УДК 004.056.53:658
DOI: 10.31673/2409-7292.2024.010001

Савченко В. А., Рибальченко О. Г.

ПОБУДОВА ЕФЕКТИВНОЇ СИСТЕМИ МЕРЕЖЕВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА НА ОСНОВІ МЕТОДУ АНАЛІЗУ ІЄРАРХІЙ ПОКАЗНИКІВ ЯКОСТІ

Стаття присвячена аналізу оптимального вибору систем мережевої безпеки для підприємств на основі методу попарного порівняння критеріїв. Досліджено швидкість реакції, рівень захисту, інтегрованість та достовірність систем. Розглянуті загальні вимоги щодо якості та вартості. Висновок робиться про необхідність комплексного підходу до вибору системи та уважного врахування всіх аспектів для забезпечення ефективного захисту інформації. Стаття аналізує важливість збалансованого підходу між ефективністю та вартістю при виборі системи мережевої безпеки. Підкреслено значення інтеграції з існуючими системами та врахування вимог щодо відповідності стандартам безпеки. Результати дослідження вказують на необхідність уважного аналізу перед прийняттям рішення щодо вибору системи мережевої безпеки для підприємства. Додатково, стаття розглядає вплив кожного з розглянутих критеріїв на загальний рівень захищеності мережі підприємства та надійність захисту інформації. Запропоновані рекомендації щодо оптимального вибору систем мережевої безпеки можуть стати корисними для керівництва підприємства та фахівців з інформаційної безпеки, сприяючи покращенню загального рівня кіберзахисту. У підсумку, стаття пропонує комплексний підхід до вибору систем мережевої безпеки на основі об'єктивного порівняння різних критеріїв. Врахування швидкості реакції, рівня захисту, інтегрованості та вартості допомагає підприємствам забезпечити ефективний та економічний захист їхніх інформаційних ресурсів. Дослідження може бути корисним як для керівництва, що вирішує питання інвестування в безпеку, так і для фахівців з інформаційної безпеки, що шукають оптимальні рішення для конкретних потреб підприємства.

Ключові слова: мережева безпека, IDS, IPS, попарне порівняння, кіберзагрози, вибір системи, ефективність, вартість, захищеність, інтегрованість, критерії.

Вступ

Сучасні підприємства стикаються зі зростаючою загрозою кібератак та інших форм кіберзлочинності, що робить побудову ефективної системи мережевої безпеки надзвичайно важливою задачею. Захист конфіденційності, цілісності та доступності даних стає ключовим аспектом в управлінні бізнесом та забезпеченні стабільності операцій. У зв'язку зі складністю та динамічністю кіберзагроз, вибір та належна настройка систем мережевої безпеки стають завданнями, які потребують уважного аналізу та професійного підходу. Проблема побудови ефективної системи мережевої безпеки полягає в пошуку оптимального балансу між витратами на захист та рівнем захищеності, а також у відповідності системи специфіці підприємства та його потребам.

Ця стаття присвячена розгляду основних вимог до побудови ефективної системи мережевої безпеки на підприємстві та шляхів їх вирішення. Аналіз існуючих підходів та найкращих практик у цій галузі дозволить виявити ключові аспекти успішної реалізації такої системи. Результати цього дослідження будуть корисними для керівників з інформаційної безпеки, адміністраторів та всіх зацікавлених у покращенні захисту мережевих ресурсів.

Постановка проблеми

В сучасному світі з кіберзагрозами та інформаційною безпекою підприємства стикаються з необхідністю вибору та належної настройки комплексу систем виявлення та запобігання вторгнень (IDS/IPS). Вірогідність кібератак зростає, і від цих систем залежить не лише виявлення потенційних загроз, але й захист від них.

Проблема вибору ефективного комплексу IDS/IPS полягає в необхідності знаходження оптимального балансу між рівнем захисту та витратами на реалізацію та підтримку. З одного боку, системи повинні ефективно виявляти широкий спектр загроз, включаючи відомі та нові типи атак. З іншого боку, вони повинні мати низький рівень фальшивих позитивів, щоб уникнути надмірної кількості неправомірних спрацювань, які можуть призвести до перевантаження та втрати часу на аналіз. Додатковою складністю є необхідність інтеграції цих систем з існуючою інфраструктурою безпеки та забезпечення відповідності вимогам

законодавства та стандартам безпеки. Успішний вибір комплексу IDS/IPS є критичним для забезпечення надійного захисту мережевих ресурсів підприємства.

Аналіз публікацій

Аналіз публікацій щодо методики вибору ефективного комплексу IDS/IPS показує, що для вибору правильного рішення необхідно визначити критичні активи в мережі та розбити їх на зони, вибрати апаратне та програмне забезпечення, яке відповідає вимогам організації, та періодично проводити аудит безпеки та тестування на проникнення. IDS та IPS постійно моніторять мережу, ідентифікують підозрілі активності та приймають відповідні заходи для зменшення потенційних загроз. IDS використовується для виявлення загроз на основі відомих експлойтів, зловмисних поведінок та технік атак, тоді як IPS виконує функції IDS та зупиняє виявлені загрози. IDS використовується для спостереження, тоді як IPS для контролю.

У статті [1] розглянуті головні фактори, які необхідно врахувати при проектуванні безпечної мережі. Проаналізовано найпоширеніші методи Інтернет-атак та інших загроз в сучасних комп'ютерних мережах. Досліджено механізми безпеки до набору протоколів Інтернету на різних рівнях, що забезпечують логічний захист даних у мережі.

Стаття [2] досліджує можливі мережеві загрози, які можна виявити за допомогою інтелектуального моніторингу трафіку комп'ютерної мережі, а також визначено перспективи застосування інтелектуального моніторингу для покращення систем виявлення атак. В публікації [3] описано, як можна вплинути на продуктивність завдяки використанню брандмауера Microsoft. Також, у статті перевірено багато ситуацій і проектів та показані результати для визначення ефекту використання брандмауерів на продуктивність.

У статті [4] наведено пояснення мережевих вторгнень, виявлення та запобігання для їх подолання. Основна мета статті [5] полягає в тому, щоб детально обговорити різні типи IPS/IDS та їх унікальність, яка виділяє їх з різних причин. Додатковий пункт для обговорення вказує на те, які IDS/IPS можна використовувати відповідно до вимог безпеки, їх функціональні можливості та ефективність, щоб зупинити зловмисну діяльність у комп'ютерній мережі. Буде наведено причини вибору конкретного IDS/IPS. Однією з головних цілей документу є підвищення обізнаності про доступність IDS/IPS та інформацію про те, який з них вибрати для своїх вимог.

Стаття [6] має на меті визначити відмінності між системами виявлення вторгнень на основі хоста (HIDS) і мережевими системами виявлення вторгнень (NIDS) і порівняти інструменти, які використовують HIDS і NIDS. Стверджується, що для кращої гарантії APT-атак має бути гібридний підхід IDS, який охоплює як мережі, так і хости, використовуючи як сигнатурні, так і поведінкові механізми виявлення на основі алгоритмів глибокого навчання.

У статті [7] автори детально досліджують багато нещодавніх і відповідних IDS/IPS, запропонованих між 2019 і 2022 роками для мереж Інтернету речей, надають їх ключові особливості, сильні сторони, недоліки та проблеми, щоб виявити проблеми, які все ще потребують вирішення. Стаття також викладає основний напрямок досліджень і відкриває шлях до нових напрямків дослідження для майбутніх дослідників.

Не зважаючи на значну кількість публікацій, наразі ще не створено достатньо простої методики побудови ефективної системи мережевої безпеки, яка б враховувала ключові фактори та передумови організації.

Мета нашого дослідження полягає в розробці моделі системи захисту інформації, яка б враховувала специфіку потреб підприємства та забезпечувала високий рівень безпеки даних. Ця стаття пропонує аналіз існуючих підходів до захисту інформації, огляд методу аналізу ієрархій показників якості та його застосування до розробки ефективних систем захисту інформації.

Результати цього дослідження можуть бути корисними для керівників інформаційної безпеки, менеджерів технологічних підрозділів та всіх зацікавлених у підвищенні рівня захисту інформації на підприємстві.

Виклад основного матеріалу

Визначення вагомості параметрів у складній системі вважається важкою задачею, що сильно впливає на результати її створення. Ретроспективний аналіз виявляє чотири основні напрямки у процесі розробки складних систем [8].

Перший напрямок ("Працездатність") характеризується обмеженим досвідом у вирішенні нових завдань і використанням спеціалізованих методів, щоб елементи системи функціонували відповідно.

Другий напрямок ("Оптимальність") спрямований на поліпшення методології проектування та покращення характеристик системи шляхом оптимізації показників якості.

Третій напрямок ("Вартість") передбачає створення економічно ефективних систем, замість оптимізації технічних характеристик.

Четвертий напрямок ("Ефективність") включає системний підхід, який охоплює всі аспекти життєвого циклу складних систем, враховуючи їх взаємодію з навколишнім середовищем.

Враховуючи складність створення нової методології, доцільним є розгляд цього завдання поетапно, з проведенням порівняльного аналізу напрямків розвитку системи для визначення їх важливості та порядку пріоритетів.

Для вирішення цієї проблеми скористаємось одним з інструментів кластерного аналізу – методом аналізу ієрархій. Суть методу полягає у наступному [9–10].

1. Побудова багаторівневої ієрархії проблеми (рис.1).

Перший рівень визначає головну мету I_1 розробки ефективної методології проектування.

Другий рівень – сукупність критеріїв I_{2i}, $i=\overline{1,k}$ за якими можна порівняти різні підходи при виборі “найкращої” методології. У якості таких підходів на другому рівні можуть використовуватись наступні:

I_{21} – *повнота* урахування факторів, які впливають на якість проектованої системи;

I_{22} – *адекватність* (відповідність вимогам та завданням);

I_{23} – *довготривалість,* або здатність враховувати наслідки функціонування системи;

I_{24} – *реалізованість*, або можливість використання методології на практиці з прийнятними витратами часу та ресурсів.

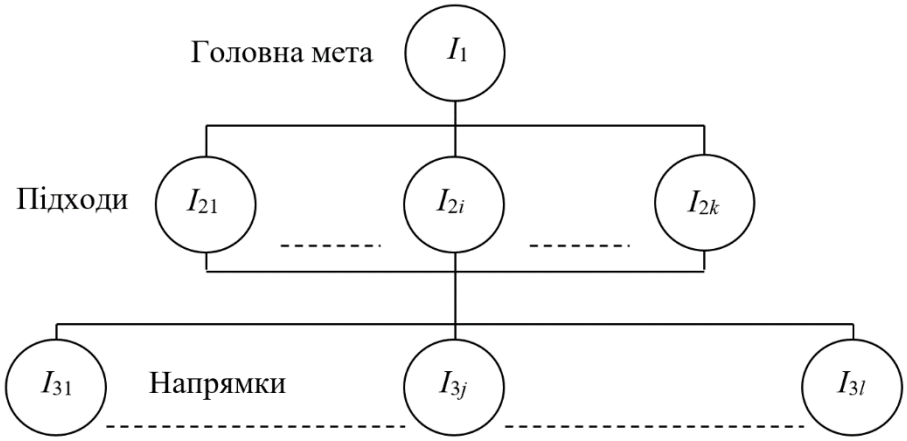

Рис.1. Багаторівнева ієрархія проблеми

Третій рівень I_{31}, ..., I_{3l} – сукупність критеріїв, за якими будемо порівнювати можливі напрямки розвитку методології проектування, наприклад:

I_{31} – забезпечення ефективності на великому часовому інтервалі;

I_{32} – модифікація критеріїв ефективності системи (економічність, безпека, надійність та ін.);

I_{33} – перехід від проектування об'єкта до проектування майбутнього штучного середовища існування об'єкта;

I_{34} – прогнозування можливостей об'єкта;

I_{35} – урахування зміни параметрів зовнішнього середовища;

I_{36} – пошук нових ідей та рішень, в т.ч. в інших галузях науки.

2. Попарне порівняння елементів ієрархії на другому рівні: $I_{2i} \sim I_{2j}$, $i \neq j$, $i, j = \overline{1,4}$.

З цією метою складемо матрицю попарних порівнянь критеріїв (табл.1).

Таблиця 1

Матриця попарних порівнянь критеріїв

для I_1	I_{21}	I_{22}	I_{2i}	I_{2k}	$\tilde{P}_2(\bullet)$
I_{21}	1	α_{21}^{22}	α_{21}^{2i}	α_{21}^{2k}	$\tilde{P}_2(I_{21})$
I_{22}	α_{22}^{21}	1	α_{22}^{2i}	α_{22}^{2k}	$\tilde{P}_2(I_{22})$
I_{2i}	α_{2i}^{21}	α_{2i}^{22}	1	α_{2i}^{2k}	$\tilde{P}_2(I_{2i})$
I_{2k}	α_{2k}^{21}	α_{2k}^{22}	α_{2k}^{2i}	1	$\tilde{P}_2(I_{2k})$

По діагоналі матриці записуються 1.

Порівняння проводимо у нормалізованій формі по відношенню відповідних I_{2j} до головної мети I_1. Результат порівняння α_{2n}^{2m}, $n,m=\overline{1,k}$ носить суб'єктивний характер, тобто не може бути суворо формалізованим.

Практика свідчить, що таке порівняння зручно виконувати за шкалою 0–10. Результат порівняння характеризує відношення ваги I_{2i}, I_{2j}, тобто у скільки разів вплив критерію I_{2i} є важливішим, ніж вплив I_{2j} на головну мету I_1. Таким чином параметр α_{2n}^{2m} буде характеризувати вагу критерію I_{2n} по відношенню до критерію I_{2m} за впливом на загальний критерій I_1

$$\alpha_{21}^{22} = \frac{I_{21}}{I_{22}};\ \alpha_{2l}^{2i} = \frac{I_{2l}}{I_{2i}};\ \alpha_{2l}^{2k} = \frac{I_{2l}}{I_{2k}};\ \alpha_{2j}^{2j} = 1;\ \alpha_{2n}^{2m} = \frac{I_{2n}}{I_{2m}},\ m,n = \overline{1,k},$$

при чому $\alpha_{2n}^{2m} = \dfrac{1}{\alpha_{2m}^{2n}} = \left[\alpha_{2m}^{2n}\right]^{-1}$.

3. Визначення пріоритетів $\tilde{P}_2(I_{2k})$ критеріїв I_{2i}, $i = \overline{1,k}$ як нормованої суми рядків елементів матриці парних порівнянь. Попередньо визначимо суму рядків елементів матриці

$$P_2(I_{21}) = 1 + \alpha_{21}^{22} + \ldots + \alpha_{21}^{2i} + \ldots + \alpha_{21}^{2k} = \sum_{r=1}^{k} \alpha_{21}^{2r};\ P_2(I_{22}) = \alpha_{22}^{21} + 1 + \ldots + \alpha_{22}^{2i} + \ldots + \alpha_{22}^{2k} = \sum_{r=1}^{k} \alpha_{22}^{2r};\ \ldots;$$

$$P_2(I_{2i}) = \alpha_{2i}^{21} + \alpha_{2i}^{22} + \ldots + 1 + \ldots + \alpha_{2i}^{2k} = \sum_{r=1}^{k} \alpha_{2i}^{2r};\ \ldots;\ P_2(I_{2k}) = \alpha_{2k}^{21} + \alpha_{2k}^{22} + \ldots + \alpha_{2k}^{2i} \ldots + 1 = \sum_{r=1}^{k} \alpha_{2k}^{2r}.$$

Пріоритети критеріїв другого рівня визначаємо шляхом нормування сум рядків

$$\tilde{P}_2(I_{21}) = \frac{P_2(I_{21})}{\sum_{r=1}^{k} P_2(I_{2r})};\ \tilde{P}_2(I_{22}) = \frac{P_2(I_{22})}{\sum_{r=1}^{k} P_2(I_{2r})};\ \ldots;\ \tilde{P}_2(I_{2i}) = \frac{P_2(I_{2i})}{\sum_{r=1}^{k} P_2(I_{2r})};\ \ldots;\ \tilde{P}_2(I_{2k}) = \frac{P_2(I_{2k})}{\sum_{r=1}^{k} P_2(I_{2r})}.$$

Тобто $\tilde{P}_2(I_{2i}) = \dfrac{\sum_{r=1}^{k} \alpha_{2k}^{2r}}{\sum_{r=1}^{k} \alpha_{21}^{2r} + \sum_{r=1}^{k} \alpha_{22}^{2r} + \cdots + \sum_{r=1}^{k} \alpha_{2k}^{2r}} = \dfrac{\sum_{r=1}^{k} \alpha_{2k}^{2r}}{\sum_{s=1}^{k}\sum_{r=1}^{k} \alpha_{2s}^{2r}}$.

4. Здійснення попарного порівняння елементів ієрархії на третьому рівні для кожного $I_{3i} \sim I_{3j},\ i \neq j,\ i, j = \overline{1,6}$ з елементів ієрархії на другому рівні (табл. 2, 3, 4, 5).

Таблиця 2

для I_{21}	I_{31}	I_{32}	...	I_{3i}	...	I_{3l}	${}_1\tilde{P}_3(\bullet)$
I_{31}	1	${}_1\beta_{31}^{32}$	...	${}_1\beta_{31}^{3i}$	...	${}_1\beta_{31}^{3l}$	${}_1\tilde{P}_3(I_{31})$
I_{32}	${}_1\beta_{32}^{31}$	1	...	${}_1\beta_{32}^{3i}$	...	${}_1\beta_{32}^{3l}$	${}_1\tilde{P}_3(I_{32})$
...	...	...	1	...	...	...	…
I_{3i}	${}_1\beta_{3i}^{31}$	${}_1\beta_{3i}^{32}$	...	1	...	${}_1\beta_{3i}^{3l}$	${}_1\tilde{P}_3(I_{3i})$
...	...	...	...	...	1	...	…
I_{3l}	${}_1\beta_{3l}^{31}$	${}_1\beta_{3l}^{32}$	...	${}_1\beta_{3l}^{3i}$	...	1	${}_1\tilde{P}_3(I_{3l})$

Таблиця 3

для I_{22}	I_{31}	I_{32}	...	I_{3i}	...	I_{3l}	${}_2\tilde{P}_3(\bullet)$
I_{31}	1	${}_2\beta_{31}^{32}$	...	${}_2\beta_{31}^{3i}$	...	${}_2\beta_{31}^{3l}$	${}_2\tilde{P}_3(I_{31})$
I_{32}	${}_2\beta_{32}^{31}$	1	...	${}_2\beta_{32}^{3i}$	...	${}_2\beta_{32}^{3l}$	${}_2\tilde{P}_3(I_{32})$
...	...	...	1	...	...	...	…
I_{3i}	${}_2\beta_{3i}^{31}$	${}_2\beta_{3i}^{32}$	...	1	...	${}_2\beta_{3i}^{3l}$	${}_2\tilde{P}_3(I_{3i})$
...	...	...	...	...	1	...	…
I_{3l}	${}_2\beta_{3l}^{31}$	${}_2\beta_{3l}^{32}$	...	${}_2\beta_{3l}^{3i}$	...	1	${}_2\tilde{P}_3(I_{3l})$

Таблиця 4

для I_{2j}	I_{31}	I_{32}	...	I_{3i}	...	I_{3l}	${}_j\tilde{P}_3(\bullet)$
I_{31}	1	${}_j\beta_{31}^{32}$	...	${}_j\beta_{31}^{3i}$	...	${}_j\beta_{31}^{3l}$	${}_j\tilde{P}_3(I_{31})$
I_{32}	${}_j\beta_{32}^{31}$	1	...	${}_j\beta_{32}^{3i}$	...	${}_j\beta_{32}^{3l}$	${}_j\tilde{P}_3(I_{32})$
...	...	...	1	...	...	...	…
I_{3i}	${}_j\beta_{3i}^{31}$	${}_j\beta_{3i}^{32}$	...	1	...	${}_j\beta_{3i}^{3l}$	${}_j\tilde{P}_3(I_{3i})$
...	...	...	...	...	1	...	…
I_{3l}	${}_j\beta_{3l}^{31}$	${}_j\beta_{3l}^{32}$	...	${}_j\beta_{3l}^{3i}$	...	1	${}_j\tilde{P}_3(I_{3l})$

Таблиця 5

для I_{2k}	I_{31}	I_{32}	...	I_{3i}	...	I_{3l}	${}_k\tilde{P}_3(\bullet)$
I_{31}	1	${}_k\beta_{31}^{32}$	...	${}_k\beta_{31}^{3i}$	...	${}_k\beta_{31}^{3l}$	${}_k\tilde{P}_3(I_{31})$
I_{32}	${}_k\beta_{32}^{31}$	1	...	${}_k\beta_{32}^{3i}$	...	${}_k\beta_{32}^{3l}$	${}_k\tilde{P}_3(I_{32})$
...	...	...	1	...	...	...	…
I_{3i}	${}_k\beta_{3i}^{31}$	${}_k\beta_{3i}^{32}$	...	1	...	${}_k\beta_{3i}^{3l}$	${}_k\tilde{P}_3(I_{3i})$
...	...	...	...	...	1	...	…
I_{3l}	${}_k\beta_{3l}^{31}$	${}_k\beta_{3l}^{32}$	...	${}_k\beta_{3l}^{3i}$	...	1	${}_k\tilde{P}_3(I_{3l})$

Порівняння проводять аналогічно у нормованій формі. Елементи матриці парних порівнянь мають зміст відношення критеріїв I_{3i} та I_{3j} $i,j=\overline{1,l}$ до ступеня їх впливу на I_{2l}, $l=\overline{1,k}$, ${}_1\beta_{3n}^{3m}=\dfrac{I_{3n}}{I_{3m}}$, $m,n=\overline{1,l}$, ${}_1\beta_{3i}^{3i}=1$.

5. Визначення пріоритетів ${}_i\tilde{P}_3(I_{3i})$ $j=\overline{1,l}$, $i=\overline{1,k}$ критеріїв I_{3i}, як нормовану суму рядків елементів відповідної матриці парних порівнянь

$${}_1P_3(I_{31})=1+{}_1\beta_{31}^{32}+...+{}_1\beta_{31}^{3i}+...+{}_1\beta_{31}^{3l}=\sum_{r=1}^{l}{}_1\beta_{31}^{3r};\ {}_1P_3(I_{32})={}_1\beta_{32}^{31}+1+...+{}_1\beta_{32}^{3i}+...+{}_1\beta_{32}^{3l}=\sum_{r=1}^{l}{}_1\beta_{32}^{3r};$$

$$\ldots;\ {}_kP_3(I_{3i})=\sum_{r=1}^{l}{}_k\beta_{3i}^{3r}.$$

6. Визначення узагальнених ваг напрямків по відношенню до головної мети. Урахування впливу критеріїв другого рівня на третій (рис. 1) може бути здійснено відповідною корекцією елементів матриці $\tilde{P}_3$, яка складається з пріоритетів критеріїв I_{3i} (табл. 2, 3, 4, 5) і має назву матриці пріоритетів напрямків. Колонками матриці $\tilde{P}_3$ є праві стовпчики таблиць 2, 3, 4, 5

$$\tilde{P}_3=\begin{bmatrix} {}_1\tilde{P}_3(I_{31}) & {}_2\tilde{P}_3(I_{31}) & \cdots & {}_k\tilde{P}_3(I_{31}) \\ {}_1\tilde{P}_3(I_{32}) & {}_2\tilde{P}_3(I_{32}) & \cdots & {}_k\tilde{P}_3(I_{32}) \\ \cdots & \cdots & \cdots & \cdots \\ {}_1\tilde{P}_3(I_{3l}) & {}_1\tilde{P}_3(I_{3l}) & \cdots & {}_k\tilde{P}_3(I_{3l}) \end{bmatrix}.$$

Далі визначаємо модифіковану матрицю ${}_м\tilde{P}_3$ пріоритетів $\tilde{P}_3$ з урахуванням пріоритетів критеріїв $\tilde{P}_2$. Матриця ${}_м\tilde{P}_3$ отримується шляхом множення матриці $\tilde{P}_3$ на діагональну матрицю $\tilde{P}_2$, де

$$\tilde{P}_2=\begin{bmatrix} \tilde{P}_2(I_{21}) & 0 & 0 & 0 & 0 & 0 \\ 0 & \tilde{P}_2(I_{22}) & 0 & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \tilde{P}_2(I_{2i}) & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & 0 & \tilde{P}_2(I_{2k}) \end{bmatrix},$$

$$ {}_{\text{м}}\tilde{P}_3 = \tilde{P}_3\ \tilde{P}_2 = \begin{bmatrix} \tilde{P}_2(I_{21})\cdot {}_1\tilde{P}_3(I_{31}) & \tilde{P}_2(I_{22})\cdot {}_2\tilde{P}_3(I_{31}) & \cdots & \tilde{P}_2(I_{2k})\cdot {}_k\tilde{P}_3(I_{31}) \\ \tilde{P}_2(I_{21})\cdot {}_1\tilde{P}_3(I_{32}) & \tilde{P}_2(I_{22})\cdot {}_2\tilde{P}_3(I_{32}) & \cdots & \tilde{P}_2(I_{2k})\cdot {}_k\tilde{P}_3(I_{32}) \\ \cdots & \cdots & \cdots & \cdots \\ \tilde{P}_2(I_{21})\cdot {}_1\tilde{P}_3(I_{3l}) & \tilde{P}_2(I_{22})\cdot {}_2\tilde{P}_3(I_{3l}) & \cdots & \tilde{P}_2(I_{2k})\cdot {}_k\tilde{P}_3(I_{3l}) \end{bmatrix}. $$

Узагальнення ваги V напрямків I_{3i}, $i=\overline{1,l}$ по відношенню до головної мети I_1 знаходимо шляхом множення матриці ${}_{\text{м}}\tilde{P}_3$ на одиничний вектор $\mathbf{1}_{(l)}$, $\mathbf{1}_{(l)} \in \mathrm{R}^l$, $V = {}_{\text{м}}\tilde{P}_3 \cdot \mathbf{1}_{(l)} = [V_1\ V_2\ \ldots\ V_l]^{\mathrm{T}}$

$$ \tilde{P}_2(I_{21})\cdot {}_1\tilde{P}_3(I_{31}) + \tilde{P}_2(I_{22})\cdot {}_2\tilde{P}_3(I_{31}) + \ldots + \tilde{P}_2(I_{2k})\cdot {}_k\tilde{P}_3(I_{31}) = \sum_{i=1}^{k} \tilde{P}_2(I_{2i})\cdot {}_i\tilde{P}_3(I_{31}); $$

$$ \tilde{P}_2(I_{21})\cdot {}_1\tilde{P}_3(I_{32}) + \tilde{P}_2(I_{22})\cdot {}_2\tilde{P}_3(I_{32}) + \ldots + \tilde{P}_2(I_{2k})\cdot {}_k\tilde{P}_3(I_{32}) = \sum_{i=1}^{k} \tilde{P}_2(I_{2i})\cdot {}_i\tilde{P}_3(I_{32}); $$

. . . . . .

$$ \tilde{P}_2(I_{21})\cdot {}_1\tilde{P}_3(I_{3l}) + \tilde{P}_2(I_{22})\cdot {}_2\tilde{P}_3(I_{3l}) + \ldots + \tilde{P}_2(I_{2k})\cdot {}_k\tilde{P}_3(I_{3l}) = \sum_{i=1}^{k} \tilde{P}_2(I_{2i})\cdot {}_i\tilde{P}_3(I_{3l}). $$

7. Визначаємо пріоритетні напрямки побудови складної системи по максимальному впливу на головну мету I_1, V_i: $\max[V_1\ V_2\ \ldots V_l]$.

Приклад застосування методології вибору ефективного комплекту засобів мережевої безпеки

Основні вимоги до систем виявлення та запобігання вторгнень (IDS та IPS) включають:

Швидкість реакції: IDS/IPS повинні мати здатність до швидкої реакції на виявлені загрози, щоб запобігти або пом'якшити їх наслідки.

Захищеність від обхідних атак: IDS/IPS мають бути стійкими до спроб обходу або обману, які можуть використовуватися зловмисниками для ухилення від виявлення.

Інтегрованість з іншими системами безпеки: IDS/IPS повинні бути здатними інтегруватися з іншими системами безпеки, такими як файерволи, системи авторизації та інші, для створення комплексної захисної інфраструктури.

Достовірність виявлення вторгнень: Система IDS/IPS повинна ефективно виявляти різноманітні види вторгнень, включаючи відому, нові та невідому загрози.

Запропоновану процедуру синтезу структури складної системи розглянемо на модельному прикладі визначення перспективних напрямків системи у якій граф критеріїв (рис. 2) та відповідна матриця парних порівнянь другого рівня мають вигляд (табл. 6).

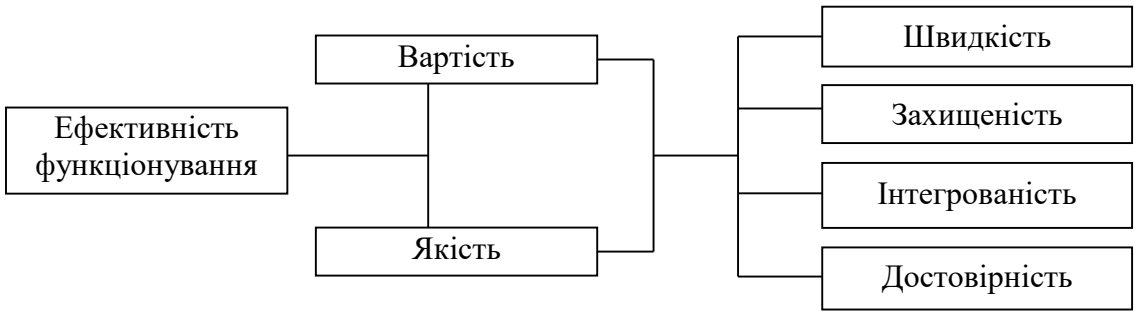

Рис. 2. Граф критеріїв

Таблиця 6

Ефективність	Вартість	Якість	Σ	Пріоритети $\tilde{P}_2$
Вартість	1	0,5	1,5	0,33
Якість	2	1	3	0,67

Матриці парних порівнянь третього рівня мають вигляд (табл. 7, 8).

Таблиця 7

Вартість	Швидкість	Захищеність	Інтегрованість	Достовірність	Σ	$\tilde{P}_3$
Швидкість	1	0,2	5	0,5	6,7	0,22
Захищеність	2	1	2	0,5	5,5	0,18
Інтегрованість	0,5	0,5	1	5	7	0,23
Достовірність	5	2	3	1	11	0,36

Таблиця 8

Якість	Швидкість	Захищеність	Інтегрованість	Достовірність	Σ	$\tilde{P}_3$
Швидкість	1	1	0,2	0,2	2,4	0,09
Захищеність	3	1	4	0,5	8,5	0,32
Інтегрованість	2	0,5	1	0,5	4	0,15
Достовірність	5	3	3	1	12	0,45

Матриця узагальнених ваг $\tilde{P}_3 = \begin{bmatrix} 0,22 & 0,09 \\ 0,18 & 0,32 \\ 0,23 & 0,15 \\ 0,36 & 0,45 \end{bmatrix}$.

Модифікована матриця ${}_{\text{м}}\tilde{P}_3 = \begin{bmatrix} 0,22 & 0,09 \\ 0,18 & 0,32 \\ 0,23 & 0,15 \\ 0,36 & 0,45 \end{bmatrix} \cdot \begin{bmatrix} 0,33 & 0 \\ 0 & 0,67 \end{bmatrix} = \begin{bmatrix} 0,0732 & 0,0598 \\ 0,0601 & 0,2117 \\ 0,0765 & 0,0996 \\ 0,1202 & 0,2989 \end{bmatrix}$.

Узагальнені ваги (рис. 3) $V = \begin{bmatrix} 0,0732 & 0,0598 \\ 0,0601 & 0,2117 \\ 0,0765 & 0,0996 \\ 0,1202 & 0,2989 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0,1330 \\ 0,2718 \\ 0,1761 \\ 0,4191 \end{bmatrix}$.

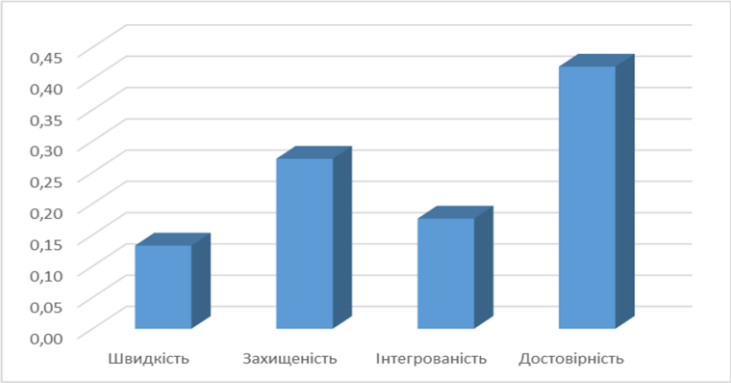

Рис. 3. Узагальнені ваги критеріїв

© Савченко, В. А., & Рибальченко, О. Г. (2024). Побудова ефективної системи мережевої безпеки підприємства на основі методу аналізу ієрархій показників якості. Сучасний захист інформації, 1(57), 6–14. https://doi.org/10.31673/2409-7292.2024.010001.

Як бачимо з рис. 3, пріоритетними напрямками удосконалення систем захисту інформації є напрямки V_2 та V_4, тобто для системи яка розглядається найбільш важливими є «Захищеність» та «Достовірність». Запропонований підхід доцільно використовувати при виборі напрямків розвитку, удосконалення існуючих, побудови перспективних систем захисту інформації. Це дозволить підвищити ефективність функціонування, відшукати найкращий компроміс між суперечливими показниками якості функціонування системи, обрати та обґрунтувати пріоритетні напрямки розвитку складної системи. Подальшим етапом удосконалення запропонованої методології багатокритеріального синтезу є теоретичне обґрунтування виважених коефіцієнтів парних порівнянь з урахуванням експертних оцінок існуючих та бажаних характеристик перспективних систем.

Висновок

В результаті дослідження було виявлено, що оптимальний вибір системи мережевої безпеки вимагає комплексного підходу та уважного аналізу кожного з критеріїв. Швидкість реакції на загрози, рівень захисту від різних видів атак, можливість інтеграції з існуючими системами безпеки та достовірність результатів аналізу виявлених загроз є ключовими аспектами, які слід враховувати при виборі системи. Загальні вимоги щодо якості та вартості системи також мають велике значення. Надійність, масштабованість та простота в управлінні є важливими факторами, які допомагають забезпечити ефективну та економічну реалізацію захисту інформації на підприємстві. Отже, вибір оптимальної системи мережевої безпеки є складним завданням, яке вимагає уважного аналізу та врахування різноманітних факторів. Лише з урахуванням всіх аспектів і відповідно до потреб та можливостей підприємства можна забезпечити надійний та ефективний захист інформації в сучасному кіберпросторі.

Перелік посилань

1. Yanko, A. Система захисту комп’ютерної мережі / A. Yanko, R. Vyhivskyi // Системи управління, навігації та зв’язку. Збірник наукових праць. – Полтава: ПНТУ, 2022. – Т. 2 (68). – С. 91-94. – doi: https://doi.org/10.26906/SUNZ.2022.2.091.

2. Мєшков, В. (2023). Аналіз систем інтелектуального моніторингу трафіку комп’ютерної мережі для систем виявлення атак. Information Technology: Computer Science, Software Engineering and Cyber Security, 1, 85–92, doi: https://doi.org/10.32782/IT/2023-1-11

3. Khalil, R. & Zaki, F. & Ashour, M. & Mohamed, M. (2010). A study of network security systems. Proceedings of the 10th WSEAS international conference on Applied computer science. 96-105. https://www.researchgate.net/publication/262365481_A_study_of_network_security_systems

4. Abbas, S. & Naser, W. & Kadhim, A. (2023). Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). Global Journal of Engineering and Technology Advances. 14. 155-158. 10.30574/gjeta.2023.14.2.0031.

5. Mutyala, P. Comparison of Intrusion Detection Systems / Intrusion Prevention Systems – A Selection Criterion. (2018). Culminating Projects in Information Assurance. 49. https://repository.stcloudstate.edu/msia_etds/49

6. Efe, A., Abacı, İ. N. Comparison of the Host-Based Intrusion Detection Systems and Network-Based Intrusion Detection Systems. Celal Bayar University Journal of Science. Volume 18, Issue 1, 2022, p 23-32. Doi: 10.18466/cbayarfbe.832533

7. Chiba, Z., Abghour, N., Moussaid, K., Lifandali, O., Kinta, R. A Deep Study of Novel Intrusion Detection Systems and Intrusion Prevention Systems for Internet of Things Networks, Procedia Computer Science, Volume 210, 2022, Pages 94-103, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2022.10.124.

8. Савченко, В. А., Машков, О. А., Кравченко, Ю. В. Синтез високоточної радіонавігаційної системи на основі метода аналізу ієрархій показників якості. Зб. наук. праць інституту проблем моделювання в енергетиці. – № 22. – К.: ІПМЕ. – 2003. – С.41–48.

9. Нісфоян, С. С., Сисоліна, Н. П, Савеленко, Г. В. Розвиток методу аналізу ієрархій як механізму вибору інвестиційного проєкту на підприємстві. Центральноукраїнський науковий вісник. Економічні науки, 2020, вип. 5(38), 228-237. DOI: https://doi.org/10.32515/2663-1636.2020.5(38).228-237

10. Шаповалова, О.О & Бурменський, Р.В. (2017). Розробка програмного додатка для реалізації методу аналізу ієрархій. Системи обробки інформації. 3(149). 45-48. 10.30748/soi.2017.149.09.

Надійшла 23.12.2023