідним значенням. На рис. 6 наведена логічна схема підсистеми реєстрації подій безпеки, реалізована із застосуванням засобу захисту інформації Dallas Lock 8.0-К.

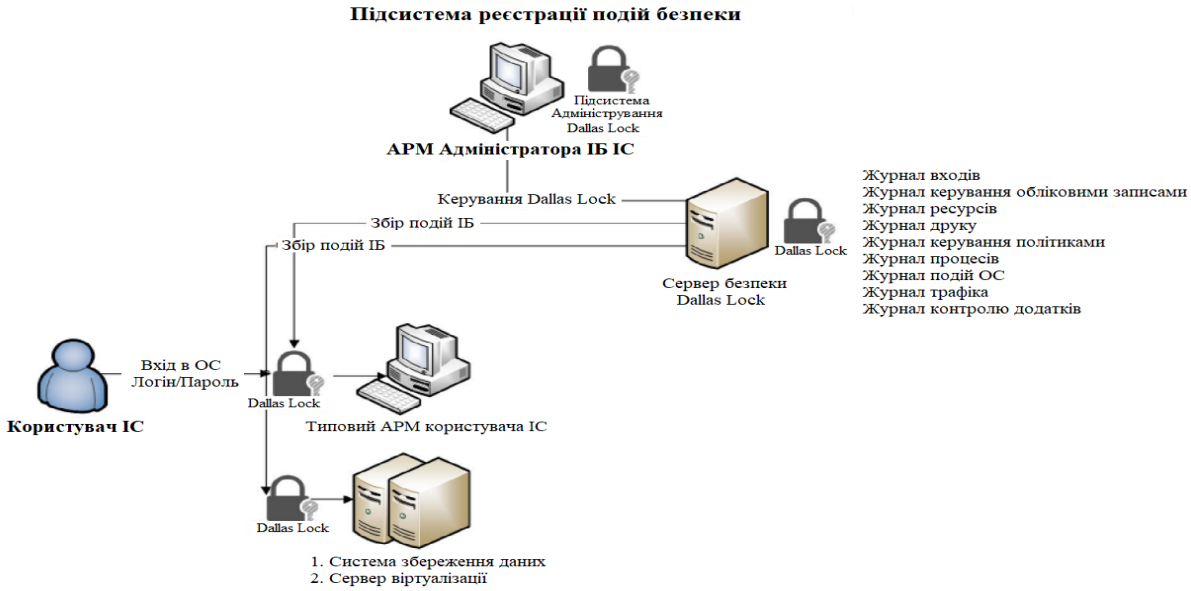

Рис. 6. Логічна схема підсистеми реєстрації подій

Перелік підсистем та функцій захисту інформації в досліджувальній роботі системи захисту наведено в табл. 2.

Таблиця 2

Підсистеми та функції захисту конфіденційних даних

Підсистема	Функції
Підсистема автентифікації та ідентифікації суб'єктів доступу, об'єктів доступу	Аутентифікація ідентифікація користувачів. Управління ідентифікаторами. Управління засобами аутентифікації, видача, ініціалізація, зберігання, блокування. Захист зворотного зв'язку. Аутентифікація та ідентифікація пристроїв (стаціонарних, мобільних, портативних)
Підсистема управління доступом	Управління обліковими записами користувачів. Реалізація рольового або дискреційного методу доступу. Управління інформаційними потоками між пристроями, сегментами розподіленої інформаційної системи, а також між інформаційними підсистемами. Розподіл повноважень користувачів, адміністраторів. Призначення мінімально необхідних прав та привілеїв користувачам, адміністраторам. Обмеження неуспішних спроб входу до ОС. Реалізація захищеного дистанційного доступу суб'єктів до об'єктів через зовнішні інформаційно-телекомунікаційні мережі. Дозвіл (заборона) дій користувачів, дозволених до аутентифікації та ідентифікації.
Підсистема обмеження ПС	Забезпечення можливості встановлення лише дозволеного до використання програмного забезпечення
Підсистема захисту машинних носіїв	Облік МН. Управління доступом до МН. Контроль переміщення МН за межі контрольованої зони системи. Контроль підключення МН.
Підсистема реєстрації подій безпеки	Визначення подій безпеки, що підлягають реєстрації та термінів їх зберігання. Визначення складу та змісту інформації про події безпеки, що підлягають реєстрації. Збір, запис та зберігання інформації про події безпеки протягом встановленого часу зберігання. Моніторинг (перегляд, аналіз) результатів реєстрації подій безпеки
Підсистема антивірусного захисту	Антивірусний захист АРМ та серверів розподіленої інформаційної системи. Оновлення бази даних ознак шкідливих програм (вірусів)
Підсистема аналізу захищенності	Виявлення, аналіз уразливостей інформаційної системи Контроль установки оновлень програмного забезпечення, Контроль працездатності, параметрів налаштування та правильності функціонування програмного забезпечення. Контроль складу технічних засобів, програмного забезпечення. Контроль правил генерації та зміни паролів користувачів, реалізації правил розмежування доступу, повноважень користувачів.
Підсистема виявлення вторгнень	Виявлення вторгнень. Оновлення бази вирішальних правил
Підсистема забезпечення мережевої безпеки	Реалізація функції міжмережевого екранування в точках взаємодії розподіленої інформаційної системи. Захист мережевої інфраструктури розподіленої інформаційної системи.
Підсистема централізованого управління засобами захисту інформації	Управління засобами захисту інформації. Адміністрування засобів захисту інформації. Управління оновленнями програмного забезпечення. Розповсюдження виправлень ПЗ. Отримання виправлень та інших оновлень безпеки ПЗ для централізованої установки на сервери та АРМ

Отримані результати проведеної оцінки показали ефективність запропонованих рішень щодо захисту конфіденційної інформації: ефективність системи захисту інформації можна підвищити за рахунок зменшення вартості запланованих засобів.

Проведена оцінка ефективності системи захисту інформації дозволить внести коригування в проектні рішення системи захисту інформації на ранньому етапі, що

дозволяє заощадити фінансові витрати на створення системи захисту конфіденційної інформації розподілених інформаційних систем, запобігти ризикам витоку даних.

Для оцінки ефективності запропонованих підходів необхідно враховувати порядок проведення оцінки виходячи з визначення вимог власників розподілених інформаційних систем. Ефективність системи захисту інформації досягається шляхом створення системи захисту, здатної максимально нейтралізувати актуальні загрози інформаційній безпеці у розподіленій інформаційній системі, виконати вимоги щодо захисту конфіденційних даних, які пред'являються до розподілених систем на підставі вимог власників в області забезпечення інформаційній безпеці, дозволяє знизити фінансові витрати на створення системи захисту.

Однією з форм оцінки відповідності системи є атестація. За умовами задачі, поставленими в роботі, оцінка ефективності системи захисту розподіленої інформаційної системи має бути використаний на всіх етапах життєвого циклу інформаційної системи для своєчасного внесення змін до проектних рішень щодо захисту конфіденційних даних. Методичні рекомендації, запропоновані показники, а також метод визначення актуальних загроз інформаційній безпепці, метод оцінки ефективності системи захисту дозволяють проводити оцінку ефективності системи захисту конфіденційних даних на всіх етапах життєвого циклу розподіленої інформаційної системи. Таким чином, поставлена задача, в дослідженні підвищення якості оцінки ефективності системи захисту інформаційної системи досягнута.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Розроблені заходи щодо оцінки ефективності систем захисту конфіденційних даних у розподілених інформаційних системах, на відміну від відомих, дозволяють власникам розподілених інформаційних систем в режимі реального часу оцінювати ефективність системи захисту, знизити фінансові витрати на розробку системи захисту. Використання запропонованих заходів не потребує великих обчислювальних ресурсів, залучення висококваліфікованих фахівців з інформаційної безпеки, ефективність систем захисту в розподілених інформаційних системах сягає 97%.

Запропоновані в роботі дослідженні заходи дозволяють: мінімізувати проведення непотрібних та зайвих кроків визначення оцінки ефективності систем захисту; враховувати всі аспекти процесу проведення оцінки ефективності системи захисту конфіденційних даних у розподіленої інформаційної системи; враховувати під час проведення оцінки ефективності системи захисту інформації вимоги у сфері забезпечення інформаційної безпеки; автоматизувати процес оцінки, не потребує залучення висококваліфікованих спеціалістів у області інформаційної безпеки, виключити недоліки експертних методів; може бути адаптована під умови власників розподілених інформаційних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lenkov, S. V., та ін. (2023). Model vyznachennia aktualnykh zahroz bezpeky konfidentsiinykh danykh v rozpodilenii informatsiinii systemi. *Underwater Technologies: Industrial and Civil Engineering, 4*(13), 25–59.
2. Lenkov, S. V., Dzhulii, V. M., & Muliar, I. V. (2024). Metod otsinky efektyvnosti bezpeky konfidentsiinykh danykh rozpodilenoi informatsiinoi systemy. *Underwater Technologies: Industrial and Civil Engineering, 1*(14), 18–34.

3. Ukaz Prezydenta Ukrainy № 47/2017. (2017, Liutyi 25). Doktryna informatsiinoi bezpeky Ukrainy.
4. Derzhavnyi standart Ukrainy. (1996). *DSTU 3396.0-96. Zakhyst informatsii. Tekhnichnyi zakhyst informatsii. Osnovni polozhennia*. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38883&cat_id=38836
5. Verkhovna Rada Ukrainy. (2017). *Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy"* (zi zminamy). https://zakon.rada.gov.ua/laws/show/2163
6. Tsybulnyk, S. O., & Barandych, K. S. (2022). *Tekhnolohii rozroblennia prohramnoho zabezpechennia. Chastyna 1. Zhyttievyi tsykl prohramnoho zabezpechennia: Pidruchnyk*. Kyiv: KPI im. Ihoria Sikorskoho.
7. Lysenko, S. M., & Shchuka, R. V. (2020). Analiz metodiv vyiavlennia shkidlyvoho prohramnoho zabezpechennia v kompiuternykh systemakh. *Visnyk Khmelnytskoho natsionalnoho universytetu, 2*(283), 101–107.
8. Lenkov, S., та ін. (2023). Metod prohnozuvannia vrazlyvostei informatsiinoi bezpeky na osnovi analizu danykh tematychnykh internet-resursiv. *Zbirnyk naukovykh prats Viiskovoho instytutu KNU im. T. Shevchenka, 78*, 123–134.
9. Lenkov, S. V., Dzhulii, V., & Solodieieva, L. V. (2022). Metod protydii poshyrenniu ta vyiavlennia shkidlyvoi informatsii v sotsialnykh merezhakh. *Zbirnyk naukovykh prats Viiskovoho instytutu KNU im. T. Shevchenka, 77*, 103–117.
10. Lenkov, S., та ін. (2020). Model bezpeky poshyrennia zaboronenoi informatsii v informatsiino-telekomunikatsiinykh merezhakh. *Zbirnyk naukovykh prats Viiskovoho instytutu KNU im. T. Shevchenka, 68*, 53–64.
11. Krepych, S. Ya., & Spivak, I. Ya. (2020). *Yakist prohramnoho zabezpechennia ta testuvannia: Bazovyi kurs*. Ternopil: FOP Palianytsia V. A.
12. Zolotukhina, O. A., та ін. (2020). *Iakist ta testuvannia informatsiinykh system: Navchalnyi posibnyk dlia samostiinoi roboty studentiv*. Kyiv: NNIIT DUT.
13. Vyshnia, V. B., Ryzhkov, E. V., & Havrysh, O. S. (2020). *Osnovy informatsiinoi bezpeky: Navchalnyi posibnyk*. Dnipro: Dnipropetrovskyi derzh. un-t vnutrish. sprav.
14. OGO.ua. (2025, Lypen 4). *Cotsialni merezhi – realni zahrozy virtualnoho svitu*. http://ogo.ua/articles/view/011–02–23/26490.htm
15. Ostapov, S., Korol, O., & Yevseiev, S. (2016). *Tekhnolohii zakhystu informatsii: Navchalnyi posibnyk*. Kharkiv: Vyd-vo KhNEU.
16. Lienkov, S., та ін. (2017). Analiz isnuiuchykh metodiv ta alhorytmiv vyiavlennia atak v bezdrotovykh merezhakh peredachi danykh. *Zbirnyk naukovykh prats Viiskovoho instytutu KNU im. T. Shevchenka, 56*, 124–132.
17. Buriachok, V. L., & Toliupa, S. V. (2016). *Informatsiinyi ta kiberprostory: Problemy bezpeky, metody ta zasoby borotby: Posibnyk*. Kyiv: DUT-KNU.
18. Rybalchenko, L., & Kosychenko, O. (2019). Problemy bezpeky personalnykh danykh v Ukraini. *Rehionalna ekonomika, 2*, 57–62.
19. Dzhulii, V. M., Miroshnichenko, O. V., & Solodieieva, L. V. (2022). Metod klasyfikatsii dodatkiv trafika kompiuternykh merezh na osnovi mashynnoho navchannia v umovakh nevyznachenosti. *Zbirnyk naukovykh prats Viiskovoho instytutu KNU im. T. Shevchenka, 74*, 73–82.
20. Lavrov, Ye. A., Perkhun, L. P., & Shendryk, V. V. (2017). *Matematychni metody doslidzhennia operatsii: Pidruchnyk*. Sumy: SumDU.
21. Honchar, S. F. (2019). *Otsiniuvannia ryzykiv kiberbezpeky informatsiinykh system obiektiv krytychnoi infrastruktury: Monohrafiia*. Kyiv.
22. Yemchuk, L., Zhylinska, O., Chornyi, A., & Dzhulii, V. (2020). Organizational network analysis as a tool for leadership assessment in software development team. In *2020 International Conference on Advanced Computer Information Technologies (ACIT)*. IEEE. https://doi.org/10.1109/ACIT49673.2020

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Serhii Lenkov
doctor of technical sciences, professor
Military Institute of Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID ID: 0000-0001-7689-239X
lenkov_s@ukr.net

Volodymyr Dzhulii
Ph.D., associate professor
Khmelnytsky National University, Khmelnitsky, Ukraine
ORCID ID: 0000-0003-1878-4301
dzhuliivm@khmnu.edu.ua

Igor Muliar
Ph.D., associate professor
Khmelnytsky National University, Khmelnitsky, Ukraine
ORCID ID: 0000-0002-6659-605X
muliariv@khmnu.edu.ua

Yevhen Lenkov
Ph.D., senior researcher, Leading specialist of the Ministry of Energy of Ukraine
Ministry of Energy of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0001-5819-2656
lenkov85es@gmail.com

Ruslan Koltsov
Ph.D., associate professor
Military Institute of Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID ID: 0000-0002-8441-9575
vsrus34@ukr.net

ASSESSMENT OF THE EFFECTIVENESS OF THE CONFIDENTIAL INFORMATION PROTECTION SYSTEM OF DISTRIBUTED INFORMATION SYSTEMS

Abstract. The article proposes algorithms for assessing the effectiveness of security of confidential data of an enterprise in a distributed information system, based on a model for determining current threats to the security of confidential data in a distributed information system, on fuzzy inference algorithms and the theory of fuzzy neural systems, and on a method for assessing the effectiveness of security of confidential data in a distributed information system. Unlike known approaches, sufficient and necessary indicators are used, and expert errors are eliminated, the identification of current threats to the security of confidential enterprise data is increasing, the following factors are taken into account: the IT infrastructure of the distributed information system, the capabilities of attackers and their level of motivation in the enterprise's distributed information system. The proposed approach to assessing the effectiveness of security of confidential data of an enterprise of a distributed information system differs from existing ones in the following: lack of involvement of highly qualified specialists in the field of information security; the process is automated, has low computational complexity; allows determining the list of current threats to information security in information systems of different classes and types. The developed algorithms for assessing the effectiveness of information security will allow owners of distributed information systems to assess the effectiveness of the protection system in real time, reduce financial costs for developing a protection system. The algorithms proposed in the research for assessing the effectiveness of the system for protecting confidential information of distributed information systems allow: to minimize unnecessary and redundant steps in assessing the protection system; to take into account all aspects of the process of assessing the effectiveness of the system for protecting distributed information systems; to take into account the requirements in the field of ensuring information security when assessing the effectiveness of the system for protecting protection; can be adapted to the conditions of the owners of distributed information systems. Improving the quality of assessing the effectiveness of distributed information systems protection systems by determining sufficient and

necessary evaluation indicators using promising information technologies will allow the following tasks to be most effectively solved: determining the operating parameters of adaptive production fuzzy neural systems, applying Data Science technologies in data processing, and fuzzy inference algorithms. The results of the study on assessing the effectiveness of the distributed information systems protection system can be used to manage the life cycle of information systems, assess the state of IT infrastructure, and the fleet of automated workplaces — in order to assess the compliance of enterprises with approaches to information technology management.

Keywords: information security; vulnerabilities; confidential data; secure operation; algorithms; data set.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Lenkov, S. V., та ін. (2023). Model vyznachennia aktualnykh zahroz bezpeky konfidentsiinykh danykh v rozpodilenii informatsiinii systemi. *Underwater Technologies: Industrial and Civil Engineering, 4*(13), 25–59.
2. Lenkov, S. V., Dzhulii, V. M., & Muliar, I. V. (2024). Metod otsinky efektyvnosti bezpeky konfidentsiinykh danykh rozpodilenoi informatsiinoi systemy. *Underwater Technologies: Industrial and Civil Engineering, 1*(14), 18–34.
3. Ukaz Prezydenta Ukrainy № 47/2017. (2017, Liutyi 25). Doktryna informatsiinoi bezpeky Ukrainy.
4. Derzhavnyi standart Ukrainy. (1996). *DSTU 3396.0-96. Zakhyst informatsii. Tekhnichnyi zakhyst informatsii. Osnovni polozhennia*. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38883&cat_id=38836
5. Verkhovna Rada Ukrainy. (2017). *Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy"* (zi zminamy). https://zakon.rada.gov.ua/laws/show/2163
6. Tsybulnyk, S. O., & Barandych, K. S. (2022). *Tekhnolohii rozroblennia prohramnoho zabezpechennia. Chastyna 1. Zhyttievyi tsykl prohramnoho zabezpechennia: Pidruchnyk*. Kyiv: KPI im. Ihoria Sikorskoho.
7. Lysenko, S. M., & Shchuka, R. V. (2020). Analiz metodiv vyiavlennia shkidlyvoho prohramnoho zabezpechennia v kompiuternykh systemakh. *Visnyk Khmelnytskoho natsionalnoho universytetu, 2*(283), 101–107.
8. Lenkov, S., та ін. (2023). Metod prohnozuvannia vrazlyvostei informatsiinoi bezpeky na osnovi analizu danykh tematychnykh internet-resursiv. *Zbirnyk naukovykh prats Viiskovoho instytutu KNU im. T. Shevchenka, 78*, 123–134.
9. Lenkov, S. V., Dzhulii, V., & Solodieieva, L. V. (2022). Metod protydii poshyrenniu ta vyiavlennia shkidlyvoi informatsii v sotsialnykh merezhakh. *Zbirnyk naukovykh prats Viiskovoho instytutu KNU im. T. Shevchenka, 77*, 103–117.
10. Lenkov, S., та ін. (2020). Model bezpeky poshyrennia zaboronenoi informatsii v informatsiino-telekomunikatsiinykh merezhakh. *Zbirnyk naukovykh prats Viiskovoho instytutu KNU im. T. Shevchenka, 68*, 53–64.
11. Krepych, S. Ya., & Spivak, I. Ya. (2020). *Yakist prohramnoho zabezpechennia ta testuvannia: Bazovyi kurs*. Ternopil: FOP Palianytsia V. A.
12. Zolotukhina, O. A., та ін. (2020). *Iakist ta testuvannia informatsiinykh system: Navchalnyi posibnyk dlia samostiinoi roboty studentiv*. Kyiv: NNIIT DUT.
13. Vyshnia, V. B., Ryzhkov, E. V., & Havrysh, O. S. (2020). *Osnovy informatsiinoi bezpeky: Navchalnyi posibnyk*. Dnipro: Dnipropetrovskyi derzh. un-t vnutrish. sprav.
14. OGO.ua. (2025, Lypen 4). *Cotsialni merezhi – realni zahrozy virtualnoho svitu*. http://ogo.ua/articles/view/011–02–23/26490.htm
15. Ostapov, S., Korol, O., & Yevseiev, S. (2016). *Tekhnolohii zakhystu informatsii: Navchalnyi posibnyk*. Kharkiv: Vyd-vo KhNEU.
16. Lienkov, S., та ін. (2017). Analiz isnuiuchykh metodiv ta alhorytmiv vyiavlennia atak v bezdrotovykh merezhakh peredachi danykh. *Zbirnyk naukovykh prats Viiskovoho instytutu KNU im. T. Shevchenka, 56*, 124–132.
17. Buriachok, V. L., & Toliupa, S. V. (2016). *Informatsiinyi ta kiberprostory: Problemy bezpeky, metody ta zasoby borotby: Posibnyk*. Kyiv: DUT-KNU.
18. Rybalchenko, L., & Kosychenko, O. (2019). Problemy bezpeky personalnykh danykh v Ukraini. *Rehionalna ekonomika, 2*, 57–62.

19. Dzhulii, V. M., Miroshnichenko, O. V., & Solodieieva, L. V. (2022). Metod klasyfikatsii dodatkiv trafika kompiuternykh merezh na osnovi mashynnoho navchannia v umovakh nevyznachenosti. *Zbirnyk naukovykh prats Viiskovoho instytutu KNU im. T. Shevchenka*, *74*, 73–82.
20. Lavrov, Ye. A., Perkhun, L. P., & Shendryk, V. V. (2017). *Matematychni metody doslidzhennia operatsii: Pidruchnyk*. Sumy: SumDU.
21. Honchar, S. F. (2019). *Otsiniuvannia ryzykiv kiberbezpeky informatsiinykh system obiektiv krytychnoi infrastruktury: Monohrafiia*. Kyiv.
22. Yemchuk, L., Zhylinska, O., Chornyi, A., & Dzhulii, V. (2020). Organizational network analysis as a tool for leadership assessment in software development team. In *2020 International Conference on Advanced Computer Information Technologies (ACIT)*. IEEE. https://doi.org/10.1109/ACIT49673.2020