DOI 10.15276/imms.v13.no1-2.87
УДК 004.42:004.056.57

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 1-2, pp. 87-96

СИСТЕМИ АВТОМАТИЗОВАНОГО ВИБОРУ СКЛАДОВИХ ПРОГРАМНОГО ТА АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ КОРПОРАТИВНИХ КОМП'ЮТЕРІВ

А.В.Князєв, Р. І.Назаренко, О.А.Стопакевич, А.О.Стопакевич

Національний університет «Одеська політехніка»,
Проспект Шевченка, 1, Одеса, 65044, Україна; E-mail:
stopakevich@gmail.com

Забезпечення ефективної кібербезпеки для корпоративних комп'ютерів є надзвичайно важливою та складною задачею, яка вимагає ретельного вибору програмного та апаратного забезпечення. У даній статті розглядаються ключові компоненти програмного та апаратного забезпечення систем кібербезпеки – антивірусні програми та апаратні файрволи (мережеві екрани). З огляду на швидкий розвиток кіберзагроз, стає зрозумілим, що порівняння окремих характеристик вже не дозволяє зробити коректний вибір. Наприклад, коли мова йде про антивірусне програмне забезпечення, вже не можна просто орієнтуватися на розмір бази вірусів, оскільки їхня кількість сягає мільярда одиниць, і навіть найпотужнішому комп'ютеру не вистачить, щоб постійно ретельно перевіряти на збіг кожен виконавчий файл. Аналогічні виклики виникають із вибором апаратного забезпечення. Сучасні апаратні файрволи більше не обмежуються простим аналізом трафіку за заголовками пакетів та відкиданням небажаних адрес або портів. Вони повинні фільтрувати складний за структурою трафік, у тому числі зашифрований, і забезпечувати надійний захист, одночасно забезпечуючи високу продуктивність для задоволення потреб користувачів. Також варто зазначити, що вибір апаратного забезпечення має враховувати архітектуру мережі, масштабування та планування майбутніх потреб. Оскільки зробити відповідний вибір програмного та апаратного забезпечення кібербезпеки стає все складніше, автори статті пропонують автоматизувати вибір з використання досягнень в сучасній теорії прийняття рішень. Наведені алгоритми вибору інструментів, орієнтовані на персональні потреби та на думки експертної групи. Продемонстрована ефективність вказаних алгоритмів для розв'язку реальних задач вибору в галузі за допомогою спеціально розробленого авторами програмного забезпечення для автоматизованого вибору складових програмного та апаратного забезпечення системи кібербезпеки корпоративних комп'ютерів.

Ключові слова: вибір антивіруса, важливість альтернатив, вибір файрвола, експертний метод, програмне забезпечення, кібербезпека.

Вступ. Вибір складових програмного та апаратного забезпечення системи кібербезпеки корпоративних комп'ютерів є відповідальною й одночасно достатньо творчою задачею, кількість можливих розв'язків якої дуже велика. Забезпечення кібербезпеки включає широкий спектр компонентів, які мають бути відповідним чином вибрані та налаштовані для забезпечення захисту інформації в мережах корпоративних комп'ютерів. Складовими програмного забезпечення систем кібербезпеки в першу чергу є антивірусні та антишпигунські програми, також це системи виявлення вторгнень, програмні файрволи, парольні менеджери, криптографічне програмне забезпечення. Складовими апаратного забезпечення систем в першу чергу є апаратні файрволи, а також пристрої ідентифікації та фізичні засоби збереження даних. Тенденція розвитку апаратного й програмного забезпечення

полягає в постійному ускладненні інтелектуальних алгоритмів, тому порівняння за окремими характеристиками втрачає сенс й тільки вводить в оману.

Так, наприклад, задача функціонування сучасного антивірусу – це вже давно не задача пошуку фрагментів у виконавчих файлах. Експерти стверджують, що кількість створених вірусів сягнуло відмітки одного мільярда одиниць – таку перевірку кожного виконавчого файлу не витримає найпотужніший комп'ютер [1]. Виходячи з цього такий відомий критерій як розмір бази вірусів давно вже перестав бути показником. Сучасний антивірус в ідеалі має виявити шкідливу програму за її поведінкою, однак чим більше ми орієнтуємось на поведінку, а не на відомі фрагменти коду, тим більшим стає ризик виникнення хибних спрацьовувань антивірусу при перевірці системного програмного забезпечення, програм зі спеціальними алгоритмами захисту від піратства тощо. Чим складніший алгоритм антивірусу, тим більше він вимагає ресурсів, теж саме можливо сказати й про недосконалий алгоритм [2]. Відсутність простих критеріїв для порівняння антивірусів компенсується можливістю переходу до порівняння за результатами синтетичних тестів. Кількість відомих антивірусних програм становить більше ніж 200, звісно, серед них можна знайти узагальнено якісно виконані й узагальнено неякісно виконані антивіруси. Однак, власне кажучи, серед найкращих на ринку антивірусів абсолютно найкращий знайти складно, кожен з них відповідає певному критерію ефективності.

Аналогічна проблема виникає й з апаратним програмним забезпеченням. Сучасний апаратний файрвол – це не проста система, яка аналізує трафік за заголовками пакетів й відкидає такі, які належать до переліку певних адрес чи портів. Напроти, це звичайно дуже коштовна система, яка має фільтрувати зміст складного за структурою трафіку. Класичний параметр – кількість з'єднань, за якими визначають лінійки апаратних файрволів з ускладненням програмних алгоритмів, з впровадженням шифрування й мультимедіа трафіку, вже втратив себе як надійний показник для порівняння. Фактично продуктивність файрвола залежить від типу трафіку, а значить якість роботи з ним залежить як від архітектури мікропроцесора, обсягу пам'яті, так і від складності алгоритмів. Синтетичні тести можуть також створити перевірку продуктивності за певними узагальненими типами трафіку, однак, як і в випадку антивірусів, серед топових продуктів не можна знайти певного абсолютного лідера для всіх задач.

Виходячи зі сказаного, необхідно переходити до застосування автоматизованих інструментів вибору, які дозволяють обробити результати синтетичних тестів й знайти оптимум для конкретних потреб спеціалістів. Саме розробці таких інструментів й присвячена ця стаття.

Розв'язок задачі вибору найкращого антивірусу. Задача сучасного антивірусу – визначення та блокування активності різноманітного, за метою своєї розробки, способом поширення та принциповими алгоритмами програмного забезпечення [1-7].

Антивірус має виявити та блокувати активність наступних типів програмного забезпечення .

Класичні віруси – це тип шкідливого ПЗ яке вбудовується в інші виконувані файли або програми. Віруси можуть саморозповсюджуватися шляхом впровадження свого коду в інші файли та інфікувати інші системи.

Шкідливе програмне забезпечення можна поділити на наступні категорії [3]:

Вимагацьке ПЗ – намагається вимагати гроші у жертв, блокуючи їхні файли або пристрої, доки вони не заплатять кіберзловмиснику суму викупу.

Шпигунське ПЗ – дозволяє зловмисникам віддалено відстежувати активність на зараженому комп'ютері без відома або згоди користувача.

Трояни – замасковане під законне програмне забезпечення, які надають віддалений доступ до системи користувача для зловмисних цілей, таких як крадіжка конфіденційної інформації.

Хробаки – самовідтворюваний код, призначений для поширення мережами і спричинення збоїв; можуть використовуватися для різних шкідливих дій, таких як видалення файлів, поширення інших шкідливих програм або навіть захоплення контролю над комп'ютерами.

Рекламне ПЗ – принципово так ПЗ може бути не шкідливим, але постійно спричиняє незручності користувачу.

Перша проблема вибору антивірусів – це проблема вибору критеріїв для оцінки. Ця проблема не є тривіальною. Так, наприклад, в роботі [5] проведено аналіз різних критеріїв та зроблено висновок, що задача вибору має ставитись як принципово багатокритеріальна. Певні орієнтовні критерії вибору це: функціональні можливості, ефективність виявлення і блокування загроз, вплив на продуктивність операційної системи, сумісність, вартість, юзабіліті. В роботі [5] запропоновано класифікувати всі критерії у дві великі категорії: безпека та операційність.

Друга проблема вибору антивірусів – це проблема вибору методу багатокритеріальної оцінки. Відзначимо роботу [7], в якій запропоновано застосовувати метод діаграм Рея для вибору найкращого антивірусу. Недоліками роботи є те, що порівняння виконано лише для чотирьох антивірусів та й критерії, за якими виконано порівняння не зовсім обґрунтовані.

Розв’язок першої проблеми став можливим з впровадженням технології проведення синтетичних тестів, аналогічно до тестів, які проводяться щодо апаратного забезпечення комп’ютерів. Дослідження, що проводились з початку століття [8], дозволили створити технологію тестування антивірусів, полягає в оцінці за спеціальними узагальненими критеріями. На базі застосування цієї технології була сформована незалежна організація Av-Comparatives [9]. AV-Comparatives розробляє сценарії, що відтворюють реальні умови використання антивірусів, а також застосовує тестові файли та шкідливі програми для оцінки рівня виявлення і блокування. Організація також проводить тестування продуктивності, перевіряючи вплив антивірусного програмного забезпечення на швидкодію системи. AV-Comparatives отримала визнання у сфері безпеки і премії і відзнаки за свою роботу. Зокрема це премія "За видатні досягнення в галузі тестування безпеки" на конференції EICAR (European Institute for Computer Antivirus Research) й відзнака AV-Comparatives як лабораторії ІТ-тестування, яка заслуговує на довіру на цій же конференції.

Для антивірусів під ОС Windows компанія застосовує наступні критерії: Advanced Threat Protection (ATP), Mailware Protection (MWP), Perfomance, Real World Protection, False Alarms.

Advanced Threat Protection (ATP). Оцінює якість інтелектуального алгоритму для виявлення потенційно шкідливої активності програмного забезпечення, що працює на комп’ютері, зважаючи на якість виявлення вірусів, які не відомі програмі.

Malware Protection (MWP). Оцінює якість захисту користувача від запуску шкідливих програм, які розміщуються на локальних, мережевих та хмарних сховищах.

Perfomance. Оцінює швидкість роботи антивірусу. Критерій визначається експериментально за часом перевірки значної за обсягом бази.

Real World Protection (RWP). Оцінює ймовірність зараження вірусом через браузер при відвідуванні шкідливих сайтів.

Результати оцінювання критеріїв, отримані в результаті тестів, нормуються від 0 (найгірше значення) до 3 (найкраще значення).

Як основні ненормовані показники якості антивірусів застосовані такі показники.

False Alarms (FA). Оцінює не тільки кількість правильних спрацювань, але й кількість хибних. Визначається за великою тестовою базою даних. Кількісні показники адекватні для порівняння в межах тільки використаної БД вірусів.

Price. Оцінює вартість програми. Чим вища величина параметра, тим менш ймовірне зараження вірусом через браузер при відвідуванні шкідливих сайтів.

Оцінювання критеріїв якості для вибору антивірусів десктопної версії ОС Windows за результатами тестування у 2023 році приведені в табл. 1.

Таблиця 1

Результати оцінювання критеріїв якості для вибору антивірусів [9]

Антивірус	**ATP**	**MWP**	**Perfomance**	**RWP**	**ATP**	**FA**	**Ціна за рік**
Bitdefender	3	3	3	3	3	6	50
Avast	2	3	3	3	2	2	0
AVG	2	3	3	3	2	2	0
G Data	2	3	3	3	2	2	50
Avira	0	3	3	3	0	1	100
McAfee	0	3	3	3	0	9	86
ESET	3	2	3	1	3	0	35
VIPRE	0	3	2	3	0	6	40
NornonLifeLock	0	3	3	2	0	3	100
Microsoft	2	2	1	3	2	32	0
K7	0	1	3	3	0	67	26
Total Defense	0	3	1	2	0	6	57
TotalAV	0	3	2	2	0	0	119
Panda	0	0	3	2	0	102	0
Trend Micro	0	0	3	1	0	10	50
Mailwarebytes	0	0	3	0	0	25	40

Ціна за рік не є результатом тесту, а мається на увазі вартість річної підписки для персонального використання за рік в доларах США.

Далі розв’яжемо другу проблему, що дозволить знайти комплексний розв’язок задачі. Пропонуємо застосовувати метод прийняття рішень з урахуванням важливості альтернатив [10]. Цей метод дозволяє користувачеві задати свої переваги між кожною парою альтернатив. Кількість РС альтернатив формується виходячи з формули перестановок $PC = 0.5 \cdot C!/(C\text{-}2)!$, де C – кількість критеріїв вибору. Аналізуючи вихідні дані (табл. 1) треба зробити висновок, що критерії вибору дещо відрізняються за характером оцінки. Так, для перших чотирьох критеріїв порівняння в межах критерію однозначно просто – чим більше, тим краще. Для критеріїв FA і Price – чим більше, тим гірше й результати мають бути безумовно масштабовані.

Система автоматизованого вибору антивірусу реалізується як програма з графічним інтерфейсом, яка забезпечує можливість зручної заміни величин результатів синтетичних тестів, які регулярно оновлюються Av-Comparatives. Вибір пріоритетів реалізований в вигляді повзунків, які дозволяють графічно й інтуїтивно зрозуміло до користувача відобразити обраний пріоритет. Користувач має чітко визначитись з кожним пріоритетом. Якщо будь-який параметр йому не потрібний, то користувач має можливість його просто відімкнути й тоді кількість альтернатив, які необхідно обрати, зменшується. Також введено додатковий фільтр, який дозволяє, за

необхідності, чітко відокремити безплатні антивіруси від таких, які вимагають придбання комерційної ліцензії. Основні результати відображуються за допомогою гістограми, нормованої до 100% шкали. Також, для користувача графічно зображено фактичні ваги пріоритетів в вигляді кругової діаграми. Для реалізації програми обрано мову системи MATLAB, яка орієнтована на математичні розрахунки. Алгоритм вибору, закладений в програмі, застосовує матриці – саме на цей тип даних орієнтована мова. Також застосовано графічне середовище App Designer для швидкої розробки програм з графічним інтерфейсів, яке має графічний конструктор форм та розвинуті засоби візуалізації даних. Вікно екрану розробленої програми для введення відносної важливості критеріїв якості показано на рис. 1.

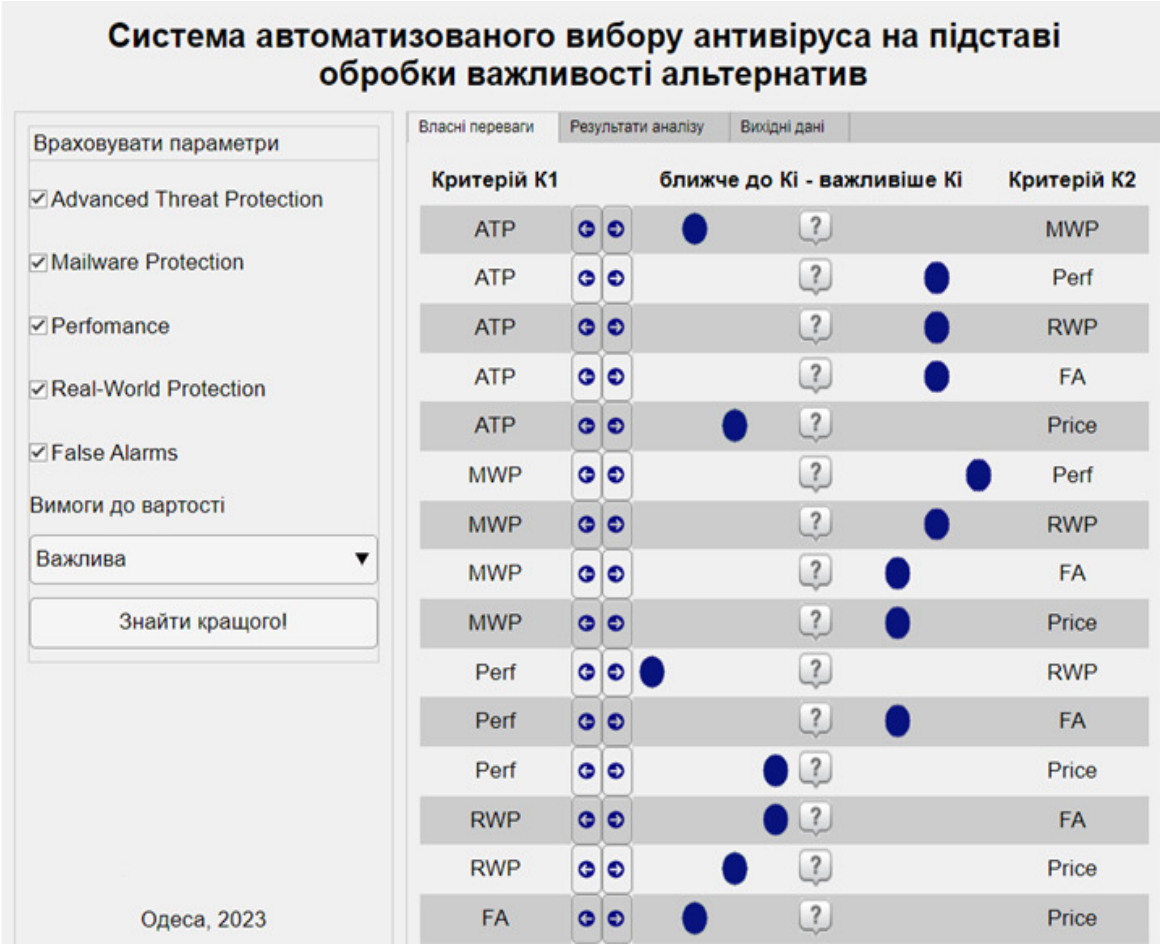

Рис.1. Вікно екрану програми для введення відносної важливості критеріїв якості

Вікно екрану розробленої програми з результатами розрахунку якостей антивірусів приведено на рис. 2.

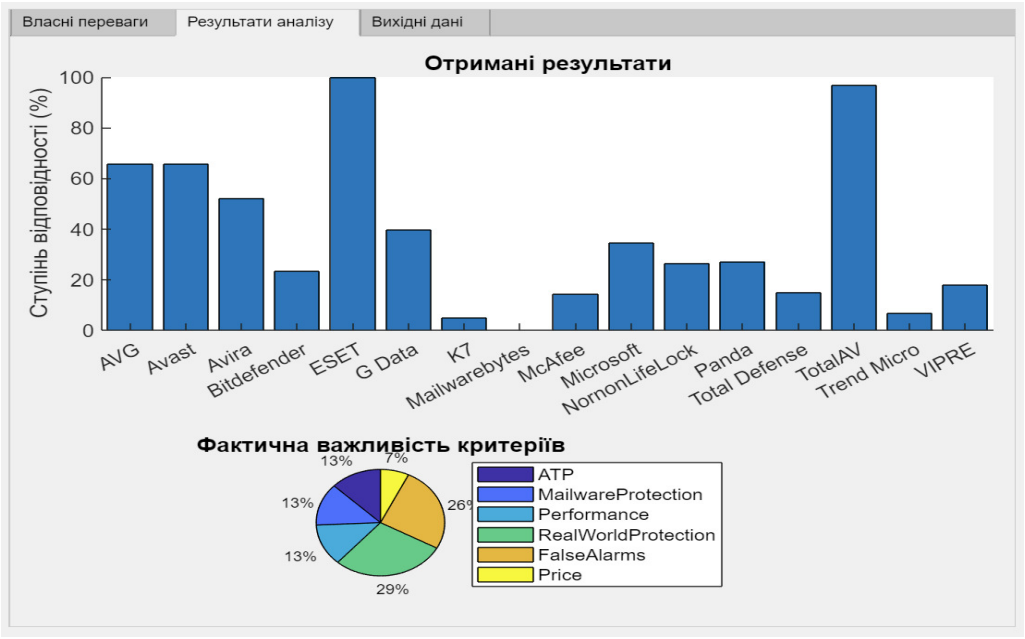

Рис.2. Вікно екрану програми з результатами розрахунку якостей антивірусів

Таким чином, бачимо що програма розв'язує поставлену задачу й є зручною для користування.

Розв'язок задачі вибору найкращого апаратного файрвола. Як і попередня задача, ця задача має дві проблеми.

Перша проблема – це проблема критерію вибору. Класичним основним критерієм вибору для апаратних файрволів є кількість можливих підключень. Виходячи з цього критерію, апаратні файрволи випускаються в межах лінійок, градація в яких проводиться по оціненій виробниками кількості можливих підключень. Файрволи для малого бізнесу призначені для обслуговування 50-200 користувачів; для середнього бізнесу – від 200 до 500 користувачів; для великого бізнесу – від 500 до 3000; для датацентрів - 3000 й більше. Однак, вибір за цим критерієм не має сенсу автоматизувати, він однозначно визначається масштабом підприємства. Після визначення лінійки файрволів основним стає критерій продуктивності обробки трафіку. Класифікація видів трафіку, який обробляє файрвол, показана на рис. 3.

Рис. 3. Класифікація трафіку, який обробляє файрвол

Таким чином, бачимо, що трафік має дві схеми класифікації, тому ми можемо виділити 6 типів трафіку з точки зору роботи файрвола. Зазвичай продуктивність по простому й мультимедіа трафіку відрізняється в 1.5-4 рази в залежності від типу пристрою. Продуктивність по нефільтрованому трафіку близька до продуктивності портів й мережевих пристроїв файрволу. Продуктивність по фільтрованому трафіку є меншою, кратність продуктивності фільтрованого до нефільтрованого трафіку залежить від апаратних та програмних можливостей пристрою, й становить звичайно від 0.3 до 0.9 раз. Продуктивність по трафіку протоколів зв'язку IPSec. В першу чергу це VPN. Продуктивність по IPSec трафіку є ще меншою, кратність продуктивності фільтрованого до нефільтрованого трафіку дуже залежить від апаратних та програмних можливостей пристрою (важливим є математичний сопроцесор, якість, ефективність та масштабованість криптографічних алгоритмів й відповідно програмного забезпечення), й становить звичайно від 0.1 до 0.8 раз до нефільтрованого трафіку.

Позначимо введені критерії якості файрволів наступним чином:

–FWD-B - максимальна здатність перенаправлення простого трафіку (Мбіт/с);

–FW-B - максимальна здатність фільтрації простого трафіку (Мбіт/с);

– IPS-B - максимальна здатність фільтрації простого VPN трафіку за технологією IpSEC (Мбіт/с);

–FWD-C - максимальна здатність перенаправлення мультимедіа (та іншого складного) трафіку (Мбіт/с);

–FW-C - максимальна здатність фільтрації мультимедіа (та іншого складного) трафіку (Мбіт/с);

–IPS-C - максимальна здатність фільтрації мультимедіа (та іншого складного) VPN трафіку за технологією IpSEC (Мбіт/с).

Також додамо критерій не пов'язаний з трафіком – CPU, тобто тактову частоту процесора файрвола (ГГц).

Вибір файрвола будемо проводити серед лінійки апаратних файрволів, яка відповідає потребам середнього бізнесу Відносні значення продуктивності 10 обраних файрволів різних виробників з близькою загальною продуктивністю приведені на рис. 4.

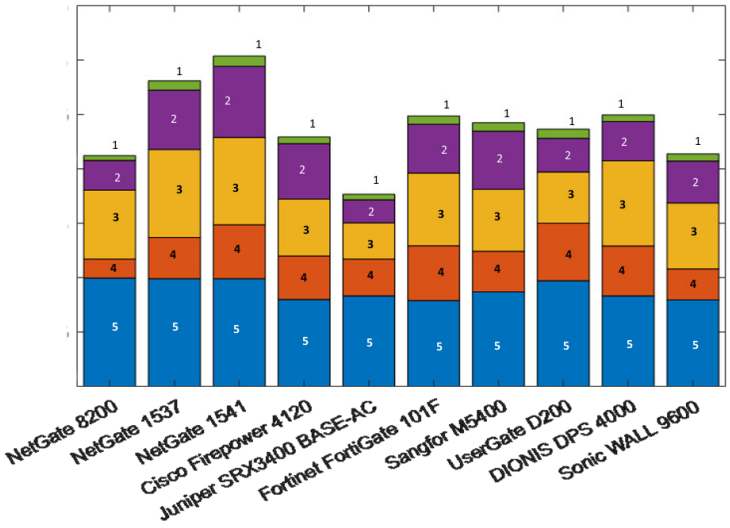

Рис.4. Відносні значення продуктивності файрволів

На рис. 4 висота стовпця характеризує величину FWD-B. Висота підстовпців характеризує нормоване відношення: 1. IPS-C/FWD-B; 2. FW-C/FWD-B; 3. FWD-C/FWD-B; 4.IPS-B/FWD-B; 5. FW-B/FWD-B).

Друга проблема – проблема методу вибору. Аналізуючи рис. 4, бачимо, що розподіл характеристик доволі нерівномірний. Таким чином, для підприємств з різним характером трафіку оптимальним буде вибір різних файрволів. На відміну від задачі вибору антивірусу, задача вибору файрволу для підприємства середнього бізнесу є задачею колективного вибору, яка має базуватись на розумінні специфіки роботи різних підрозділів підприємства. Характер трафіку в підприємстві (поточний й прогнозований) можуть знати експерти – системні адміністратори, мережевики. Отже, вибір має орієнтуватись на їх думки. Однак, щоб виключити суб'єктивність, думки експертів мають надаватись анонімно й оброблятись за спеціальним алгоритмом [10]. При цьому експертна група має формуватися таким чином, щоб думки експертів були узгодженими. Узгодженість визначається коефіцієнтом конкордації, який повинен бути не меншим за 0.7.

Система автоматизованого вибору апаратного файрвола реалізується як програма з графічним інтерфейсом, яка забезпечує можливість швидкого введення та модифікації бази параметрів пристроїв та думок експертів. Діалогове вікно програми має вигляд, приведений на рис. 5. Програму реалізовано як класичну десктоп-програму. Для цієї задачі також підходить MATLAB та App Designer. Зміна елементів таблиць думок експертів та технічних характеристик проводиться аналогічно редакторам електронних таблиць. Кожен рядок таблиць має опцію відмічення. Відмічені рядки враховуються при виборі найкращої моделі, не відмічені – не враховуються. Додавання елементів реалізовано шляхом заповнення спеціальних діалогів, введення параметрів в яких перевіряється. Видалення проводиться для елементів, які не відмічені. При зміні елементів таблиць перевіряються вхідні дані, а зміна думок експертів проводиться шляхом вибору з можливих варіантів оцінки. При зміні думок оцінки перераховуються та відображається новий коефіцієнт узгодженості. Значення таблиць зберігаються у текстових csv файлах. Таким чином, зміна кожного параметру зберігається автоматично.

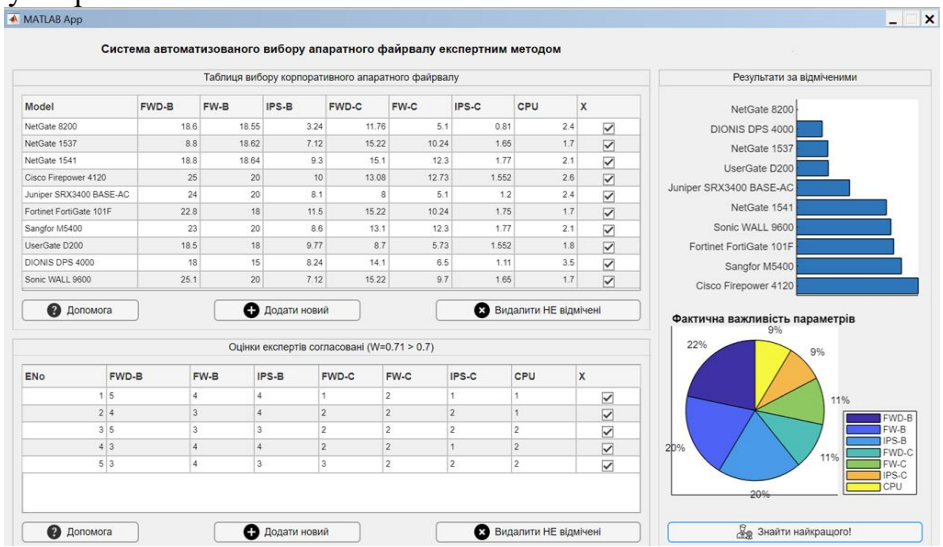

Рис.5. Діалогове вікно програми вибору файрвола

Розрахунок має проводитись лише при відповідному коефіцієнті узгодженості (конкордації) та наявності коректних вхідних даних. Основні результати розрахунку

представляються в вигляді двох графіків. Перший графік – гістограма, нормована до 100% шкали з відсортованими результатами, яка показує «ефективність моделі». Другий графік виконаний в вигляді кругової діаграми, в якій зображуються пріоритети параметрів.

Висновки. Розроблені системи автоматизованого вибору складових програмного та апаратного забезпечення системи кібербезпеки корпоративних комп'ютерів.

Запропоновано замість класичних критеріїв порівняння антивірусів застосовувати результати синтетичних тестів. Вибір проводиться на базі суб'єктивних переваг користувача для кожного з обраних критеріїв. Об'єктивні значення критеріїв беруться з результатів періодичних тестів AV-Comparatives.

Запропоновано замість класичного критерію порівняння апаратних файрволів застосовувати 7 критеріїв, 6 з яких належать до продуктивності апаратного файрвола за різними типами трафіку. Вибір проводиться на базі обробки думок експертної групи, яка має узгодженість. Значення критеріїв беруться з документації файрволів або результатів незалежних тестів.

Розроблені системи автоматизованого вибору антивірусу та файрвола як програми з графічним інтерфейсом. Продемонстровані функціональні можливості програм показують, що вони зручно та ефективно виконують усі поставлені задачі.

Розроблені системи автоматизованого вибору рекомендуються для застосування спеціалістами з кібербезпеки та системними адміністраторами.

Список літератури

1 Jovanovic B.A. Not-So-Common Cold: Malware Statistics in 2023. URL: https://dataprot.net/statistics/malware-statistics/

2 Fahad A. The Evolution of Antivirus Software to Face Modern Threats in 2023. URL: https://securityintelligence.com/posts/antivirus-evolution-to-face-modern-threats/

3 Alenezi M.N., Alabdulrazzaq H.K., Alshaher A.A., Alkharang M.M. Evolution of Malware Threats and Techniques: a Review. *International Journal of Communication Networks and Information Security (IJCNIS)*, 2020. Vol. 12. No.3. P.326-337. URL: https://doi.org/10.17762/ijcnis.v12i3.4723

4 Leka C., Ntantogian C., Karagiannis S., Magkos E., Verykios V. A Comparative Analysis of VirusTotal and Desktop Antivirus Detection Capabilities. *13th International Conference on Information, Intelligence, Systems & Applications (IISA)*, 2022. P.1-6. URL: https://doi.org/10.1109/IISA56318.2022.9904382.

5 Alharbi B., Asseri A., Alzahrani H., Taramisi K. Anti-Malware Efficiency Evaluation Framework. Anti-Malware Efficiency Evaluation Framework. *2nd International Conference on Computer and Information Sciences (ICCIS),* 2020. P. 1-4. URL: http://doi.org/10.1109/ICCIS49240.2020.9257637

6 Al-Saleh M., Hamdan H. Precise Performance Characterization of Antivirus on the File System Operations. *Journal of Universal Computer Science,* 2019. Vol. 25. P.1089-1108. URL: https://doi.org/10.3217/jucs-025-09-1089

7 Gorshkov A.V., Lokhvitskii V.A., Khomonenko A.D., Rybakova E.A., Gorshkov V.N. Multi-criteria choice of Antivirus tools with using the Ray diagrams. *Intellectual technologies on transport*, 2016. No. 2. P. 23-29.

8 Marx A., Rautenstrauch C. Systematisches Testen von Anti-Viren-Software. Wirtschaftsinf 45, 435–443 (2003). https://doi.org/10.1007/BF03250908

9 AV Comparatives. URL: https://www.av-comparatives.org/

10 Стопакевич О.А. Теорія прийняття рішень: конспект лекцій. Одеса: НУОП, 2021.

А.В.Князєв, Р. І.Назаренко, О.А.Стопакевич, А.О.Стопакевич

AUTOMATED SOFTWARE AND HARDWARE SELECTION SYSTEMS FOR ENTERPRISE COMPUTERS' CYBERSECURITY

A.V.Knyazev, R.I.Nazarenko, O.A.Stopakevych, A.O.Stopakevych

National Odesa Polytechnic University, Shevchenko str., 1, Odesa, 65044, Ukraine
stopakevich@gmail.com

Providing effective cybersecurity for corporate computers is an extremely important and complex task that requires careful choice of software and hardware. This article discusses the key components of cybersecurity software and hardware - antivirus programs and hardware firewalls. Considering the rapid growth of cyber threats, it becomes clear that comparing individual characteristics no longer allows users to make the right choice. For example, when it comes to antivirus software, it is no longer possible to simply focus on the size of the virus database, as the number of viruses reaches a billion, and even the most powerful computer is not enough to scan every executable file for a match. Similar challenges arise with the choice of hardware. Modern hardware firewalls are no longer limited to simply analyzing traffic by packet headers and dropping unwanted addresses or ports. They must filter complex traffic, including encrypted traffic, and provide reliable protection while delivering high performance to meet user needs. It is also worth noting that the choice of hardware should take into account the network architecture, scalability, and planning for future needs. Since it is becoming increasingly difficult to make the appropriate choice of cybersecurity software and hardware, the authors of the article propose to automate the choice using advances in modern decision theory. The authors present algorithms for choosing tools based on personal needs and the opinions of an expert group. The authors demonstrate the effectiveness of these algorithms for solving real-world selection problems in the industry with the help of software specially developed by the authors for automated selection of software and hardware components of the corporate computer cybersecurity system.

Keywords: choice of antivirus, importance of alternatives, choice of firewall, expert method, software, cybersecurity