МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

Кафедра комп'ютерних технологій та інформаційної безпеки

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент
_____ С.М. Нужний
«_28_» _____12_____ 2024 р.

Кваліфікаційна робота
на правах рукопису

КВАЛІФІКАЦІЙНА РОБОТА

Розробка системи підтримки прийняття рішень щодо вибору систем виявлення вторгнень

Ступінь вищої освіти: магістр
Галузь знань: 14 Електрична інженерія
Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»
Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

Виконала: студентка 6 курсу групи 6366м
Тотх Мишелл _____

Кваліфікаційна робота містить результати самостійного виконання навчального завдання. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ М. Тотх

Керівник:
к.т.н., доцент, доцент кафедри комп'ютерних технологій та інформаційної безпеки
Турти Марина Валентинівна _____

Миколаїв – 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

ЗАТВЕРДЖУЮ
Гарант освітньої програми, к.т.н.,
доцент, доцент кафедри КТІБ
_____ Турти М.В.
«_4_» _____ 2024 р.

ЗАВДАННЯ
на кваліфікаційну роботу

Студентка: Тотх Мишелл

Курс:6

Група: 6366м

Ступінь вищої освіти: магістр

Галузь знань: 14 Електрична інженерія

Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»

Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

1. Тема роботи: Розробка системи підтримки прийняття рішень щодо вибору систем виявлення вторгнень
затверджена наказом НУК від «_14__» жовтня 2024 р. № 1075 - уч

2. Вихідні дані до роботи: нормативно-правова база і теоретичні основи побудови захищених комп'ютерних систем, теоретичні основи систем підтримки прийняття рішень

3. Перелік питань, які необхідно розробити: провести аналіз відкритих літературних джерел; визначити критерії класифікації систем виявлення вторгнень та критерії прийняття рішень щодо їх вибору; розробити основні алгоритми та структуру системи прийняття рішень щодо вибору систем виявлення вторгнень як складової комплексу засобів захисту комп'ютерних мереж

4. Терміни виконання завдання:
термін видачі завдання: «_04_» вересня 2024 р.
термін подання роботи: «_19_» грудня 2024 р.

6. План-графік виконання кваліфікаційної роботи

№ п/п	Заходи	Дата		Готовність	Відмітка про виконання
		Навч. тиждень	Контрольна дата		
1.	Наукове стажування	1 - 8	25.10.2024	Звіт з наукового стажування	Виконано
2.	Організаційні збори	9	31.10.2024	Попередній варіант змісту КР	Виконано
3.	Рубіжний контроль	10	05.11.2024	Попередній варіант оглядових розділів	Виконано
4.	Рубіжний контроль	13	28-29.11.2024	1. Попередній варіант повної КР. 2. Попередній варіант презентації.	Виконано
5.	Рубіжний контроль	15	12.12.2024	Доповідь на 12-ій Всеукраїнській науково-технічній конференції з міжнародною участю «СПІБТ–2024»	Виконано
6.	Перевірка на плагіат	15	12-13.12.2024	Електронний варіант кваліфікаційної роботи	Виконано
7.	КЕ на рівень « магістра»	16	17-18.12.2024	Здавання державного екзамену зі спеціальності на ступінь бакалавра	Виконано
8.	Кафедральний захист	16	19.12.2024	1. Оформлена КР (в форматі pdf) (передається студентом на кафедрі для внутрішньої рецензії). У разі отримання позитивної внутрішньої рецензії, КР подається на зовнішню рецензію. 2. Оформлена презентація (в форматі pdf).	Виконано
9.	Подання документів на захист	16	20.12.2024	1. Подання щодо захисту КР: тема, успішність, висновок керівника та висновок кафедри про КР. 2. Зовнішня рецензія (окремо від КР). Резюме на КР. 3. Електронний варіант та роздрукована презентація в кількості 5 примірників. 4. Електронний варіант КР на диску	Виконано
10.	Захист ДР	17	24,26,27, 28.12.2024	1. Приєднання студента до засідання кваліфікаційної комісії (конференції) у встановлений час для проведення процедури дистанційного захисту 2. Процедура захисту КР.	Виконано

ПРИМІТКА: Завдання додається до виконаної роботи та подається до атестаційної комісії.

Керівник
доцент кафедри комп'ютерних технологій
та інформаційної безпеки, к.т.н., доцент _____М.В. Турти

Студентка _____М.Тотх

АННОТАЦІЯ

Томх Мішелл Розробка системи підтримки прийняття рішень щодо вибору систем виявлення вторгнень. – Кваліфікаційна праця на правах рукопису.

Кваліфікаційна робота на здобуття ступеня вищої освіти «магістр» за спеціальністю 141 «Електроенергетика, електротехніка та електромеханіка» галузі знань: 14 «Електрична інженерія» і освітньо-професійною програмою «Системи технічного захисту інформації, автоматизація її обробки». – Національний університет кораблебудування імені адмірала Макарова, Миколаїв, 2024.

Пояснювальна записка: 126 с., 27 рис., 4 табл., 47 посилань.

Кваліфікаційна робота присвячена актуальній темі – розробці ефективних систем захисту комп'ютерних мереж.

Об'єктом даного дослідження виступають системи технічного захисту інформаційних ресурсів з обмеженим доступом, а предметом – системи виявлення вторгнень (СВВ). У роботі використано теоретичні основи проектування захищених мереж, систем підтримки прийняття рішень (СППР) та метод аналізу ієрархій. Метою дослідження є розробка СППР щодо вибору систем виявлення вторгнень як складової комплексу засобів захисту комп'ютерних мереж. У рамках дослідження проведено аналіз літературних джерел, визначено критерії класифікації та прийняття рішень для вибору СВВ; розроблено алгоритми і структуру СППР.

Результати цієї роботи можуть бути корисними під час проектування захищених локальних мереж, а також у навчальному процесі за освітньою програмою «Системи технічного захисту інформації, автоматизація її обробки» зі спеціальностей 125 «Кібербезпека» та 141 «Електроенергетика, електротехніка та електромеханіка».

Результати цієї кваліфікаційної роботи були апробовані на XII Всеукраїнській науково-технічній конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті» у 2024 році.

Ключові слова: кібербезпека, комп'ютерна мережа, система виявлення вторгнень, система підтримки прийняття рішень, критерії вибору.

ANNOTATION

Toth Michell Development of a decision support system for the selection of intrusion detection systems.

Qualifying work on receiving degree of "Master" in the specialty 141 "Electrical energetics, Electrical Engineering and Electromechanics" in the field of knowledge 14 "Electrical Engineering" and educational and professional program "Systems of technical protection of information, automation of its processing." - Admiral Makarov National University of Shipbuilding, Mykolaiv, 2024.

Explanatory note: 126 p., 27 figs., 4 tabl., 47 references.

Qualification work is devoted to a topical issue - the development of effective computer network protection systems.

The object of research in this work is systems of technical protection of restricted access information resources, while the subject is intrusion detection systems (IDS). The study employs theoretical foundations for designing secure networks, decision support systems (DSS), and hierarchy analysis method. The purpose of this qualification work is to develop DSS for selecting IDS as a component of the comprehensive protection of computer networks. As part of the research, an analysis of literary sources have been carried out, classification criteria and decision-making criteria for selecting IDS have been identified; algorithms and structure for DSS have been developed.

The results of this work can be used in the design of secure local networks and in the educational process under the educational program "Technical information protection systems, automation of its processing" in specialties 125 "Cybersecurity" and 141 "Electric power engineering, electrical engineering and electromechanics".

The results of the qualification work were tested at the XII All-Ukrainian Scientific and Technical Conference with International Participation "Modern Problems of Information Security in Transport" in 2024.

Keywords: cybersecurity, computer network, intrusion detection system, decision support system, selection criteria

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

AAFID - Autonomous Agents for Intrusion Detection;

AES - Advanced Encryption Standard;

ASAX - Advanced Security audit trail Analyzer on uniX;

ATM - Asynchronous Transfer Mode;

CIDF - Common Intrusion Detection Framework;

DoS - Disk Operating System;

HIDS - Host-based intrusion detection system;

HTTP - HyperText Transfer Protocol;

ICMP - Internet Control Message Protocol;

IDPS - intrusion detection and prevention systems;

IDS –Intrusion Detection System;

IP − Internet Protocol;

IPS − Intrusion Prevention System;

KNN - K-Nearest Neighbor - k найближчих сусідів;

NIDS - Network Intrusion Detection System;

OSI − Open Systems Interconnection Basic Reference Mode;

PGP - Pretty Good Privacy;

PPP - Point-to-Point Protocol;

SIEM - Security information and event management;

SLIP - Serial line Interface Protocol;

TCP - Transmission Control Protocol;

UDP - User Datagram Protocol;

UPM - Unified Performance Management;

ІБ – інформаційна безпека;

ІзОД − інформація з обмеженим доступом;

ІКС − інформаційно-телекомунікаційна система;

МАІ – метод аналізу ієрархій;

НСД – несанкціонований доступ;

ОПР – особа, що приймає рішення;

ОС – операційна система;

ПЗ – програмне забезпечення;

СВВ – система виявлення вторгнень;

СЗВ – система запобігання вторгненням;

СППР – система підтримки прийняття рішень;

ТЗІ − технічний захист інформації.

ВСТУП

Інтенсивний розвиток інформаційно-комунікаційних технологій, поширення цифровізації в усіх сферах діяльності та зростання обсягів обробки інформації з обмеженим доступом роблять питання безпеки інформаційних систем критично важливими. Актуальність забезпечення захисту даних стосується як державних установ і приватного бізнесу, так і окремих користувачів, адже кіберзагрози еволюціонують із винятковою швидкістю, створюючи виклики для існуючих систем захисту.

Ключовою проблемою є зростаюча кількість кіберзлочинів, значна частина яких реалізується у формі віддалених атак на інформаційно-комунікаційні системи (ІКС). Переважну більшість таких атак можна виявити й нейтралізувати завдяки впровадженню сучасних організаційних, технічних і криптографічних засобів захисту, серед яких особливе місце займають системи виявлення вторгнень (СВВ).

Важливість оперативного виявлення вразливостей і реагування на кібератаки підкреслюється в Стратегії кібербезпеки України [45] і в планах її реалізації [39, 40]. Документ наголошує на необхідності створення інструментів автоматизованого моніторингу загроз у реальному часі для забезпечення стійкості об’єктів критичної інфраструктури. Одним із основних компонентів такої інфраструктури є СВВ, що виконують функції контролю інформаційних потоків, виявлення аномальних дій та формування попереджень про потенційні загрози.

Різноманітність доступних на ринку СВВ, їх функціональні особливості та складність вибору оптимального рішення для конкретних умов використання визначають необхідність системного підходу до їх оцінки та впровадження. Попри значну кількість наукових досліджень у цій галузі вітчизняних [24-26, 29, 30, 32-35, 38, 41-43,46, 47] і зарубіжних [1-23] науковців і практиків,

питання методології оптимального вибору СВВ залишається недостатньо розробленим.

Метою даної магістерської роботи є розробка системи підтримки прийняття рішень (СППР) для вибору систем виявлення вторгнень, яка стане частиною комплексної системи захисту інформації.

Для досягнення цієї мети у роботі вирішуються такі завдання:

– провести аналіз існуючих систем виявлення вторгнень та визначити критерії їх класифікації;

– визначити критерії вибору СВВ;

– створити алгоритми та структуру СППР для вибору СВВ.

Об’єктом дослідження є системи технічного захисту інформаційних ресурсів, які містять інформацію з обмеженим доступом (ІзОД).

Предметом дослідження є методи та засоби вибору систем виявлення вторгнень.

Методи дослідження, які застосовані у даній кваліфікаційній роботі включають:

– теоретичні основи побудови захищених мереж, необхідні для визначення критеріїв вибору СВВ;

– теоретичні основи побудови систем підтримки прийняття рішень, необхідні для розробки алгоритмів і структури СППР;

– метод аналізу ієрархій для проведення порівняльного аналізу СВВ.

Результати цієї роботи можуть бути використані для підвищення ефективності забезпечення безпеки ІКС у різних організаціях, зокрема в контексті захисту об’єктів критичної інфраструктури.

1 ПОСТАНОВКА ПРОБЛЕМИ ДОСЛІДЖЕННЯ

1.1 Призначення і принципи функціонування систем виявлення вторгнень

Система виявлення вторгнень (англ. *Intrusion Detection System, IDS*) — це засіб, призначений для ідентифікації спроб атак на ІКС з боку зловмисників. Основною метою таких атак може бути отримання несанкціонованого доступу до ресурсів або несанкціоноване управління елементами ІКС.

СВВ можуть реалізовуватися як програмні рішення або ж у вигляді апаратно-програмних комплексів. У багатьох випадках їхня робота тісно пов’язана із застосуванням Інтернет-ресурсів, що дозволяє забезпечити широкий спектр можливостей для моніторингу і аналізу мережевої активності.

Методи виявлення вторгнень ґрунтуються на аналізі сигнатур або аномалій. У першому випадку система порівнює поточну активність із базою даних відомих шаблонів загроз, тоді як у другому – шукає відхилення від встановлених норм у поведінці системи чи її окремих компонентів. Дані про підозрілі прояви активності, наприклад ознаки роботи шкідливого програмного забезпечення або аномальні зміни в контрольованих показниках, збираються і обробляються централізовано за допомогою системи управління інформаційною безпекою, відомої як *SIEM* (англ. *Security Information and Event Management*).

SIEM-система інтегрує дані з різноманітних джерел, таких як мережеві пристрої, сервери, бази даних, і проводить їх глибокий аналіз. На основі встановлених правил фільтрації вона виділяє події, які потенційно можуть бути небезпечними, і генерує сигнали тривоги. Такі сповіщення, зазвичай у вигляді повідомлень, надсилаються відповідальним фахівцям або до операційного центру безпеки для подальшого реагування.

Таким чином, СВВ є важливим інструментом для своєчасного виявлення загроз, що дозволяє запобігти несанкціонованим діям і знизити можливий

вплив атак на функціонування ІКС. СВВ є ключовими компонентами сучасних інформаційних систем, які забезпечують контроль і захист від несанкціонованого доступу (НСД), атак або шкідливих дій у комп'ютерних мережах та системах. Їх робота базується на фундаментальних принципах, що визначають функціонування цих систем і забезпечують ефективне виявлення та реагування на потенційні загрози у динамічному інформаційному середовищі.

Одним із базових принципів функціонування СВВ є безперервний моніторинг активності в мережі чи на окремих вузлах. Постійне спостереження дозволяє збирати великі обсяги даних про вхідний і вихідний трафік, поведінку користувачів та внутрішні процеси в системах. Цей моніторинг забезпечує основу для створення картини нормальної поведінки інформаційної системи, що дозволяє у подальшому виявляти аномалії, які можуть свідчити про потенційну загрозу.

Системи виявлення вторгнень активно використовують принцип аналізу поведінки. На основі зібраних даних вони ідентифікують характерні моделі нормальної діяльності та відстежують відхилення від цих шаблонів. Аномальні дії, такі як незвичне підключення до сервера, підозрілі зміни у системних файлах чи спроби доступу до закритих ресурсів, викликають реакцію системи. Такий підхід дозволяє не лише виявляти відомі типи атак, але й ідентифікувати нові, ще невідомі загрози, які можуть становити серйозну небезпеку.

Іншою важливою рисою СВВ є їхня здатність до оперативної реакції. При виявленні потенційної загрози система автоматично фіксує інцидент, повідомляє адміністратора про підозрілу активність або навіть вживає відповідних заходів для нейтралізації загрози. Це може бути, наприклад, блокування підозрілого з'єднання, ізоляція зараженого сегмента мережі чи автоматичне налаштування додаткових правил безпеки.

Принцип масштабованості та адаптивності також є важливим аспектом роботи систем виявлення вторгнень. У сучасних умовах обсяги даних, які необхідно обробляти для забезпечення безпеки, постійно зростають. Системи повинні легко адаптуватися до змін мережевої архітектури, оновлювати свої

бази знань про нові загрози та враховувати специфіку конкретних організацій або галузей.

Автоматизація процесів є невід'ємною складовою ефективної роботи СВВ. Завдяки застосуванню сучасних технологій, таких як алгоритми машинного навчання та штучного інтелекту, системи здатні значно підвищувати точність і швидкість аналізу, мінімізуючи вплив людського фактору. Це дозволяє не лише оперативно виявляти загрози, але й зменшувати кількість хибних спрацювань, які можуть відволікати адміністратора від реальних проблем.

Процес функціонування СВВ можна розділити на кілька ключових етапів. Спочатку система збирає інформацію з різних джерел, таких як файли журналів, мережевий трафік або події на кінцевих пристроях. Зібрані дані проходять попередню обробку, яка включає фільтрацію, нормалізацію та перетворення у формат, придатний для подальшого аналізу. Далі відбувається аналіз даних, який може базуватися на сигнатурному підході або виявленні аномалій. Після аналізу система оцінює рівень загрози, і в разі потреби вживає заходів для її нейтралізації.

Функціонування СВВ також супроводжується певними викликами. Одним із них є необхідність обробки величезного обсягу даних у реальному часі, що включає зашифрований трафік, який потребує додаткових ресурсів для аналізу. Ще одним викликом є постійна еволюція кіберзагроз, через що СВВ мають регулярно оновлювати свої механізми виявлення та бази знань.

Узагальнюючи, системи виявлення вторгнень виконують важливу роль у забезпеченні безпеки інформаційних ресурсів. Їхні основні принципи роботи – моніторинг, аналіз поведінки, автоматизація процесів, адаптивність та оперативна реакція – створюють надійний фундамент для боротьби з кіберзагрозами та мінімізації можливих збитків від атак. Ці принципи є базисом для подальшого вдосконалення СВВ у відповідь на виклики сучасного кіберпростору.

1.2 Аналіз нормативно-правової бази застосування систем виявлення вторгнень

Захист інформації, що обробляється в ІКС, від загроз та викликів у кіберпросторі є однією з найважливіших проблем сучасного світу. В умовах глобалізації, активного обміну даними та стрімкого впровадження інформаційних технологій ця проблема торкається всіх країн та сфер життя суспільства. Сьогодні стабільність функціонування економіки, політики, національної і міжнародної безпеки залежить від рівня захисту інформаційних ресурсів та ефективності їх використання. Особливе значення цей аспект набуває для об’єктів критичної інфраструктури, несправності в роботі яких можуть спричинити масштабні негативні наслідки для довкілля, систем життєзабезпечення, а також загрожувати національній безпеці.

Використання інформаційних технологій у кіберпросторі для терористичних дій, військових чи політичних конфліктів підкреслює необхідність захисту національного кіберпростору нарівні із традиційним захистом території, повітряного та водного простору країни. У цьому контексті кібербезпека стала невід'ємною частиною національної безпеки України. У Стратегії національної безпеки України, ухваленій у 2021 році, визначено один із ключових напрямків – зміцнення можливостей системи кібербезпеки для протидії сучасним загрозам у сфері інформаційної безпеки. Завданням держави є забезпечення стійкості інформаційних систем, боротьба з підривною пропагандою, розвідувальною діяльністю, інформаційними операціями та кібератаками.

Правова база України у сфері кібербезпеки включає низку документів, серед яких Конвенція Ради Європи про кіберзлочинність, ратифікована у 2005 році, а також закони України, укази Президента, положення Кримінального кодексу, постанови Кабінету Міністрів, стандарти у сфері технічного захисту інформації тощо. Ці документи формують підґрунтя для боротьби з кіберзлочинністю, забезпечення інформаційної безпеки та створення сприятливого середовища для розвитку інформаційного суспільства.

У 2021 році була затверджена Стратегія кібербезпеки України, яка визначає пріоритети у сфері кіберзахисту, потенційні кіберзагрози, а також умови безпечного функціонування кіберпростору. У цьому документі передбачено створення технологічних можливостей для автоматичного виявлення кібератак у режимі реального часу та їх нейтралізації, особливо на об'єктах критичної інформаційної інфраструктури. Важливим завданням є запровадження систем моніторингу кіберпростору, які здатні ідентифікувати ознаки вторгнень, аналізувати аномалії та реагувати на загрози.

Національний координаційний центр кібербезпеки та інші органи, що займаються питаннями кіберзахисту, здійснюють постійний моніторинг електронних мереж, виявляють загрози та аналізують їх вплив. Індикатори кіберзагроз, визначені як технічні дані, що використовуються для виявлення атак, можуть мати різну форму, зокрема сигнатури або аномалії.

Системи виявлення вторгнень (СВВ) є важливою складовою комплексу заходів із забезпечення інформаційної безпеки. Вони виконують функції, що визначаються вимогами до конфіденційності, цілісності, доступності та спостережуваності інформації. При цьому вибір функціонального профілю захисту здійснюється з урахуванням стандартів і класу автоматизованих систем. Для систем, що працюють із Інтернетом, використовуються профілі, розроблені для автоматизованих систем третього класу.

Такі заходи спрямовані на створення надійної системи кібербезпеки, здатної протидіяти сучасним викликам у цифровому середовищі та гарантувати безпеку інформаційних ресурсів держави.

1.3 Класифікація системи підтримки прийняття рішень щодо виявлення вторгнень

СППР (англ. *Decision Support System, DSS*) є інформаційною системою, яка допомагає користувачам знаходити найкращі рішення в конкретних

предметних галузях. Вона забезпечує зручний доступ до даних, їх обробку та надає рекомендації щодо оптимальних рішень у певних умовах. СППР застосовують моделі та алгоритми для вирішення задач із різним рівнем структурованості: структурованих, слабо структурованих і неструктурованих. СППР актуальна у випадках, коли повна автоматизація процесів неможлива або небажана. Такі системи часто використовуються у підприємництві, бізнесі чи інших галузях, де важливе прийняття керівних рішень. СППР поєднує базу даних із інформаційною моделлю підтримки рішень, зберігаючи за людиною остаточне слово. Система лише допомагає аналізувати великий обсяг інформації та мінімізувати ризики.

Актуальність СППР зумовлена сучасними викликами: зростанням обсягу інформації, складністю щоденних питань, множинністю факторів для врахування та непередбачуваністю наслідків деяких рішень. Основна мета СППР — допомогти користувачеві знайти оптимальне рішення, полегшуючи виконання етапів прийняття рішень, як-от збір даних, аналіз альтернатив та вибір найкращого варіанта.

Завдання СППР класифікуються за ступенем структурованості:

- структуровані — задачі з чіткими кількісними характеристиками.
- слабоструктуровані — задачі, де поєднуються кількісні та якісні критерії.
- неструктуровані — задачі, що базуються на логіці, інтуїції чи досвіді.

Переваги СППР включають:

- швидкість і ефективність прийняття рішень.
- можливість аналізу великих обсягів інформації.
- допомогу у визначенні, розробці та впровадженні оптимальних рішень.

Етапи прийняття рішень у СППР:

- постановка завдання: визначення проблеми, оцінка часу та ресурсів для її вирішення;4
- аналіз варіантів: формування можливих рішень, оцінка їхніх переваг і недоліків;

– вибір оптимального рішення: відбір СППР найперспективніших варіантів, надання СППР рекомендованих рішень особі, що приймає рішення, (ОПР); остаточний вибір рішення ОПР.

Комп’ютеризовані СППР мають такі характеристики:

– підтримка рішень для задач різного ступеня складності;

– адаптивність і гнучкість до змін середовища;

– простота у використанні навіть для недосвідчених користувачів;

– інтерактивність, що дозволяє безперервну взаємодію;

– можливість модифікації бази даних та правил адміністратором.

На рис.2.1 наведена класифікація СППР, де кольором позначені характеристики СППР, розроблюваної у межах даної кваліфікаційної роботи. Виходячи із специфіки об’єкту і предмету досліджень, ця СППР призначена для:

– використання однією ОПР;

– розв’язання слабоструктурованих задач;

– отримання послідовних рішень в умовах ризику на основі дескриптивної моделі і вибору оптимального чи множини близьких до оптимального рішень за множиною критеріїв;

– систематизації і представлення структурованих знань експертів в галузі захисту комп’ютерних мереж у вбудованій базі знань у вигляді базових наборів даних і правил;

– використання у вузькоспеціалізованих і стратегічних питаннях.

Така СППР є активною статичною системою, яка управляється адміністратором, і містить інтерфейси адміністратора і користувача, база знань, база даних, система отримання висновків і візуалізації їх для користувача-ОПР. Користувач-ОПР через свій інтерфейс має можливість формувати запити до СППР і отримувати рекомендовані рішення у зручній формі, а адміністратор через свій інтерфейс - модифікувати базові набори даних і правила, тобто модифікувати відповідно до поточних умов відомості, надані експертами щодо переваг і недоліків різних СВВ, умов їх використання, функціональних можливостей тощо.

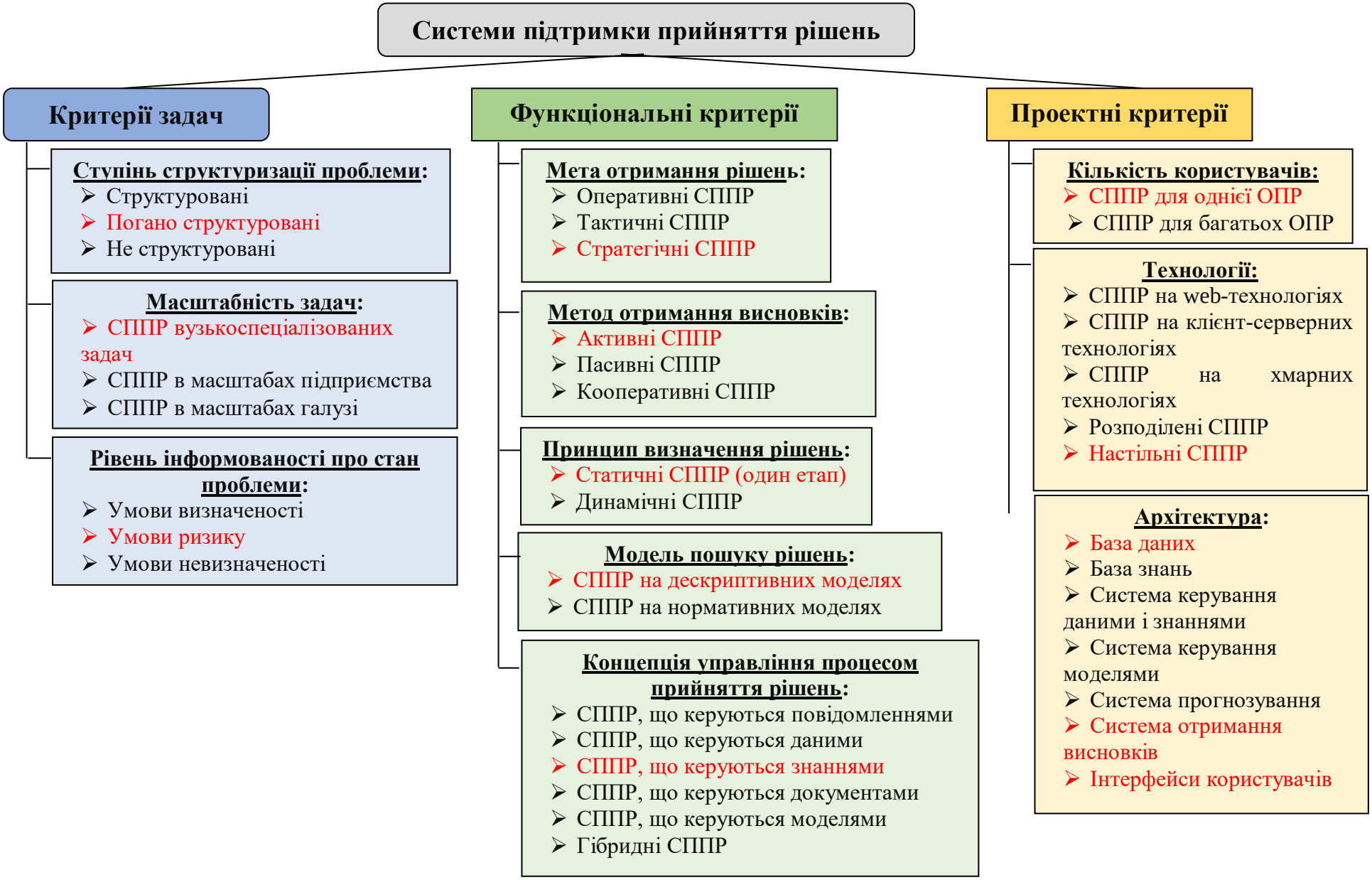


Рисунок 1.1 – Класифікація систем підтримки прийняття рішення

1.4 Методи і критерії прийняття рішень при виборі альтернативних рішень в кібербезпеці

Вибір системи СВВ є важливим управлінським рішенням при створенні комплексу засобів захисту ІКС. Процес прийняття рішень в різних сферах, включаючи інформаційну безпеку (ІБ), можна розглядати як послідовність з семи етапів (рис. 1.2).

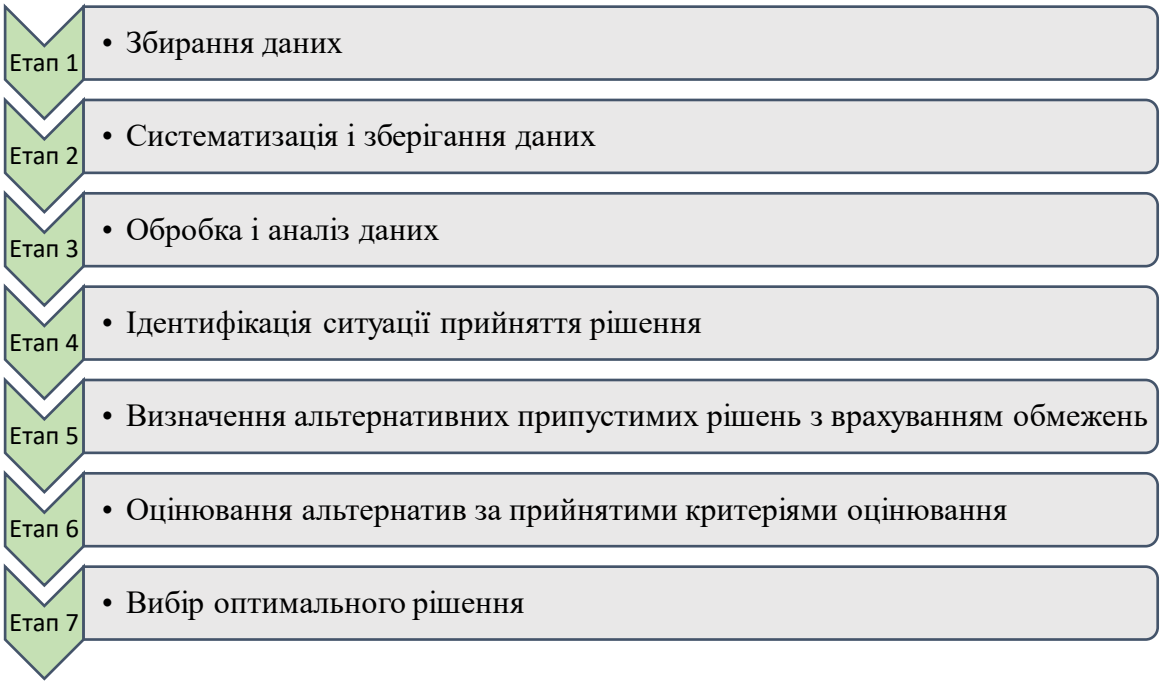


Рисунок 1.2 – Ієрархія етапів прийняття рішення

Як зазначено у статті [38], на кожному з рівнів ієрархії, зображеній на рис. 1.2, можна та доцільно застосовувати різні методи обробки даних і форми їх представлення. Це пов'язано з тим, що використання лише окремих методів під час розробки та впровадження систем управління інформаційною безпекою може бути менш ефективним порівняно з комплексним підходом.

Серед методів прийняття рішень можна виділити чотири основні мета-сімейства, які в свою чергу поділяються на десять груп за використовуваними інструментами і методами (рис.1.3). Прийняття управлінських рішень може відбуватися за різних умов, зокрема:

– у випадку невизначеності, коли інформації недостатньо;

– в умовах ризику, коли інформації є достатньо для оцінки можливих варіантів, але не всі наслідки можна точно передбачити;

– в умовах визначеності, коли інформації достатньо для прийняття чіткого оптимального рішення.

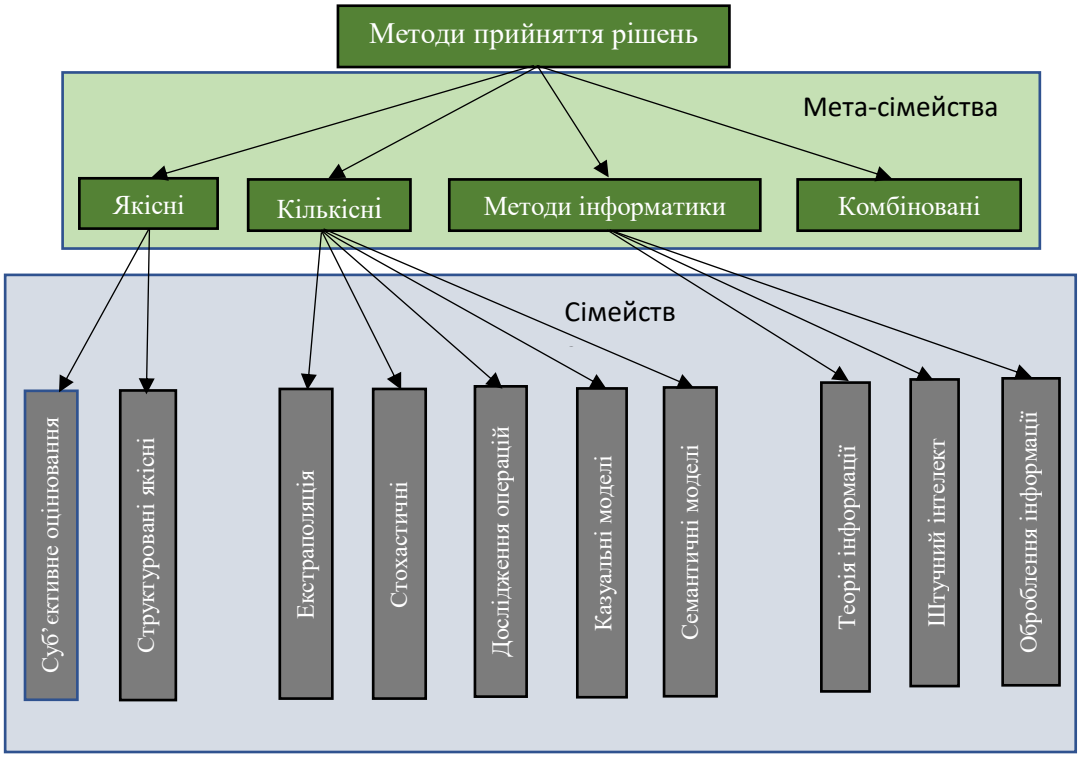


Рисунок 1.3 – Ієрархія методів прийняття рішень

Для кожного з цих випадків існують відповідні методи прийняття рішень (рис. 1.4), які можуть відрізнятися залежно від рівня в ієрархії процесу. Виділений на рис.1.4 метод аналізу ієрархій (MAI) [28] є аналітичним методом, однак вимагає на перших етапах отримання інформації від експертів.

У загальному випадку процес прийняття рішень є ітераційною процедурою. Оцінка якості кожного можливого варіанту (етап 5, рис. 1.2) здійснюється за заздалегідь визначеними критеріями. В результаті роботи СППР користувач отримує або простий список можливих рішень (для пасивних СППР), або їх ранжування за оцінками якості (для активних СППР), де найкраще оцінене рішення вважається оптимальним.

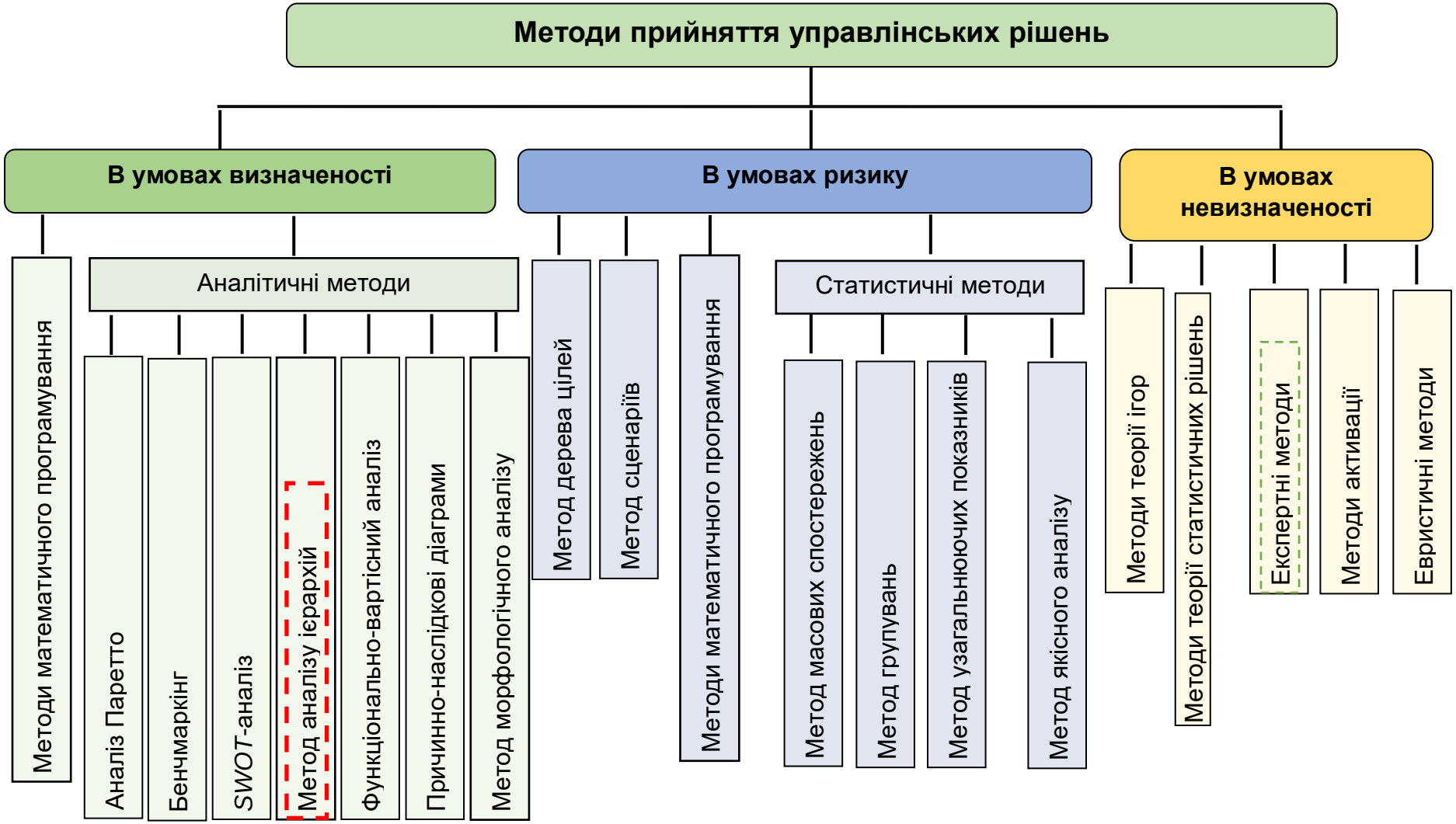


Рисунок 1.4 – Класифікація методів прийняття рішень за обсягом вхідної інформації

Критерії прийняття рішень можуть змінюватися в залежності від повноти вхідної інформації та застосованого методу. Наприклад, при повній визначеності використовуються методи математичного програмування, де критерієм є мінімізація або максимізація певної функції при заданих обмеженнях, і зміна будь-якого параметру призводить до погіршення результату.

Метод бенчмаркінгу передбачає переймання успішного досвіду конкурентів, для чого вибирається еталонний об’єкт, результати якого аналізуються. Після виявлення слабких місць власного об’єкта, розробляється план впровадження найкращих практик.

Метод *SWOT*-аналізу використовують для стратегічного планування, де внутрішні фактори діляться на сильні та слабкі сторони, а зовнішні – на можливості та загрози. Оцінка цих факторів відбувається за допомогою спеціальної функції корисності.

Аналіз ієрархій дозволяє вибрати оптимальне рішення за багатьма критеріями, організованими в ієрархічну структуру. Альтернативи порівнюються за ваговими коефіцієнтами, і оптимальним вважається варіант із найвищим глобальним пріоритетом.

Функціонально-вартісний аналіз дозволяє визначити оптимальне рішення через порівняння витрат та корисності різних варіантів. Вибір оптимального рішення за допомогою причинно-наслідкових діаграм (наприклад, діаграми Ішікави) передбачає послідовний аналіз факторів, що впливають на результат.

Методи вибору з морфологічної скрині оцінюють можливі варіанти рішень через виявлення їх складових і оцінку усіх можливих комбінацій.

Вибір рішення в умовах невизначеності може бути здійснений методами експертних оцінок, коли не можна застосувати кількісні методи, але є необхідність і можливість врахувати суб’єктивні думки експертів, або стохастичними методами, коли всі можливі наслідки мають визначену ймовірність. У випадку ризику використовуються критерії очікуваного значення або критерії на основі теорії ігор, які визначають оптимальні стратегії в умовах конфлікту або невизначеності.

2 АНАЛІЗ ІСНУЮЧИХ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

2.1 Класифікація систем виявлення вторгнень

Системи виявлення мережевих вторгнень і виявлення ознак кібератак на ІКС є важливою частиною захисту інформаційно-комунікаційних систем. Для вибору найбільш підходящої СВВ для конкретної ІКС необхідно оцінювати характеристики систем, доступних на ринку. Класифікація СВВ здійснюється за трьома основними категоріями: функціональні, проектні та експлуатаційні характеристики (рис.2.1).

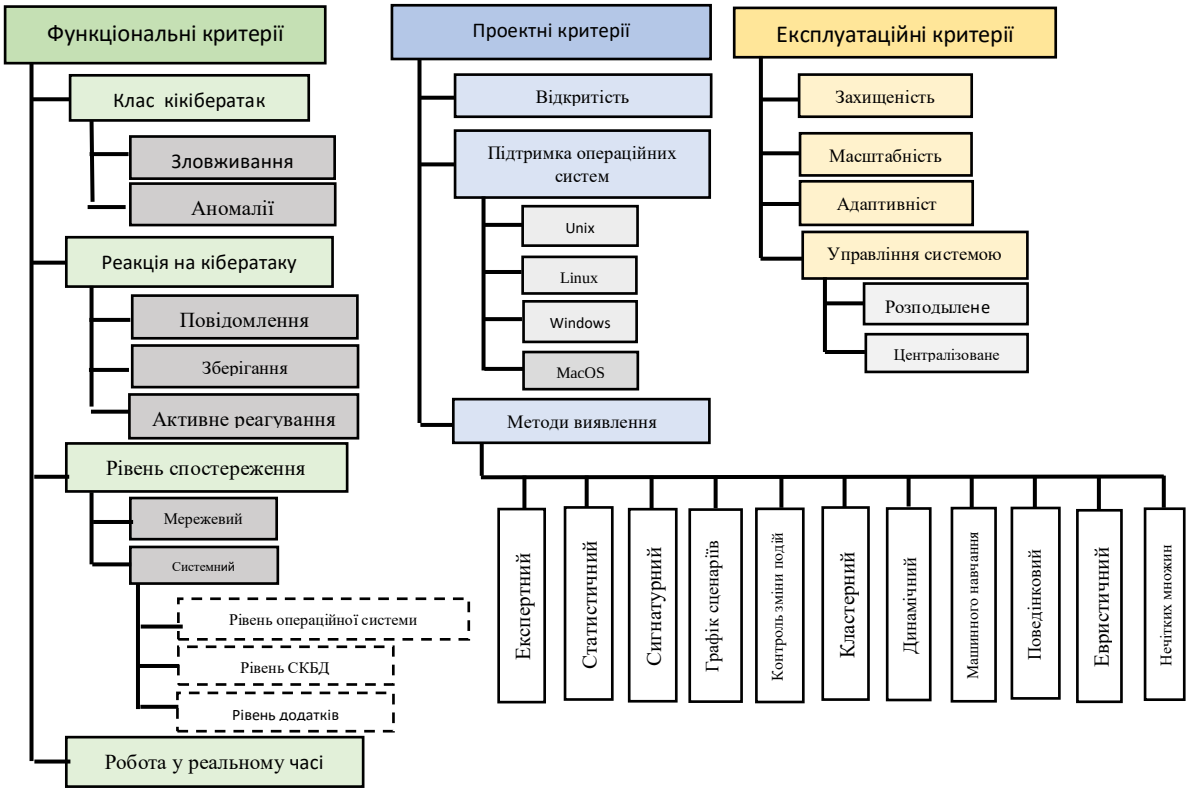


Рисунок 2.1. – Система критеріїв класифікації СВВ

Розглянемо першу групу критеріїв - функціональні характеристики, які визначають здатність СВВ виконувати задачі користувачів. До функціональних параметрів відносяться такі підкатегорії, як Ф1, Ф2, Ф3 і Ф4.

Ф1. Клас кібератак. Це характеристика, яка вказує на здатність СВВ ідентифікувати різні види атак на різних рівнях ІКС, зокрема, на основі аномалій або зловживань.

Ф1.1. *Misuse detection* (детекція зловживань) або *Signature-based IDS*. Ці системи виявляють вторгнення на основі порівняння мережевого трафіку з відомими сигнатурами атак. Виявлення зловживань базується на шаблонах атак, подібно до антивірусних програм, які використовують відомі сигнатури для ідентифікації шкідливого коду. Перевагою цього підходу є висока точність виявлення відомих загроз, але недоліком є неможливість виявлення нових або модифікованих атак, які не відповідають відомим шаблонам. Крім того, цей метод потребує регулярного оновлення бази сигнатур.

Ф1.2. *Anomaly-based IDS* (виявлення аномалій). Система виявляє атаки шляхом аналізу відхилень від нормальних параметрів мережі, таких як кількість з'єднань або завантаження центрального процесора. Цей метод дозволяє виявляти нові загрози, оскільки він ґрунтується на навчанні системи розпізнавати "нормальну" поведінку користувачів і трафіку. Після навчання система порівнює поточні дії з встановленими шаблонами нормальної поведінки. Виявлення аномалій дає можливість ідентифікувати нетипові ситуації, такі як *DDoS*-атаки, що відрізняються різким збільшенням або зменшенням певних параметрів. Основним недоліком цього методу є необхідність постійного перегляду шаблонів нормальної поведінки для забезпечення актуальності виявлення загроз.

Перевагами методу аномалій є здатність виявляти нові типи атак, які ще не були зафіксовані або не мають сигнатур, а отже, для таких загроз не потрібні сигнатурні бази даних, що позбавляє від необхідності їх регулярного оновлення. Цей метод також може ідентифікувати складні загрози, такі як поліморфні віруси.

Основним недоліком методу є наявність хибних спрацьовувань, які можуть виникати через незвичні, але допустимі дії, що неправильно інтерпретуються як атаки. В результаті цього нові або рідкісні, але правомірні

дії можуть бути визначені як загроза. Система сповіщає адміністратора (і іноді користувача) про будь-яку аномальну поведінку та запитує про подальші дії. Часті помилкові сповіщення можуть призвести до зниження чутливості користувача до попереджень, що знижує ефективність системи захисту, оскільки важливі попередження можуть бути проігноровані серед помилкових. Крім того, цей метод вимагає складного налаштування та точних параметрів, що потребує високої кваліфікації персоналу.

Ф1.3. Гібридна система виявлення вторгнень поєднує різні методи чи системи для досягнення найвищого рівня захисту, усуваючи слабкі місця окремих підходів і зміцнюючи їх переваги.

Ф2. Реакція на кібератаку може бути активною або пасивною, в залежності від типу системи.

Ф2.1. Пасивні системи виявлення атак генерують попередження про загрози після їх виявлення та зберігають інформацію про інцидент. Вони здійснюють моніторинг комп'ютерних мереж, додатків чи систем для виявлення порушень безпеки або зловмисних дій. Якщо пасивна система виявляє загрозу, вона негайно інформує користувача або адміністратора, що дозволяє вжити заходів для запобігання вторгненням чи порушенням безпеки. Пасивні системи використовуються для зменшення кількості атак шляхом створення інформаційної бази для розслідування інцидентів та підготовки до блокування нових загроз з використанням інших засобів, які не входять до складу СВВ.

Ф2.2. Активні системи виявлення вторгнень після виявлення атаки генерують сповіщення для користувача і/або адміністратора, зберігають дані про атаку та містять базу контрзаходів і модулі для їх автоматичного активування. Це дозволяє швидко реагувати на інцидент, зупиняючи атаку або мінімізуючи її негативні наслідки. Активні СВВ здатні не лише виявити атаку після того, як зловмисник проник в об'єкт захисту, але й одразу реагувати на потенційну загрозу, яка може призвести до атаки. Такі системи також відомі як системи запобігання вторгненням, оскільки вони автоматично забезпечують

захист від атак і порушень безпеки (рис.2.3). Активні СВВ вважаються більш досконалими за пасивні, оскільки, окрім виявлення атак, вони також відслідковують активність в реальному часі та нейтралізують загрози. Реакція СВВ на виявлені порушення безпеки може включати такі дії, як реєстрація, надсилання сповіщень, відключення з'єднань, блокування зловмисного трафіку, а також відновлення важливих даних, наприклад:

– реєстрація інформації про можливу та/або здійснену атаку в журналі;
– надсилання сповіщень користувачу та/або адміністратору;
– відключення з'єднання;
– відключення системи;
– блокування шкідливого трафіку;
– блокування *IP*-адреси;
– блокування небезпечних акаунтів;
– відновлення лог-файлів у разі їх втрати;
– відновлення *TCP*-потоку;
– відновлення *HTTP*-сторінки.

Таким чином, пасивні та активні системи можуть здійснювати моніторинг мережі, реєструвати дані, сповіщати про загрози та вживати контрзаходів. Вони часто розміщуються за межами брандмауера організації для захисту локальної мережі від атак, таких як хакерські вторгнення або вірусні загрози (рис.2.2-2.4). Системи виявлення вторгнень мають за мету виявляти проблеми в стратегії безпеки мережі, документувати поточні загрози та гарантувати дотримання політики безпеки.

Ф3. Рівень спостереження відноситься до рівня системи, з якої за допомогою спеціальних сенсорів отримуються дані для виявлення кібератак. Розрізняють два рівні збору даних: мережевий та хостовий, які часто поєднуються в сучасних СВВ для підвищення швидкості обробки даних, точності інформації та ефективності моніторингу поточного трафіку і систем.

Ф3.1. Мережевий рівень спостереження передбачає використання сенсорів для аналізу даних, здебільшого на основі сигнатурного аналізу, що

дозволяє генерувати і передавати тривожні повідомлення до модулів управління у разі виявлення атак.

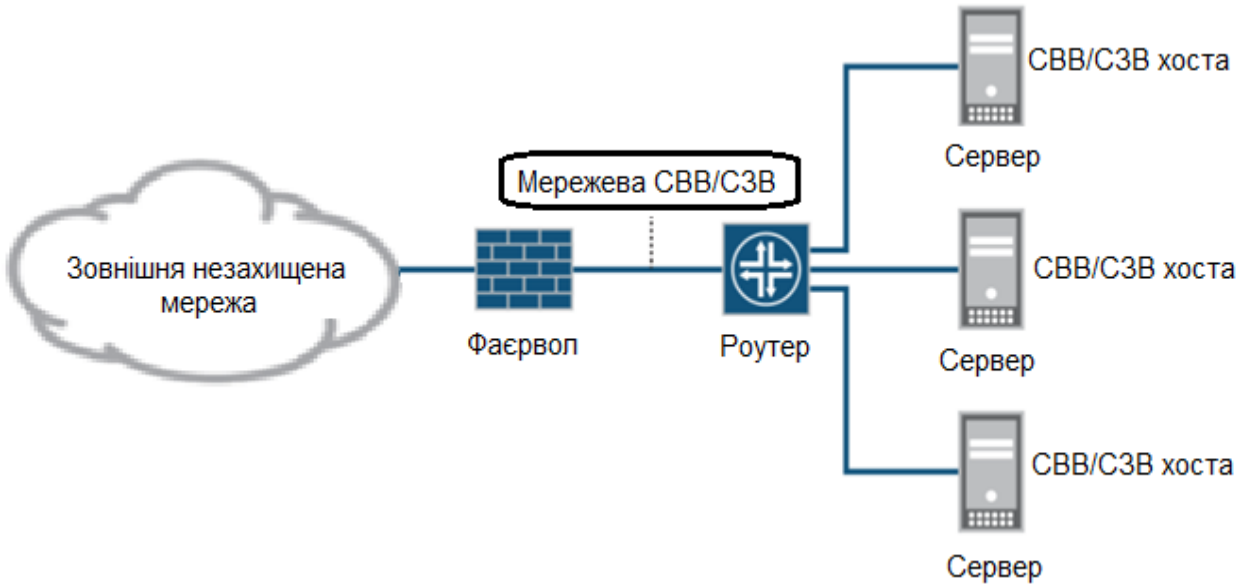


Рисунок 2.2 – Підключення мережевих СВВ/СЗВ та СВВ/СЗВ хостів у системі з фаєрволом

а) система виявлення вторгнень б) система запобігання вторгненням

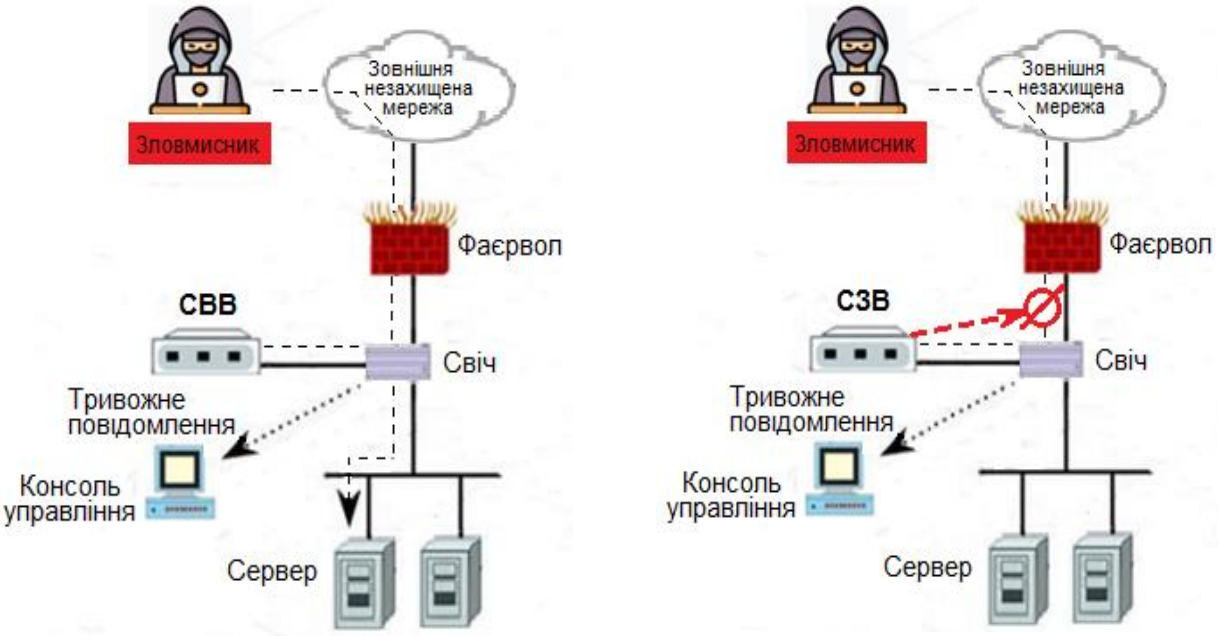


Рисунок 2.3 – Функціонування СВВ та СЗВ

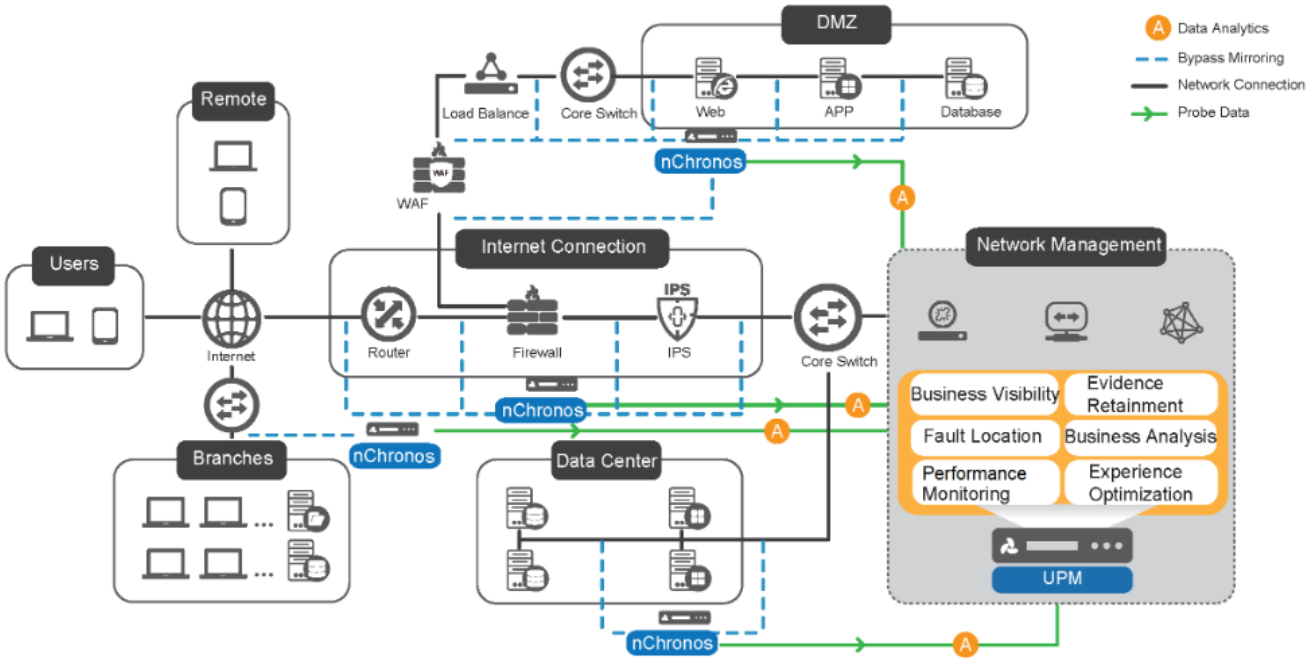


Рисунок 2.4 – Уніфікована система управління захистом ІКС [19]

Системи виявлення вторгнень, що працюють на мережевому рівні, називаються мережевими системами виявлення вторгнень (*NIDS*, англ. *Network Intrusion Detection System*). Вони досліджують трафік у всій мережі, шукаючи підозрілі дії, що можуть свідчити про спроби атаки. *NIDS* аналізує як вхідний, так і вихідний трафік на всіх пристроях мережі, порівнюючи його із заздалегідь заданими сигнатурами. При виявленні атаки або спроби вторгнення система сповіщає користувача. На відміну від інших систем, мережеві СВВ контролюють кілька комп'ютерів, а не тільки один, і шукають відомі шаблони вторгнення. Зазвичай *NIDS* розміщується в місцях, де весь трафік мережі може бути під контролем, наприклад, біля мережевого екрану, щоб забезпечити контроль брандмауера.

Переваги мережевих СВВ:

– широке покриття для моніторингу;
– відсутність впливу на продуктивність мережі;
– відсутність потреби змінювати топологію мережі;

– здатність протистояти dos-атакам, що можуть блокувати доступ користувачів до комп'ютерних ресурсів;

– централізоване управління, що не впливає на продуктивність;

– можливість використання обох методів аналізу (сигнатурного і аномального) або одного з них.

Основні недоліки *NIDS*:

– контроль лише за зовнішнім трафіком, без контролю внутрішньої структури;

– високе навантаження на систему;

– потрібні додаткові налаштування та функціональність мережевих пристроїв;

– не здатні аналізувати та розпізнавати зашифровану інформацію;

– пасивність: *NIDS* лише надає інформацію про атаку, але не реагує на неї.

Ф3.2. Системний рівень спостереження передбачає аналіз журналів операційних систем, програмних застосунків і додатків з метою виявлення можливих аномалій або загроз. Сенсори цього рівня генерують повідомлення, які передаються до модулів управління. До системного рівня відносяться рівні операційних систем, управління базами даних та додатків. Системи виявлення вторгнень, що працюють на системному рівні, називаються хостовими системами виявлення вторгнень (*HIDS*, англ. *Host-based Intrusion Detection System*).

Основні типи сенсорів *HIDS* включають: контроль цілісності файлів, аналіз журналів, сенсори ознак, аналіз системних викликів, аналіз поведінки програм. *HIDS* встановлюється на хості і виявляє атаки або спроби вторгнення безпосередньо на цьому комп'ютері. Хостові системи можуть контролювати цілісність файлів, моніторити файли реєстрації, перевіряти вразливості, спостерігати за доступом до ресурсів та змінювати паролі в системних базах даних.

Переваги хостової системи:

– можливість контролю не лише зовнішнього трафіку, а й внутрішньої структури хосту.

– висока точність у виявленні підозрілих процесів і користувачів, що мають відношення до атаки.

– використання двох джерел інформації: результатів аудиту та системних журналів подій.

– здатність виявляти атаки, які не бачить *NIDS*.

– здатність аналізувати та розпізнавати зашифровану інформацію.

– контроль лог-файлів та виправлення аномалій у потоках подій.

– можливість перевірки файлів на зміни завдяки збереженню критичних сум конфігурацій.

Основні недоліки *HIDS*:

– обмежене покриття для моніторингу, оскільки система встановлюється лише на один комп'ютер;

– високе навантаження на хост;

– відсутність централізованого управління, що вимагає значних ресурсів і впливає на продуктивність;

– нездатність протистояти *DoS*-атакам, як і *NIDS*, є пасивною системою, що лише надає інформацію про атаку, але не реагує на неї.

Ф4. Робота в реальному часі визначає здатність СВВ обробляти поточний трафік і виявляти поточні атаки. *NIDS*-системи, які працюють із сигнатурами атак, зазвичай обробляють події в реальному часі, оскільки вони аналізують мережевий трафік без значних затримок. У той час як *HIDS*-системи, що отримують інформацію із журналів операційних систем та додатків, опрацьовують події з певною затримкою, оскільки вони аналізують вже зафіксовану інформацію про події, яка була збережена в журналах.

До проектних характеристик СВВ можна віднести наступні критерії.

П1. Відкритість системи до взаємодії з іншим програмним забезпеченням (ПЗ): Цей критерій важливий для корпоративних ІКС, де комплекс засобів захисту може включати кілька спеціалізованих програм для різних частин системи. Відкритою є та система, яка дозволяє здійснювати взаємодію та обмін

даними з іншими ПЗ. Така відкритість полегшує процес модифікації, розвитку та вдосконалення системи, оскільки початковий код відкритих систем доступний для перегляду, модифікації (за наявністю дозволу), що дозволяє виправляти помилки або розробляти нові програмні продукти.

П2. Підтримка операційних систем: Цей критерій визначає, з якими операційними системами (ОС) може працювати СВВ. ОС є основою для роботи комп'ютерних систем і взаємодії з користувачем. Системи виявлення вторгнень повинні мати змогу працювати з різними операційними системами, такими як *Windows, Unix, Linux, MacOS* тощо, щоб мати змогу забезпечити захист комп'ютерів, що використовують ці системи. Важливим є забезпечення сумісності з більшістю ОС для покращення рівня безпеки на різних пристроях в мережі.

Ці критерії визначають здатність СВВ бути ефективними і забезпечувати необхідний рівень захисту ІКС на різних рівнях та з урахуванням специфіки технологій, які використовуються в організації.

П3. Методи виявлення атак у СВВ:

П3.1. Експертні методи: Ці методи використовують базу знань, яка містить набір правил для класифікації подій як атак. Системи, що застосовують експертні методи, мають здатність виявляти атаки "першого дня", тобто нові, ще не відомі атаки. Це робить такі системи потужними, але база знань потребує постійного оновлення, що може бути складною задачею;

П3.2. Сигнатурні методи, що є найпоширенішими у сучасних СВВ, оскільки вони ефективні для знайомих загроз (однак не здатні виявляти нові або невідомі типи вторгнень). Ці методи полягають у порівнянні подій з вже відомими сигнатурами атак, які були класифіковані раніше.

П3.3. Методи контролю зміни подій: Ці методи використовують базу даних атак, в якій описуються послідовності станів інформаційної системи. Для виявлення атаки система аналізує зміни в станах, що дозволяє виявити нетипові переходи або аномалії в поведінці системи;

П3.4. Методи кластерного аналізу: Ці методи передбачають поділ мережевого трафіку на групи типів, які відповідають звичайній роботі системи.

Все, що не підпадає під ці класифікації, вважається аномалією, що може вказувати на атаку. Такими методами виявляють нові або невідомі загрози;

П3.5. Динамічні методи: Ці методи здійснюють контроль над станами та змінами в станах процесів і об'єктів системи, аналізують динаміку змін у реальному часі і виявляють зміни, характерні для атак/ шкідливої діяльності;

П3.6. Методи машинного навчання: Машинне навчання, зокрема використання нейронних мереж, є одним із найбільш інноваційних методів в СВВ. Система може автоматично адаптувати свою модель виявлення вторгнень на основі аналізу даних, що дозволяє їй приймати рішення про реакцію на шкідливу активність, подібно до того, як це робили б люди з досвідом. Це потребує спеціальних знань та підготовки навчальної вибірки даних;

П3.7. Поведінкові методи: Поведінкові методи базуються на порівнянні поточної поведінки системи з нормальними показниками, встановленими на основі експериментальних даних. Якщо система виявляє відхилення від норми, таке поводження класифікується як аномальне і, ймовірно, вказує на атаку;

П3.8. Евристичні методи: Ці методи використовують стандартну лінію роботи системи для виявлення нетипової діяльності. Хоча вони можуть генерувати більше хибних спрацьовувань, вони здатні враховувати практичні поради та рекомендації, які наразі не мають теоретичного обґрунтування, що робить їх корисними для виявлення нових/ непередбачуваних загроз.

Експлуатаційні характеристики СВВ визначаються критеріями Е1-Е4:

Е1. Захищеність: наявність в СВВ вбудованих засобів захисту від негативного зовнішнього впливу і засобів забезпечення кіберстійкості;

Е2. Масштабованість: здатність СВВ збільшувати обсяг виконуваної роботи, коли додаються нові ресурси до мережі. Масштабованість є важливим критерієм вибору СВВ для довгострокового використання, оскільки дозволяє забезпечити сталу і надійну роботу навіть у випадку значних змін в IT-інфраструктурі. Ключовими аспектами масштабованості є:

– збереження надійності та стабільності при зміні розміру системи;

– оптимізація продуктивності через синергізм, коли окремі компоненти системи працюють краще разом, ніж поодинці;

Е3. Адаптивність: здатність СВВ змінювати алгоритми функціонування для ефективного реагування на нові типи атак або кібератак з мінімальними модифікаціями. Це важливий аспект для СВВ, оскільки сигнатурні методи виявлення можуть бути неефективними проти нових загроз, які не мають чітко визначених характеристик у базах даних. Адаптивні системи здатні підтримувати високий рівень захисту, коригуючи свої стратегії виявлення відповідно до нових атак чи модифікацій уже відомих загроз;

Е4. Управління системою: Управління СВВ включає в себе організацію схем і рівнів управління системою, які можуть бути централізованими або розподіленими. Управління системою має важливе значення для ефективної роботи і підтримки її надійності;

Е4.1. Централізоване управління: управління всіма функціями СВВ з одного хоста або станції. Це дозволяє зосередити контроль і забезпечити вищу надійність, оскільки всі зміни та налаштування вносяться централізовано. У таких системах забезпечується висока ефективність виявлення аномалій та швидке реагування на загрози через централізоване адміністрування;4

Е4.2. Розподілене управління: кожен хост або модуль відповідає за певну функцію в системі. Це дозволяє здійснювати більш детальне управління різними частинами системи, проте також потребує ефективної взаємодії між модулями для забезпечення єдиного рівня захисту. Розподілене управління може бути корисним у великих, складних мережах, де необхідно організувати захист для різних компонентів системи.

У даному контексті розглядаються кілька важливих аспектів для ефективного вибору та використання СВВ, а саме:

1. Захист по периметру, динамічний та сталий захист:

– захист по периметру фокусується на виявленні та запобіганні вторгнень через зовнішній доступ до мережі або системи;

– динамічний захист забезпечує адаптацію системи до нових, непередбачених загроз, змінюючи алгоритми та параметри захисту в реальному часі;

– сталий захист спрямований на забезпечення стабільності та неперервної роботи системи навіть у випадку атак чи змін у зовнішньому середовищі.

2. Проактивний захист інформації: Це підхід, що передбачає активне запобігання кіберзагрозам через моніторинг та швидке реагування на потенційно шкідливі дії, ще до того, як вони можуть завдати шкоди.

3. Типи СВВ:

– сучасні СВВ представлені програмними та апаратно-програмними засобами, що здійснюють автоматизований контроль та аналіз подій в інформаційних системах;

– програмні реалізації СВВ порівнюються за різними характеристиками, такими як обсяг пам'яті, швидкодія, зручність інтерфейсу, складність оновлень тощо;

– вибір СВВ має враховувати недоліки окремих типів систем і їх здатність ефективно працювати в специфічних умовах.

4. Підхід до вибору СВВ: Зростання кількості кіберзагроз та розвиток методів кібератак веде до необхідності оптимального вибору СВВ. Системи, здатні своєчасно виявляти й запобігати атакам, дозволяють значно зменшити витрати на нейтралізацію наслідків атак та економити ресурси, що витрачаються на забезпечення безпеки.

5. Методика обробки атак в СВВ: У СВВ, які використовують метод сигнатур для виявлення атак, кожна сигнатура є елементом визначення фази кібератаки. Розрізнення фаз кібератак дає змогу виявляти загрози ще на етапі їх підготовки, а не лише після активації. Фази кібератаки можуть включати програмну та апаратну ідентифікацію, збір банерів, використання експлойтів, роздроблення мережі, пошук бекдорів, троянів, проксі-серверів тощо.

6. Переваги сигнатурного підходу: Сигнатурний пошук дозволяє швидко виявляти загрози на основі відомих шаблонів атак, але також можна

використовувати інші методи, такі як виявлення аномалій, експертні системи чи довірчі стосунки для підвищення точності виявлення.

7. Класифікація СВВ: Кожна СВВ має здатність розпізнавати різні фази кібератак, що може бути використано як додатковий критерій для їх класифікації та вибору. Однак, на практиці, користувачі більше орієнтуються на кінцеві результати роботи СВВ, такі як ефективність виявлення атак, масштабованість, адаптивність та зручність використання.

8. Оптимальний вибір СВВ для конкретної ІКС: Для забезпечення найкращої ефективності необхідно вибрати таку СВВ, яка буде оптимальною для конкретної інформаційної системи чи мережі, забезпечуючи надійний захист без значних знижених характеристик продуктивності, з масштабованістю та адаптивністю до нових загроз.

Вибір та впровадження СВВ має бути обґрунтованим, з урахуванням специфічних вимог користувача та особливостей інформаційної системи.

2.2 Порівняльний аналіз властивостей популярних систем виявлення вторгнень

AAFID — це система виявлення вторгнень, орієнтована на виявлення атак у розподілених системах. Вона використовує методи аномалійного аналізу для ідентифікації шкідливих дій на основі порівняння з базою нормальних шаблонів. Основною особливістю є її здатність працювати в масштабованих розподілених середовищах, що робить її ідеальною для великих мереж і інфраструктур.

Переваги *AAFID*: Підходить для великих та розподілених систем. Користувачі можуть адаптувати систему під специфічні вимоги інфраструктури. Аномальні патерни можуть бути виявлені навіть при мінімальній кількості підозрілих дій. Може виявляти нові типи атак без необхідності оновлення сигнатур.

Недоліки *AAFID*: Потрібно багато обчислювальних потужностей для обробки великої кількості даних в реальному часі. Для ефективного використання необхідне детальне налаштування, яке може вимагати додаткових знань та часу. Як і більшість систем аномалійного аналізу, може мати хибні спрацьовування через неточності в налаштуваннях.

Snort — це один з найпопулярніших відкритих *IDS/IP*S, що використовує методи сигнатурного та аномалійного аналізу для виявлення атак. Система має гнучку архітектуру, що дозволяє налаштовувати правила та сигнатури для різних видів атак, а також підтримує інтеграцію з іншими засобами безпеки, такими як *SIEM*-системи.

Переваги *Snort*: Snort є безкоштовним та відкритим, що дозволяє його модифікацію та інтеграцію. Підтримує сигнатурні, аномалійні та протокол-аналітичні методи виявлення атак. Завдяки великій кількості користувачів і розробників, Snort має постійну підтримку та оновлення. Виявляє велику кількість атак за допомогою ефективних сигнатур.

Недоліки *Snort*: Особливо при недостатньо налаштованих сигнатурах. Snort сильно залежить від наявних сигнатур, тому може бути менш ефективним у виявленні нових чи модифікованих атак. Потрібне глибоке розуміння для налаштування та оптимізації системи.

Prelude SEIM є рішенням для моніторингу безпеки, яке дозволяє збирати, зберігати і аналізувати інформацію про безпеку з різних джерел, таких як *IDS*, фаєрволи, системи моніторингу та інші джерела подій. *Prelude* надає централізовану платформу для збору і кореляції подій, що дозволяє виявляти складні атаки та порушення безпеки.

Переваги *Prelude SEIM*: Збір та кореляція подій з різних джерел для створення єдиної картини безпеки. Легко інтегрується з іншими інструментами безпеки, такими як *Snort, OSSEC*, та ін. Підтримує як сигнатурні, так і аномалійні методи виявлення атак. Можливість додавання нових джерел подій для підвищення ефективності.

Недоліки *Prelude SEIM*: Як комерційне рішення, *Prelude* може бути дорогим для малих підприємств. Обробка великої кількості подій в реальному часі може вимагати великих обчислювальних ресурсів. Для досягнення максимальної ефективності необхідне детальне налаштування та великий досвід у системах *SIEM*.

NetSTAT (англ. *Network Statistics*) — це утиліта, яка надає дані про активні з'єднання в комп'ютерних мережах, зокрема *TCP/IP* з'єднання, порти, протоколи та маршрути. Вона часто використовується для моніторингу та аналізу мережевої активності на локальних машинах або в системах безпеки. Хоча *NetSTAT* зазвичай є інструментом для виведення статистики мережі, у контексті систем виявлення вторгнень він може використовуватись для аналізу підозрілих активних з'єднань, визначення вразливих точок мережі та з'ясування, чи не здійснюється несанкціонований доступ.

Переваги *NetSTAT*: Інтерфейс є досить простим і зрозумілим, тому *NetSTAT* можна легко використовувати навіть без глибоких технічних знань. Дає можливість переглядати поточний стан мережевих з'єднань і виявляти підозрілі активності в реальному часі. Використовується на більшості операційних систем (*Linux, Windows, MacOS*), що робить його універсальним інструментом для моніторингу мережевих підключень.

Недоліки *NetSTAT*: *NetSTAT* не є повноцінною системою виявлення вторгнень і не може проводити детальний аналіз або кореляцію подій. Розпізнавання атак через *NetSTAT* може бути ускладнене, оскільки сама утиліта не здатна визначити зловмисні дії без додаткових інструментів чи аналізу. Вона не надає глибокого аналізу щодо потенційних загроз або атак, а лише відображає поточні з'єднання.

Shadow — це система моніторингу та виявлення атак, яка зосереджена на аналізі поведінки користувачів і процесів у реальному часі. *Shadow* застосовується для аналізу внутрішніх загроз, коли шкідливі дії здійснюються зсередини організації. Система надає інструменти для виявлення аномальної

поведінки користувачів, несанкціонованого доступу до чутливих даних або використання ресурсів, що можуть вказувати на компрометацію системи.

Переваги *Shadow*: *Shadow* здатний працювати в режимі реального часу, що дозволяє вчасно виявляти аномалії в поведінці користувачів і запобігати атакам. Система допомагає виявляти зловмисну активність, яка може походити від авторизованих користувачів або співробітників. *Shadow* дозволяє налаштовувати політики для виявлення та реагування на різні типи аномальних дій, що забезпечує високу кастомізацію під конкретні потреби організації.

Недоліки *Shadow*: Потрібно значні ресурси для збору та аналізу даних, особливо при великих обсягах інформації. Для досягнення ефективного використання необхідне детальне налаштування і правильно визначені правила для виявлення аномалій. Через високу гнучкість налаштувань може виникати багато хибних спрацьовувань, якщо не налаштовано правильні критерії для оцінки поведінки користувачів.

ASAX — це інструмент для виявлення вторгнень та управління безпекою мережі, який спеціалізується на комплексному аналізі та кореляції подій, зокрема для великих корпоративних мереж. Ця система підтримує інтеграцію з іншими інструментами безпеки та пропонує потужні можливості для моніторингу, аналізу і реагування на кібератаки в реальному часі. *ASAX* зосереджений на адаптивності, дозволяючи системі змінювати свої алгоритми для виявлення нових типів атак.

Переваги *ASAX*: Підтримує детальний аналіз подій та кореляцію різних даних з різних джерел для точного виявлення атак. Здатен адаптуватися до нових методів атак, що є важливим для сучасних загроз. Система легко інтегрується з іншими засобами безпеки, такими як *SIEM*, для покращеного моніторингу.

Недоліки *ASAX*: Для оптимального використання *ASAX* необхідні глибокі технічні знання та досвід. Як і більшість передових рішень, *ASAX* може бути дорогим для малих підприємств через витрати на ліцензії та підтримку. Для

правильного функціонування *ASAX* потребує наявності потужної інфраструктури з високими вимогами до ресурсів.

Bro (тепер відомий як ***Zeek***) — це потужна система для моніторингу мережевої безпеки, яка фокусується на аналізі мережевого трафіку та виявленні аномалій. *Zeek* аналізує дані на рівні мережевих протоколів та взаємодії між мережами, забезпечуючи високий рівень детекції мережевих атак. Він є не лише *IDS*, а й платформою для аналізу мережевого трафіку, що дозволяє створювати кастомізовані скрипти для різноманітних типів атак. *Zeek* застосовує гнучку систему скриптів, що дозволяє здійснювати детальну аналізу на різних рівнях мережі.

Переваги *Zeek*: Застосування власної мови скриптів дозволяє налаштувати систему для виявлення специфічних атак та аномалій, забезпечуючи великі можливості для кастомізації. *Zeek* дозволяє здійснювати глибокий аналіз мережевого трафіку, виявляючи не лише очевидні атаки, але й аномальні патерни. Завдяки великій спільноті розробників Zeek має постійне оновлення та вдосконалення.

Недоліки *Zeek*: Для обробки великих обсягів трафіку та проведення детального аналізу потрібно значне обладнання та ресурси. Необхідно мати певні знання для налаштування та використання власних скриптів для виявлення атак, що може бути складно для новачків. Враховуючи високу гнучкість і вимоги до ресурсів, *Zeek* може бути надмірним для невеликих або середніх організацій.

OSSEC є *HIDS*, яка фокусується на моніторингу та аналізі системних журналів, а також на виявленні змін у файлових системах, спробах несанкціонованого доступу і конфігураціях безпеки. *OSSEC* підтримує централізовану консоль управління, що дозволяє ефективно управляти системою безпеки на великій кількості хостів, та функціонал для виявлення атак на основі поведінки та забезпечує можливості для аналізу логів.

Переваги *OSSEC*: *OSSEC* є відкритим ПЗ, що дозволяє знизити витрати на придбання ліцензій. Підтримує широкий спектр операційних систем, зокрема

Linux, Windows, macOS. *OSSEC* легко інтегрується з іншими засобами безпеки, такими як *SIEM* системи. *OSSEC* забезпечує глибокий моніторинг на рівні хостів, дозволяючи виявляти не тільки зовнішні атаки, а й внутрішні загрози.

Недоліки *OSSEC*: Як HIDS система, OSSEC може не справлятися з великими та складними атаками, які відбуваються на рівні мережі. Оскільки система працює на основі журналів та змін у файловій системі, вона може давати багато помилкових спрацьовувань, якщо не налаштувати правила детекції правильно. Хоча OSSEC підтримує централізоване управління, для великих інфраструктур можуть виникати проблеми з масштабованістю.

Cisco IPS — це система виявлення та запобігання вторгненням, яка надає високу ефективність для мережевої безпеки, використовуючи як підписи для виявлення атак, так і аналіз аномалій для забезпечення захисту від нових загроз. *Cisco IPS* інтегрується з іншими продуктами *Cisco* для забезпечення комплексного захисту мережі, застосовує глибоке сканування трафіку та блокує зловмисні дії в реальному часі. Він може працювати як самостійний продукт або бути частиною більш широкої інфраструктури безпеки.

Переваги *Cisco IPS*: *Cisco IPS* здатен швидко реагувати на загрози, блокуя їх ще до того, як вони зможуть вплинути на систему. Враховуючи популярність *Cisco* в корпоративних середовищах, інтеграція з іншими продуктами цієї компанії дозволяє забезпечити єдину платформу для управління безпекою. *Cisco IPS* використовує глибоке вивчення трафіку, що дозволяє йому виявляти більш складні загрози.

Недоліки *Cisco IPS*: *Cisco IPS* є досить дорогим рішенням, що може бути недоступним для малих та середніх підприємств. Потребує потужної інфраструктури та ресурсів для обробки трафіку на великих підприємствах. Якщо неправильно налаштований, *Cisco IPS* може спричиняти затримки в мережі, особливо на великих пропускних здатностях.

Arbor Networks Spectrum — це *SIEM* та рішення для виявлення та запобігання мережевим атакам, що орієнтується на великий трафік та захист від *DDoS*-атак. *Arbor Networks Spectrum* застосовує аналіз трафіку в реальному часі

для виявлення аномалій та аномальних поведінкових патернів в мережі. Він використовує потужні алгоритми для моніторингу потоків і виявлення загроз, таких як *DDoS*-атаки, ботнети та інші зловмисні активності в мережі. Arbor також дозволяє здійснювати розширену кореляцію подій для полегшення управління безпекою.

Переваги *Arbor Networks Spectrum*: спеціалізується на виявленні та блокуванні *DDoS*-атак, що робить його ідеальним для компаній, що мають високий рівень ризику таких атак. Виявлення аномалій у трафіку в реальному часі дозволяє швидко реагувати на загрози, зменшуючи ризики для мережі. Spectrum можна інтегрувати з іншими засобами безпеки, що забезпечує комплексний захист. Рішення підтримує великі інфраструктури та здатне обробляти великі обсяги даних з мінімальними затримками.

Недоліки *Arbor Networks Spectrum*: Рішення може бути дорогим, особливо для малих та середніх підприємств. Враховуючи багатофункціональність і широкі можливості, налаштування Arbor може бути складним і вимагати спеціалізованих знань. Хоча продукт пропонує комплексний захист, його сильний акцент на *DDoS*-атаки може бути обмеженням для деяких організацій, які потребують ширшого спектру захисту.

InfoWatch ASAP — це система виявлення загроз і запобігання витокам даних, що забезпечує моніторинг та захист від несанкціонованого доступу до інформації та її витоку. *InfoWatch ASAP* фокусується на запобіганні витоків конфіденційних даних за допомогою багаторівневої системи контролю доступу, що дозволяє виявляти несанкціоновані дії з інформацією, включаючи моніторинг файлів, інтернет-активності, електронної пошти та інших засобів комунікації. Він також здатний здійснювати управління політиками безпеки на рівні документів і запобігати порушенням з боку внутрішніх користувачів.

Переваги *InfoWatch ASAP*: спеціалізується на виявленні та попередженні витоків даних, що є важливим для компаній, які працюють з конфіденційною інформацією. Система дозволяє налаштовувати детальні політики доступу до інформації, з урахуванням специфічних вимог компанії. *InfoWatch ASAP* може

інтегруватися з іншими засобами безпеки, що підвищує ефективність захисту інформації. Система здатна моніторити широкий спектр каналів передачі даних (пошта, файлові системи, інтернет), що дозволяє детально контролювати виведення конфіденційної інформації.

Недоліки *InfoWatch ASAP*: Залежно від інфраструктури організації, можуть виникати проблеми з інтеграцією та сумісністю з іншими програмами. Система вимагає точного налаштування для ефективної роботи, оскільки неправильні налаштування політик доступу можуть призвести до помилкових спрацьовувань або упущення важливих подій. Програмне забезпечення може бути дорогим для малих і середніх компаній, особливо з урахуванням вартості впровадження та підтримки.

Symantec DeepSight — це система управління загрозами, яка забезпечує моніторинг та аналіз кіберзагроз в реальному часі. Вона використовує величезну базу даних, щоб виявляти нові загрози та зловмисні дії, допомагаючи організаціям швидко реагувати на інциденти безпеки. *DeepSight* інтегрується з іншими системами безпеки та дозволяє отримувати детальну інформацію про виявлені загрози, в тому числі через сповіщення і аналітичні інструменти. Система також включає можливості для кореляції подій, що дозволяє здійснювати більш глибокий аналіз інцидентів.

Переваги *DeepSight*: DeepSight може обробляти та корелювати події в реальному часі, що дозволяє швидко реагувати на загрози. Symantec має величезну базу даних загроз, що дозволяє отримати детальну інформацію про нові типи атак та методи їх виявлення. *Symantec DeepSight* можна інтегрувати з іншими продуктами безпеки для забезпечення більш комплексного захисту. Система має високий рівень автоматизації, що дозволяє зменшити навантаження на персонал, а також збільшити швидкість реагування на інциденти.

Недоліки *DeepSight*: Як і багато продуктів *Symantec, DeepSight* є дорогим рішенням, що може бути недоступним для малих та середніх підприємств. Враховуючи потужність і функціональність, налаштування та інтеграція з існуючими інфраструктурами може бути складним і вимагати високої

кваліфікації. Для великих організацій з високими вимогами до масштабованості можуть виникнути проблеми з продуктивністю, якщо система неправильно налаштована або перевантажена.

Tipping Point NGIPS (англ. Next-Generation Intrusion Prevention System) - це рішення наступного покоління для запобігання вторгненням, що поєднує в собі функціональність традиційних IPS з додатковими можливостями для глибокого аналізу мережевого трафіку, виявлення складних загроз і атак та забезпечення високої ефективності захисту. Вона використовує розширену сигнатуру, перевірку контексту атак та можливості для адаптивного захисту від нових загроз.

Переваги *Tipping Point NGIPS*: використовує методи машинного навчання та аналізу контексту для адаптації до нових загроз і безперервного вдосконалення захисту. Завдяки інноваційним технологіям глибокого аналізу пакетів і виявлення складних загроз, NGIPS забезпечує високу ефективність захисту. *Tipping Point* легко інтегрується з іншими рішеннями для управління безпекою (*SIEM, IDS*, та іншими), що дозволяє досягти більш ефективного результату в захисті мережі. Зручний інтерфейс користувача і автоматизовані процеси дозволяють спростити моніторинг та налаштування системи.

Недоліки *Tipping Point NGIPS*: вартість *Tipping Point NGIPS* може бути високою, особливо для малих та середніх підприємств, що робить його менш доступним для них. Хоча система чудово працює в умовах середніх і великих компаній, на великих і розподілених мережах можуть виникнути питання з продуктивністю. Для ефективної роботи потрібно потужне обладнання та мережеві ресурси, що може створити додаткові витрати на інфраструктуру.

Axoft invGUARD — це система захисту від вторгнень, що використовує новітні технології для аналізу та запобігання мережевим атакам в реальному часі. Вона включає в себе комплексні засоби для захисту від широкого спектру загроз, зокрема на основі сигнатур, аналізу аномалій і поведінкового моніторингу. Також система має інтерфейси для інтеграції з іншими системами безпеки та підтримує масштабованість для роботи в умовах великих підприємств.

Переваги *Axoft invGUARD*: має можливість масштабування та легко адаптується до потреб організацій будь-якого розміру. Легко інтегрується з іншими продуктами безпеки, що дозволяє створити комплексну систему захисту. Простота в налаштуванні та управлінні системою забезпечує зручність для користувачів і адміністраторів. Система активно використовує методи виявлення аномалій, що дозволяє ефективно виявляти нові або раніше невідомі загрози.

Недоліки *Axoft invGUARD*: при великих обсягах мережевого трафіку можливі затримки в обробці, що може вплинути на загальну продуктивність. Як і інші системи запобігання вторгненням, *invGUARD* може інколи мати проблеми з точністю, блокуючи дозволені дії через *false positives*. Для забезпечення оптимального захисту система потребує ретельного налаштування, що може бути складно для непідготовлених користувачів.

DefensePro — це система захисту мережі в реальному часі, яка забезпечує високоякісну профілактику від різноманітних типів кібератак, включаючи *DDoS*-атаки, атаки на відмову в обслуговуванні, а також інші загрози, пов'язані з шкідливим трафіком. Система використовує аналіз аномалій, підхід поведінкової аналітики та методи машинного навчання для виявлення та запобігання атакам на ранніх стадіях.

Переваги *DefensePro*: здійснює моніторинг і аналіз мережевого трафіку в реальному часі, дозволяючи оперативно виявляти і блокувати загрози. Система спеціалізується на виявленні та блокуванні DDoS-атак, що робить її ідеальним рішенням для захисту від цієї поширеної загрози. Використовує передові методи для виявлення нових та невідомих загроз, що не засновані на сигнатурах. *DefensePro* може бути інтегрована з іншими системами, такими як *SIEM* та *IPS*, для більш комплексного захисту мережі.

Недоліки *DefensePro*: може бути дорогим для невеликих підприємств і організацій, що обмежує його доступність. Для ефективного використання системи потрібна глибока настройка та розуміння мережевих загроз, що може бути складним для деяких користувачів. У разі великих обсягів трафіку або при

складних атаках можуть бути затримки в обробці даних, що впливає на загальну ефективність системи.

KATA Platform — це потужне рішення для забезпечення безпеки, яке пропонує інноваційні методи захисту від вторгнень, моніторинг в реальному часі та автоматизований аналіз загроз. Система включає в себе функції виявлення аномалій, управління ризиками та інтеграцію з іншими засобами безпеки, такими як SIEM, для покращення ефективності захисту.

Переваги *KATA Platform*: може бути інтегрована з різноманітними інструментами для управління безпекою, що дозволяє створювати комплексні рішення для захисту мережі. Система використовує передові алгоритми для виявлення аномальних шаблонів трафіку, що дозволяє виявляти нові загрози, навіть якщо вони не відповідають відомим сигнатурам. *KATA Platform* може бути налаштована для роботи в різноманітних мережах, від малих організацій до великих підприємств, що забезпечує гнучкість та масштабованість. Платформа автоматично налаштовується під нові умови та зростаючі вимоги, що дозволяє підтримувати високий рівень захисту.

Недоліки *KATA Platform*: для ефективної роботи потрібно провести детальну інтеграцію з іншими системами безпеки та налаштування, що може бути складним. Як і багато інноваційних рішень, *KATA Platform* може мати високу ціну, що може обмежити її використання в малих і середніх компаніях. Для ефективної роботи платформи потрібно багато обчислювальних потужностей, що може призвести до додаткових витрат на інфраструктуру.

Suricata — це потужна система виявлення і запобігання вторгнень, яка використовує технології для моніторингу мережевого трафіку, зокрема через аналіз на основі сигнатур, аномалій і протоколів. *Suricata* підтримує високу пропускну здатність і є відкритим програмним забезпеченням, що дозволяє гнучко налаштовувати її під потреби різних організацій.

Переваги *Suricata*: *Suricata* є безкоштовною і відкритою, що робить її доступною для широкого кола користувачів, включаючи малий та середній бізнес. *Suricata* розроблена для ефективного оброблення великих обсягів

мережевого трафіку, що дозволяє використовувати її в великих організаціях і для великих мереж. Система підтримує аналіз різних мережевих протоколів, що дозволяє виявляти загрози в широкому спектрі застосувань. *Suricata* підтримує різні рівні масштабування, що дозволяє використовувати її в різних середовищах — від малих до великих організацій.

Недоліки *Suricata*: як відкрите ПЗ *Suricata* вимагає додаткових налаштувань для досягнення оптимальної ефективності, що може бути складним для не досвідчених користувачів. Попри високу пропускну здатність, при дуже великих обсягах трафіку можуть виникати затримки в обробці даних. Хоча *Suricata* активно підтримується спільнотою, відсутність офіційної підтримки комерційними компаніями може бути проблемою для деяких підприємств.

Samhain — це IDS, яка спеціалізується на виявленні та моніторингу змін в системних файлах і параметрах, зокрема виявляє аномалії та шкідливі зміни в цілісності даних. Вона є відкритим програмним забезпеченням і добре підходить для моніторингу серверів та важливих систем.

Переваги *Samhain*: є відкритим ПЗ, що робить його доступним для широкого кола користувачів, включаючи малий та середній бізнес. Система забезпечує виявлення змін у важливих файлах і директоріях, що дозволяє виявляти несанкціоновані зміни і потенційні загрози безпеці. Samhain дозволяє централізовано здійснювати моніторинг великих і розподілених мереж, що зручно для великих організацій. Підтримує кілька платформ, включаючи *Linux* і *Windows*, що дозволяє використовувати її в різних середовищах.

Недоліки *Samhain*: не підходить для мережевого моніторингу, бо більше зосереджений на моніторингу цілісності файлів. Як відкрите ПЗ, *Samhain* має обмежену комерційну підтримку і може бути складним у налаштуванні для користувачів без досвіду в адмініструванні. *Samhain* не підтримує складніші методи аналізу аномалій або поведінкового моніторингу, що обмежує його здатність виявляти нові типи атак.

Security Onion — це збірка відкритих інструментів для моніторингу та виявлення загроз, включаючи такі засоби, як *Suricata, Zeek, ELK stack* (англ.

Elasticsearch, Logstash, Kibana) і багато інших. Це потужне рішення для аналізу безпеки, яке дозволяє виконувати збір, аналіз і візуалізацію даних з мереж і систем у реальному часі.

Переваги *Security Onion*: є безкоштовним і відкритим ПЗ, що дозволяє організаціям з обмеженим бюджетом використовувати ефективні інструменти для забезпечення безпеки. *Security Onion* включає в себе кілька потужних інструментів для виявлення атак, моніторингу трафіку і аналізу подій, що забезпечує комплексний підхід до безпеки. Система дозволяє масштабувати інфраструктуру в залежності від розміру організації, що робить її гнучким рішенням для малих і великих підприємств. Завдяки підтримці інструментів для збору та аналізу даних, *Security Onion* може бути інтегрована з іншими системами безпеки, такими як *SIEM* або *IDS*.

Недоліки *Security Onion*: налаштування і інтеграція можуть бути складними для новачків або невеликих організацій без досвіду в адмініструванні. Для ефективної роботи *Security Onion* потрібно чимало обчислювальних ресурсів, що може стати проблемою для підприємств з обмеженими бюджетами або інфраструктурою. Хоча є активна спільнота, офіційна комерційна підтримка може бути відсутня, що ускладнює вирішення специфічних проблем.

***SolarWinds Security Event Manager* (*SEM*)** — це комерційне рішення для управління подіями та інформацією безпеки (*SIEM*), яке дозволяє збирати, корелювати та аналізувати дані з різних джерел для виявлення загроз. Система забезпечує автоматизований процес моніторингу, виявлення інцидентів безпеки та реагування на них в реальному часі.

Переваги: *SEM* здатний корелювати дані з різних джерел, що дозволяє виявляти складні інциденти безпеки. Зрозумілий інтерфейс користувача та простота налаштування дозволяють швидко інтегрувати систему в робоче середовище без необхідності в глибоких технічних знаннях. *SolarWinds SEM* дозволяє масштабувати рішення залежно від потреб організації, підтримуючи як малий, так і великий бізнес. *SEM* легко інтегрується з іншими інструментами

безпеки, такими як *IDS/IPS*, що дозволяє створювати комплексні рішення для моніторингу та захисту.

Недоліки: *SolarWinds SEM* є комерційним продуктом, і його ліцензія може бути дорогою для малих організацій. Хоча *SolarWinds* має сильну підтримку, для вирішення специфічних проблем може знадобитися оплачувана підтримка, що додатково збільшує витрати. Як і багато комерційних рішень, SEM може бути менш гнучким в порівнянні з відкритими системами, що дозволяють глибшу кастомізацію для специфічних потреб.

Splunk — це потужне рішення для збору, моніторингу та аналізу машинних даних у реальному часі. В основному використовується як *SIEM*, що дозволяє здійснювати збір і аналіз даних з різних джерел, таких як сервери, мережі, пристрої та додатки. *Splunk* надає користувачам можливість аналізувати великі обсяги даних для виявлення аномалій та інцидентів безпеки.

Переваги: *Splunk* може масштабуватися в залежності від розміру підприємства та обсягу даних. Це робить його підходящим як для малих, так і для великих організацій. Splunk надає широкі можливості для аналізу великих обсягів логів, зокрема за допомогою інтерактивних панелей управління та розширених запитів. *Splunk* може інтегруватися з численними джерелами даних, що дозволяє використовувати його для аналізу всієї інфраструктури безпеки. *Splunk* автоматично корелює події для виявлення складних загроз і допомагає реагувати на інциденти в реальному часі.

Недоліки: *Splunk* є дорогим рішенням, особливо в разі обробки великих обсягів даних. Ліцензії зазвичай залежать від обсягу даних, що ускладнює бюджетування для малих підприємств. Хоча *Splunk* має потужний функціонал, його налаштування може бути складним для недосвідчених користувачів, а виведення корисних результатів із даних може вимагати спеціальних знань. *Splunk* потребує значних обчислювальних ресурсів для обробки та зберігання даних, що може стати проблемою для організацій з обмеженою інфраструктурою.

McAfee Network Security Platform (*NSP*) — це мережева *IPS*, яка використовує потужні методи аналізу трафіку для виявлення та блокування

загроз у реальному часі. *NSP* інтегрує різні методи виявлення, зокрема аналіз поведінки, аналіз сигнатур і виявлення аномалій.

Переваги: *McAfee NSP* поєднує кілька технологій для забезпечення виявлення та блокування мережевих атак, що дозволяє знизити ризики для мережі. Система забезпечує швидке виявлення і блокування загроз, що важливо для організацій, які працюють в режимі реального часу. *NSP* використовує методи глибокого аналізу трафіку для виявлення складних атак, зокрема для пошуку аномалій у поведінці користувачів або додатків. Платформа має гнучкі налаштування для налаштування політик безпеки та адаптації до потреб організації.

Недоліки: *McAfee NSP* є комерційним рішенням, і його вартість може бути значною для малих і середніх підприємств. Платформа потребує детального налаштування і може бути складною для новачків або організацій без досвіду в налаштуванні *IPS*. Хоча *NSP* використовує різні методи виявлення, значна частина його ефективності залежить від актуальності оновлень сигнатур, що може бути проблемою при швидкому розвитку нових типів атак.

IBM QRadar — це потужна *SIEM*, яка дозволяє збирати, корелювати і аналізувати дані для виявлення загроз в реальному часі. *QRadar* використовує машинне навчання та інші сучасні технології для автоматизованого виявлення інцидентів і їх аналізу.

Переваги: *QRadar* має потужний механізм кореляції подій, що дозволяє виявляти складні інциденти безпеки за допомогою аналізу великого обсягу даних. *QRadar* добре інтегрується з іншими рішеннями для забезпечення комплексної безпеки, такими як *IPS, IDS*, антивірусне ПЗ і платформи для моніторингу мереж. Завдяки використанню методів машинного навчання та виявлення аномалій *QRadar* може ефективно боротися з новими, раніше невідомими загрозами. *QRadar* здатен масштабуватися, дозволяючи використовувати його як у великих корпораціях, так і в середніх підприємствах.

Недоліки: як комерційне рішення, *QRadar* має високу вартість, що може бути обтяжливим для малих підприємств. *QRadar* є потужним, але складним

для освоєння рішенням, яке потребує певного часу для налаштування та ефективного використання. Для ефективної роботи *QRadar* потребує значних обчислювальних і мережевих ресурсів, що може бути проблемою для малих підприємств з обмеженою інфраструктурою.

Check Point Security Management — це система для централізованого управління політиками безпеки та моніторингу в режимі реального часу, що дозволяє адмініструвати інфраструктуру безпеки за допомогою інтегрованих інструментів для управління фаєрволами, *VPN*, *IPS*, антивірусним захистом і іншими елементами захисту. Система підтримує гнучку політику доступу, аналіз загроз, управління подіями безпеки та спрощує інтеграцію з іншими системами захисту.

Переваги: Можливість централізовано керувати всіма компонентами безпеки (фаєрволи, *VPN*, *IPS*, антивірусний захист), що значно спрощує адміністрування та забезпечення безпеки. Check Point має сильні можливості для кореляції подій і аналізу загроз, що дозволяє швидко реагувати на інциденти безпеки. Зручний інтерфейс користувача та інструменти для аналізу і візуалізації даних спрощують роботу адміністраторів. *Check Poin*t може інтегруватися з іншими рішеннями для безпеки, включаючи різні *IDS/IPS*, антивірусне ПЗ та *SIEM*-системи.

Недоліки: ПЗ *Check Point* має високу вартість, що може бути непосильним для малих підприємств. Встановлення та налаштування системи може бути складним і вимагати висококваліфікованих фахівців. Деякі користувачі вважають, що система не завжди підтримує всі відкриті стандарти та може бути менш гнучкою для інтеграції з іншими платформами безпеки.

AlienVault OSSIM — це відкрите рішення *SIEM*, яке включає в себе інструменти для моніторингу загроз, збору та аналізу даних, кореляції подій та виявлення аномалій. *OSSIM* об'єднує кілька функцій безпеки, включаючи виявлення вторгнень (*IDS*), аналіз вразливостей, управління подіями безпеки та захист від зловмисних програм.

Переваги: *OSSIM* є відкритим ПЗ, тому користувачі можуть безкоштовно отримати доступ до основних функцій. *AlienVault OSSIM* здатний масштабуватися для підтримки різних типів організацій, від малих до великих підприємств. *OSSIM* включає потужні інструменти для виявлення загроз та кореляції подій, що дозволяє швидко реагувати на інциденти. Як продукт з відкритим кодом, OSSIM має активну спільноту, що надає підтримку, документи та інші ресурси для налаштування і розширення.

Недоліки: *OSSIM* може не бути таким потужним, як комерційні альтернативи для великих підприємств, які потребують складніших функцій і підтримки великих обсягів даних. Для тих, хто не має досвіду в роботі з *SIEM*-системами, налаштування *OSSIM* може бути складним і вимагати часу для освоєння. Для комерційних версій існує більш глибока підтримка, тоді як у відкритому коді можуть бути обмеження в допомозі.

LogRhythm — це комплексне *SIEM*-рішення для збору, аналізу та кореляції подій безпеки. *LogRhythm* надає організаціям можливість централізовано контролювати їхні мережі та дані, виявляти потенційні загрози в реальному часі та автоматизувати реакцію на інциденти. Платформа також має вбудовані інструменти для моніторингу мережевого трафіку та забезпечення відповідності нормативним вимогам.

Переваги: *LogRhythm* використовує просунуті методи кореляції для виявлення складних загроз і забезпечує глибокий аналіз подій безпеки. Платформа дозволяє швидко виявляти загрози і реагувати на них, що знижує ризик серйозних порушень безпеки. *LogRhythm* підходить для організацій різних розмірів, від малих до великих, і може бути налаштований для різних типів інфраструктури. Платформа включає функціональність для моніторингу відповідності нормативним вимогам, таким як *PCI-DSS, HIPAA, GDPR*.

Недоліки: *LogRhythm* є дорогим рішенням, що може бути важким для малих і середніх підприємств, оскільки вартість ліцензій та інтеграції може бути значною. Платформа має потужний функціонал, що може бути складним для адміністраторів без досвіду в роботі з *SIEM*-системами. Для досягнення

найкращих результатів необхідно ретельне налаштування системи, що може вимагати значних зусиль для адаптації до специфічних потреб організації.

FortiSIEM — це рішення *SIEM*, розроблене компанією *Fortinet*, яке поєднує в собі можливості моніторингу, кореляції та управління подіями безпеки. *FortiSIEM* пропонує централізований контроль за інцидентами безпеки, моніторинг мережевих загроз, виявлення аномалій та відповіді на інциденти. Платформа інтегрується з іншими інструментами *Fortinet* для забезпечення комплексної безпеки мережі.

Переваги: *FortiSIEM* є частиною екосистеми *Fortinet,* що дозволяє ефективно працювати з іншими продуктами цього бренду, такими як *FortiGate*, *FortiAnalyzer, FortiManager*. *FortiSIEM* підходить для підприємств різних розмірів і може масштабуватися в залежності від потреб користувача. Платформа автоматизує процеси моніторингу та відповіді на інциденти, дозволяючи знижувати час реагування. Зручний інтерфейс дозволяє швидко налаштовувати систему та управляти подіями безпеки.

Недоліки: Для невеликих підприємств вартість ліцензій та обслуговування може бути високою. Платформа вимагає досвіду та часу для налаштування, щоб максимально використовувати її потенціал. Для ефективної роботи *FortiSIEM* необхідно мати потужну інфраструктуру та ресурси для підтримки системи.

Rapid7 Nexpose — це платформа для управління вразливостями, яка дозволяє підприємствам виявляти, оцінювати та управляти вразливостями в їхній інфраструктурі. *Nexpose* пропонує функціональність для моніторингу вразливостей, оцінки ризиків та визначення пріоритетів для виправлення проблем безпеки. Вона може працювати в інтеграції з іншими інструментами *Rapid7*, такими як *InsightIDR* для моніторингу інцидентів.

Переваги: *Nexpose* може глибоко аналізувати мережу для виявлення вразливостей та надає детальну інформацію про ризики для кожної вразливості. Платформа дозволяє визначати пріоритети для виправлення вразливостей залежно від ризику та впливу на інфраструктуру. Інтерфейс простий у використанні і дозволяє швидко налаштовувати сканування та звіти. *Nexpose*

добре інтегрується з іншими продуктами компанії, такими як *InsightIDR*, що дозволяє створювати комплексні рішення для безпеки.

Недоліки: *Nexpose* більше орієнтований на виявлення вразливостей і менш ефективний у реальному часі для виявлення інцидентів безпеки. Вартість ліцензій та налаштування може бути високою для малих і середніх підприємств. *Nexpose* може бути менш ефективним для дуже великих або складних мереж, де потрібні більш спеціалізовані рішення для управління вразливостями.

OpenDXL (англ. *Open Data Exchange Layer*) від *McAfee* — це платформа для інтеграції різних рішень безпеки в єдину екосистему, що дозволяє здійснювати автоматизацію процесів безпеки, обмін даними між продуктами і прискорення виявлення загроз. *OpenDXL* підтримує інтеграцію з численними продуктами безпеки, що дозволяє організаціям швидко реагувати на інциденти та покращувати загальну ефективність безпеки.

Переваги: *OpenDXL* дозволяє інтегрувати різні продукти безпеки, що підвищує ефективність управління загрозами та автоматизацію процесів безпеки. Платформа дозволяє швидко реагувати на інциденти, автоматизуючи обмін інформацією між різними системами. *OpenDXL* є відкритою платформою, що дозволяє розширювати можливості системи відповідно до специфічних потреб організації. Оскільки це продукт *McAfee*, він добре інтегрується з іншими продуктами цієї компанії, такими як *McAfee ePolicy Orchestrator, McAfee Endpoint Security* тощо.

Недоліки: для повного використання потенціалу *OpenDXL* необхідно мати досвід у налаштуванні і інтеграції з іншими системами безпеки. Платформа оптимізована для використання в екосистемі *McAfee*, що може обмежити вибір продуктів безпеки для організацій, які використовують рішення інших виробників. Враховуючи потреби у високій кваліфікації для налаштування та інтеграції, *OpenDXL* може бути надто складним для малих підприємств з обмеженими ресурсами.

RSA NetWitness — це розвинута платформа для виявлення та реагування на інциденти, що спеціалізується на збиранні, зберіганні і аналізі великих

обсягів мережевого трафіку для виявлення та розслідування атак. Вона забезпечує повний огляд усіх етапів кіберзагрози, використовуючи методи машинного навчання та аналізу загроз.

Переваги: *RSA NetWitness* забезпечує глибокий аналіз мережевих сесій, дозволяючи виявляти складні загрози і аномалії на всіх етапах атаки. Платформа підтримує інтеграцію з іншими інструментами безпеки та *SIEM* для централізованого управління безпекою. Використовує інтелектуальні алгоритми для автоматичного виявлення аномалій та потенційних загроз. Підтримує різні формати даних, включаючи мережеві пакети, журнали подій та інші джерела.

Недоліки: *RSA NetWitness* може бути дорогим рішенням, що обмежує його доступність для малих і середніх підприємств. Для налаштування та оптимального використання потрібен досвід і знання в області кібербезпеки. Платформа потребує значних обчислювальних ресурсів для обробки великих обсягів даних.

Juniper Networks SRX — це рішення для забезпечення захисту мережі та запобігання загрозам, яке пропонує потужні функції брандмауера, *VPN, IPS* та інших функцій для підприємств різного масштабу. *SRX* забезпечує гнучкий контроль за трафіком та виявлення загроз у реальному часі.

Переваги: *Juniper SRX* пропонує високу пропускну здатність, що робить його підходящим для великих організацій з великим обсягом трафіку. Легко інтегрується з іншими продуктами Juniper, такими як мережеві маршрутизатори та комутатори. Підходить для розширення з обмеженою необхідністю в оновленнях і додаткових ресурсах. Включає функціонал *IPS*, захист від атак, *VPN* та інші функції для запобігання загрозам.

Недоліки *Juniper SRX*: для оптимального використання потрібен досвід адміністрування мереж і систем безпеки. Як і інші продукти високого класу, *Juniper SRX* може бути дорогим для малих компаній. Інтерфейс управління не завжди є інтуїтивно зрозумілим для нових користувачів, що вимагає додаткового навчання.

Trustwave SIEM — це система для управління інформаційною безпекою та подіями (SIEM), що надає підприємствам інструменти для збору, аналізу та реагування на події безпеки в реальному часі. Вона включає в себе автоматизовані інструменти для виявлення загроз, моніторингу інцидентів та комплексного аналізу безпеки для великих і середніх компаній.

Переваги: *Trustwave SIEM* включає в себе ефективні функції аналізу та виявлення складних загроз за допомогою кореляційних правил і інтеграції з іншими системами безпеки. Має зручний інтерфейс для моніторингу подій безпеки і управління інцидентами, що полегшує користування. Платформа може інтегруватися з іншими продуктами безпеки для створення єдиної архітектури управління безпекою. Підходить як для малих, так і для великих підприємств завдяки своїй здатності масштабуватися.

Недоліки: Платформа може бути дорогим рішенням для малих та середніх підприємств, особливо через ліцензійні збори та витрати на впровадження. Для роботи *Trustwave SIEM* потрібні значні обчислювальні ресурси, що може бути проблемою для деяких організацій. Інтеграція та налаштування потребують часу та досвіду, щоб ефективно використовувати всі можливості платформи.

SIEMonster — це потужне рішення з відкритим вихідним кодом для управління інформаційною безпекою та подіями, яке надає підприємствам можливість реалізувати рішення *SIEM* на основі кращих інструментів відкритого коду. Це система для збору, аналізу та кореляції даних безпеки з усіх джерел для виявлення загроз і запобігання атакам.

Переваги: *SIEMonster* є платформою з відкритим кодом, що дає можливість повної кастомізації і розширення під специфічні вимоги. Легко інтегрується з іншими системами безпеки та використовує інструменти, як-то *ElasticSearch, Apache Kafka* та інші популярні рішення. Ідеально підходить для організацій, які шукають гнучку та масштабовану платформу для управління безпекою. Можливість безкоштовного використання основних функцій може бути дуже корисною для малих підприємств.

Недоліки: Інтерфейс і налаштування вимагають певних технічних навичок для правильного використання та інтеграції. Оскільки це продукт з відкритим кодом, офіційна підтримка обмежена, що може бути проблемою для деяких компаній. Для великих обсягів даних і високої продуктивності потрібно досить потужне обладнання та налаштування.

Fortinet FortiGate IPS — це система виявлення та запобігання вторгненням (IPS), яка є частиною брандмауерів *FortiGate*. Вона забезпечує захист від атак в реальному часі, виявляючи та блокуючи загрози на рівні мережі та додатків, використовуючи як сигнатурні, так і аномальні методи виявлення.

Переваги: *FortiGate IPS* забезпечує високопродуктивний захист, не впливаючи на швидкість роботи мережі. Продукт чудово інтегрується з іншими рішеннями від *Fortinet* для створення єдиного рішення безпеки. Завдяки зручному інтерфейсу та зручній системі налаштувань, *IPS* можна швидко налаштувати і розгорнути. *FortiGate IPS* здатен блокувати широкий спектр загроз, включаючи відомі віруси, експлойти, та атаки типу *DoS*.

Недоліки: для малого та середнього бізнесу ціна на *FortiGate IPS* може бути високою, особливо коли мова йде про масштабовані рішення. У порівнянні з іншими більш гнучкими рішеннями, *FortiGate IPS* може мати обмежені можливості для детального налаштування та адаптації під специфічні потреби. Хоча *FortiGate IPS* пропонує потужний захист, окремі *IPS*-рішення можуть мати більше спеціалізованих функцій для складних загроз.

Blue Coat ProxySG — це потужне апаратно-програмний рішення для забезпечення безпеки веб-трафіку і контролю за доступом до Інтернету. Воно надає функції проксі-сервера, фільтрації контенту, захисту від загроз і оптимізації мережевого трафіку. *ProxySG* дозволяє організаціям контролювати і аналізувати трафік для покращення продуктивності та безпеки.

Переваги: *Blue Coat ProxySG* використовує передові методи для фільтрації веб-контенту, що дозволяє блокувати небажані або шкідливі ресурси. Пропонує вбудовані функції для виявлення та блокування загроз, таких як шкідливі сайти, віруси та інші кіберзагрози. Дозволяє знижувати

затримки і покращувати продуктивність мережі шляхом кешування і оптимізації трафіку. Підтримка *SSL/TLS: ProxySG* може аналізувати зашифрований трафік *SSL/TLS*, що допомагає виявляти приховані загрози, які йдуть через зашифровані канали.

Недоліки: для малих і середніх організацій ціна може бути значною через дорогі ліцензії та апаратні вимоги. Для налаштування і керування потрібні значні технічні ресурси, особливо для великих підприємств. Через велику кількість функцій та складність налаштувань, продукт може бути занадто комплексним для малих компаній без спеціалізованих IT-ресурсів.

EventTracker — це рішення *SIEM*, яке надає можливість централізованого збору, моніторингу та аналізу журналів подій і інформації про загрози в реальному часі. *EventTracker* дозволяє організаціям автоматично виявляти загрози, генерувати звіти та реагувати на інциденти безпеки.

Переваги: *EventTracker* автоматично виявляє загрози та дозволяє оперативно реагувати на них, знижуючи час між виявленням і реагуванням. Система може інтегруватися з численними джерелами подій та безпеки, що забезпечує комплексний підхід до моніторингу. Простий у використанні інтерфейс з можливістю налаштування дашбордів і звітів за потребами. Система підтримує інтеграцію з багатьма сторонніми продуктами та сервісами для створення комплексних рішень.

Недоліки: для ефективної роботи *EventTracker* потрібні значні обчислювальні потужності, особливо при великій кількості даних. Хоча інтерфейс є інтуїтивно зрозумілим, налаштування і конфігурація можуть вимагати спеціалізованих знань у галузі безпеки. Вартість рішень може бути високою для організацій з обмеженим бюджетом, що може обмежити їх використання для малих компаній.

NetFlow Analyzer — це система для моніторингу мережевого трафіку, яка допомагає виявляти та аналізувати мережеві потоки для виявлення аномалій, атак і забезпечення ефективності роботи мережі. Вона використовує технології *NetFlow, sFlow* та *IPFIX* для збору та аналізу даних про мережевий трафік.

Переваги: *NetFlow Analyzer* дозволяє виявляти і відстежувати мережевий трафік в реальному часі, що допомагає швидко реагувати на потенційні загрози. Це ПЗ надає можливість створювати детальні графіки та звіти для кращого розуміння мережевого трафіку та його аномалій. Може інтегруватися з іншими інструментами безпеки для створення єдиної стратегії моніторингу та виявлення загроз. Підходить для організацій з великими мережами, що дозволяє аналізувати великий потік даних без втрати продуктивності.

Недоліки: потрібні потужні сервери для збору та обробки великого обсягу даних, що може бути проблемою для невеликих організацій. Якщо мережа невелика, функціональність продукту може бути надмірною для потреб таких організацій. *NetFlow Analyzer* може бути дорогим для малих компаній, зокрема з врахуванням ліцензійних зборів та необхідних апаратних ресурсів для роботи.

WatchGuard IPS — це *IPS*, яка є частиною комплексних рішень з безпеки, що пропонує широкі можливості для виявлення і нейтралізації загроз в реальному часі. Вона інтегрується з іншими рішеннями *WatchGuard*, зокрема з брандмауерами та системами безпеки в мережі.

Переваги: *WatchGuard IPS* добре працює в комбінації з іншими рішеннями від *WatchGuard*, забезпечуючи централізовану безпеку для організацій. Платформа включає в себе не тільки *IDS/IPS*, але й підтримку *VPN*, фільтрацію трафіку, захист від *DDoS* атак і багато іншого. Система має інтуїтивно зрозумілий інтерфейс для моніторингу і управління безпекою, що робить її доступною для адміністраторів без високої кваліфікації. Вбудовані інструменти аналітики дозволяють детально відслідковувати події і потенційні загрози.

Недоліки *WatchGuard IPS*: lля великих компаній із великим обсягом трафіку може бути необхідно додаткове налаштування або використання більш потужних рішень для забезпечення належного рівня захисту. Як і багато систем *IPS, WatchGuard* може генерувати фальшиві позитивні спрацьовування, що вимагає додаткових налаштувань. Хоча система підтримує деякі зовнішні рішення, її інтеграція з іншими системами безпеки не завжди є гладкою, особливо якщо це специфічні платформи.

Huawei FusionSphere Cloud IDS — це *IDS*, яка інтегрується в хмарні середовища для забезпечення безпеки даних і інфраструктури в реальному часі. Ця система використовується для моніторингу та аналізу трафіку в хмарних середовищах, щоб виявляти аномалії та зловмисну активність.

Переваги: *Huawei FusionSphere Cloud IDS* призначена для роботи з сучасними хмарними інфраструктурами, що забезпечує високий рівень безпеки для хмарних додатків і даних. Система розроблена для масштабування під потреби великих і середніх організацій, що робить її придатною для компаній, що використовують хмарні технології. Використовує сучасні методи для виявлення та запобігання загроз, таких як аналіз аномалій та сигнатур. Автоматичне виявлення та реагування на інциденти безпеки забезпечує швидке реагування і мінімізує людський фактор.

Недоліки: для ефективного використання *Huawei FusionSphere Cloud IDS* потрібні досвідчені фахівці з налаштування та адміністрування хмарних середовищ, що може бути складно для менш підготовлених команд. Це рішення оптимізовано для використання з інфраструктурою *Huawei*, що може обмежити його застосування для користувачів інших платформ. Як і багато інших спеціалізованих рішень для хмарних середовищ, ціна може бути високою, що може стати обмеженням для малих підприємств.

Sumo Logic — це платформа для збору, аналізу і візуалізації великих обсягів даних із журналів, що дозволяє організаціям моніторити свої системи, аналізувати загрози та отримувати цінні аналітичні дані для покращення безпеки. Платформа підтримує хмарну інфраструктуру і забезпечує можливість моніторингу додатків, хмарних середовищ та великих мереж.

Переваги: *Sumo Logic* пропонує хмарну архітектуру, що дозволяє легко масштабувати ресурси в залежності від потреб компанії без необхідності у великих капітальних витратах. Платформа підтримує інтеграцію з численними джерелами, включаючи мережеві пристрої, сервери, додатки і т.д., що дозволяє здійснювати моніторинг у реальному часі. Використовує алгоритми машинного навчання для автоматичного виявлення аномалій та потенційних загроз, що

підвищує точність виявлення. Програмне забезпечення має інтуїтивно зрозумілий інтерфейс і можливості для створення кастомізованих дашбордів і звітів.

Недоліки: Як хмарна платформа, *Sumo Logic* повністю залежить від стабільності і швидкості Інтернет-з'єднання. Для малих і середніх організацій ціна може бути високою, оскільки розрахунки базуються на обсязі зібраних даних. Для отримання найкращих результатів від платформи потрібно великі обсяги даних, що може бути проблемою для менших організацій.

ArcSight — це потужна платформа для *SIEM*, яка надає організаціям можливість централізовано збирати, аналізувати та реагувати на події в реальному часі. *ArcSight* забезпечує безпеку за рахунок потужного збору даних і гнучких можливостей налаштування звітів і автоматизації процесів реагування на інциденти.

Переваги: *ArcSight* забезпечує централізоване управління всіма подіями безпеки, що дозволяє зменшити ризики для організації завдяки швидкому виявленню загроз. Платформа може працювати як для малих, так і для великих організацій, оскільки її можна налаштовувати та масштабувати в залежності від потреб бізнесу. *ArcSight* підтримує інтеграцію з численними пристроями та додатками, що дозволяє отримати комплексний погляд на безпеку всієї організації. Система дозволяє автоматично реагувати на інциденти безпеки, скорочуючи час між виявленням загрози та її усуненням.

Недоліки: для оптимальної роботи *ArcSight* потрібні потужні сервери та великий обсяг пам'яті, що може бути дорогим для малих компаній. *ArcSight* може бути складним у налаштуванні і вимагає кваліфікованих фахівців для ефективного використання. Це рішення може бути дорогим для невеликих і середніх організацій через високу вартість ліцензій та підтримки.

Trend Micro Deep Discovery — це система для виявлення і запобігання складним загрозам, яка використовує потужні методи аналізу в реальному часі, щоб виявляти та нейтралізувати загрози на ранніх етапах. Вона спеціалізується на аналізі мережевого трафіку, виявленні аномалій, експлойтів та іншої шкідливої активності.

Переваги: Система здатна проводити глибокий аналіз як вхідного, так і вихідного трафіку для виявлення складних загроз, таких як екзотичні експлойти та *zero-day* атаки. *Trend Micro Deep Discovery* забезпечує комплексний підхід до безпеки, комбінуючи можливості аналізу мережі і кінцевих точок. Використовує передові алгоритми для автоматичного виявлення аномалій і потенційно небезпечної поведінки. Платформа добре інтегрується з іншими рішеннями *Trend Micro*, такими як *Endpoint Protection* і *XDR (Extended Detection and Response*).

Недоліки: *Trend Micro Deep Discovery* може бути дорогим для малих і середніх підприємств, особливо з урахуванням додаткових ліцензій на інтеграцію з іншими рішеннями. Система має вимоги до потужних апаратних ресурсів для ефективної роботи, що може бути проблемою для компаній з обмеженими бюджетами. Хоча система надає багатий набір функцій, інтерфейс може здатися складним для користувачів, які не мають досвіду в управлінні безпековими продуктами.

Vectra AI — це платформа для виявлення загроз на основі штучного інтелекту, яка використовує машинне навчання для аналізу трафіку і виявлення аномалій в мережі. *Vectra AI* здатна виявляти загрози в реальному часі, навіть якщо зловмисники використовують приховані методи атак.

Переваги: Використовує передові алгоритми машинного навчання для виявлення аномальних патернів в мережевому трафіку, що дозволяє швидко і точно виявляти нові та невідомі загрози. *Vectra AI* може автоматично реагувати на загрози, що дозволяє зменшити час реакції на інциденти безпеки. Платформа надає високий рівень точності, зменшуючи кількість фальшивих позитивних спрацьовувань. *Vectra AI* призначена для великих організацій і має можливість масштабуватися в залежності від потреб підприємства.

Недоліки: Вартість рішення може бути досить високою, що обмежує його доступність для малих і середніх підприємств. Платформа ефективно працює лише в умовах великого потоку даних, що може бути проблемою для організацій з обмеженими ресурсами. Для повноцінного використання та

налаштування системи потрібні фахівці з досвідом в області кібербезпеки та машинного навчання.

FireEye Network Security — це система *IDS/IPS*, яка використовує інноваційні методи аналізу для виявлення та захисту від сучасних кіберзагроз, зокрема *APT* (англ. *Advanced Persistent Threats*) та складних атак. *FireEye Network Security* є частиною інтегрованого портфеля рішень компанії *FireEye* для захисту від загроз в мережі.

Переваги: Використовує інноваційні методи, включаючи аналіз з використанням пісочниць (sandboxing) для виявлення нових та складних загроз, таких як *APT*. Легко інтегрується з іншими продуктами *FireEye*, такими як платформою для моніторингу безпеки (*Helix*), що дозволяє створювати єдину екосистему для управління безпекою. Платформа підтримує автоматизоване реагування на загрози в реальному часі, що дозволяє швидко нейтралізувати загрози. Гнучкість та масштабованість: Підходить як для малих компаній, так і для великих організацій з різними потребами в безпеці.

Недоліки: *FireEye Network Security* — одне з найдорожчих рішень на ринку, що може бути проблемою для малих та середніх підприємств. Платформа потребує великих обчислювальних потужностей для ефективної роботи, що може бути недоліком для компаній з обмеженими ресурсами. Для повноцінної експлуатації системи потрібен досвідченіший персонал, оскільки налаштування може бути складним.

Zabbix — це рішення з моніторингу мереж, серверів і додатків, яке широко використовується для виявлення аномалій і порушень в інфраструктурі IT. *Zabbix* надає велику кількість інструментів для збору даних, аналітики та управління подіями, що дозволяє здійснювати цілісне спостереження за здоров’ям мережі і серверів.

Переваги: *Zabbix* є безкоштовним, що робить його доступним для організацій будь-якого розміру. Висока налаштовуваність дозволяє інтегрувати *Zabbix* з іншими інструментами та системами. Платформа підтримує моніторинг різноманітних типів обладнання і ПЗ, включаючи сервери, мережі

та додатки. *Zabbix* підходить як для малих, так і для великих компаній, дозволяючи масштабувати систему залежно від потреб бізнесу.

Недоліки: *Zabbix* вимагає значного досвіду для налаштування та ефективного використання, особливо в складних середовищах. Обмежені можливості для виявлення загроз: В основному орієнтований на моніторинг, а не на активний захист або реагування на кіберзагрози. Для отримання більш глибокої аналітики або спеціалізованих функцій можуть знадобитись додаткові модулі або інтеграція з іншими рішеннями.

CrowdStrike Falcon — це платформа для виявлення та реагування на кінцевих точках (*EDR*), яка використовує штучний інтелект і машинне навчання для виявлення і нейтралізації загроз в реальному часі. *Falcon* забезпечує захист від всіх типів шкідливих програм, в тому числі від складних загроз типу *APT*, і дозволяє здійснювати постійний моніторинг та аналіз.

Переваги: Використовує передові технології машинного навчання для виявлення нових і невідомих загроз без потреби в постійному оновленні підписів. Забезпечує постійний моніторинг всіх кінцевих точок та можливість миттєвого реагування на загрози. *Falcon* забезпечує низький рівень фальшивих спрацьовувань, що дозволяє зменшити кількість помилок в процесі виявлення загроз. Платформа легко інтегрується з іншими рішеннями для забезпечення комплексної безпеки.

Недоліки: Платформа є однією з найдорожчих на ринку, що може бути обмеженням для малих організацій. *CrowdStrike Falcon* вимагає підключення до хмарних сервісів, що може бути проблемою для компаній з високими вимогами до конфіденційності даних. Хоча система надає потужні можливості для професіоналів з кібербезпеки, її інтерфейс може бути важким для новачків або недосвідчених адміністраторів.

Dynatrace — це інтелектуальна платформа моніторингу продуктивності програм, яка забезпечує аналіз інфраструктури, додатків та кінцевих користувачів за допомогою автоматизованого моніторингу в реальному часі.

Вона використовує штучний інтелект для глибокого аналізу та надання інсайтів у разі виявлення проблем або аномалій.

Переваги: *Dynatrace* добре інтегрується з хмарними платформами, такими як *AWS, Azure* та *Google Cloud*, що дозволяє здійснювати ефективний моніторинг і аналітику в мультихмарних середовищах. Платформа пропонує автоматичне виявлення аномалій і аналізу даних у реальному часі, що дозволяє вчасно виявляти потенційні проблеми. *Dynatrace* використовує штучний інтелект для виявлення причин проблем та надання рекомендацій для їх усунення. Підходить для підприємств різного розміру завдяки своїй здатності масштабуватися без шкоди для продуктивності.

Недоліки: вартість *Dynatrace* може бути значною для малих і середніх підприємств, що обмежує її використання в таких середовищах. Платформа може вимагати досвідченого персоналу для повноцінного налаштування та оптимізації. Залежність від підключення до інтернету: *Dynatrace* працює в основному через хмару, тому відсутність інтернет-з'єднання може обмежити її функціональність.

Symantec Endpoint Protection — це рішення для забезпечення безпеки кінцевих точок, яке включає в себе антивірусний захист, виявлення та запобігання вторгненням, захист від шкідливих програм, моніторинг поведінки та захист від фішингу. Рішення пропонує комплексний підхід до захисту кінцевих точок від широкого спектру кіберзагроз.

Переваги: міцний антивірусний захист: Використовує багатошарову систему захисту, яка включає традиційні сигнатурні методи і новітні технології для виявлення нових загроз. Запобігання вторгненням та виявлення шкідливих програм: Платформа забезпечує захист від шкідливих програм і кібератак, таких як експлойти і зловмисне ПЗ. Підтримка багатьох операційних систем: *Symantec Endpoint Protection* підтримує операційні системи *Windows, macOS, Linux*, а також мобільні платформи, що дозволяє покривати широкий спектр пристроїв. Дозволяє централізовано керувати політиками безпеки для великої кількості кінцевих точок з одного інтерфейсу.

Недоліки: *Symantec Endpoint Protection* може споживати значні ресурси на пристроях, що може уповільнювати роботу старих або малопотужних комп'ютерів. Налаштування та адміністрування платформи може бути складним для недосвідчених користувачів. Висока вартість ліцензій обмежує доступність продукту для малих підприємств.

AlienVault USM (англ. *Unified Security Management*) — це платформа для керування безпекою, яка об'єднує різні функціональні можливості, такі як моніторинг безпеки, виявлення загроз, управління подіями та інцидентами (*SIEM*), виявлення аномалій та аналіз подій. Вона включає у себе розширену базу даних про загрози та використання функцій автоматичного реагування.

Переваги: єдине рішення для *SIEM* та управління подіями. *AlienVault USM* об'єднує функціональність *SIEM*, виявлення загроз та управління інцидентами, що знижує складність управління безпекою. Платформа постійно оновлюється з базою даних про загрози, що дозволяє користувачам швидко реагувати на нові кіберзагрози. *AlienVault USM* пропонує просте налаштування і може бути швидко розгорнуто в середовищах малого та середнього бізнесу. Інтеграція з іншими рішеннями: Платформа підтримує інтеграцію з іншими продуктами безпеки, що дозволяє створювати більш ефективні системи захисту.

Недоліки: платформа може бути менш ефективною для дуже великих організацій з високими вимогами до обробки даних і масштабованості. Залежність від хмарних рішень: Хоча є можливість локальної установки, багато функцій найкраще працюють у хмарному середовищі, що може бути проблемою для деяких організацій з суворими вимогами до конфіденційності. Деякі користувачі вважають, що система може бути обмежена в налаштуваннях для більш складних або спеціалізованих інфраструктур.

Nmap (англ. *Network Mapper*) — це потужний інструмент для сканування мереж, який дозволяє здійснювати виявлення хостів, визначати відкриті порти, перевіряти вразливості мережі та аналізувати інформацію про мережеві сервіси. *Nmap* підтримує різноманітні методи сканування, включаючи *TCP, UDP* і сканування за допомогою скриптів (*NSE*).

Переваги: *Nmap* підтримує різноманітні варіанти сканування, дозволяючи здійснювати детальний аналіз мережі за допомогою різних протоколів і методів. *Nmap* є безкоштовним і з відкритим кодом, що дозволяє розширювати його функціональність та інтегрувати в інші системи. Окрім стандартного TCP/IP, Nmap може працювати з безліччю інших протоколів і служить для глибокого аналізу мережевих інтерфейсів. Широка підтримка платформ: *Nmap* працює на багатьох операційних системах, включаючи *Linux, Windows* і *macOS*.

Недоліки: відсутність інтегрованої підтримки для багатьох функцій безпеки. *Nmap* в основному фокусується на скануванні та виявленні вразливостей, і не включає інші важливі функції, такі як моніторинг і аналіз поведінки мережі. Може бути заблокованим: Оскільки *Nmap* може бути використаний для сканування чужих мереж, багато мережевих адміністраторів блокують його використання через безпекові заходи. Складність у налаштуванні для початківців: Для нових користувачів може бути складним освоєння всіх функцій і параметрів *Nmap*.

Wazuh — це платформа для *SIEM*, яка забезпечує моніторинг подій, виявлення аномалій, аналіз безпеки та реагування на інциденти. *Wazuh* є розширенням *OSSEC* і поєднує в собі багато функцій для захисту інфраструктури в реальному часі. Вона підтримує багатофункціональне управління політиками безпеки та інтеграцію з іншими інструментами безпеки.

Переваги: *Wazuh* — це рішення з відкритим кодом, що дозволяє використовувати його безкоштовно та налаштовувати згідно з індивідуальними потребами. *Wazuh* підтримує інтеграцію з іншими *SIEM*-системами, такими як Elastic Stack, що дозволяє створювати більш потужні рішення. Платформа надає потужні інструменти для виявлення аномалій та невідповідностей, що допомагає ідентифікувати потенційні загрози. *Wazuh* підтримує *Linux, Windows, macOS*, а також інші ОС, що дозволяє застосовувати його в різноманітних середовищах.

Недоліки: Для належної роботи *Wazuh* необхідна потужна інфраструктура та значні ресурси для обробки та аналізу великих обсягів даних. Платформа має складний процес налаштування та потребує знань у сфері кібербезпеки для

ефективного використання. Для малих компаній *Wazuh* може бути занадто складним і вимагати великих витрат на обслуговування та підтримку.

Palo Alto Networks Cortex XDR — це платформа для розширеного виявлення та реагування (*XDR*), яка об'єднує дані з різних точок мережі, кінцевих точок і хмарних середовищ для забезпечення всебічного захисту від загроз. Вона використовує штучний інтелект та машинне навчання для аналізу і виявлення складних загроз та аномалій.

Переваги: *Cortex XDR* підтримує інтеграцію з іншими продуктами *Palo Alto,* що дозволяє створювати єдину екосистему для управління безпекою. Платформа використовує передові методи аналізу, включаючи машинне навчання, для виявлення навіть найскладніших і непомітних загроз. *Cortex XDR* надає можливість автоматизованого реагування на інциденти, знижуючи час реагування на загрози. Система може масштабуватися для великих корпоративних середовищ і адаптуватися до змінюваних вимог безпеки.

Недоліки: *Cortex XDR* є преміальним продуктом з високими витратами, що робить його менш доступним для малих і середніх підприємств. Для повного використання потенціалу *Cortex XDR* потрібно достатньо досвіду в налаштуванні систем безпеки. Платформа для оптимальної роботи потребує потужної інфраструктури і ресурсів для обробки великих обсягів даних.

Malwarebytes Endpoint Protection — це рішення для захисту кінцевих точок, яке забезпечує виявлення і видалення шкідливих програм, вірусів, троянів та інших загроз на комп'ютерах, мобільних пристроях та серверних системах. *Malwarebytes* використовує гібридні методи захисту, що поєднують традиційні сигнатури та методи машинного навчання для виявлення нових загроз.

Переваги: використовує різноманітні методи виявлення, такі як сигнатурне виявлення, поведінковий аналіз та машинне навчання, що дозволяє виявляти нові та невідомі загрози. Має хорошу репутацію в боротьбі з шкідливими програмами, зокрема для виявлення та видалення вірусів і троянів. Легкість у використанні: Зрозумілий інтерфейс та простота налаштування роблять продукт доступним для малих і середніх підприємств. Реальне

реагування на загрози: Платформа надає можливість для оперативного реагування на загрози, включаючи автоматичне усунення знайдених проблем.

Недоліки: хоча *Malwarebytes* є ефективним для індивідуальних користувачів та малих компаній, його можливості для великих організацій можуть бути обмеженими. Під час сканування система може бути досить вимогливою до ресурсів, що може впливати на продуктивність пристроїв, особливо в великих корпоративних середовищах. Хоча продукт має базові можливості інтеграції, він не надає такого рівня гнучкості в порівнянні з іншими корпоративними рішеннями з управління безпекою.

ESET NOD32 Network Detection є частиною антивірусного рішення *ESET*, спеціалізується на виявленні та нейтралізації загроз, пов'язаних з мережевим трафіком. Цей інструмент активно використовує машинне навчання та інтелектуальний аналіз для виявлення аномалій і загроз на рівні мережі, при цьому пропонує потужні функції для захисту від шкідливих програм, експлойтів і несанкціонованого доступу.

Переваги: використовує алгоритми для автоматичного виявлення аномалій у мережевому трафіку, що допомагає оперативно ідентифікувати можливі загрози. Містить зрозумілий інтерфейс, що полегшує адміністрування та налаштування системи, навіть для користувачів без глибоких знань в області безпеки. *ESET NOD32* добре оптимізований, тому має мінімальний вплив на продуктивність пристроїв і систем. Поєднує в собі захист від мережевих атак та шкідливих програм, що дозволяє виявляти широкий спектр загроз.

Недоліки: порівняно з іншими більш універсальними рішеннями, *ESET NOD32* може мати обмежену інтеграцію з іншими інструментами для забезпечення повного захисту інфраструктури. У великих підприємствах або при високих вимогах до безпеки, може не вистачати гнучкості в налаштуваннях і можливостей для інтеграції з іншими рішеннями. Як і багато інших традиційних антивірусних програм, може бути менш ефективним у виявленні нових або нульових загроз, які ще не є в базах даних сигнатур.

OpenVAS (англ. *Open Vulnerability Assessment System*) є популярною системою для виявлення вразливостей з відкритим кодом. Вона забезпечує комплексний підхід до сканування безпеки, дозволяючи перевіряти різноманітні системи на наявність уразливостей і дефектів. *OpenVAS* активно використовує велику базу плагінів для виявлення вразливих місць у програмному забезпеченні, мережевому обладнанні та серверах.

Переваги: *OpenVAS* є безкоштовним і відкритим для використання, що робить його доступним для малих і середніх компаній. Містить велику кількість плагінів для перевірки різних типів вразливостей, що забезпечує високу гнучкість і можливість налаштування під конкретні потреби. Підходить для використання як в малих, так і в великих підприємствах, і може бути налаштований для регулярних сканувань великих мереж. *OpenVAS* підтримує різноманітні стандарти для сканування вразливостей, що дозволяє використовувати систему у різноманітних середовищах.

Недоліки: для не досвідчених користувачів налаштування *OpenVAS* може бути складним, і багато часу може знадобитися на конфігурацію і підтримку системи. Хоча *OpenVAS* підтримує різні плагіни і інтеграцію з іншими інструментами, він не завжди має безперебійну сумісність з більш складними інфраструктурами безпеки. Велика кількість помилкових спрацьовувань: В деяких випадках *OpenVAS* може генерувати великі кількості помилкових спрацьовувань, що може ускладнювати аналіз результатів сканування.

Cybereason Endpoint Detection and Response (*EDR*) є потужною платформою для виявлення та реагування на загрози на кінцевих точках, яка використовує передові методи для аналізу і виявлення шкідливих дій в реальному часі. Ця система поєднує в собі виявлення аномалій, аналіз поведінки та інтелектуальний пошук загроз, щоб запобігти серйозним інцидентам безпеки.

Переваги: використовує машинне навчання та штучний інтелект для автоматичного виявлення нових загроз на основі аналізу поведінки та аномалій. *Cybereason* надає можливість миттєво реагувати на загрози, що дозволяє

швидко нейтралізувати потенційні ризики без великих витрат часу. Проста та інтуїтивно зрозуміла платформа, яка дозволяє користувачам швидко орієнтуватися у даних і швидко приймати необхідні дії. Масштабованість та гнучкість: Підходить для малих, середніх та великих підприємств, що дозволяє масштабувати рішення відповідно до потреб компанії.

Недоліки: *Cybereason* є преміум-рішенням, що робить його дорогим для малих і середніх організацій. Потребує обробки великої кількості даних: Через інтеграцію з великими масивами даних може вимагати значних ресурсів для обробки та зберігання інформації. Як і інші *EDR*-рішення, *Cybereason* може іноді генерувати помилкові спрацьовування, що потребує додаткових зусиль для перевірки і підтвердження загроз.

Результати порівняльного аналізу СВВ за властивостями, що є їх класифікаційними критеріями, які визначені в п.2.1 даної кваліфікаційної роботи, наведені в табл.2.1.

2.3 Недоліки сучасних систем виявлення вторгнень та перспективи вдосконалення

Системи виявлення вторгнень (СВВ), поряд із перевагами, мають і низку недоліків, які можна розділити на три основні групи:

1) недоліки, зумовлені впливом середовища функціонування. Наприклад, «шумність» мережі, викликана некоректними або викривленими пакетами даних, може значно збільшити кількість хибних тривог. Це ускладнює виявлення реальних атак і може бути використано зловмисниками для обходу системи;

2) недоліки організації проектування. Сюди відноситься відсутність універсальної методології проектування, складність оперативного оновлення бази даних сигнатур нових типів атак і проблеми з підтримкою наборів правил функціонування системи. Крім того, існує недостатній рівень тестування ефективності та покриття мережі;

Таблиця 2.1 - – Результати порівняння систем виявлення вторгнень за класифікаційними властивостями

№	СВВ	Критерії																								
		Функціональні					Проектні																Експлуатаційні				
		Клас кібератак		Активна реакція на кібератаку	Рівень спостереження		Методи виявлення												Підтримка операційних систем				Адаптивність	Масштабованість	Захищеність	Управління системою	
		Зловживання	Аномалії		Системний	Мережевий	Відкритість	Експертний	Статистичний	Сигнатурний	Графи сценаріїв	Контроль зміни подій	Кластерний	Динамічний.	Машинного навчання	Поведінковий	Евристичний	Нечітких множин	Unix	Linux	Windows	MacOS				Централізоване	Розподілене
1	*AAFID*	+	+	-	+	-	+	+	-	+	-	-	-	-	-	-	-	-	+	+	-	-	-	+	-	+	-
2	*Snort*	+	+	+	-	+	+	-	+	+	-	-	-	-	-	-	-	-	+	+	+	-	-	+	+	+	-
3	*Prelude SEIM*	+	+	+	-	+	+	-	-	+	-	-	-	-	-	-	-	-	+	+	-	-	-	+	+	+	-
4	*NetSTAT*	+	+	+	+	+	+	-	-	+	-	+	-	-	-	-	-	-	+	+	-	-	+	+	+	-	+
5	*Shadow*	+	+	-	-	+	-	-	-	-	-	+	-	-	-	-	-	-	+	+	-	-	-	+	+	-	+
6	*ASAX*	+	-	-	+	-	+	+	-	-	-	-	-	-	-	-	-	-	+	+	-	-	-	+	-	+	-
7	*Bro*	+	+	+	-	+	+	-	-	+	-	-	-	-	-	-	-	-	+	+	-	+	-	-	-	+	-
8	*OSSEC*	+	+	+	+	-	+	-	-	+	-	-	-	-	-	-	-	-	+	+	+	+	-	+	+	+	+
9	*Cisco IPS*	+	+	+	+	+	-	-	+	+	-	-	+	-	-	-	-	-	+	+	+	-	+	+	+	+	+
10	*Arbor Networks Spectrum*	+	+	+	+	+	-	-	+	+	-	-	-	+	-	-	-	-	+	+	+	-	+	+	-	+	-
11	*InfoWatch ASAP*	+	+	-	+	+	-	-	+	+	-	-	-	-	-	-	-	-	+	+	+	+	+	+	-	+	-

Продовження таблиці 2.1

№	СВВ	Критерії																										
		Функціональні					Проектні																		Експлуатаційні				
		Клас кібератак		Активна реакція на кібератаку	Рівень спостереження		Відкритість	Методи виявлення											Підтримка операційних систем				Адаптивність	Масштабованість	Захищеність	Управління системою	
		Зловживання	Аномалії		Системний	Мережевий		Експертний	Статистичний	Сигнатурний	Графи сценаріїв	Контроль зміни подій	Кластерний	Динамічний.	Машинного навчання	Поведінковий	Евристичний	Нечітких множин	Unix	Linux	Windows	MacOS				Централізоване	Розподілене
12	*Symantec DeepSight Threat Management System*	+	+	+	+	+	-	+	+	+	-	-	-	+	+	-	-	-	+	+	+	+	+	+	-	+	+
13	*IPS*	+	+	+	+	+	-	-	+	+	-	-	-	+	-	+	-	-	-	-	+	-	+	+	+	+	-
14	*Tipping Poing NGIPS*	+	+	+	+	+	-	-	-	+	-	-	-	+	+	-	-	-	-	-	+	+	+	+	+	-	+
15	*Axoft invGUARD*	+	+	-	+	+	-	-	+	+	-	-	-	+	-	+	+	-	+	+	-	-	-	+	-	+	-
16	*DefensePro*	+	+	+	-	+	-	-	+	+	-	-	-	-	-	+	-	-	+	+	+	+	+	+	+	+	-
17	*KATA Platform*	+	+	+	+	+	-	-	+	+	-	-	-	+	-	+	-	-	+	+	+	+	+	+	+	-	+
18	*Suricata*	+	+	+	-	+	+	-	+	+	-	-	-	-	-	-	-	-	+	+	+	+	+	+	-	+	-
19	*Samhain*	+	+	+	+	-	+	-	+	-	-	-	-	+	-	+	-	-	+	+	+	+	+	+	+	+	+

Продовження таблиці 2.1

№	СВВ	Критерії																										
		Функціональні					Проектні																		Експлуатаційні				
		Клас кібератак		Активна реакція на кібератаку	Рівень спостереження		Методи виявлення												Підтримка операційних систем				Адаптивність	Масштабованість	Захищеність	Управління системою	
		Зловживання	Аномалії		Системний	Мережевий	Відкритість	Експертний	Статистичний	Сигнатурний	Графи сценаріїв	Контроль зміни подій	Кластерний	Динамічний.	Машинного навчання	Поведінковий	Евристичний	Нечітких множин	Unix	Linux	Windows	MacOS				Централізоване	Розподілене
20	*Security Onion*	+	+	+	+	+	+	-	+	+	-	+	-	+	-	+	-	-	+	+	-	-	+	+	-	+	+
21	*SolarWinds Security Event Manager*	-	+	+	+	+	-	+	+	-	-	-	-	-	-	-	-	-	-	-	+	-	+	+	+	+	-
22	Splunk	-	+	-	+	_	-	+	+	-	-	-	-	-	+	-	-	-	-	+	+	+	+	+	+	+	-
23	McAfee Network Security Platform	+	-	+	-	+	-	-	-	+	-	-	-	-	+	+	-	-	-	+	+	-	+	+	+	+	-
24	IBM QRadar	+	+	+	+	+	-	+	+	-	-	-	-	-	+	-	-	-	-	+	-	-	+	+	+	+	-
25	Check Point Security Management	+	-	+	-	+	-	-	-	+	-	-	-	-	-	+	+	-	-	+	-	-	+	+	+	+	-
26	AlienVault OSSIM	+	+	+	+	+	+	+	-	+	-	+	-	-	-	-	-	-	-	+	-	-	+	+	+	+	-
27	LogRhythm	-	+	+	+	-	-	+	+	-	-	-	-	-	+	-	-	-	-	+	+	-	+	+	+	+	-

Продовження таблиці 2.1

№	СВВ	Критерії																										
		Функціональні					Проектні																		Експлуатаційні				
		Клас кібератак		Активна реакція на кібератаку	Рівень спостереження		Відкритість	Методи виявлення											Підтримка операційних систем				Адаптивність	Масштабованість	Захищеність	Управління системою	
		Зловживання	Аномалії		Системний	Мережевий		Експертний	Статистичний	Сигнатурний	Графи сценаріїв	Контроль зміни подій	Кластерний	Динамічний.	Машинного навчання	Поведінковий	Евристичний	Нечітких множин	Unix	Linux	Windows	MacOS				Централізоване	Розподілене
28	FortiSIEM	-	+	+	+	+	-	-	+	+	-	-	-	-	+	-	-	-	-	+	+	-	+	+	+	+	-
29	Rapid7 Nexpose	+	-	-	+	-	-	-		+	-	-	-	-	-	-	+	-	-	+	+	-	+	+	+	+	-
30	OpenDXL by McAfee	+	+	+	+	+	+	+	-	-	-	-	-	-	+	-	-	-	-	+	+	-	+	+	+	-	+
31	RSA NetWitness	+	+	+	-	+	-	-	+	+	-	-	-	-	-	+	-	-	-	+	+	-	+	+	+	+	-
32	Palo Alto Networks Threat Prevention	+	-	+	-	+	-	-	-	+	-	-	-	-	+	+	-	-	-	+	+	-	+	+	+	+	-
33	Juniper Networks SRX	+	-	+	-	+	-	-	-	+	-	-	-	-	-	+	-	-	-	+	-	-	+	+	+	+	-
34	Trustwave SIEM	-	+	+	+	+	-	+	+	-	-	-	-	-	-	-	-	-	-	+	+	-	+	+	+	+	-
35	SIEMonster	-	+	+	+	+	+	-	+	-	-	-	-	-	+	-	-	-	-	+	-	-	+	+	+	-	+
36	Fortinet FortiGate IPS	+	-	+	-	+	-	-	-	+	-	-	-	-	-	+	-	-	-	+	+	-	+	+	+	+	-

Продовження таблиці 2.1

№	СВВ	Критерії																										
		Функціональні					Проектні																		Експлуатаційні				
		Клас кібератак		Активна реакція на кібератаку	Рівень спостереження		Відкритість	Методи виявлення											Підтримка операційних систем				Адаптивність	Масштабованість	Захищеність	Управління системою	
		Зловживання	Аномалії		Системний	Мережевий		Експертний	Статистичний	Сигнатурний	Графи сценаріїв	Контроль зміни подій	Кластерний	Динамічний.	Машинного навчання	Поведінковий	Евристичний	Нечітких множин	Unix	Linux	Windows	MacOS				Централізоване	Розподілене
37	Blue Coat ProxySG	+	-	+	-	+	-	+	-	-	-	-	-	-	-	+	-	-	-	+	–	–	-	+	-	+	-
38	EventTracker	-	+	+	+	-	-	-	+	+	-	-	-	-	-	-	-	-	-	-	+	-	+	+	+	+	-
39	NetFlow Analyzer	-	+	-	-	+	-	-	+	-	-	-	+	-	-	-	-	-	-	+	+	-	+	+	-	+	-
40	WatchGuard IPS	+	-	+	-	+	-	-	-	+	-	-	-	-	-	+	-	-	-	+	+	-	+	+	+	+	-
41	Huawei FusionSphere Cloud IDS	-	+	+	-	+	-	-	-	+	-	-	-	-	+	-	-	-	-	+	-	-	+	+	+	+	-
42	Sumo Logic	-	+	+	+	+	-	-	+	-	-	-	-	-	+	-	-	-	-	+	+	-	+	+	+	+	-
43	ArcSight by Micro Focus	-	+	+	+	+	-	+	+	+	-	-	-	-	-	-	-	-	-	+	+	-	+	+	+	+	-
44	Trend Micro Deep Discovery	+	-	+	-	+	-	-	-	+	-	-	-	-	+	+	-	-	-	+	+	-	+	+	+	+	-

Продовження таблиці 2.1

№	СВВ	Критерії																										
		Функціональні					Проектні																		Експлуатаційні				
		Клас кібератак		Активна реакція на кібератаку	Рівень спостереження		Відкритість	Методи виявлення											Підтримка операційних систем				Адаптивність	Масштабованість	Захищеність	Управління системою	
		Зловживання	Аномалії		Системний	Мережевий		Експертний	Статистичний	Сигнатурний	Графи сценаріїв	Контроль зміни подій	Кластерний	Динамічний.	Машинного навчання	Поведінковий	Евристичний	Нечітких множин	Unix	Linux	Windows	MacOS				Централізоване	Розподілене
45	Vectra AI	-	+	+	-	+	-	-	-	-	-	-	-	-	+	+	-	-	-	+	+	-	+	+	+	+	+
46	FireEye Network Security	+	-	+	-	+	-	-	-	+	-	-	-	-	+	+	-	-	-	+	+	-	+	+	+	+	-
47	Zabbix	-	+	+	+	-	+	+	+	-	-	-	-	-	-	-	-	-	-	+	-	-	+	+	-	+	-
48	CrowdStrike Falcon	+	-	+	+	+	-	-	-	-	-	-	-	-	+	+	-	-	-	-	+	+	+	+	+	+	-
49	Dynatrace	-	+	-	+	-	-	-	-	-	-	-	-	-	+	-	+	-	-	+	+	-	+	+	+	+	-
50	Symantec Endpoint Protection	+	-	+	+	-	-	-	-	+	-	-	-	-	-	+	-	-	-	+	+	+	+	+	+	+	-
51	AlienVault USM	+	+	+	+	+	-	+	+	+	-	-	-	-	-	-	-	-	-	+	-	-	+	+	+	+	-
52	Nmap	-	+	-	-	+	+	+	-			+	-	-	-	-	-	-	-	+	+	+	-	+	-	-	+
53	Wazuh	+	+	+	+	+	+	-	-	+	-	+	-	-	-	-	-	-	-	+	+	+	+	+	+	+	-

Продовження таблиці 2.1

№	СВВ	Критерії																										
		Функціональні					Проектні																		Експлуатаційні				
		Клас кібератак		Активна реакція на кібератаку	Рівень спостереження		Методи виявлення														Підтримка операційних систем				Адаптивність	Масштабованість	Захищеність	Управління системою	
		Зловживання	Аномалії		Системний	Мережевий	Відкритість	Експертний	Статистичний	Сигнатурний	Графи сценаріїв	Контроль зміни подій	Кластерний	Динамічний.	Машинного навчання	Поведінковий	Евристичний	Нечітких множин	Unix	Linux	Windows	MacOS				Централізоване	Розподілене
54	Palo Alto Networks Cortex XDR	+	-	+	+	+	-	-	-	-	-	-	-	-	+	+	-	-	-	+	+	+	+	+	+	+	-
55	Suricata IDS	+	+	+	-	+	+	-	+	+	-	-	-	-	-	+	-	-	-	+	+	-	+	+	+	+	-
56	Malwarebytes Endpoint Protection	+	-	+	+	-	-	-	-	+	-	-	-	-	-	+	-	-	-		+	+	+	+	+	+	-
57	Sumo Logic Cloud SIEM	-	+	+	+	+	-	-	+	-	-	-	-	-	+	-	-	-	-	+	+	-	+	+	+	+	-
58	ESET NOD32 Network Detection	-	+	-	-	+	-	-	-	+	-	-	-	-	-	-	+	-	-	+	+	+	+	+	+	+	-
59	OpenVAS	+	-	-	+	-	+	+	-	+	-	-	-	-	-	-	-	-	-	+	-	-	+	+	+	+	-
60	Cybereason EDR	+	-	+	+	-	-	-	-	-	-	-	-	-	+	+	-	-	-	+	+	+	+	+	+	+	-

3) недоліки, зумовлені внутрішньою будовою системи. До цієї групи належать такі проблеми, як швидке застарівання сигнатур, обмежена гнучкість та ефективність методів виявлення атак, а також необхідність регулярного оновлення програмного забезпечення. Крім того, СВВ мають труднощі з обробкою зашифрованих пакетів і нездатні компенсувати недоліки інфраструктури безпеки або слабкі методи автентифікації.

Також серед інших недоліків варто зазначити:

– складність розслідувань комп'ютерних злочинів через можливе викривлення мережевих адрес,

– вразливість до атак на стек TCP/IP або протокол-орієнтованих атак,

– обмежену мобільність та гнучкість у динамічних умовах,

– схильність до обходу зловмисниками.

Зловмисники можуть спричинити перенавантаження системи, порушити її точність за допомогою великої кількості хибних тривог, або уникнути виявлення справжньої атаки.

Хоча деякі з цих недоліків можуть бути усунені шляхом удосконалення вбудованих методів виявлення або впровадження нових технологій, наприклад, використання мобільних агентів, такі рішення також мають свої обмеження. Попри це, багатокомпонентні системи можуть підвищити продуктивність і точність СВВ у певних умовах. Однак їхня здатність працювати в реальному часі, збираючи дані з багатьох джерел, може уповільнювати обробку подій і знижувати ефективність системи.

Зловмисники можуть обійти СВВ різними способами, найбільш розповсюджені з яких наведені в табл.2.2, однак запобігти таким злочинним діям можна за допомогою засобів протидії обходу СВВ, які наведені в табл.2.3. для наступних способів обходу СВВ:

– фрагментація пакетів;

– використання невеликих пакетів;

– шифрування і тунелювання;

– поліморфізм і зміна поведінки.

Таблиця 2.2 – Способи обходу СВВ

Спосіб обходу		Атаки	
Назва	Зміст	Назва	Зміст
Фрагментація пакетів	Зловмисник надсилає фрагментовані пакети. СВВ. Також СВВ повинна знати порядок, в якому пакети мають бути зібрані адресатом, і зберігати в пам'яті послідовність пакетів до того часу, як зможе порівняти їх з шаблонами. Фрагментація пакетів не дозволяє СВВ виявити сигнатуру атаки. Спосіб ефективний для обходу сигнатурних СВВ. Атаки із застосуванням фрагментації не є дуже ефективними, але зазвичай їх використовують як складову комплексної (складеної) атаки	Накладання фрагментів	Фрагмент, що надходить, перезаписує дані з попереднього фрагменту, що не дозволяє СВВ розпізнати атаку
		Перезапис фрагменту	Фрагмент, що надходить, повністю перезаписує дані з попереднього фрагменту, що не дозволяє СВВ розпізнати атаку
		Тайм-аут фрагментів	Затримка в часі відправлення частини послідовності пакетів. Деякі СВВ, перш ніж відкинути незавершену послідовність пакетів певний час зберігають її в пам'яті. В більшості простих СВВ цей час становить 60 секунд. Затримка відправлення частини послідовності на цей час не дозволить СВВ розпізнати атаку.
Використання невеликих пакетів	Зловмисник розподіляє корисне навантаження на кілька невеликих пакетів, які СВВ повинна зібрати з потоку пакетів для виявлення атаки.	Тайм-аут фрагментів	
		Відправка пакетів в неправильному порядку	Може обманути прості СВВ системи.
Шифрування і тунелювання	Умова успіху обходу – встановлення зловмисником зашифрованого з'єднання (тунелю) з атакованою системою, наприклад, SSH, SSL, IPSec, RDP. СВВ атакованої системи не зможе перевірити трафік, що йде через тунель, оскільки не має ключів дешифрування. Шифрування трафіку значно збільшує шанси успіху вторгнення поза увагою СВВ.	Використання ключа і побітової операції XOR для шифрування	СВВ не матиме змоги перевірити трафік без ключів дешифрування
Поліморфізм і зміна поведінки	В разі використання сигнатурних СВВ, яких є переважна більшість, зловмисник може уникнути виявлення атаки, якщо буде трохи змінювати вміст пакетів атаки	Шифрування,	СВВ не виявить співпадіння із сигнатурою атаки
		Перестановка байтів і	
		«Заплутування» коду	
	СВВ, що виявляють атаки за аномаліями поведінки використовують статистичні та евристичні профілі (шаблони, образи) нормальної поведінки системи і нормального трафіку, які визначаються під час навчання системи. Якщо характеристики поточного трафіку відрізняються від «норми» на певне значення, то така ситуація визначається СВВ як атака. Контролю можуть підлягати розподіл частоти байтів, розподіл символів, довжини пакетів, виникнення послідовності байтів. Зловмисник маскує шкідливий трафік під нормальний	Маскування під профіль нормальної поведінки	Шкідливе ПЗ досліджує атаковану систему і виявляє параметри «нормального трафіку», а потім створює поліморфні копії атакуючих програм з такими самими параметрами. СВВ тоді сприйматиме шкідливий трафік за нормальний не генеруватиме тривогу. Для того, щоб параметри шкідливого трафіку і профілю мережі співпадали, шкідливе ПЗ може застосовувати вставку у шкідливий код команд (наприклад, асемблерної команди *NOP*), які нічого не виконують, але дозволяють підігнати кількість байтів і частотні статистики шкідливого трафіку під профіль мережі.

Продовження таблиці 2.2

Спосіб обходу		Атаки	
Назва	Зміст	Назва	Зміст
		Вставки	Шкідливе ПЗ досліджує атаковану систему і виявляє «нормальний трафік», а потім вставляє фрагменти «нормального трафіку у шкідливий
Проксінг і підміна адреси	Зловмисник перекидає трафік атаки через погано захищені або погано сконфігуровані проксі сервери	Проксінг	Ідентифікація джерела атаки для СВВ суттєво ускладнюється
Використання ботнет	Зловмисник визначає для кожного бота з ботнет різну мету і порт.	Сканування мережі	Кількість пакетів від одного бота мала, цілі і порти у ботів різні, тому СВВ важко визначити якийсь зв'язок між пакетами, що надходять з різних хостів, і виявити факт сканування мережі організації
Відмова від установок за замовчуванням	Якщо база даних чи база знань СВВ передбачає троянські атаки на певний порт, а зловмисник змінює порт, що використовується трояном, то СВВ може пропустити атаку	Троянська атака	Троянська атака із зміненим портом відносно установок СВВ за замовчуванням, які мають бути відомі зловмиснику для успіху обходу СВВ
Обхід системи розпізнавання шаблонів	СВВ перевіряє вміст кожного з пакетів на співпадіння з шаблонами атак, однак атакуюча команда може мати різні представлення або може виконуватися у різних ситуаціях. Наприклад, в коді *utf*-8 “/” може бути представлений як U+005C, 0x5C, C191C, E0819C. Чим довший рядок, тим більше існує варіантів його представлення. Такі варіанти рядків атакуючої команди мають однакове значення для сервера, однак вони є різними для СВВ. Всі варіанти неможливо ввести в базу СВВ.	Використанні кодування *utf*-8	За допомогою *utf*-8 кожен символ рядка команди, що має розпізнаватися СВВ як атака, зловмисник може представити декількома способами. Зловмисник генерує багато варіантів представлення команди, якийсь із котрих може бути пропущений СВВ.
		Обхід файлової системи	Зловмисник може зайти в певну доступну папку, а потім вийти з неї за командою ‘..’, і тільки вже на третьом кроці - зайти в потрібну папку, яка, наприклад, містить паролі
Відмова в обслуговуванні	Організація відмови в обслуговуванні СВВ, тобто успіх *DoS* або *DDos* атаки на СВВ створює умови для обходу одного з механізмів захисту мережі. Для відмови в обслуговуванні СВВ зловмисник може використовувати помилки в СВВ і різні способи вичерпування обчислювальних ресурсів	Перенавантаження процесора і переповненя буферу СВВ	Пакети, захоплені СВВ, до початку їх обробки процесором зберігаються в буфері ядра. Якщо навантаження на процесор велике, то кількість оброблених пакетів в одиницю часу буде меншою за кількість нових пакетів, що надходять до буфера. Буфер заповнюється, і після цього нові пакети (серед яких можуть бути шкідливі) вже не заходять у переповнений буфер. Чим більше часу витрачається на обробку одного пакета, тим швидше заповнюється буфер.

Продовження таблиці 2.2

Спосіб обходу		Атаки	
Назва	Зміст	Назва	Зміст
			Зловмисник може: - надсилати пакети, які вимагають зіставлення із складними сигнатурами атак. На процедуру зіставлення вмісту пакетів із сигнатурами витрачається найбільше ресурсів порівняно з іншими операціями, оскільки вона є алгоритмічно складною. Атака може мати успіх при наявності малопотужних сигнатурних СВВ, здатних обробляти відносно невеликий трафік; - надсилати зашифрований тарфік, на розшифровку якого СВВ також витрачає багато часу процесора; - надсилати зашифрований трафік, що відповідає складним сигнатурам. Такий підхід об'єднує два попередні способи і найшвидше переповнює буфер.
		Переповнення оперативної пам'яті	Сигнатурні СВВ до перевірки пакетів на відповідність сигнатурам має зберігати стан кожного контрольованого з'єднання і інформацію щодо нього (*TCBs* - контрольні блоки *TCP*; порядкові номери і стани з'єднання, наприклад, *ESTABLISHED, RELATED, CLOSED* тощо). Коли оперативна пам'ять (*RAM*) СВВ вичерпується, то СВВ починає використовувати віртуальну пам'ять на жорсткому диску (файл підкачки), яка працює значно повільніше, ніж оперативна пам'ять. Це, подібно до перенавантаження процесора, знижує продуктивність СВВ і можк спричинити пропускання пакетів шкідливого трафіку. Якщо наявні якісь вади у зберіганні *TCBs* в СВВ, то пам'ять СВВ може бути швидко вичерпана зловмисником шляхом: - швидкого запуску великої кількості *TCP* з'єднань; - збільшення кількості пакетів шляхом фрагментації пакетів; - відправка в невірному порядку великої кількості сегментів *TCP*.
		Перенавантаження (втома) оператора	СВВ надсилає сповіщення про початок атаки оператору. Якщо таких сповіщень забагато, то оператор може якесь із них пропустити. Зловмисник може змусити СВВ генерувати велику кількість тривожних попереджень шляхом надсилання потужного «шкідливого» трафіку і потім використати шум попереднього попередження як прикриття для виконання бажаної атаки, використовуючи спеціальні утиліти, наприклад, *Stick* та *Snot*.

Таблиця 2.3 – Засоби протидії обходу СВВ

Спосіб обходу	Атаки	Засоби протидії
Фрагментація пакетів	Накладання фрагментів	Фільтрація пакетів невеликого розміру Команда *Snort* : alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"MISC Tiny Fragments"; dsize:< 25; fragbits:M; classtype:bad-unknown; sid:522; rev:3;)
	Перезапис фрагменту	
	Тайм-аут фрагментів	
Використання невеликих пакетів	Тайм-аут фрагментів	Фільтрація пакетів, корисне навантаження яких має розмір (dsize)=1, і пакет містить лише пробіл Команда *Snort*: alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-MISC whisker space splice attack"; flow:to_server,established; dsize:1; content:" "; reference:arachnids,296; reference:url,www.wiretrip.net/rfp/pages/whitepapers/whiskerids.html; classtype:attempted-recon; sid:1104; rev:11;)
	Відправлення пакетів в неправильному порядку	
Шифрування і тунелювання	Використання ключа і побітової операції XOR для шифрування	Потужні мережеві СВВ здатні розшифрувати пакети.
		Статистичний аналіз, наприклад частоти байтів, дозволяє виявити шкідливі програми, що зашифровані операцією XOR
		Вимірювання ентропії дозволяє виявити трафік IPSec, однак можливі хибні спрацьовування внаслідок того, що аналогічні рівні ентропії можуть мати архівовані дані
Поліморфізм і зміна поведінки	Шифрування	Поліморфні коди часто виявляються при застосування машинного навчання СВВ
	Перестановка байтів	
	«Заплутування» коду	
	Маскування під профіль нормальної поведінки	Розподіл частот байтів для різних випадків атаки часто є однаковим. Існує загальна крива розподілу для певної атаки, незалежно від того, що значення байтів внаслідок заміни або шифрування, можуть бути різними. Ця крива може бути використана для виявлення атаки.
	Вставки	Зростання кількості помилкових спрацьовувань може свідчити про наявність атаки, оскільки воно може бути наслідком змішування шкідливого і нормального трафіку

3 РОЗРОБКА СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

3.1 Визначення методів вибору систем виявлення вторгнень

Вибір СВВ виконується за допомогою методу аналізу ієрархій (MAI), який передбачає побудову матриць попарних порівнянь критеріїв та альтернатив, представлених в ієрархічній структурі типу «дерево». Коренем дерева є оптимальна СВВ, визначена за сукупністю критеріїв, листям – доступні альтернативи СВВ, а проміжні рівні формують критерії порівняння та їх групи.

Матриці попарних порівнянь формуються для всіх елементів-нащадків, що належать до кожного вузла-предка в ієрархічній системі. Процес порівняння реалізується послідовно «згори донизу». На першому рівні метою є вибір оптимальної СВВ, а критеріями – агреговані показники другого рівня ієрархії. На кожному наступному рівні вузли-агрегати розглядаються як предки, а їх нащадки аналізуються на основі попарного порівняння. Множині елементів $B = \{B_1, B_2, \ldots, B_n\}$, що є нащадками одного предка, відповідає множина ваг цих елементів $W = \{w_1, w_2, \ldots, w_n\}$, які характеризують інтенсивність або силу впливу елемента-нащадка на предка. Для кожної множини нащадків визначається вектор ваг, який відображає вплив елементів-нащадків на вузол-предок. Основною метою попарного порівняння є визначення вагових коефіцієнтів альтернатив для кожного елементарного критерію, що дозволяє оцінити відповідність кожної альтернативи критеріям задачі.

Алгоритм включає три етапи:

1) попарне порівняння критеріїв:

– користувач оцінює відносну важливість груп критеріїв, заповнюючи матрицю попарних порівнянь відповідно до шкали Сааті, яка має 9 рівнів інтенсивності. При цьому формування матриці попарних порівнянь A здійснюється за формулою

$$a_{ij} = \begin{cases} 1 \quad при \quad i = j; \\ \dfrac{1}{a_{ji}} \quad при \quad i \neq j \quad та \quad i > j; \\ \dfrac{a_{1j}}{a_{1i}} \quad при \quad i \neq j \quad та \quad i < j. \end{cases} \tag{3.1}$$

– визначаються вектори пріоритетів для кожної групи критеріїв:

$$x_i = \frac{\sqrt[n]{\prod_{j=1}^{n} a_{ij}}}{\sum_{i=1}^{n} \sqrt[n]{\prod_{j=1}^{n} a_{ij}}} \tag{3.2}$$

– видаляються малозначимі групи критеріїв і повторюється процедура оцінювання пріоритетів для залишкових груп. Процедуру повторюють до досягнення значимості всіх груп;

– для кожної обраної групи f визначаються пріоритети підгруп s у групі ($P_{pgr}^{f.s}$) аналогічно пріоритетам груп. Процедуру повторюють до досягнення листя дерева критеріїв $P_k^{f.s.d}$. При цьому d – номер критерію в підгрупі;

– обчислюють пріоритети елементарних критеріїв

$$P_{Gk}^{f.s.d} = P_{gr}^{f} \cdot P_{pgr}^{f.s} \cdot P_k^{f.s.d}. \tag{3.3}$$

2) порівняння альтернатив за критеріями:

– для кожного елементарного критерію складаються матриці попарних порівнянь альтернатив за формулою (3.1), за якими обчислюються вектори пріоритетів альтернатив за формулою (3.2);

3) обчислення глобальних пріоритетів:

– з векторів пріоритетів альтернатив за окремими критеріями формується матриця пріоритетів альтернатив;

– обчислюється вектор глобальних пріоритетів альтернатив *PG* шляхом множення матриці пріоритетів альтернатив на вектор ваг критеріїв

$$PG = \begin{bmatrix} p_1^1 & p_1^2 & \cdots & p_1^r & \cdots & p_1^m \\ p_2^1 & p_2^2 & \cdots & p_2^r & \cdots & p_2^n \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p_t^1 & p_t^2 & \cdots & p_t^r & \cdots & p_t^m \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ p_n^1 & p_n^2 & \cdots & p_n^r & \cdots & p_n^m \end{bmatrix} \times \begin{bmatrix} pk_1 \\ pk_2 \\ \cdots \\ pk_r \\ \cdots \\ pk_m \end{bmatrix} = \begin{bmatrix} pg_1 \\ pg_2 \\ \cdots \\ pg_t \\ \cdots \\ pg_n \end{bmatrix}. \quad (3.4)$$

– альтернатива з найбільшим глобальним пріоритетом визнається оптимальною.

Якщо всі критерії рівнозначні, спрощеним варіантом аналізу є метод комбінаторно-морфологічного синтезу, що передбачає оцінювання кожної альтернативи за всіма критеріями та порівняння їх сукупних балів. У цьому випадку оптимальна альтернатива визначається максимальною сумою балів.

Оцінювання також може враховувати недоліки СВВ, які оцінюються попарним порівнянням, формуючи вектор пріоритетів недоліків. На його основі обчислюється штраф, що зменшує загальну оцінку СВВ, дозволяючи враховувати як позитивні, так і негативні аспекти. У складних випадках результуюча оцінка може базуватися на різниці між середніми оцінками позитивних та негативних властивостей.

Цей підхід забезпечує структуроване оцінювання альтернатив та дозволяє обґрунтовано вибирати оптимальну СВВ відповідно до конкретних умов та вимог.

3.2 Визначення критеріїв вибору систем виявлення вторгнень

3.2.1 Загальна характеристика системи критеріїв

СВВ є ключовим компонентом для забезпечення безпеки ІКС. Вибір оптимальної СВВ є критично важливим, адже вона виступає першою лінією оборони від кібератак. Для цього необхідно застосовувати чітко визначені критерії оцінки, які дозволяють не лише визначити найефективнішу систему для конкретного випадку, але й сформувати рейтинги, що можуть бути використані в СППР для допомоги у виборі.

Розробка системи критеріїв є багатогранним завданням, що враховує численні технічні, експлуатаційні та організаційні аспекти. У даній роботі запропоновано набір критеріїв для оцінки програмних і програмно-апаратних СВВ, що враховують різні умови їх використання. Ця ієрархічна система критеріїв включає як загальні характеристики, так і специфічні параметри, що визначають якість реалізації СВВ.

Головний критерій оцінювання – здатність системи ідентифікувати якомога більшу кількість потенційних атак, адже саме це є основною функцією СВВ. Іншими важливими критеріями є продуктивність системи, яка визначає швидкість обробки даних, та зручність її використання для операторів.

Охоплення рівнів моделі *OSI* є важливим фактором, адже здатність аналізувати пакети на кількох рівнях розширює можливості системи щодо виявлення різних типів загроз. Однак це вимагає значних обчислювальних ресурсів, які можуть перевищувати доступні можливості апаратного забезпечення. Системи, що використовують багатоядерні процесори або графічні адаптери, забезпечують вищу продуктивність, хоча потребують складніших налаштувань.

Підтримка сигнатур також є критерієм, що впливає на ефективність СВВ. Розробники зазвичай надають власні бази сигнатур, однак можливість додавати або змінювати ці бази користувачами, а також використовувати сигнатури інших

виробників, підвищує гнучкість системи. У цьому контексті запропонована система критеріїв містить підкатегорії: "Сигнатури користувачів", "Сигнатури інших розробників" та "Нові сигнатури виробників СВВ".

Багатопоточний режим роботи є важливим через зростання обсягів інтернет-трафіку, що вимагає підвищеної швидкості обробки даних. Використання багатоядерних процесорів або графічних адаптерів дозволяє оптимізувати роботу СВВ, розподіляючи навантаження між ядрами, що забезпечує стабільність і ефективність системи навіть під час атак типу DDoS.

Документація та зв’язок з розробниками виступають ключовими параметрами, що забезпечують коректність експлуатації СВВ. Документація повинна включати всі необхідні інструкції для встановлення, налаштування, обслуговування та оновлення програмного забезпечення. У разі виникнення проблем користувачі мають мати доступ до технічної підтримки, яка може надаватися у вигляді патчів, консультацій чи оновлень системи. Якісна документація та підтримка свідчать про надійність постачальника програмного забезпечення.

Таким чином, розробка та впровадження критеріїв для оцінки СВВ є необхідним кроком для створення ефективних і надійних рішень, які враховують потреби користувачів і відповідають сучасним вимогам безпеки.

3.2.2 Розробка системи критеріїв оцінювання систем виявлення вторгнень

Як показав аналіз систем виявлення вторгнень, проведений у розділі 2 цієї кваліфікаційної роботи, вибір оптимальної СВВ може здійснюватися на основі множини критеріїв, яку доцільно поділити на чотири групи:

– функціональні критерії, що визначають здатність СВВ виконувати задані функції;

– експлуатаційні критерії, які оцінюють ефективність виконання СВВ своїх функцій за певних умов експлуатації;

– ресурсні критерії, що враховують відповідність СВВ доступним фінансовим, часовим, кадровим та апаратним ресурсам;

– якісні критерії, які характеризують зручність використання СВВ та їх результативність.

До групи функціональних критеріїв відносяться *F*1 - *F*18:

*F*1. Клас кібератак, що розпізнаються СВВ.

*F*1.1. СВВ на основі виявлення зловживань методом сигнатур.

*F*1.2. СВВ на основі виявлення аномалій

*F*1.3. Гібридні СВВ

*F*2. Реакція на кібератаку

*F*2.1. Пасивні СВВ.

*F*2.1.1. Реєстрація відомостей про можливу чи здійснену атаку в журналі

*F*2.1.2. Реєстрація відомостей про можливу атаку і здійснену атаку в журналі і надсилання тривожних повідомлень адміністратору

*F*2.1.3. Реєстрація відомостей про можливу атаку і здійснену атаку в журналі і надсилання тривожних повідомлень адміністратору і/або користувачу

*F*2.2. Активні СВВ

*F*2.2.1. Реєстрація відомостей про можливу чи здійснену атаку в журналі

F.2.2.2. Надсилання тривожних повідомлень

F.2.2.2.1. Надсилання тривожних повідомлень адміністратору

F.2.2.2.2. Надсилання тривожних повідомлень користувачу

F.2.2.2.3. Надсилання тривожних повідомлень адміністратору і користувачу

F.2.2.3. Відключення і блокування

F.2.2.3.1. Відімикання з’єднання

F.2.2.3.2. Відключення системи

F.2.2.3.3. Блокування зловмисного трафіку

F.2.2.3.4. Блокування *IP* адреси

F.2.2.3.5. Блокування потенційно небезпечних акаунтів

F.2.2.4. Відключення і блокування

F.2.2.4.1. Відмикання з’єднання

F.2.2.4.2. Відключення системи

F.2.2.4.3. Блокування зловмисного трафіку

F.2.2.5. Відновлення

F.2.2.3.1. Відновлення лог файлів у разі їх втрати

F.2.2.3.2. Відновлення *TCP* потоку

F.2.2.3.3. Відновлення *HTTP web*- сторінки

*F*3. Робота у реальному часі.

*F*3.1. Параметри, що обробляються у реальному часі

*F*3.2. Затримки в часі при обробці різних параметрів трафіку

*F*4. Атаки, що розпізнаються СВВ

*F*4.1. Типи атак, що розпізнаються СВВ

*F*4.2. Кількість типів атак, що розпізнаються СВВ

*F*5. Підтримувані операційні системи

*F*5.1. Типи підтримуваних ОС

*F*5.2. Кількість підтримуваних ОС

*F*6. Можливість роботи у багатопоточному режимі

*F*7. Рівень спостереження

*F*7.1. Мережеві СВВ

*F*7.1.1. Дослідження вхідного трафіку

*F*7.1.2. Дослідження вихідного трафіку

*F*7.1.3. Відсутність впливу на продуктивність мережі

*F*7.1.4. Відсутність змін у топології мережі

*F*7.1.5. здатність давати відсіч *DoS* атакам

*F*7.1.6. Велике покриття для моніторингу

*F*7.2. Хостові СВВ

*F*7.2.1. Можливість контролювати зашифровану інформацію

*F*7.2.2. Можливість контролювати цілісність файлів

*F*7.2.3. Можливість контролювати внутрішню структуру

*F*7.2.4. Можливість відслідкувати лог-файли і виправляти аномалії в потоці подій

*F*7.2.5. Можливість здійснювати контроль на рівні ОС

*F*7.2.6. Можливість здійснювати контроль на рівні баз даних

*F*7.2.7. Можливість здійснювати контроль на рівні додатків

*F*7.2.8. Можливість здійснювати контроль на рівні ОС

*F*8. Рівні моделі *OSI*

*F*8.1. Рівні моделі *OSI*, які охоплює СВВ

*F*8.2. Кількість рівнів моделі *OSI*, які охоплює СВВ

*F*9. Відкритість системи до взаємодії з іншим ПЗ

*F*9.1. ПЗ, з яким може взаємодіяти СВВ

*F*9.2. Кількість ПЗ, з якими може взаємодіяти СВВ

*F*10. Управління системою.

*F*10.1. Централізоване управління з одного хоста,

*F*10.2. Розподілене управління з окремих, але взаємопов’язаних, хостів

*F*11. Протоколи.

*F*11.1. Типи підтримуваних протоколів

*F*11.2. Кількість підтримуваних протоколів.

*F*12. Відкритість коду

*F*13. Можливість виявляти атаки «0-*day*»

*F*14. Наявність шаблонів «нормальної» поведінки системи

*F*15. Доступні методи виявлення атак

*F*15.1. Експертні методи

*F*15.2. Сигнатурні методи

*F*15.3. Методи контролю зміни подій

*F*15.4. Методи кластерного аналізу

*F*15.5. Динамічні методи

*F*15.6. Методи машинного навчання

*F*15.7. Поведінкові методи

*F*15.8. Евристичні методи

*F*16. Область захисту: сайт, сервер, мережа, мобільний зв’язок, Інтернет речей, летючі мережі.

*F*17. Пропускна здатність.

*F*18. Місце розташування відносно мережевого екрану: до мережевого екрану, після мережевого екрану.

Структура функціональних критеріїв наведена на рис.3.1.

До експлуатаційних критеріїв вибору СВВ можна віднести *E*1 - *E*4.

*E*1. Захищеність.

*E*1.1. Кількість уразливостей СВВ

*E*1.2. Критичність уразливостей СВВ

*E*1.3. Наявність власних вбудованих засобів захисту від кібератак і негативного зовнішнього інформаційного впливу

*E*1.3.1. Наявність засобів протидії фрагментації пакетів

*E*1.3.2. Наявність засобів протидії використанню невеликих пакетів

*E*1.3.3. Наявність засобів протидії шифруванню і тунелюванню

*E*1.3.4. Наявність засобів протидії поліморфізму і зміні поведінки

*E*1.3.5. Наявність засобів протидії проксінгу і підміні адреси

*E*1.3.6. Наявність засобів протидії ботнет

*E*1.3.7. Наявність засобів протидії відмові від установок за замовчуванням

*E*1.3.8. Наявність засобів протидії обходу системи розпізнавання шаблонів

*E*1.3.9. Наявність засобів протидії *DDoS*-атакам на СВВ

*E*1.4. Наявність засобів відновлення в разі виходу СВВ з ладу

*E*1.5. Ймовірність порушення функціонування СВВ (характеристика надійності СВВ) протягом певного інтервалу часу

*E*2. Масштабованість

*E*2.1. Масштабованість при зміні розміру і обсягу системи

*E*2.2. Забезпечення ефекту синергізму.

*E*3. Адаптивність СВВ до нових атак, які відсутні в базі даних

*E*3.1. Можливість додавання нових сигнатур і/або аномалій від розробника СВВ

.

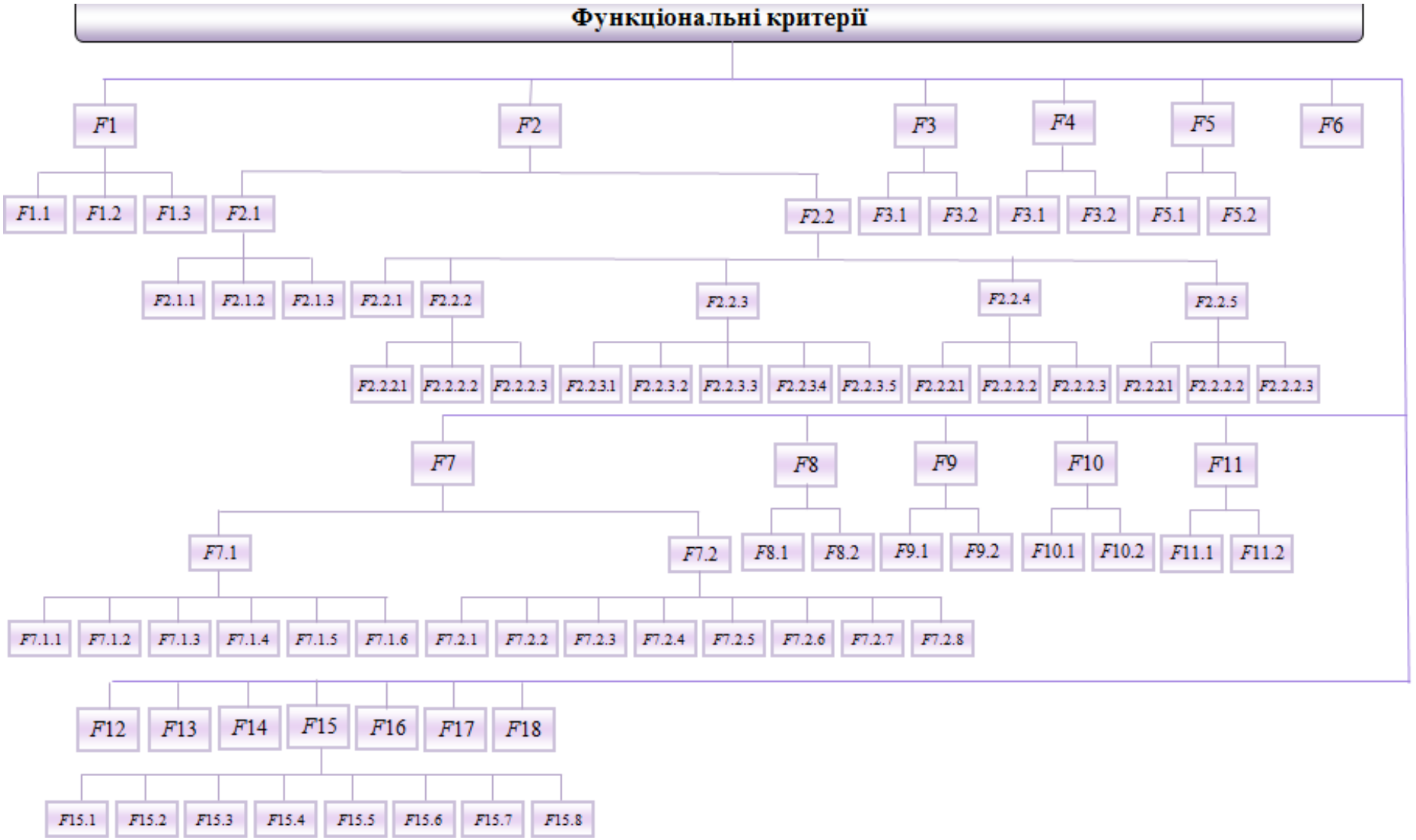


Рисунок 3.1 – Структура функціональних критеріїв вибору СВВ

*E*3.2. Можливість додавання нових сигнатур і/або аномалій від фірм, що не є розробником даної СВВ

*E*3.3. Можливість додавання нових сигнатур і/або аномалій користувачів

*E*3.4. Можливість додавання нових сигнатур і/або аномалій в результаті самонавчання в процесі роботи

*E*4. Орієнтований обсяг оброблюваної інформації:

*E*4.1. Малий бізнес

*E*4.2. Середній бізнес

*E*4.3. Великий бізнес

Структура експлуатаційних критеріїв наведене на рис.3.2.

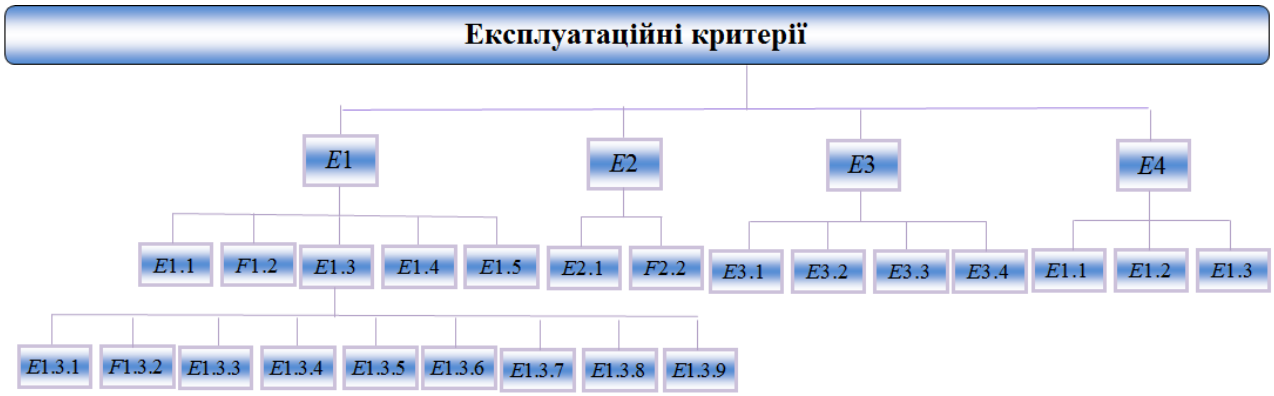


Рисунок 3.2 – Структура експлуатаційних критеріїв вибору СВВ

До підмножини ресурсних критеріїв відносяться:

*R*1. Наявність документації.

*R*2. Наявність персоналу з достатнім рівнем кваліфікації.

*R*3. Умови розпосвюдження: вільне, тріал-версія, платне.

*R*4. Вартість.

*R*5. Вартість навчання персоналу.

*R*6. Витрати часу на встановлення і налаштування засобу та підготовку персоналу.

*R*7. Вартість підтримки розробника при налаштуванні та експлуатації СВВ.

*R*8. Необхідний обсяг пам’яті.

*R*9. Можливість співпрацювати із виробниками і розповсюджувачами.

Структура ресурсних критеріїв вибору СВВ наведена на рис.3.3.

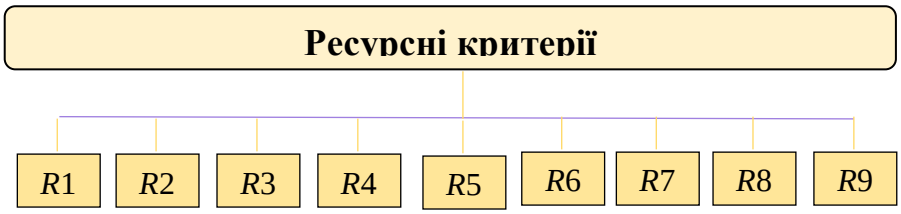


Рисунок 3.3 – Структура ресурсних критеріїв вибору СВВ

До підмножини якісних критеріїв вибору СВВ відносяться:

*Q*1. Кількість використовуваних сигнатур.

*Q*2. Кількість шаблонів нормального стану.

*Q*3. Ефективність виявлення атак:

*Q*3.1. Відносна кількість невиявлених атак;

*Q*3.2. Відносна кількість хибних спрацьовувань.

*Q*4. Ефективність протидії атакам певного типу

*Q*4.1. Ймовірність виявлення

*Q*4.2. Час придушення

*Q*4.3. Граничні значення стійкості системи

*Q*5. Зручність використання.

*Q*6. Зручність оновлення сигнатур.

*Q*7. Зручність оновлення шаблонів нормального стану.

*Q*8. Наявність підтримки розробника при налаштуванні та експлуатації.

*Q*9. Інтерфейс користувача.

*Q*10. Наявність декількох інтерфейсів.

*Q*11. Адаптовність налаштувань під вимоги користувача.

Структура якісних критеріїв вибору СВВ наведена на рис.3.4.

Визначені вище критерії можуть використовуватися як для вибору СВВ за допомогою методу аналізу ієрархій, який дозволяє врахувати важливість кожного критерію, так і для простого порівняння СВВ за бажаними

рівнозначними властивостями за вибірковими критеріями (див.п.4.1 даної кваліфікаційної роботи).

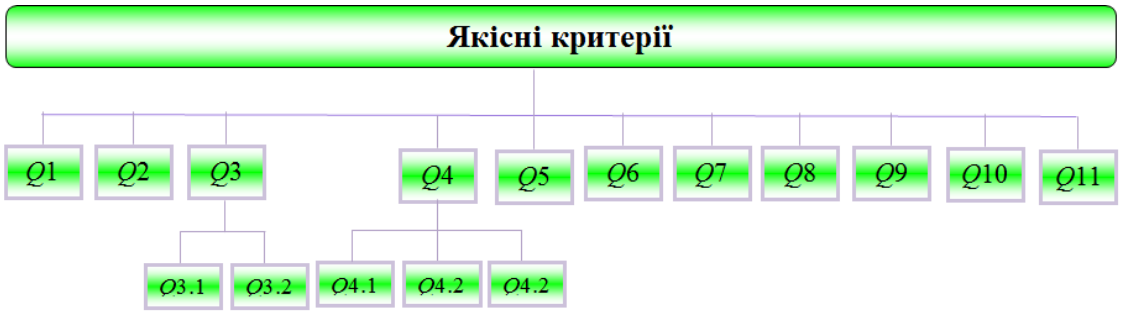


Рисунок 3.4 – Структура якісних критеріїв вибору СВВ

3.2.3 Розробка алгоритмів для вибору систем виявлення вторгнень

Вибір СВВ відповідає прийняттю управлінського рішення. Тому узагальнений алгоритм цього процесу в цілому відповідає рис.1.2., однак на окремих етапах процесу прийняття рішення задіяні різні особи, що приймають рішення, і додається ряд підпроцесів, які можуть бути виділені в окремі етапи. В результаті отримуємо алгоритм, наведений на рис.3.5:

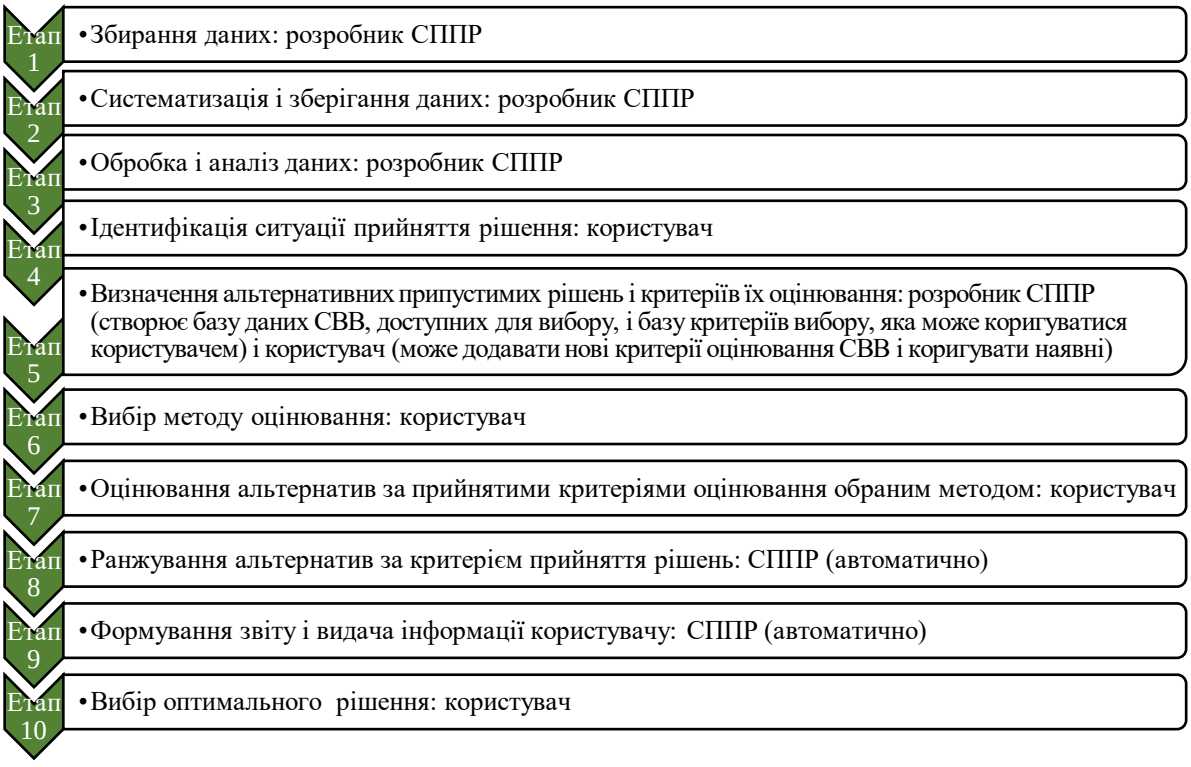


Рисунок 3.5 – Узагальнений алгоритм процесу вибору СВВ

На етапі 6 алгоритму рис.3.5 реалізується процес визначення критеріїв, які користувач прийматиме до уваги при виборі СВВ. Узагальнений алгоритм цього процесу наведено на рис.3.6.

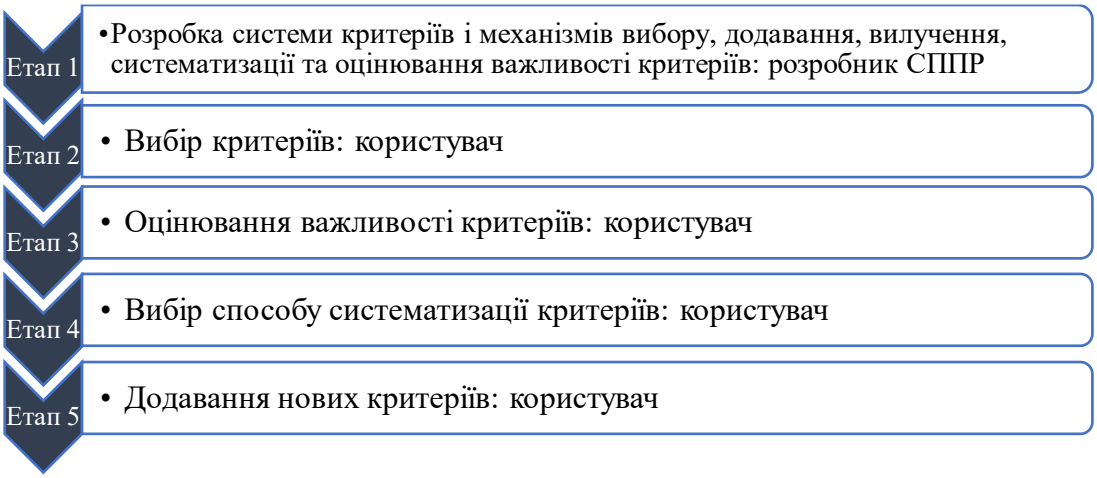


Рисунок 3.6 – Узагальнений алгоритм вибору критеріїв оцінювання СВВ

Таким чином, до початку оцінювання СВВ має бути сформований перелік важливих для користувача критеріїв оцінювання. Передбачається, що СППР надаватиме користувачу:

– можливість прийняти всі критерії із вбудованого структурованого переліку критеріїв без коригування;

– можливість вилучити не значимі для користувача критерії. З метою запобігання помилок користувача при вилученні критеріїв передбачається попереднє оцінювання користувачем всіх вбудованих критеріїв за допомогою MAI. Вилучатися можуть критерії, яким відповідають малі (порівняно з іншими критеріями) значення у векторі пріоритетів критеріїв. Після вилучення не значимих критеріїв вектор пріоритетів критеріїв має бути переобчислений;

– можливість відкоригувати вбудовані критерії без зміни їх приналежності групі критеріїв;

– можливість додати нові групи критеріїв і критерії в існуючу групу. Після додавання критеріїв і груп критеріїв вектор пріоритетів критеріїв має бути пере обчислений.

Узагальнений алгоритм цього процесу наведений на рис.3.7

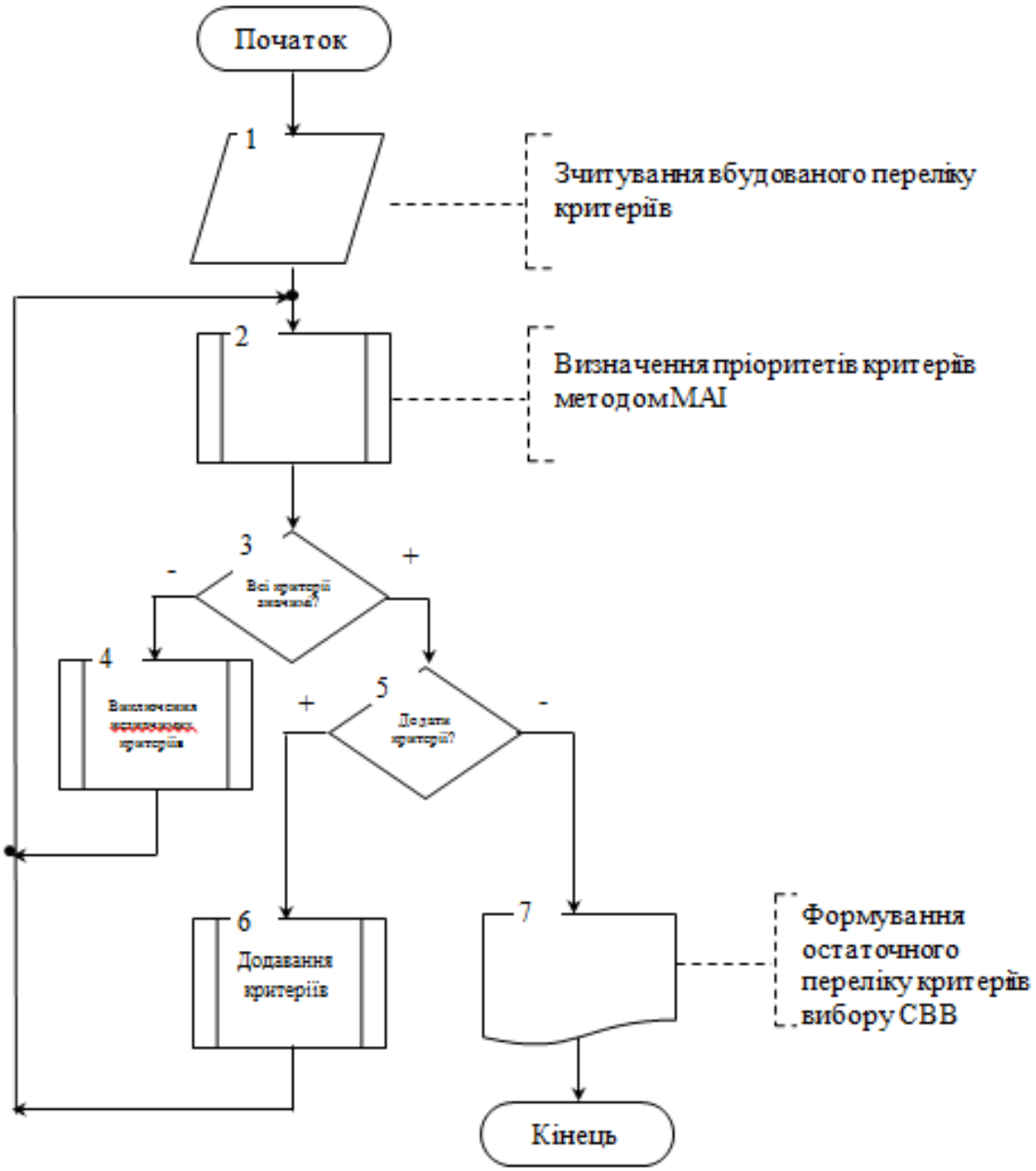


Рисунок 3.7 – Загальний алгоритм формування списку критеріїв користувача для оцінки систем виявлення вторгнень

Після визначення критеріїв вибору система виявлення вторгнень вони можуть бути прийняті користувачем:

– у структурованій формі (рис.3.1-3.4) із визначеними в процесі виконання алгоритму рис.3.7 пріоритетами;

– у вигляді неструктурованого переліку критеріїв із визначеними пріоритетами;

– у вигляді неструктурованого переліку рівнозначних критеріїв.

Оцінювання альтернативних варіантів СВВ тоді відбувається різними методами. Найпростішим є оцінювання альтернатив за неструктурованим переліком рівнозначних критеріїв. Припустимо, що необхідно оцінити M альтернативних варіантів за N критеріями. Тоді на першому кроці алгоритму обирають шкалу оцінювання з певною кількістю градацій, наприклад, 0..5 або 0..10. Шкали з кількістю градацій більшою за 10 зазвичай не застосовуються. Мінімальною кількістю градацій є 2, що відповідає бінарному оцінюванню: 0 – властивість відсутня, 1 – властивість наявна. Обрана шкала визначає мінімальну можливу оцінку $G_{\min}$ і максимальну можливу оцінку $G_{\max}$. Кожний j-ий альтернативний варіант $\left(j=\overline{1,M}\right)$ СВВ при оцінці за i–им критерієм $\left(i=\overline{1,N}\right)$ отримує оцінку a_{ij}. Оптимальним вважається варіант СВВ, що набрав найбільшу суму балів за всіма критеріями $\max\limits_{j=\overline{1,M}}\sum\limits_{i=1}^{N}a_{ij}$. Алгоритм, що відповідає цьому методу, наведено на рис.3.8, а.

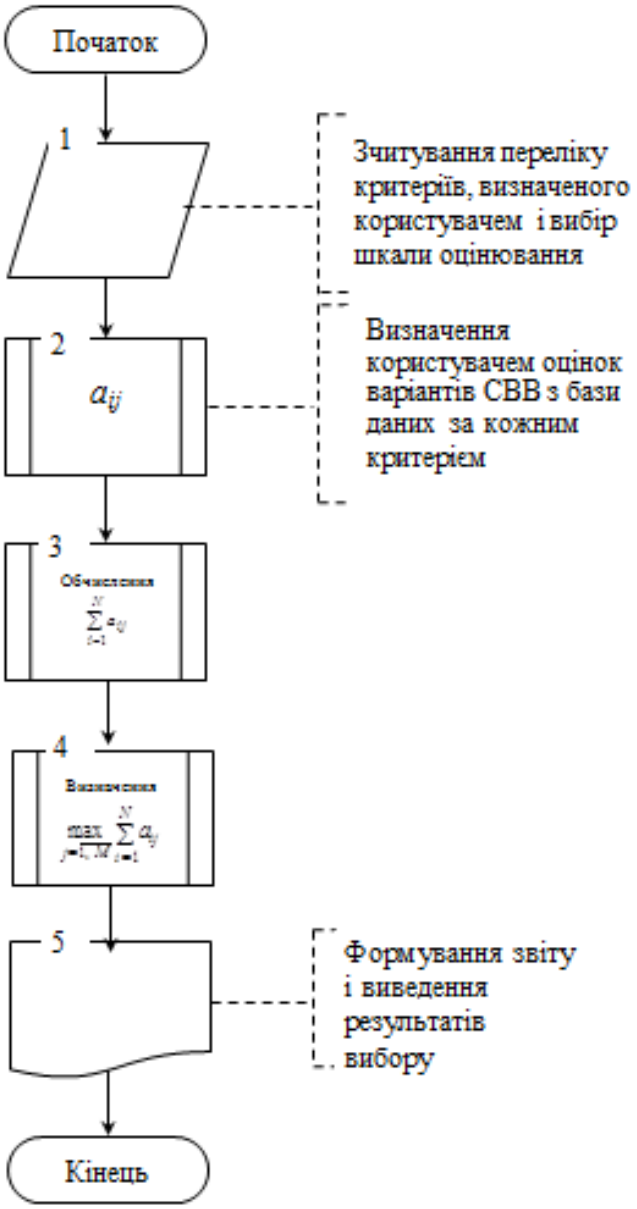
Якщо перелік критеріїв не є структурованим, але користувач хоче врахувати важливість c_i кожного i-го критерію, то оптимальний варіант СВВ визначається за алгоритмом рис.3.8, б за умовою максимуму суми зважених оцінок $\max\limits_{j=\overline{1,M}}\sum\limits_{i=1}^{N}c_i a_{ij}$ (c_i визначаються в процесі виконання алгоритму рис.3.7 як елементи вектору пріоритетів критеріїв і дорівнюють «долі важливості» пріоритетів: $\sum\limits_{i=1}^{N}c_i=1$).

Якщо користувач обирає метод вибру СВВ на основі структурованих критеріїв (рис.3.1-3.4), то алгоритм процесу вибору повністю відповідає алгоритму MAI (п.3.1 даної кваліфікаційної роботи), однак вектор пріоритетів критеріїв визначається за алгоритмом 3.7. незалежно від того, буде використовуватися MAI чи інший метод для вибору оптимальної СВВ. Детальніше цей алгоритм представлено на рис.3.9.

Визначення глобальних пріоритетів альтернатив за MAI здійснюється за алгоритмом, в якому алгоритм рис.3.9 використовується як складова: спочатку

за алгоритмом рис.3.9 попарним порівнянням визначаються пріоритети груп критеріїв найвищого рівня ієрархії («Функціональні критерії», «Експлуатаційні критерії», «Ресурсні критерії», «Якісні критерії»). Потім в кожній групі критеріїв порівнюються за важливістю наявні підгрупи.

а) з рівнозначними критеріями



б) зі зваженими критеріями

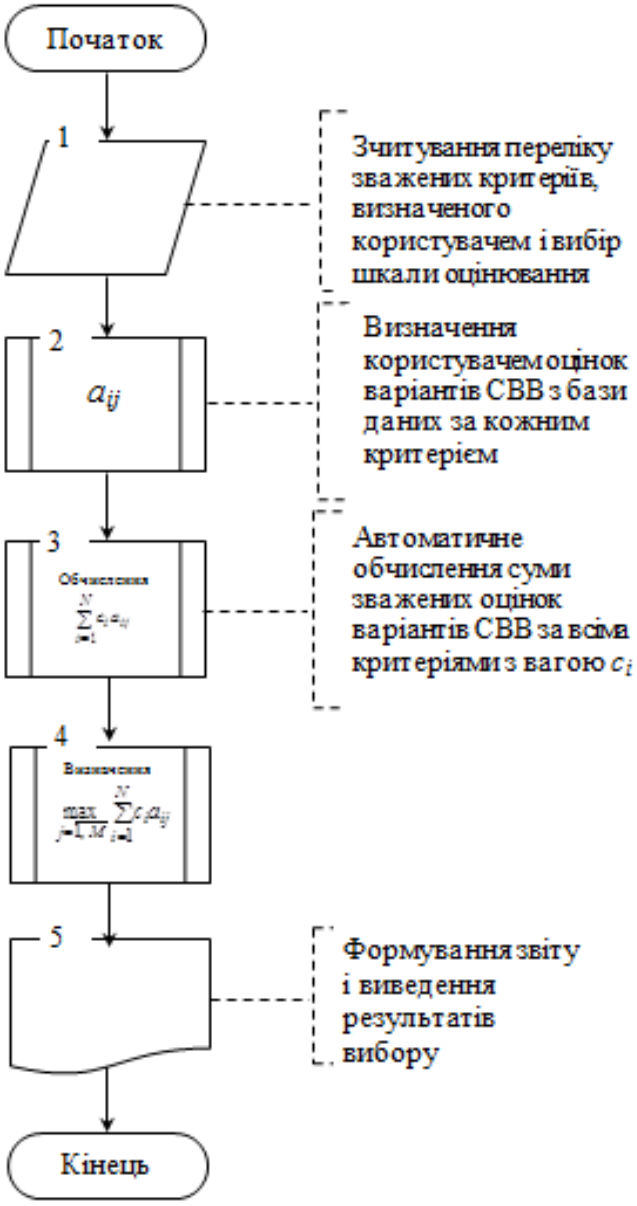


Рисунок 3.8 – Алгоритми вибору СВВ за неструктурованими критеріями

Наприклад, за рис.3.3 «Ресурсні критерії» поділяються на 9 підгруп, які не мають власних підгруп. Це означає, що *R*1-*R*9 безпосередньо ввійдуть до переліку критеріїв вибору СВВ, причому їх вага в цьому переліку буде

визначатися як добуток пріоритету групи «Ресурсні критерії» на пріоритет відповідного критерію у групі «Ресурсні критерії», який є елементом вектору пріоритетів, отриманих за матрицею розмірності 9×9 попарних порівнянь критеріїв *R*1-*R*9 між собою. В групі «Якісні критерії» наявні критерії *Q*1, *Q*2, *Q*5-*Q*11, які не мають нащадків, і узагальнені критерії *Q*3 та *Q*4, кожен з яких має 2 нащадка (підгрупу).

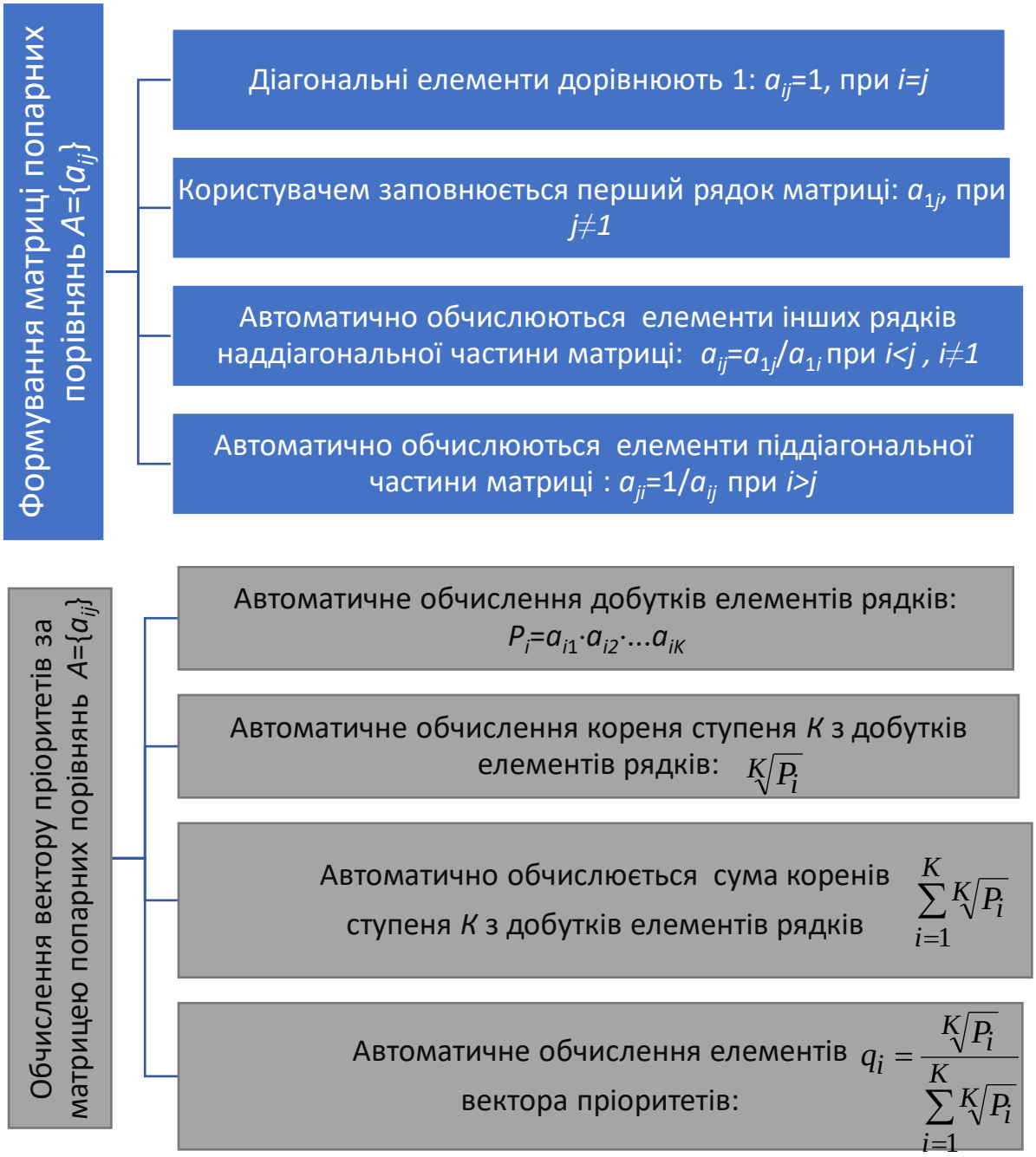


Рисунок 3.9 – Алгоритм визначення пріоритетів за матрицею попарних порівнянь

За алгоритмом рис.3.9 визначаються пріоритети критеріїв $Q1$-$Q11$, а потім - пріоритети критеріїв $Q3.1$ і $Q3.2$ в підгрупі $Q3$ та пріоритети критеріїв $Q4.1$ і $Q4.2$ в підгрупі $Q4$. В цьому випадку в перелік критеріїв вибору СВВ війдуть критерії $Q1$, $Q2$, $Q3.1$, $Q3.2$, $Q4.1$, $Q4.2$, $Q5$-$Q11$, причому вага критеріїв $Q3.1$, $Q3.2$, $Q4.1$, $Q4.2$ буде дорівнювати добутку пріоритету групи «Якісні критерії», пріоритету відповідної підгрупи в групі ($Q3$ для $Q3.1$ і $Q3.2$, $Q4$ для $Q4.1$ і $Q4.2$) і пріоритету критерію у підгрупі.

В результаті отримується перелік критеріїв із визначеними глобальними пріоритетами, що враховують важливість критеріїв у всій складній ієрархічній системі критеріїв.

Наступним кроком є оцінювання альтернативних варіантів СВВ за кожним критерієм, що увійшов до переліку, шляхом попарного порівняння СВВ між собою. Тобто, якщо потрібно оцінити M альтернативних варіантів за N критеріями, то будується N матриць попарних порівнянь розмірності $M \times M$, і за алгоритмом рис.3.9 отримується N векторів пріоритетів.

На завершальному етапі обчислень з N векторів пріоритетів альтернатив утворюється матриця пріоритетів альтернатив розмірності $M \times N$, яку множать на вектор глобальних пріоритетів критеріїв. Отриманий вектор довжиною M є вектором глобальних пріоритетів альтернативних варіантів СВВ.

На рис.3.10 зображено відповідний алгоритм, де АВПМПП відповідає рис.3.9 - алгоритм визначення пріоритетів за матрицею попарних порівнянь.

3.2.4 Можливі підходи до проведення оцінювання

Оцінювання СВВ може бути здійсненне як за всією сукупністю критеріїв, так із за їх невеликою вибіркою. При цьому можна використовувати штучно створені групи критеріїв. Наприклад, в якості критеріїв вибору СВВ обираємо:

- $F8$ - доступні для перевірки рівні моделі *OSI*;
- $E3$ - використання інших сигнатур;
- $F6$ - можливість роботи в багатопоточному режимі;
- $R1$+$R9$ - документація і зв'язок з розробниками.

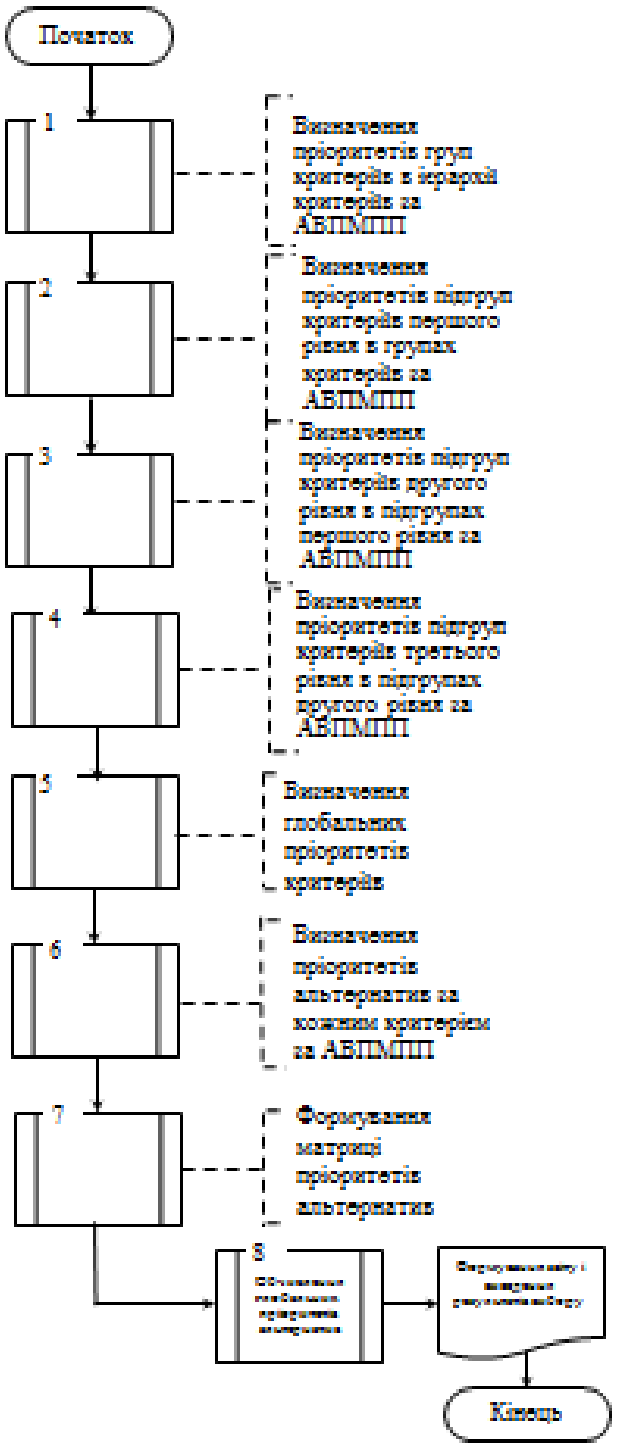


Рисунок 3.10 – Алгоритм вибору Системи виявлення вторгнення методом MAI

Критерії представлені простим списком, тобто не утворюють ієрархію, тому можна відразу почати оцінювання альтернативних варіантів СВВ.

Для кожного критерію обираємо максимально можливу оцінку, тобто використовуємо різні шкали. (табл.3.1). Максимальна оцінка за сукупністю критеріїв складає 10 балів.

Таблиця 3.1 – Критерії та оцінка

Критерій			Максимальна оцінка
№	Символ	Зміст критерію	
1	*F*8	Рівні моделі OSI доступних для перевірки	2
2	*E*3	Використання інших сигнатур	4
3	*F*6	Можливість роботи в багато поточному режимі	2
4	*R*1+*R*9	Документація і зв'язок з розробниками	2
Максимальна сумарна оцінка			10

Критерії з номерами 1, 3 та 4 мають рівноцінну вагомість, оскільки їх максимальна оцінка становить 2 бали. Водночас другий критерій — «Використання інших сигнатур» — має вдвічі вищу максимальну оцінку, що свідчить про його підвищену важливість.

Аналіз СВВ за критеріями, наведеними в таблиці 3.1, дозволяє обчислити загальну кількість балів, яку набирає кожна система, і, відповідно, скласти рейтинг на основі цих балів.

Окрім універсальних критеріїв, придатних для оцінки всіма користувачами, існують індивідуальні критерії, важливість яких варіюється залежно від специфічних потреб і цілей. Такі критерії враховують особисті вимоги, переконання та ресурси. До індивідуальних критеріїв вибору СВВ можна віднести:

- вибір методу виявлення вторгнення;
- визначення рівня аналізу атак;
- встановлення цінового діапазону;
- відповідність масштабам бізнесу, для якого призначена система;
- сумісність із бажаною операційною системою.

Бажано, щоб користувач СППР, навіть без глибоких знань у сфері СВВ, міг підібрати систему відповідно до своїх індивідуальних критеріїв. Після цього варто перейти до оцінювання СВВ за загальноприйнятими критеріями, результати якого використовуються для складання рейтингового списку. Рекомендована система, розташована на вершині списку, повинна максимально відповідати технічним характеристикам і потребам конкретного користувача.

Визначення відносної важливості критеріїв може здійснюватися не лише за допомогою методу попарного порівняння. У випадках із невеликою кількістю критеріїв користувач може встановити їхню вагомість, використовуючи шкали з різними максимальними значеннями оцінок. Наприклад, згідно з таблицею 3.1, пріоритети критеріїв 1, 3, 4 дорівнюють 2/10 = 0,2, тоді як пріоритет критерію 2 становить 4/10 = 0,4. Сума пріоритетів усіх критеріїв дорівнює одиниці.

Процес вибору СВВ доцільно розділити на два етапи. На першому етапі проводиться фільтрація систем за критеріями, невідповідність яким унеможливлює їх використання конкретним користувачем (наприклад, сумісність із певною операційною системою). На другому етапі вирішується задача пошуку оптимального рішення з урахуванням усіх релевантних критеріїв.

3.3 Розробка структури системи підтримки прийняття рішень

Система підтримки прийняття рішень, створена у межах цієї кваліфікаційної роботи, включає інтерфейс користувача, котрий виступає неначе особа, котра приймає рішення (ОПР) під час вибору СВВ, а також функціональні блоки трьох типів (рис. 3.11).

Перший тип блоків - це елементи, створені і змінювані виключно розробником СППР. Вони містять відносно статичну інформацію, котру користувач не може редагувати. До цього типу відносяться такі блоки, як «Блок методів вибору», «Блок інформаційної підтримки», «Блок вбудованих критеріїв вибору» а також «База даних СВВ». Ці блоки формують базу даний для прийняття рішень, із якої користувач обирає дані, необхідні для вибору СВВ, що відповідає заданим умовам експлуатації та оптимальна за сукупністю критеріїв.

Другий тип блоків — це функціональні елементи, для яких розробник забезпечує лише механізми, які гарантують правильність результатів, отриманих користувачем. До цього типу належать «Блок коригування критеріїв користувачем», «Блок вибору формату звіту», «Блок вибору методу».

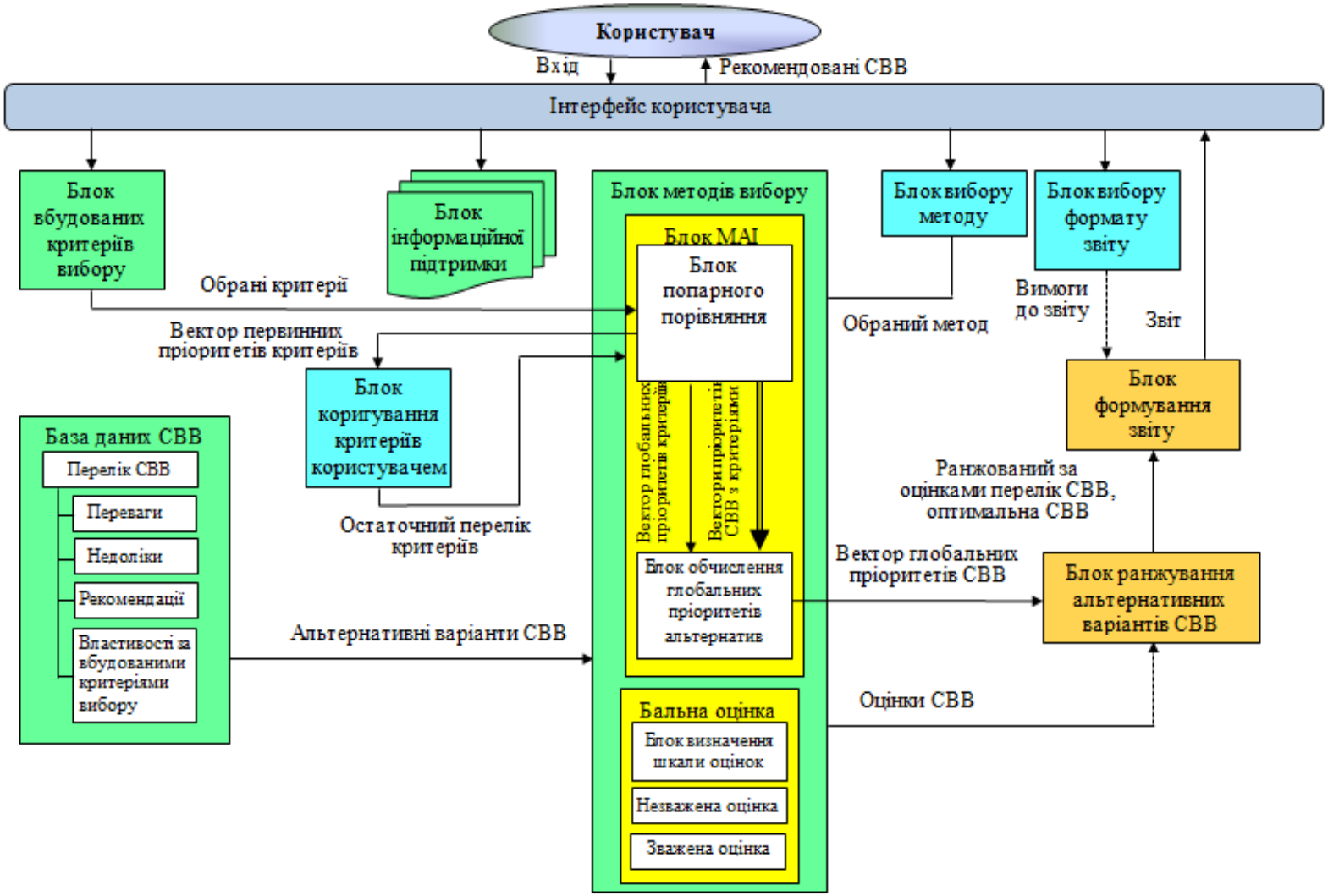


Рисунок 3.11 – Структура моделі СППР вибору СВВ

Третій тип блоків — це функціональні елементи, які автоматично обробляють вхідну інформацію. Сюди входять «Блок ранжування альтернативних варіантів СВВ» і «Блок формування звіту». Реалізація цих блоків є статичною, їх розробляє фахівець, однак вони працюють із динамічною інформацією. У процесі обробки даних участь користувача не передбачається.

На виході СППР формує звіт у форматі, заданому користувачем через інтерфейс. У звіті може бути представлена інформація про одну оптимальну СВВ (або декілька СВВ із однаковими оцінками), список систем із найвищими балами тощо.

4 АПРОБАЦІЯ РЕЗУЛЬТАТІВ РОЗРОБКИ

4.1 Інтерфейс системи підтримки прийняття рішень

Початок роботи з системою підтримки прийняття рішень починається із форми, якою передбачені кнопки для перегляду інформації щодо бібліотеки і власників (рис.4.1) і для початку роботи.

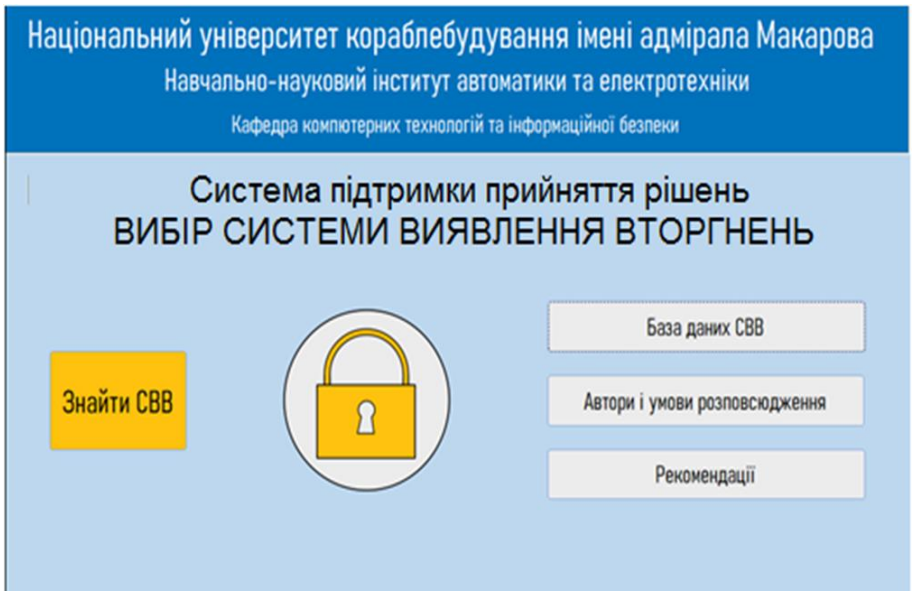


Рисунок 4.1 – Титульна форма СППР

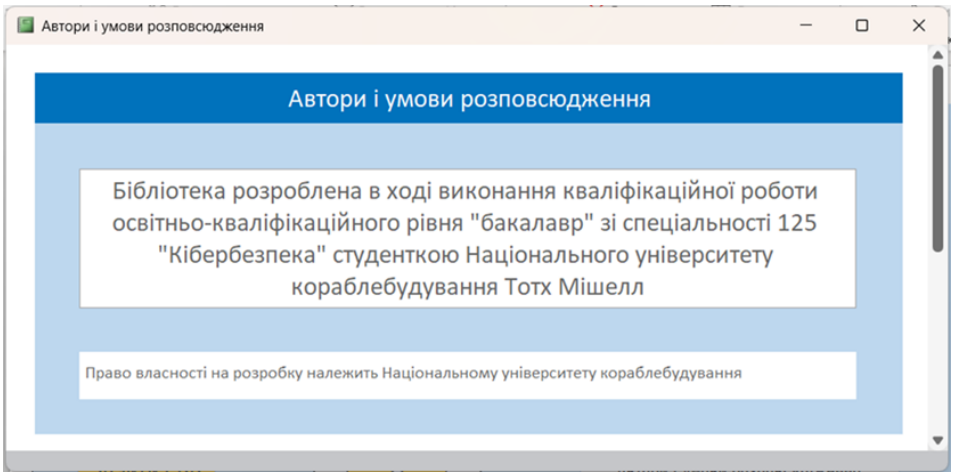


Рисунок 4.2 – Інформація про авторів та умови розповсюдження СППР

4.2 Опис нормативно-правової бази в системі підтримки прийняття рішень

В СППР передбачено можливість для користувачів переглядати при виборі СВВ перелік даних, представлені у вигляді таблиці рис.4.3.

СВВ	NIDS/HIDS	вартість	Signature/Anomaly	Unix	Linux	Windows	Mac	малий бізнес	середній бізнес	великий бізнес	номер
OSSEC	HIDS	Free	Signature	✓	✓	✓	✓		✓	✓	1
Suricata	NIDS	Free	Signature/Anomaly	✓	✓	✓	✓		✓	✓	2
Security Onion	NIDS/HIDS	Free	Signature/Anomaly	✓		✓	✓		✓	✓	3
Snort	NIDS	Free	Signature/Anomaly	✓	✓		✓	✓	✓		4
Bro	NIDS	Free	Signature/Anomaly	✓	✓	✓		✓	✓	✓	5
SolarWinds Security Event	NIDS	Costly	Signature/Anomaly	✓	✓	✓	✓			✓	6
Open WIPS-NG	NIDS	Free	Signature/Anomaly	✓	✓	✓	✓	✓	✓		7
Sagan	NIDS/HIDS	Free	Signature/Anomaly	✓	✓	✓	✓	✓	✓	✓	8
Mcafee Network Security Platform	NIDS	Costly	Signature/Anomaly	✓		✓	✓			✓	9
Palo Alto Networks	NIDS/HIDS	Costly	Anomaly	✓	✓	✓	✓			✓	10
AAFID	HIDS	Free	Signature/Anomaly			✓		✓			17
Prelude SIEM	NIDS/HIDS	Costly	Signature/Anomaly			✓			✓	✓	18
NetSTAT	HIDS	Free	Signature/Anomaly			✓		✓			19
Shadow	HIDS	Free	Signature/Anomaly	✓	✓			✓			20
ASAX	HIDS	Costly	Signature	✓	✓				✓		21
Cisco IPS	NIDS	Costly	Signature/Anomaly	✓	✓	✓			✓	✓	22
Arbor Networks Spectrum	NIDS	Free	Signature/Anomaly	✓	✓	✓				✓	23
InfoWatch ASAP	NIDS/HIDS	Costly	Signature/Anomaly	✓	✓	✓	✓			✓	24
Symantec DeepSight Threat Manage	NIDS	Costly	Signature/Anomaly	✓	✓	✓	✓			✓	25
Tipping Point NGIPS	NIDS	Costly	Signature/Anomaly			✓	✓		✓	✓	26
Aaoft invGUARD	HIDS	Costly	Signature/Anomaly	✓	✓				✓		27
DefensePro	NIDS	Costly	Signature/Anomaly	✓	✓	✓	✓			✓	28
KATA Platform	NIDS	Costly	Signature/Anomaly	✓	✓	✓	✓			✓	29
Samhain	HIDS	Free	Signature/Anomaly	✓	✓	✓	✓	✓			30
Samhain	HIDS	Free	Signature/Anomaly	✓	✓	✓	✓	✓			30
Splunk	NIDS/HIDS	Costly	Anomaly		✓	✓	✓			✓	31
IBM QRadar	NIDS/HIDS	Costly	Signature/Anomaly		✓					✓	32
Check Point Security Management	NIDS/HIDS	Costly	Signature		✓				✓		33
AlienVault OSSIM	NIDS/HIDS	Free	Signature/Anomaly		✓				✓		34
LogRhythm	NIDS/HIDS	Costly	Anomaly		✓	✓				✓	35
FortiSIEM	NIDS/HIDS	Costly	Anomaly		✓	✓			✓	✓	36
Rapid7 Nexpose	NIDS/HIDS	Costly	Signature		✓	✓			✓	✓	37
OpenDXL by McAfee	HIDS	Free	Signature/Anomaly		✓	✓			✓		38
RSA NetWitness	NIDS/HIDS	Costly	Signature/Anomaly		✓	✓				✓	39
Juniper Networks SRX	NIDS	Costly	Signature		✓	✓				✓	40
Trustwave SIEM	NIDS/HIDS	Costly	Anomaly		✓	✓				✓	41
SIEMonster	NIDS/HIDS	Free	Anomaly		✓				✓	✓	42
Fortinet FortiGate IPS	NIDS	Costly	Signature		✓	✓			✓	✓	43
Blue Coat ProxySG	NIDS	Costly	Signature		✓					✓	44
EventTracker	NIDS/HIDS	Costly	Anomaly			✓				✓	45
NetFlow Analyzer	NIDS	Costly	Anomaly		✓	✓			✓		46
WatchGuard IPS	NIDS	Costly	Signature		✓	✓			✓	✓	47
Huawei FusionSphere Cloud IDS	NIDS	Costly	Anomaly		✓					✓	48
Sumo Logic	NIDS/HIDS	Costly	Anomaly		✓	✓				✓	49
ArcSight by Micro Focus	NIDS/HIDS	Costly	Anomaly		✓	✓				✓	50
Trend Micro Deep Discovery	NIDS	Costly	Signature		✓	✓				✓	51
Vectra AI	NIDS/HIDS	Costly	Anomaly		✓	✓				✓	52
FireEye Network Security	NIDS	Costly	Signature		✓	✓				✓	53
Zabbix	HIDS	Free	Anomaly		✓			✓	✓		54
CrowdStrike Falcon	HIDS	Costly	Signature			✓	✓		✓	✓	55
Dynatrace	NIDS/HIDS	Costly	Anomaly		✓	✓				✓	56
Symantec Endpoint Protection	HIDS	Costly	Signature		✓	✓	✓		✓	✓	57
AlienVault USM	NIDS/HIDS	Costly	Signature/Anomaly		✓				✓	✓	58
Nmap	NIDS/HIDS	Free	Anomaly		✓	✓	✓	✓			59
Wazuh	HIDS	Free	Signature/Anomaly		✓	✓	✓		✓		60
Malwarebytes Endpoint Protection	HIDS	Costly	Signature			✓	✓		✓		61
Sumo Logic Cloud SIEM	NIDS/HIDS	Costly	Anomaly		✓	✓				✓	62
ESET NOD32 Network Detection	HIDS	Costly	Anomaly		✓			✓	✓		63
OpenVAS	NIDS	Free	Signature		✓				✓		64
Cybereason Endpoint Detection and	HIDS	Costly	Signature		✓	✓	✓			✓	65
											(Новий)

Рисунок 4.3 – Таблиця характеристик систем виявлення вторгнень

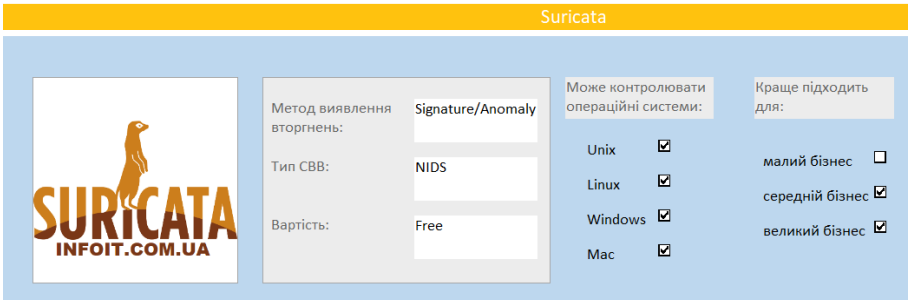
В розробленій СВВ користувач може переглядати список наявних СВВ з їх емблемами (рис.4.4), а адміністратор СВВ - додавати описи відсутніх СВВ.

numer	СВВ		Клацніть, щоб додати
1	OSSEC	(1)	
2	Suricata	(1)	
3	Security Onion	(1)	
4	Snort	(1)	
5	Bro	(1)	
6	SolarWinds Security Event	(1)	
7	Open WIPS-NG	(1)	
8	Sagan	(1)	
9	Mcafee Network Security Platform	(1)	
10	Palo Alto Networks	(1)	
11	Palo Alto Networks	(1)	
12	AAFID	(0)	
13	Prelude SIEM	(0)	
14	NetSTAT	(1)	
15	Shadow	(1)	
16	ASAX	(1)	
17	Cisco IPS	(1)	
18	Arbor Networks Spectrum	(1)	
19	InfoWatch ASAP	(1)	
20	Symantec DeepSight Threat Manag	(1)	
21	Tipping Point NGIPS	(1)	
22	Axoft invGUARD	(1)	
23	DefensePro	(1)	
24	KATA Platform	(1)	
25	Samhain	(1)	
26	Splunk	(1)	
27	IBM Qradar	(1)	
28	Check Point Security Management	(1)	
29	AlienVault OSSIM	(1)	
30	LogRhythm	(1)	
31	FortiSIEM	(1)	
32	Rapid7 Nexpose	(1)	
33	OpenDXL by McAfee	(1)	
34	RSA NetWitness	(1)	
35	Juniper Networks SRX	(1)	
36	Trustwave SIEM	(1)	
37	SIEMonster	(1)	
38	Fortinet FortiGate IPS	(1)	
39	Blue Coat ProxySG	(1)	
40	EventTracker	(1)	
41	NetFlow Analyzer	(1)	
42	WatchGuard IPS	(1)	
43	Huawei FusionSphere Cloud IDS	(1)	
44	Sumo Logic	(1)	
45	ArcSight by Micro Focus	(1)	
46	Trend Micro Deep Discovery	(1)	
47	Vectra AI	(1)	
48	FireEye Network Security	(1)	
49	Zabbix	(1)	
50	CrowdStrike Falcon	(1)	
51	Dynatrace	(1)	
52	Symantec Endpoint Protection	(1)	
53	AlienVault USM	(1)	
54	Nmap	(1)	
55	Wazuh	(1)	
56	Malwarebytes Endpoint Protection	(1)	
57	Sumo Logic Cloud SIEM	(1)	
58	ESET NOD32 Network Detection	(1)	
59	OpenVAS	(1)	

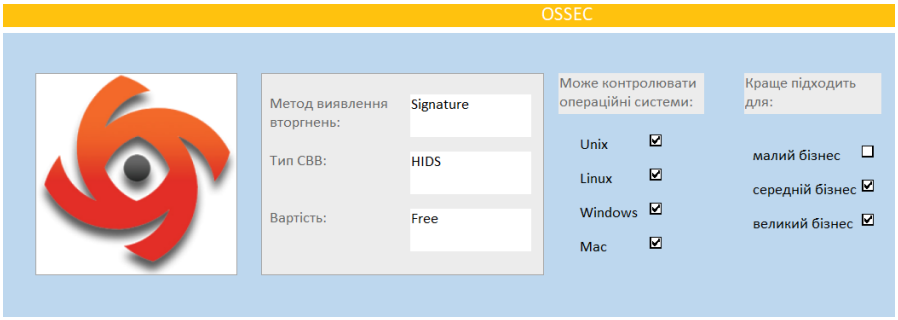
Рисунок 4.4 – Список систем виявлення вторгнень в базі із прикріпленими зображення їх емблем

Для того перегляду в СППР всіх відомостей про окремі СВВ була створена система типових форм, приклади яких наведені на рис.4.5.

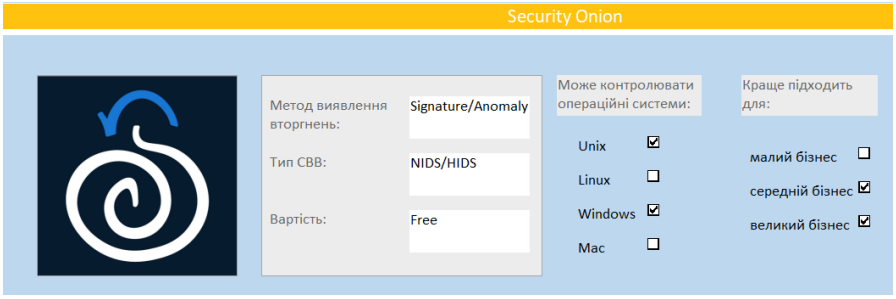
а) *Suricata*



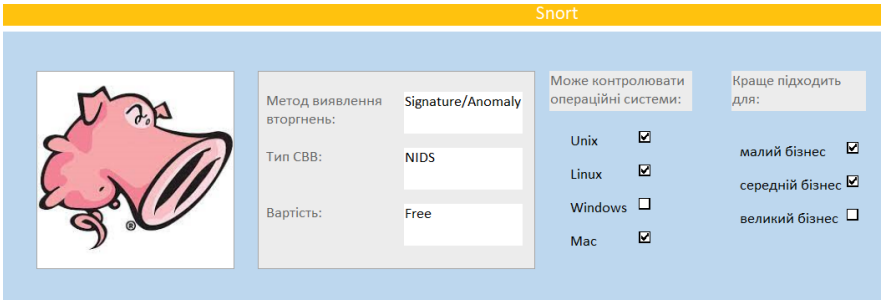
б) *OSSES*



в) *Security Onion*



г) *Snort*



д) *Bro (Zeek)*

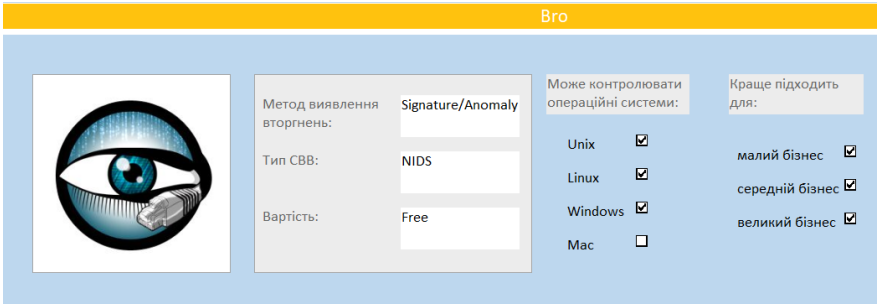
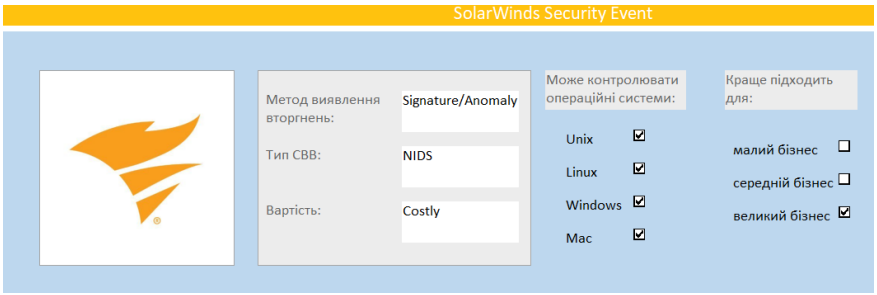
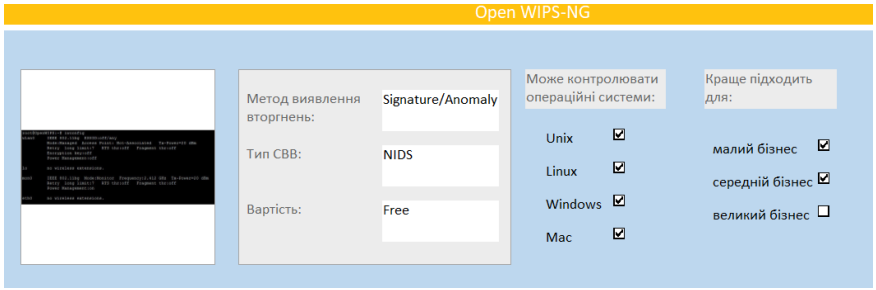


Рисунок 4.5 – Відомості про СВВ

е) *SolarWinds Security Event*

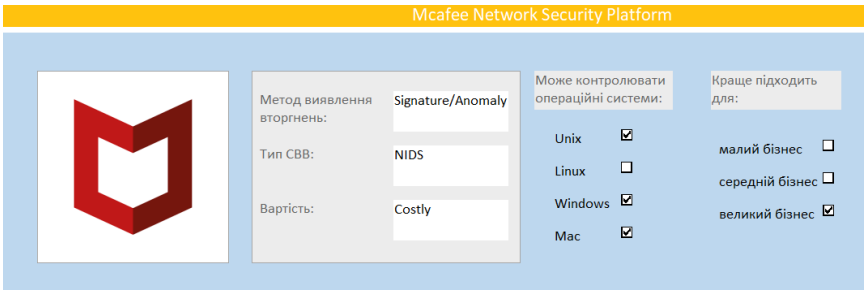


є) *Open WIPS-NG*

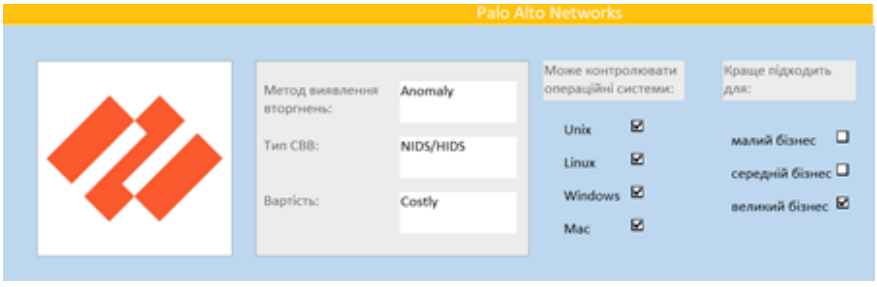


ж) *Sagan*

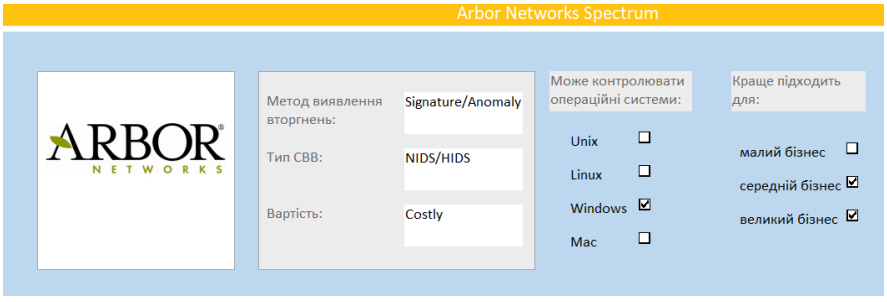
з) *Mcafee Network Security Platform*



и) *Palo Alto Networks*

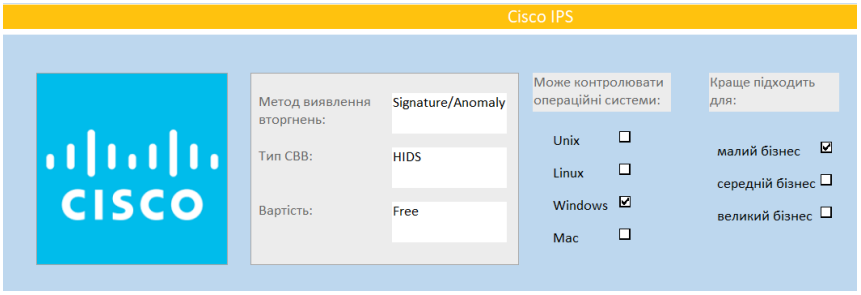


і) *Arbor Network Spectrum*

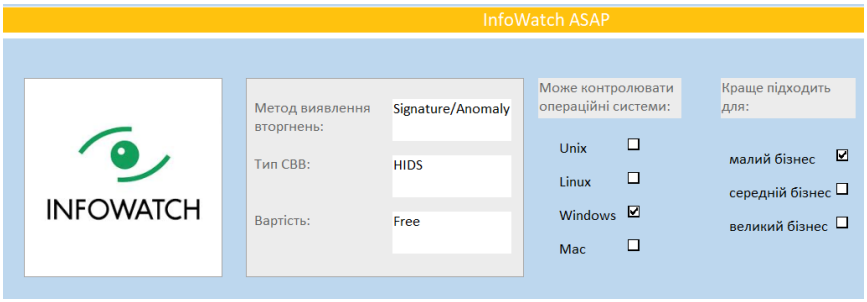


Продовження рис.4.5

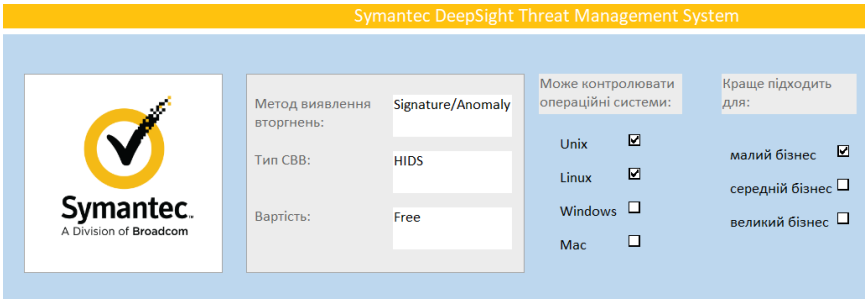
ї) *Cisco IPS*



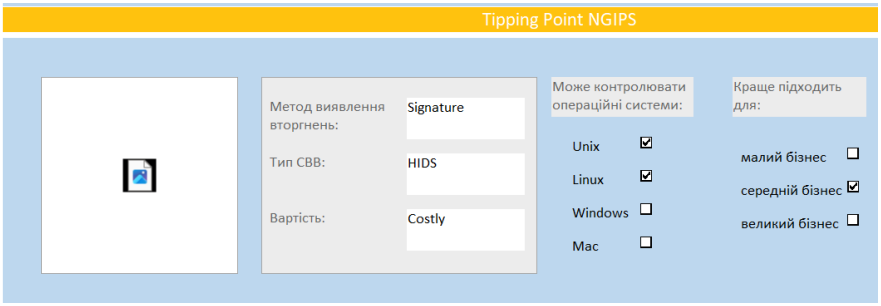
к) *InfoWatch ASAP*



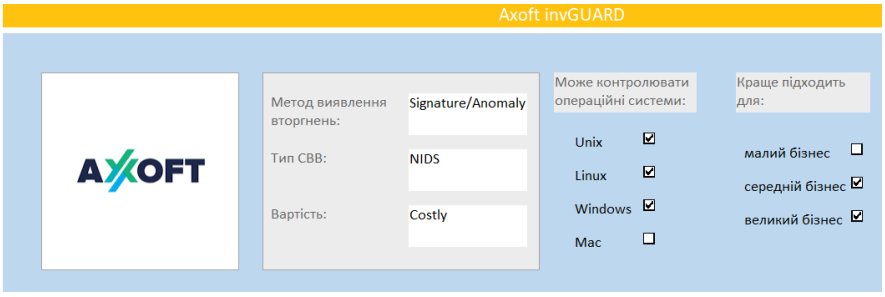
л) *Symantec DeepSight Threat Management System*



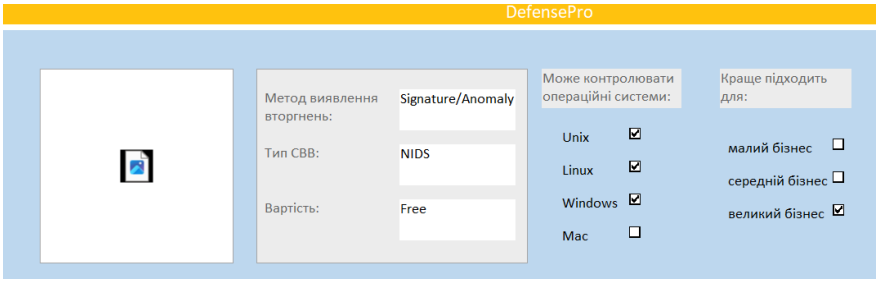
м) *Tipping Point NGIPS*



н) *Axoft invGUARD*

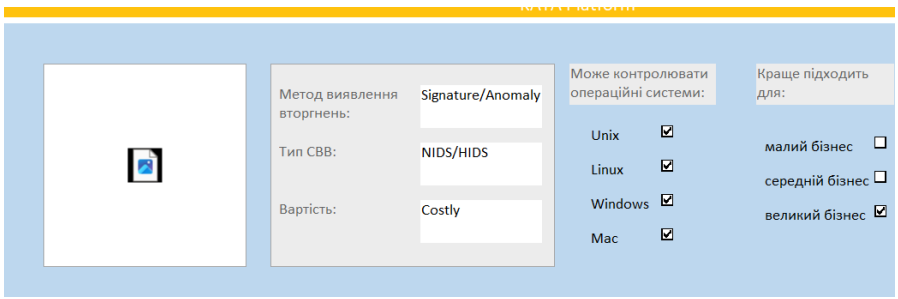


о) *DefensePro*

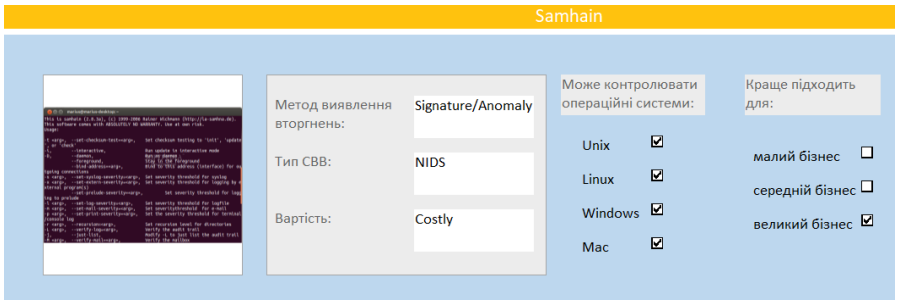


Продовження рис.4.5

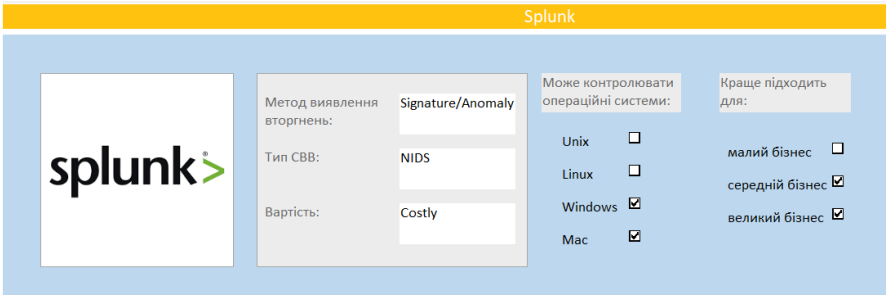
п) *KATA Platform*



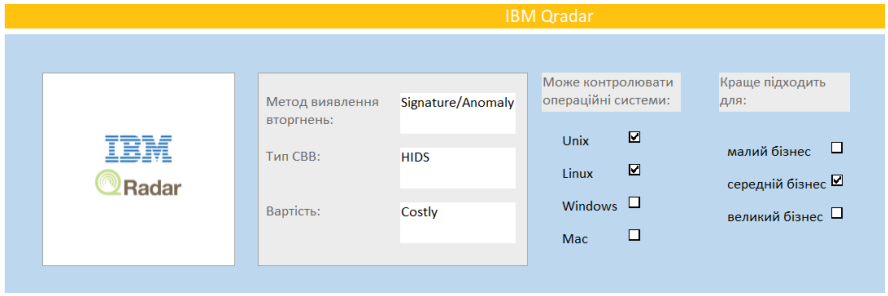
р) *Samhain*



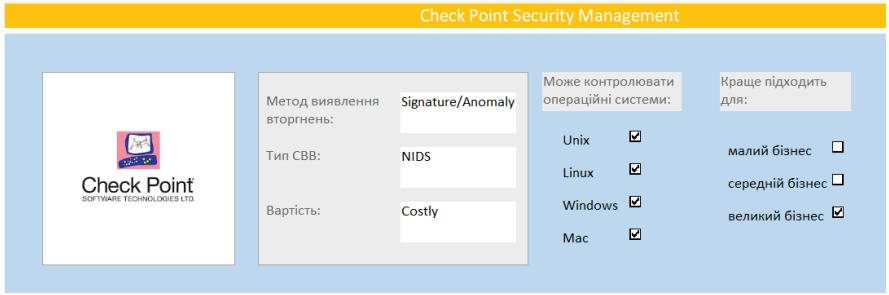
с) *Splunk*



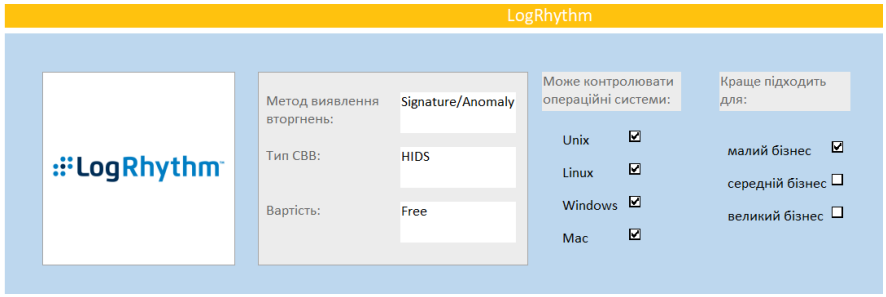
т) *IBM Qradar*



у) *Check Point Security Mamagement*

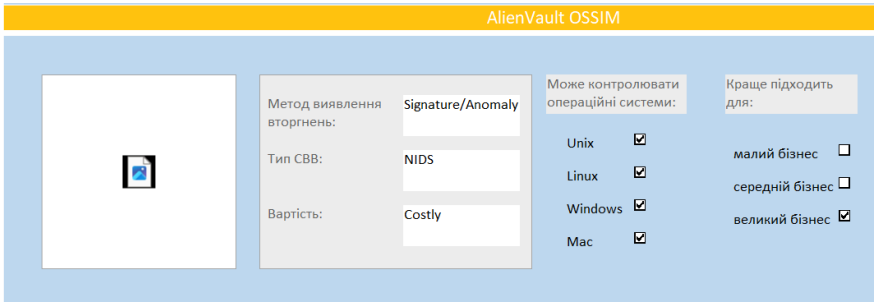


ф) *LogRhythm*

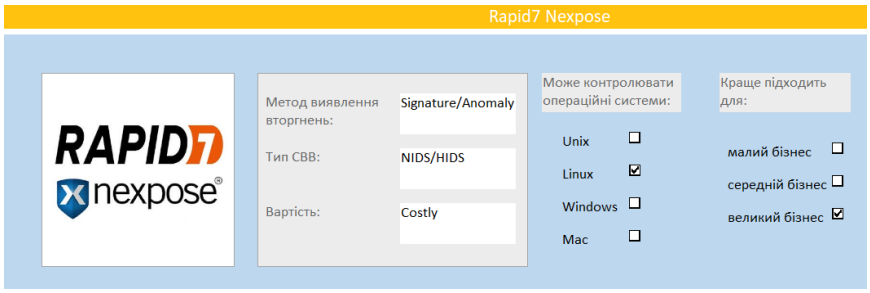


Продовження рис.4.5

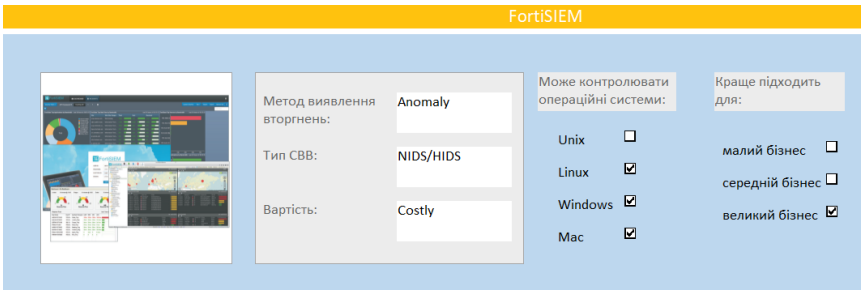
х) *AllenVault OSSIM*



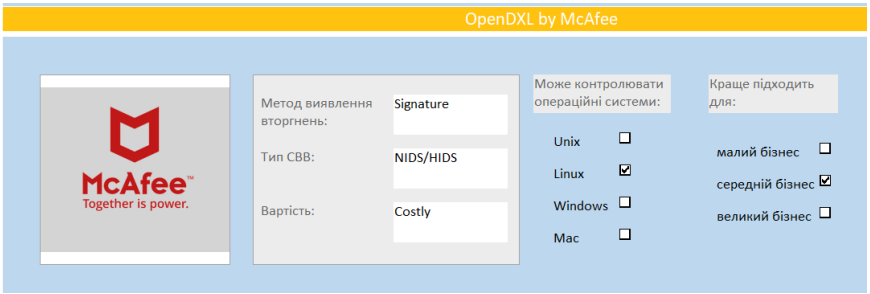
ц) *Rapid7 Nexpose*



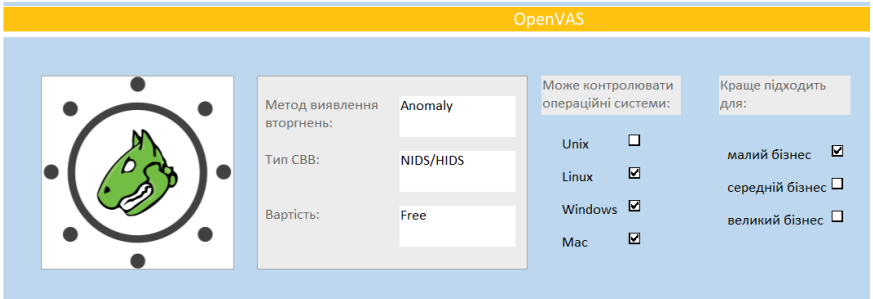
ч) *FortiSIEM*



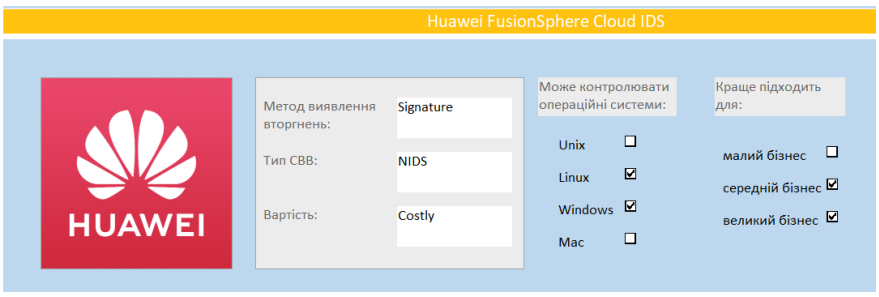
ш) *OpenDXL by McAfee*



щ) *OpenVAS*

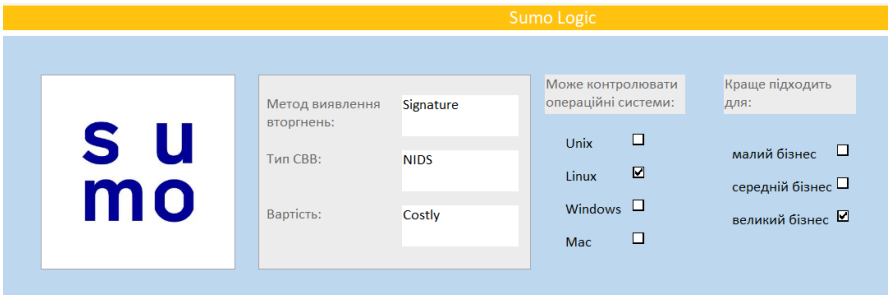


ю) *Huawei FusionSphere Cloud IDS*



Продовження рис.4.5

я) *Sumo Logic*



Продовження рис.4.5

Блок інформаційної підтримки СППР (див.рис.3.11) може містити: процедури вибірки даних з блоку «База даних» СВВ і видавати інформацію за фільтром, обраним користувачем. В цьому ж блоці, окрім опису самої СППР, містяться методичні вказівки для користувачів і посилання на інформаційні джерела (підручники, сайти виробників СВВ, тематичні форуми, наукові журнали, матеріали конференцій, копії статей і тез в базі, методичні рекомендації тощо) з різноманітних питань дослідження, проектування та експлуатації СВВ.

Відомості в блок інформаційної підтримки вносяться адміністратором СППР і дозволяють ознайомлювати користувачів із проблемами і ефективними практиками застосування СВВ та їх налаштування.

4.3 Підбір системи для виявлення вторгнень за вимогами користувача

При виборі системи виявлення вторгнення будемо враховувати критерії і вимоги перелічені в пунктах 1.3 і 4.3 даної дипломної роботи. Ці пункти включають в себе характеристики за якими ми у вікні рис.4.6 виберемо необхідну СВВ, перелічимо їх:

– за рівнем виявлення атак (*NIDS/HIDS*);

– за вартість (*Free/Costly*);

– за методами аналізу (*Signature/Anomaly*);

– операційна система, якій надається перевага (*Unix, Linux, Windows, Mac*), і здатність працювати з якою є обов’язковою для СППР;

– для якого масштабу бізнесу буде використовуватись? (малий, середній, великий).

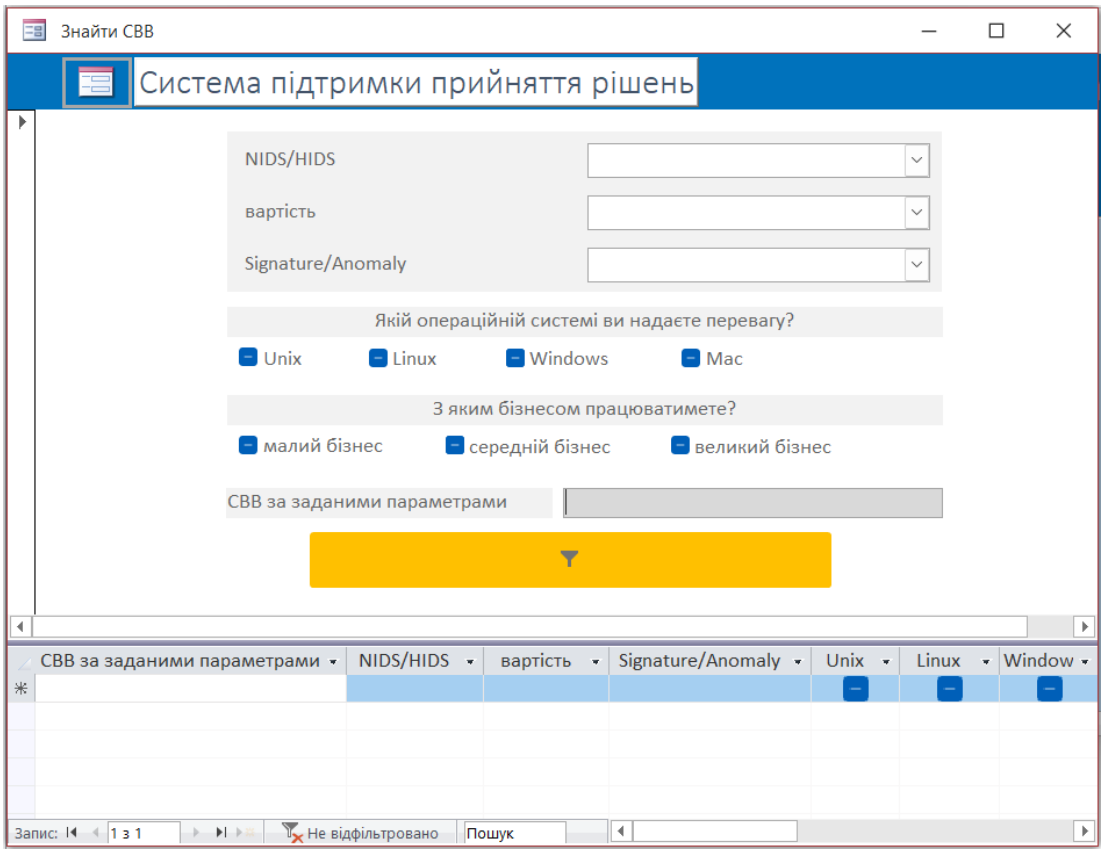


Рисунок 4.6 – Вікно СППР для вибору СВВ

Проведемо тестовий запуск системи з зазначеними нами критеріями вибору. До прикладу проведемо пошук такої СВВ щоб, вона:

– була безкоштовною;

– використовувала *Signature/Anomaly* для аналізу трафіку;

– працювала з операційною системою *Windows*;

– була орієнтована на роботу з малим бізнесом.

При введенні параметрів пошуку (критеріїв вибору СППР) частина з них обирається із списків, а частина – позначається прапорцями (рис.4.7). При цьому не обов’язково заповнювати всі критерії. Ті критерії, що не були обрані, просто не будуть грати роль фільтрів. СППР спрямована на оптимізацію роботи користувача: надає потрібну інформацію і мінімізує витрати часу.

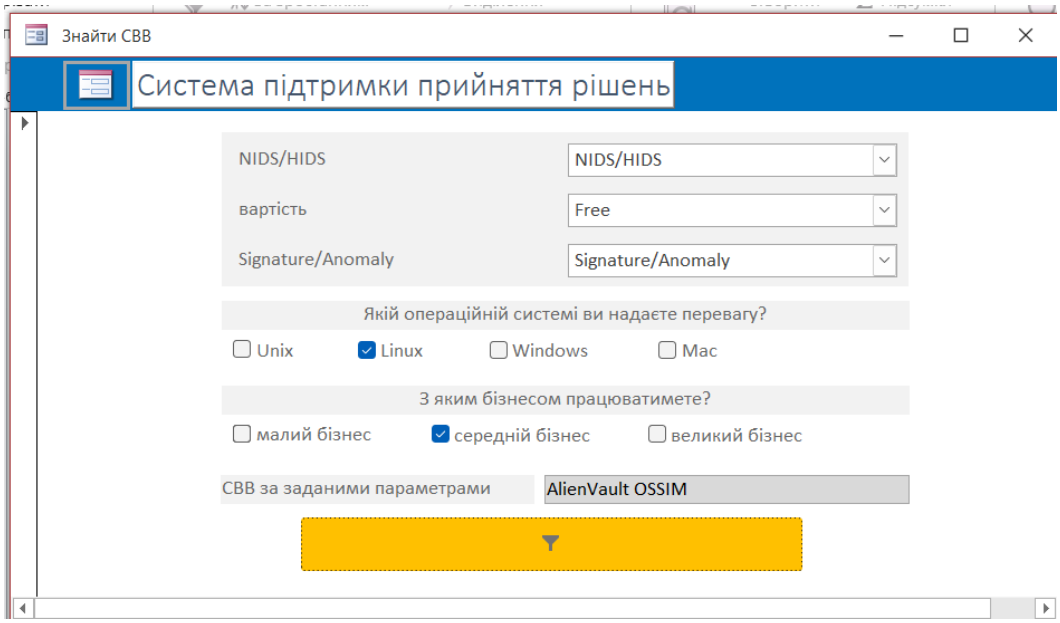


Рисунок 4.7 – Вікно вибору СППР із заданими параметрами пошуку

За критеріями які ми ввели на рис.4.7, СППР рекомендує (рис.4.8) три СВВ, які підходять за всіма критеріями: *Bro*, *Open WIPS-NG* і *Sagan*.

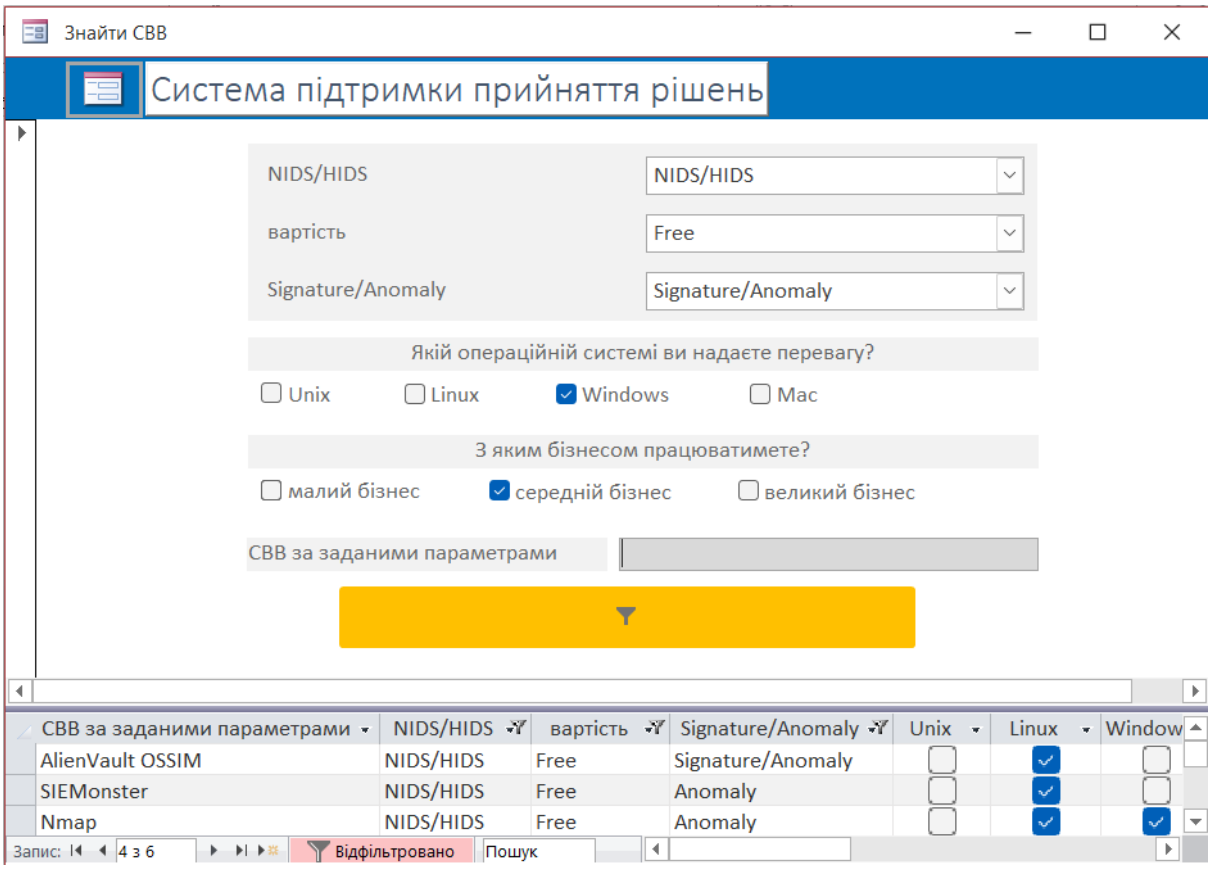


Рисунок 4.8 – СВВ, рекомендовані СППР

4.5 Рекомендації з впровадження та вдосконалення розробки

Остаточне рішення щодо вибору системи виявлення вторгнень із запропонованого СППР списку залишається за користувачем, оскільки модель лише формує перелік варіантів відповідно до визначених критеріїв.

У випадку, якщо після виконання пошуку за індивідуальними критеріями користувач отримує список відповідних систем, але не може обрати одну з них, СППР надає додаткові рекомендації. Ці рекомендації представлені у вигляді рейтингового списку, де кожній системі присвоєно оцінку, яка відображає її технічні характеристики; чим вище значення оцінки (максимальна можлива – 10 балів), тим кращими є показники системи.

Оцінювання базується на таких критеріях, як здатність виявляти атаки, підтримка роботи з іншими сигнатурами, можливість функціонування в багатопоточному режимі, а також якість документації та рівень зв’язку з розробниками, визначені в пункті 1.3.

ВИСНОВКИ

У цій кваліфікаційній роботі:

- проведено аналіз доступних літературних джерел та визначено критерії класифікації систем виявлення вторгнень, які доцільно використовувати в рамках даного дослідження;
- сформульовано критерії прийняття рішень для вибору систем виявлення вторгнень;
- розроблено основні алгоритми, а також створено структуру СППР;
- апробовано розроблені алгоритми і доведено працездатність розробленої СППР для вибору систем виявлення вторгнень як елемента комплексу захисту комп'ютерних мереж.

Робота має практичну значимість, її результати можуть бути використані при проектуванні захищених локальних мереж та в навчальному процесі за освітньою програмою «Системи технічного захисту інформації, автоматизація її обробки» зі спеціальностей 125 «Кібербезпека» та 141 «Електроенергетика, електротехніка та електромеханіка».

Дана робота була апробована на X (2022 р.), XI (2023 р.) і XII (2024 р.) Всеукраїнських науково-технічних конференціях з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті»

ПЕРЕЛІК ПОСИЛАНЬ

1. *Abdulhammed R., Faezipour M., Musafer H., Abuzneid, A. Efficient Network Intrusion Detection Using PCA-Based Dimensionality Reduction of Features. International Symposium on Networks, Computers and Communications (ISNCC 2019), 1-6. ULR: https://doi.org/10.1109/ISNCC.2019.8909140.*

2. *Alqahtani A., AlShaher H. Anomaly-Based Intrusion Detection Systems Using Machine Learning. Cybersecurity and Information Managemen. 2024. Vol. 14. No. 01. PP. 20-33. URL: https://americaspg.com/article/pdf/2836*

3. *Alsaedi A.; Moustafa N., Tari Z., Mahmood A., Anwar A.N. TON-IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems. IEEE Access 2024, 1, 165130–165150. URL: https://ieeexplore.ieee.org/document/9189760*

4. *Alsharari G.A. Developing an Intrusion Detection System (IDS) For Network Security Using Machine Learning. International Journal of Intelligent Systems and Applications in Engineering, (2024). 12(4), 2005–2026. URL: https://ijisae.org/index.php/IJISAE/article/view/6519*

5. *Ashraf Uddin A., Aryal S., Reda B.M, Al-Hawawreh M., Talukder A. Hierarchical Classification for Intrusion Detection System: Effective Design and Empirical Analysis. Computer Science: Cryptography and Security. https://doi.org/10.48550/arXiv.2403.13013 URL: https://arxiv.org/abs/2403.13013*

6. *Belarbi O., Khan A., Carnelli P.. Spyridopoulos T. An Intrusion Detection System Based on Deep Belief Networks. Science of Cyber Security. SciSec 2022. Vol. 13580. URL: https://doi.org/10.48550/arXiv.2207.02117, https://arxiv.org/abs/ 2207.02117*

7. *Bridges S.M., Vaughn R.B.. Fuzzy data mining and genetic algorithms applied to intrusion detection, USA, in in Proceedings of 12th Annual Canadian Information Technology Security Symposium, 2000. https://www.csee.umbc.edu/ csee/research/cadip/readings/DMID/005slide.pdf*

8. *Elijah M. Maseno, Zenghui Wang , Hongyan Xing. A Systematic Review on Hybrid Intrusion Detection System. Hindawi. Security and Communication Networks. Vol. 2022, Article ID 9663052, 23 pages URL: https://pdfs.semanticscholar.org/010e/79a21ab1a50036ae30db53ab9b1b369dc2fa.pdf, https://doi.org/10.1155/2022/9663052.*

9. Ibokette A. I., Ogundare T. O., Anyebe A. P., Odeh I. I., Okafor, F. C. Mitigating Maritime Cybersecurity Risks Using AI-Based Intrusion Detection Systems and Network Automation During Extreme Environmental Conditions. International Journal of Scientific Research and Modern Technology, 3(10). URL: https://doi.org/10.38124/ijsrmt.v3i10.73

10. Immastephy J., Punitha K. Systematic Review on Network Intrusion Detection System based on machine learning and deep learning approach. E3S Web of Conferences 540, 14006 (2024). ICPES 2023. URL: https://www.e3s-conferences.org/articles/e3sconf/pdf/2024/70/e3sconf_icpes2024_14006.pdf

11. Koppula M., Joseph L.M.I. Leo. A Network Intrusion Detection System Based on Enhanced CNN2D for IoT Architecture. SSRG International Journal of Electronics and Communication Engineering. VOl. 11, No. 4, pp. 68-79, 2024. Crossref, https://doi.org/10.14445/23488549/IJECE-V11I4P108

12. Ngo D.-M., Temko A., Murphy C. C., Popovici E., FPGA hardware acceleration framework for anomaly-based intrusion detection system in IoT. Proc. 31st Int. Conf. Field-Program. Logic Appl., *pp. 69-75, 2021. URL: https://cora.ucc.ie/items/175fca1d-9c48-41f6-b889-31cc128ff8e3*

13. Qingyu Zeng, Yuko Hara-Azumi Hardware/Software Codesign of Real-Time Intrusion Detection System for Internet of Things Devices. IEEE Internet of Things Journal. Vol.11, Issue: 12, 15 June 2024. PP. 22351 – 22363. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10478082

14. *Ross A. Security Engineering: A Guide to Building Dependable Distributed Systems. - Indianapolis, Indiana: Wiley Publishing, Inc, 2008. – 1083 p.URL:https://terrorgum.com/tfox/books/security_engineering_a_guide_to_building_dependable_distributed_systems.pdf.*

15. *Sen S., Clark J.A., Tapaidor J.E. Power-Aware Intrusion Detection in Mobile Ad Hoc Networks.* – 2006. *URL: https://link.springer.com/chapter/10.1007/978-3-642-11723-7_15*

16. Singh Amit, Prakash Jay, Kumar Gaurav, Jain Praphula, Ambati Loknath. Intrusion Detection System/ Journal of Database Management.2024. DO - 10.4018/JDM.338276. URL: https://www.researchgate.net/publication/378214294_Intrusion_Detection_System

17. Suzen A.A. Developing a multi-level intrusion detection system using hybrid-DBN. Ambient Intelligence and Humanized Computing, vol. 12, no. 2, pp. 1913–1923, 2021. URL: https://www.researchgate.net/publication/342365811_Developing_a_Multi-Level_Intrusion_Detection_System_Using_Hybrid-DBN

18. *Vaiyapuri T., Binbusayyis A.. Deep self-taught learning framework for intrusion detection in cloud computing environment. IAES International Journal of Artificial Intelligence (IJ-AI). 2024. ULR: https://doi.org/10.11591/ijai.v13.i1.pp747-755.*

19. *Unified Performance Management Platform. URL: https://www.colasoft.com/upm/.*

20. *Wang, C., Ye, X., He, X., Tian, Y., Gong, L.. Two-Level Feature Selection Method for Low Detection Rate Attacks in Intrusion Detection. Social Informatics and Telecommunications Engineering. 2019. ULR: https://doi.org/10.1007/978-3-030-21373-2_58.*

21. Zaid Mustafa, Amin Rashid, Aldabbas Hamza, Ahmed Naeem. Intrusion detection systems for software-defined networks: a comprehensive study on machine learning-based techniques. Cluster Computing. No.27(7). 2024. DOI: 10.1007/s10586-024-04430-6. URL: https://www.researchgate.net/publication/ 380101279 _Intrusion_detection_systems_for_software-defined_networks_a_comprehensive_study _on_machine_learning-based_techniques#read-preview

22. Zeeshan M. et al.. Protocol-based deep intrusion detection for DoS and DDoS attacks using UNSW-NB15 and Bot-IoT data-sets. IEEE Access*, vol. 10, pp. 2269-2283, 2022. URL: https://ieeexplore.ieee.org/document/9656911*

23. Zhang L., Ma D.. A hybrid approach toward efficient and accurate intrusion detection for in-vehicle networks. IEEE Access. Vol. 10. Article ID 10866. 2022. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9687591

24. Богуш В.М., Довидьков О.А. Проектування захищених комп'ютерних систем та мереж. Навчальний посібник. - К.: ДУІКТ, 2008. - 500 с. *URL: https://studfile.net/preview/5367404/page:6/*

25. Головний сайт центру виявлення кіберзагроз *URL: http://cert.gov.ua*

26. Завада А. А., Самчишин О. В., Охрімчук В. В. Аналіз сучасних систем виявлення атак і запобігання вторгненням. Інформаційні системи. Житомир: Збірник наукових праць ЖВІНАУ, 2012. Т. 6, №12. С. 97-106. *URL: http://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf*

27. Закон України «Про основні засади забезпечення кібербезпеки України». *URL*: *https://zakon.rada.gov.ua/laws/show/2163-19.*

28. Катренко А.В. Системний аналіз об'єктів та процесів комп'юте7 ризації: Навчальний посібник. - Львів : Новий Світ-2000", 2003. - 424 с.

29. Коваль Т. Метод оцінки систем виявлення вторгнень: Дипломна робота на здобуття ступеня бакалавра. – Нац. ун-т «Київський політехнічний інститут». – 2019. *URL*: *https://ela.kpi.ua/handle/123456789/31329.*

30. Колодчак О. М. Сучасні методи виявлення аномалій в системах виявлення вторгнень. Вісник Національного ун-ту «Львівська політехніка». 2012. № 745 : Комп'ютерні системи та мережі. – С. 98–104. *URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/nov/6726/16-98-104.pdf*

31. Конвенція про кіберзлочинність. *URL*: *https://zakon.rada.gov. ua/ laws/show/994_575#Text*.

32. Корченко А.О. Методи ідентифікації аномальних станів для систем виявлення вторгнень: Монографія. - Київ: ЦП «Компринт», 2019 – 361 с.

33. Литвинов В.В. Аналіз систем та методів виявлення несанкціонованих вторгнень у комп'ютерні мережі /В.В.Литвинов, Н.Стоянов, І.С.Скітер, О.В.Трунова, А.Г.Гребенник. Математичні машини і системи. 2018. №1. С.31-40. *URL*: *http://www.immsp.kiev.ua/publications/articles/2018/2018_1/ 01_2018_Lytvynov.pdf*

34. Лук’яненко Т.Ю., Поночовний П.М., Легомінова С.В. Методика виявлення мережевих вторгнень і ознак комп'ютерних атак на основі емпіричного підходу. Сучасний захист інформації №2(50), 2022. С.15-21. *URL*: *https://journals.dut.edu.ua/index.php/dataprotect/article/view/2634/2533*

35. Мохін М.І. Розробка системи виявлення вторгнень реального масштабу часу: Дипломна робота на здобуття ступеня магістра. – Нац. гірничий ун-т. – 2018. *URL: https://ir.nmu.org.ua/bitstream/handle/123456789/151303/%D0%9C%D0%BE%D1%85%D0%BD%D1%96%D0%BD.pdf?sequence=1&isAllowed=y.*

36. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. *URL*: *http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106342*.

37. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. *URL*: *http://dstszi.kmu.gov.ua/dstszi/control/uk/ publish/article;jsessionid=afd6198c23cb1f96abafd7189bbdce03?showhidden =1&art_id=101870&cat_id=89734&ctime=1344501089407.*

38. Обидєннова Т.С., Гусаров О.О., Антипцева О.Ю. Методи прийняття управлінських рішень в умовах розроблення, впровадження та функціонування системи менеджменту інформаційної безпеки //Проблеми системного підходу в економіці. - 2019. - Вип. 2(1). - С. 153-157. *URL*: *http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/PSPE_print_2019_2%281%29__25.pdf.*

39. План заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України, затверджений Розпорядженням Кабінету міністрів України № 1163-р.від 19 грудня 2023 року. *URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text*

40. План реалізації Стратегії кібербезпеки України. *URL*: *https://zakon.rada.gov.ua/laws/show/n0087525-21#Text.*

41. Стасєв Ю.В. Дослідження систем виявлення та попередження вторгнень у комп'ютерні мережі. Інформаційні технології. 2014. *URL: http://dspace.kntu.kr.ua/jspui/handle/123456789/2982*.

42. Стасюк А. И., Корченко А. А. Базовая модель параметров для построения систем выявления атак // Захист інформації. - 2012. - № 2. - С. 47–51. *URL*: *http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM =2&I21 DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name =PDF/Zi_2012_2_12.pdf*

43. Стефанюк Ю.В. Інтелектуальні засоби в системах виявлення та запобігання вторгнень. Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. Миколаїв: НУК. 2023. С.129-133. *URL: https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf*

44. Стратегія національної безпеки України. *URL*: *https://zakon.rada.gov.ua/laws/show/392/2020#Text.*

45. Стратегія кібербезпеки України. Безпечний кіберпростір - запорука безпечного розвитку країни. *URL*: *https://zakon.rada.gov.ua/ laws/show/ 447/2021#n7.*

46. Толюпа С. В., Плющ О. Г., Пархоменко І. І. Побудова систем виявлення атак в інформаційних мережах на нейромережевих структурах. К1бербезпека: освіта, наука, техніка. №2(10), 2020. С.169-181. *URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/217/194*

47. Тотх М. Системи виявлення вторгнень для водного транспорту як основний метод захисту. Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. Миколаїв: НУК. 2023. С.43-46. *URL: https://nuos.edu.ua/wp-content/uploads/2024/03/SPIBT-2023-Materiali.pdf*