КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.929
УДК 004.056.5:004.738.5:004.822

Бучик Сергій Степанович
доктор технічних наук, професор кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID ID: 0000-0003-0892-3494
buchyk@knu.ua

Маєвський Максим Олександрович
магістр
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID ID: 0009-0004-4180-5814
mixmix9966@gmail.com

КОМПЛЕКСНА МОДЕЛЬ ВИБОРУ АНТИВІРУСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Швидке зростання кібератак на критичну інфраструктуру на тлі стрімкого розвитку інформаційних технологій підкреслює нагальну потребу в ефективних механізмах захисту. Це дослідження розглядає проблему вибору найкращого антивірусного програмного забезпечення, яке ускладняється зростаючою складністю прийняття рішень та обмеженнями сучасних підходів. У статті представлено детальну, комплексну математичну модель, призначену для автоматизації процесу вибору антивірусного програмного забезпечення. Ця модель використовує багатокритеріальний аналіз та експертні оцінки для забезпечення гнучкості та об'єктивності. Вона оцінює технічні характеристики, такі як ймовірність виявлення, рівень хибних спрацьовувань, результати, навантаження на систему, час відгуку та частота оновлення баз даних, а також операційні ризики та фіксований коефіцієнт безпеки (CVSS). Методологія використовує середнє геометричне агрегування експертних думок та перевіряє їх узгодженість для зменшення суб'єктивності та підвищення надійності. Було протестовано два методи включення коефіцієнта ризику до загальної оцінки, що дозволяє адаптацію до різних стратегічних цілей. Експериментальні результати підтвердили ефективність моделі у визначенні оптимальних антивірусних рішень для критично важливих інформаційних систем. Модель ефективно обробляє експертні дані та створює організовану інформацію для прийняття рішень. Подальші дослідження можуть розширити базу знань моделі, вдосконалити алгоритми прийняття рішень щодо нових кіберзагроз та адаптувати її для ширшого застосування в інформаційній безпеці.

Ключові слова: комплексна модель; антивірусне програмне забезпечення; критична інфраструктура; кібербезпека; багатокритеріальний аналіз; прийняття рішень; база знань; інформаційна безпека.

ВСТУП

Постановка проблеми. Швидкий розвиток інформаційних технологій призвів до сплеску кібератак, особливо спрямованих на критичну інфраструктуру. CERT-UA повідомляє про зростання як частоти, так і складності цих атак, що підкреслює нагальну потребу в ефективних захисних заходах [1]. Це створює суттєве протиріччя: оскільки вибір правильного антивірусного програмного забезпечення стає все складнішим, існуючі підходи до прийняття рішень є недостатніми. Сучасні методи часто не враховують унікальні особливості різних типів критичної інфраструктури та нехтують останніми тенденціями в кіберзагрозах, що ускладнює вибір найефективніших антивірусних рішень.

Аналіз останніх досліджень і публікацій. Як вітчизняні, так і міжнародні дослідники активно досліджують питання захисту критичної інфраструктури від кіберзагроз. Аналіз

останніх досліджень та публікацій щодо комплексної моделі вибору антивірусного програмного забезпечення для об'єктів критичної інфраструктури показує, що ця тема є надзвичайно актуальною. Основний акцент зміщується з традиційного «антивірусу» на комплексні платформи, що використовують штучний інтелект та архітектури «нульової довіри» (Zero Trust). Так в [2] здійснено аналіз сучасних підходів до управління безпекою програмного забезпечення в критичних системах, ідентифікуючи загрози та рішення, які були застосовані. В [3] автори провели огляд досліджень за 2019-2024 роки, які ідентифікують уразливості, оцінюють передові системи виявлення загроз і аналізують протоколи захисту мережі. Підкреслено, що в усіх цих дослідженнях особлива увага приділяється ролі AI, що вказує на те, що антивірусні рішення вже повинні мати рішення на основі використання штучного інтелекту. В [3] автори представили дослідження фреймворка InfraGuard, який вимірює зрілість кіберстійкості та приятиме формуванню політики, інвестиційному плануванню та глобальному співробітництву в галузі кіберзахисту.

Поточні дослідження також включають методології ранжування об'єктів критичної інфраструктури та оцінки ризиків інформаційної безпеки. Міжнародні стандарти, такі як ISO/IEC 27001:2023 [5] та ISO/IEC 27002:2023 [6], визначають вимоги до систем управління безпекою, які вже адаптуються до національних умов шляхом їх імплементації в державні стандарти України. Незважаючи на значний прогрес, все ще існує потреба в комплексних моделях, що поєднують багатокритеріальний аналіз з експертними оцінками, враховуючи конкретні потреби критичної інфраструктури та кіберзагроз, що розвиваються.

Мета статті. Метою цієї статті є створення комплексної моделі для автоматизації вибору найкращого антивірусного програмного забезпечення для об'єктів критичної інфраструктури з використанням багатокритеріального аналізу та експертних оцінок. Для досягнення цієї мети було поставлено такі завдання: визначити критерії оцінки антивірусного програмного забезпечення, розробити математичну модель та алгоритми прийняття рішень, а також перевірити працездатність моделі.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Об'єкти критичної інфраструктури є життєво важливими для сучасної національної безпеки, економічної стабільності та добробуту населення. Досягнення в інформаційних технологіях зробили кібербезпеку вирішальною для захисту цих об'єктів. Коли традиційні системи, такі як електростанції, транспортні мережі та водопостачання, зазнають збоїв, кібератаки, шкідливе програмне забезпечення та витоки даних можуть спричинити значні збої в національній діяльності. Згідно із Законом України «Про критичну інфраструктуру», ці об'єкти є важливими для функціонування державних установ та надання критично важливих послуг. Перебої в їхній роботі можуть перешкоджати або навіть зупиняти економічний розвиток [7].

Комплексний підхід до захисту критичної інфраструктури, включаючи кібербезпеку, дозволяє державі ефективно протидіяти сучасним загрозам. Впровадження систем моніторингу, проведення оцінки ризиків та створення стратегій реагування як на фізичні, так і на кіберзагрози забезпечують надійний рівень безпеки.

Сучасні визначення компонентів критичної інфраструктури є важливими для впровадження ефективних заходів ІТ та кібербезпеки. Ретельна система категоризації, яка охоплює як фізичні, так і цифрові елементи, дозволяє краще організувати активи на основі їхньої значущості та вразливості до кіберзагроз. Такий підхід підтримує розробку надійних стратегій управління ризиками, ефективність використання ресурсів та впровадження

передових технологій інформаційної безпеки, тим самим підвищуючи стійкість країни до внутрішніх та зовнішніх загроз. Оскільки повсякденне життя стає дедалі більш цифровим, створення надійної системи кібербезпеки є життєво важливим для захисту національної безпеки за допомогою чітко визначених стратегій [8].

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для полегшення ефективного вибору антивірусного програмного забезпечення було створено комплексну математичну модель, яка поєднує багатокритеріальний аналіз з експертними оцінками. Основна увага в цьому дослідженні зосереджена на процесі вибору антивірусних програм, а предмет дослідження охоплює методи та критерії, що використовуються для оцінки їхньої ефективності. Модель використовує методи системного аналізу, теорії прийняття рішень та експертної оцінки.

Розробка комплексної моделі оцінки антивірусного програмного забезпечення враховує конкретні потреби об'єктів критичної інфраструктури та вдосконалює метод багатокритеріального аналізу шляхом додавання вагових коефіцієнтів до критеріїв. Вибір відповідного антивірусного програмного забезпечення для важливих інформаційних систем є життєво важливим [9]. Створення методології оцінки передбачає встановлення критеріїв, які забезпечують об'єктивний аналіз, достовірні висновки та успішні майбутні операційні рішення щодо впровадження програмного забезпечення [9]. На відміну від існуючих методів, які в основному зосереджені на основних функціях, запропонований підхід охоплює ширший набір критеріїв, пов'язаних з безпекою, адаптивністю до сучасних кіберзагроз та ефективністю виявлення вразливостей. Методологія виключно спирається на антивірусні рішення з «Переліку засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом» (https://data.gov.ua/en/dataset/eab73672-181f-4b20-8819-56d47723ff11), підвищуючи точність оцінки та забезпечуючи відповідність нормативним вимогам. Дослівно з офіційного ресурсу «Цей Перелік формується відповідно до п. 17 Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27 вересня 1999 р. № 1229. Перелік призначений для використання суб'єктами системи технічного захисту інформації (ТЗІ) під час розроблення, модернізації та впровадження комплексів ТЗІ на об'єктах інформаційної діяльності (ОІД) та комплексних систем захисту інформації (КСЗІ) в автоматизованих системах (АС)». Далі «Перелік засобів технічного захисту інформації…».

Критерії базуються на принципах багатокритеріального аналізу [10], а організації розробляють їх за допомогою експертних оцінок з використанням методів рецензування [11].

Такий підхід дозволяє ранжувати критерії за важливістю та призначати певні ваги. Експерти виконують попарні порівняння для створення матриці, яка визначає відносну важливість вимог. Геометричне середнє обробляє результати експертів в узагальнені ваги, зменшуючи суб'єктивність в особистих оцінках та сприяючи консенсусу.

Процес починається з розрахунку індексу узгодженості (CR) для кожної матриці, що є вирішальним для подальшого аналізу. Якщо CR перевищує встановлений поріг, потрібні додаткові обговорення з експертами. Ця методологія сприяє точному та об'єктивному аналізу, поєднуючи кількісні дані та якісні фактори для оцінки ефективності антивірусного захисту. Ключовим елементом є організація команди з 12-13 фахівців з кібербезпеки, IT та управління ризиками, які проводять індивідуальні попарні оцінки на основі заздалегідь визначених критеріїв, що призводить до консолідованої системи оцінювання [12].

Структура математичної моделі.

Розроблена математична модель має наступну ієрархічну структуру для оцінки ефективності антивірусних рішень для критичних інформаційних систем.

1. **Рівень 1 — Мета.** Оцінка ефективності антивірусних рішень для критичних інформаційних систем.
2. **Рівень 2 — Критерії:**

К1. Ймовірність виявлення шкідливого коду. Цей критерій відображає здатність програмного забезпечення ідентифікувати шкідливе програмне забезпечення, включаючи нові та модифіковані варіанти вірусів.

К2. Рівень хибних спрацьовувань. Відображає точність алгоритмів і адаптивність системи до змін, що впливає на зручність використання та ефективність прийняття рішень.

К3. Навантаження на систему. Оцінює вплив антивірусних операцій на системні ресурси комп'ютера.

К4. Середній час реакції. Визначає швидкість виявлення та нейтралізації загроз.

К5. Частота оновлень баз даних. Забезпечує інформованість антивірусного програмного забезпечення про найсвіжіші ризики для безпеки.

К6. Ризиковий коефіцієнт (R). Характеризує потенційні експлуатаційні ризики, враховуючи непередбачувані збої, вразливості при взаємодії з іншими компонентами інфраструктури, та можливий вплив на загальну безпеку інформаційного середовища.

К7. Загальний коефіцієнт безпеки (CVSS — Common Vulnerability Scoring System). CVSS надає уніфіковану, фіксовану оцінку, яка дозволяє фахівцям з кібербезпеки та організаціям визначати пріоритетність усунення вразливостей.

3. **Рівень 3 — Альтернативи.** Антивірусні рішення з «Переліку засобів технічного захисту інформації …..».

Агрегація експертних оцінок. Формування критеріїв включає процес експертної оцінки. Метод геометричного середнього поєднує індивідуальні оцінки. Кожен експерт створює матрицю, яка попарно порівнює критерії, а потім проводить аналогічні порівняння альтернатив для кожного критерію. Потім формула обчислює агреговану матрицю:

$$a_{ij}^{agg} = (\prod_{k=1}^{n} a_{ij}^{(k)})^{\frac{1}{n}} \quad (1)$$

де *n* — загальна кількість експертів.

Цей підхід дозволяє зменшити суб'єктивний вплив особистих думок та забезпечити більш узгоджену оцінку.

Перевірка узгодженості експертних оцінок. Вирішальним кроком є перевірка узгодженості експертних оцінок. Для кожної матриці, згенерованої експертом, та об'єднаної матриці обчислюється коефіцієнт узгодженості (CR). Якщо CR перевищує заздалегідь визначений поріг (наприклад, 0,1), експертна група переглядає оцінки для подальшого обговорення та виправлення. Цей процес допомагає забезпечити точність даних та зміцнює довіру до експертних оцінок.

Інтеграція ризикового коефіцієнта. Модель пропонує два методи включення фактору ризику до загальної оцінки, виходячи зі стратегічних пріоритетів організації.

Підхід А. Ризиковий коефіцієнт (К6) включається до матриці критеріїв як повноцінний критерій. Загальний бал альтернативи розраховується шляхом множення суми зважених оцінок за критеріями (К1-К6) на фіксований коефіцієнт CVSS (К7):

$$P_i = (\sum_{j=1}^{6} w_j \cdot s_{ij}) \cdot CVSS_i \quad (2)$$

де *wj* — ваговий коефіцієнт критерію *j*, *sij* — локальна оцінка альтернативи *i* за критерієм *j*.

Підхід В. Спочатку розраховується базова оцінка за критеріями К1-К5:

$$B_i = \sum_{j=1}^{5} w_j \cdot s_{ij} \quad (3)$$

Після цього застосовується коригувальний множник для врахування ризику, і отриманий результат множиться на $CVSS_i$:

$$P_i = (B_i \cdot (1 - k \cdot R_i)) \cdot CVSS_i \quad (4)$$

де Ri — локальна оцінка за критерієм К6 (ризиковий коефіцієнт), а k – коефіцієнт, що визначає вплив ризику (у даному дослідженні k = 0.5).

Прийняття рішення. Для кожної альтернативи загальний показник P_i обчислюється за допомогою обраного методу інтеграції ризиків та показника CVSS. Варіант з найвищим значенням P_i вважається найкращим вибором для впровадження в критичних інформаційних системах. Якщо груповий консенсус (CR) не відповідає встановленим стандартам, проводяться подальші експертні обговорення для покращення оцінок.

Експериментальна апробація моделі.

Проведено експериментальне тестування для перевірки здатності моделі ефективно оцінювати антивірусне програмне забезпечення. Проаналізовано шість рішень, обраних відповідно до критеріїв з «Переліку засобів технічного захисту інформації …..».. Тестування провела група з п’яти експертів які мають досвід у сфері кібербезпеки та захисту критичної інфраструктури.

Експертні оцінки були зібрані за допомогою стандартизованого методу, розробленого для зменшення помилок. Кожен експерт систематично проводив попарні порівняння критеріїв оцінки між собою та альтернатив (антивірусів) для кожної вимоги К1–К6 незалежно.

Після збору індивідуальних оцінок система агрегувала експертні матриці попарних порівнянь для критеріїв та альтернатив, використовуючи середнє геометричне, згідно з формулою (1).

Використовуючи об’єднану матрицю критеріїв, вагові коефіцієнти були визначені наступним чином:

- К1 (Ймовірність виявлення шкідливого коду): 0.4547
- К2 (Рівень хибних спрацьовувань): 0.2416
- К3 (Навантаження на систему): 0.1493
- К4 (Середній час реакції): 0.0818
- К5 (Частота оновлень баз даних): 0.0463
- К6 (Ризиковий коефіцієнт): 0.0264

Далі були розраховані локальні вагові коефіцієнти для кожного антивірусу за кожним критерієм К1-К6 на основі відповідних агрегованих матриць альтернатив.

Значення CVSS для антивірусів, використані в розрахунках, були наступними:

- ESET NOD32 Antivirus: 0.84
- Bitdefender Antivirus: 0.80
- Avast Business Antivirus: 0.65
- Check Point Endpoint Security: 0.68
- McAfee Total Protection: 0.72
- Zillya! Антивірус: 0.78

Результати розрахунків за Підходом А (використання формули (2)):

- ESET NOD32 Antivirus: 0.3454
- Bitdefender Antivirus: 0.1965
- Avast Business Antivirus: 0.1046
- Check Point Endpoint Security: 0.0645

- McAfee Total Protection: 0.0404
- Zillya! Антивірус: 0.0243

Рейтинг для Підходу А:

- ESET NOD32 Antivirus (0.3454)
- Bitdefender Antivirus (0.1965)
- Avast Business Antivirus (0.1046)
- Check Point Endpoint Security (0.0645)
- McAfee Total Protection (0.0404)
- Zillya! Антивірус (0.0243)

Результати розрахунків за Підходом Б (використання формули (4) з $k = 0.5$):

- ESET NOD32 Antivirus: 0.2616
- Bitdefender Antivirus: 0.1665
- Avast Business Antivirus: 0.0944
- Check Point Endpoint Security: 0.0606
- McAfee Total Protection: 0.0385
- Zillya! Антивірус: 0.0235

Рейтинг для Підходу Б:

- ESET NOD32 Antivirus (0.2616)
- Bitdefender Antivirus (0.1665)
- Avast Business Antivirus (0.0944)
- Check Point Endpoint Security (0.0606)
- McAfee Total Protection (0.0385)
- Zillya! Антивірус (0.0235)

В обох підходах антивірус ESET NOD32 виходить на перше місце, демонструючи високу продуктивність за всіма критеріями незалежно від методу інтеграції ризиків. Кінцева різниця в оцінках між підходами зумовлена різним використанням коефіцієнта ризику (R6): підхід А включає його безпосередньо до зваженої суми критеріїв, тоді як підхід В застосовує R6 як модифікатор до базової оцінки.

Експериментальне тестування підтвердило, що комплексна модель успішно збирає експертні оцінки, поєднує їх за допомогою методу аналізу ієрархій, враховуючи коефіцієнт ризику та CVSS за допомогою двох різних методів, та створює кінцеві оцінки для альтернатив. Це демонструє, що модель ефективно досягає своєї мети — оцінки антивірусних рішень для критично важливих інформаційних систем.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У дослідженні ретельно розглянуто основні концепції, пов’язані з критичною інфраструктурою та її класифікацією, оцінюючи загрози інформаційній безпеці, які мають вирішальне значення для національної безпеки та економічної стабільності. Було зроблено висновок, що класифікація активів допомагає у визначенні пріоритетів зусиль захисту та формулюванні відповідних стратегій, тоді як аналіз загроз підкреслює важливість комплексного підходу до безпеки.

Було розроблено комплексну модель вибору антивірусного програмного забезпечення на основі принципів багатокритеріального аналізу. Вона передбачає створення математичної моделі для стандартизації оцінки антивірусних рішень, що включає як технічні, так і експертні оцінки. Центральним елементом є використання середнього геометричного для об’єднання експертних оцінок, що допомагає зменшити суб’єктивність.

Крім того, було впроваджено механізм перевірки узгодженості експертних оцінок, а також включення фактору ризику, що підвищує точність та гнучкість оцінки в різних умовах експлуатації. Також впроваджено показник CVSS. Алгоритм моделі представляє структурований процес від збору даних до вибору оптимального рішення.

Практичне значення цих результатів полягає в тому, що розроблена комплексна модель може оптимізувати вибір антивірусного програмного забезпечення. Така оптимізація знизить витрати на кібербезпеку та підвищить безпеку об'єктів критичної інфраструктури.

Майбутні дослідження мають бути зосереджені на розширенні бази знань комплексної моделі, вдосконаленні алгоритмів прийняття рішень та адаптації моделі для використання в різних сферах інформаційної безпеки, враховуючи постійну еволюцію кіберзагроз. Це передбачає врахування нових типів кіберзагроз та методів їх виявлення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. CERT-UA. (б.д.). *CERT-UA минулого року опрацювала 4315 кіберінцидентів*. https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv
2. Ekşi, G. E., Tekinerdoğan, B., & Catal, C. (2022). Software security management in critical infrastructures: A systematic literature review. *Turkish Journal of Electrical Engineering and Computer Sciences, 30*(4), 1142–1161. https://doi.org/10.55730/1300-0632.3841
3. Okeke, K., & Omojola, S. (2025). Enhancing cybersecurity measures in critical infrastructure: Challenges and innovations for resilience. *Journal of Scientific Research and Reports, 31*(2), 474–484. https://doi.org/10.9734/jsrr/2025/v31i22868
4. Lubis, M., Safitra, M. F., Fakhrurroja, H., & Muttaqin, A. N. (2025). Guarding our vital systems: A metric for critical infrastructure cyber resilience. *Sensors, 25*(15), 4545. https://doi.org/10.3390/s25154545
5. ДСТУ ISO/IEC 27001:2023. (2023). *Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги*. https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104398
6. ДСТУ ISO/IEC 27002:2023. (2023). *Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Кодекс практики*. https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104399
7. Верховна Рада України. (2024). *Закон України "Про критичну інфраструктуру" від 17 листопада 2021 року № 1882-IX (в редакції від 21.09.2024)*. https://zakon.rada.gov.ua/laws/show/1882-20#Text
8. Lu, M. T., & Guimaraes, T. (2007). A guide to selecting expert systems applications. *Journal of Information Systems Management, 6*(2), 8–15. https://doi.org/10.1080/07399018908960138
9. Mukhoid, O. V., Kostornoi, O. S., & Shyfrin, D. M. (2018). Selection of the optimal software for designing expert systems. *Journal of Engineering Sciences, 5*(2), E10–E15. https://doi.org/10.21272/jes.2018.5(2).e3
10. Madanchian, M., & Taherdoost, H. (2025). Applications of multi-criteria decision making in information systems for strategic and operational decisions. *Computers, 14*(6), 208. https://doi.org/10.3390/computers14060208
11. Krisper, M., Dobaj, J., & Macher, G. (2020). Assessing risk estimations for cyber-security using expert judgment. In M. Yilmaz, P. Clarke, J. Niemann, & R. Messnarz (Eds.), *Systems, software and services process improvement – 27th European Conference, EuroSPI 2020, Proceedings* (pp. 120–134). Communications in Computer and Information Science (Vol. 1251). Springer. https://doi.org/10.1007/978-3-030-56441-4_9
12. Buchyk, C., Kondratenko, S., & Pysarchuk, O. (2006). *Systemy pidtrymky pryiniattia rishen*. Zhytomyr: ZhVIRE.

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

Serhii Buchyk
DSc (Engin.), Prof., Professor of the Department of Cybersecurity and Information Protection
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID ID: 0000-0003-0892-3494
buchyk@knu.ua

Maksym Maievskyi
Master of Arts
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID ID: 0009-0004-4180-5814
mixmix9966@gmail.com

COMPREHENSIVE MODEL FOR SELECTING ANTIVIRUS SOFTWARE FOR CRITICAL INFRASTRUCTURE FACILITIES

Abstract. The rapid growth of cyber attacks on critical infrastructure against the backdrop of rapid development of information technology highlights the urgent need for effective protection mechanisms. This study examines the problem of choosing the best antivirus software, which is complicated by the increasing complexity of decision-making and the limitations of current approaches. The article presents a detailed, comprehensive mathematical model designed to automate the process of selecting antivirus software. This model uses multi-criteria analysis and expert assessments to ensure flexibility and objectivity. It evaluates technical characteristics such as detection probability, false positive rate, performance, system load, response time, and database update frequency, as well as operational risks and the Common Vulnerability Scoring System (CVSS). The methodology uses geometric mean aggregation of expert opinions and checks their consistency to reduce subjectivity and increase reliability. Two methods of incorporating the risk factor into the overall assessment were tested, allowing adaptation to different strategic goals. Experimental results confirmed the effectiveness of the model in determining optimal antivirus solutions for mission-critical information systems. The model effectively processes expert data and creates organised information for decision-making. Further research could expand the model's knowledge base, improve decision-making algorithms for new cyber threats, and adapt it for wider application in information security.

Keywords: comprehensive model; antivirus software; critical infrastructure; cybersecurity; multi-criteria analysis; decision-making; knowledge base; information security.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. CERT-UA. (б.д.). *CERT-UA минулого року опрацювала 4315 кіберінцидентів*. https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv
2. Ekşi, G. E., Tekinerdoğan, B., & Catal, C. (2022). Software security management in critical infrastructures: A systematic literature review. *Turkish Journal of Electrical Engineering and Computer Sciences, 30*(4), 1142–1161. https://doi.org/10.55730/1300-0632.3841
3. Okeke, K., & Omojola, S. (2025). Enhancing cybersecurity measures in critical infrastructure: Challenges and innovations for resilience. *Journal of Scientific Research and Reports, 31*(2), 474–484. https://doi.org/10.9734/jsrr/2025/v31i22868
4. Lubis, M., Safitra, M. F., Fakhrurroja, H., & Muttaqin, A. N. (2025). Guarding our vital systems: A metric for critical infrastructure cyber resilience. *Sensors, 25*(15), 4545. https://doi.org/10.3390/s25154545
5. ДСТУ ISO/IEC 27001:2023. (2023). *Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги*. https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104398
6. ДСТУ ISO/IEC 27002:2023. (2023). *Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Кодекс практики*. https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104399
7. Верховна Рада України. (2024). *Закон України "Про критичну інфраструктуру" від 17 листопада 2021 року № 1882-IX (в редакції від 21.09.2024)*. https://zakon.rada.gov.ua/laws/show/1882-20#Text

8. Lu, M. T., & Guimaraes, T. (2007). A guide to selecting expert systems applications. *Journal of Information Systems Management, 6*(2), 8–15. https://doi.org/10.1080/07399018908960138
9. Mukhoid, O. V., Kostornoi, O. S., & Shyfrin, D. M. (2018). Selection of the optimal software for designing expert systems. *Journal of Engineering Sciences*, *5*(2), E10–E15. https://doi.org/10.21272/jes.2018.5(2).e3
10. Madanchian, M., & Taherdoost, H. (2025). Applications of multi-criteria decision making in information systems for strategic and operational decisions. *Computers*, *14*(6), 208. https://doi.org/10.3390/computers14060208
11. Krisper, M., Dobaj, J., & Macher, G. (2020). Assessing risk estimations for cyber-security using expert judgment. In M. Yilmaz, P. Clarke, J. Niemann, & R. Messnarz (Eds.), *Systems, software and services process improvement – 27th European Conference, EuroSPI 2020, Proceedings* (pp. 120–134). Communications in Computer and Information Science (Vol. 1251). Springer. https://doi.org/10.1007/978-3-030-56441-4_9
12. Buchyk, C., Kondratenko, S., & Pysarchuk, O. (2006). *Systemy pidtrymky pryiniattia rishen*. Zhytomyr: ZhVIRE.