МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ГАРДЄР ОЛЕКСАНДР СЕРГІЙОВИЧ

Допускається до захисту:
в. о. завідувача кафедри
прикладної математики та
кібербезпеки,
д – р філософії з математики,
_____А.В. Луценко
«__»_____20__р.

ВИЗНАЧЕННЯ ОПТИМАЛЬНИХ ПАРАМЕТРІВ КОНФІГУРАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ В УМОВАХ МЕРЕЖЕВОЇ РОЗВІДКИ

Спеціальність 125 Кібербезпека

Кваліфікаційна (бакалаврська) робота

Керівник:
канд. техн. наук, доцент,
доцент кафедри прикладної
математики та кібербезпеки,
Загоруйко Л. В.

Оцінка:___/___/_____
(бали за шкалою ЄКТС/за національною шкалою)
Голова ЕК:_____
(підпис)

Вінниця - 2024

АНОТАЦІЯ

Гардєр О.С. Визначення оптимальних параметрів конфігурації інформаційних систем в умовах мережевої розвідки. Спеціальність 125 «Кібербезпека». Донецький національний університет імені Василя Стуса, Вінниця, 2024.

У кваліфікаційній (бакалаврській) роботі досліджено оптимальні параметри конфігурації інформаційних систем в умовах мережевої розвідки, зокрема на прикладі локальної мережі. Проаналізовано основні інформаційні активи мережі, розроблено методологію налаштування та оптимізації конфігурації інформаційних систем з використанням OpenVAS та Nessus Essentials. Наведено приклад застосування OpenVAS та Nessus Essentials для сканування мережевих вузлів, виявлення вразливостей та визначення оптимальних параметрів конфігурації для забезпечення підвищеної безпеки та ефективності мережі.

Ключові слова: інформаційні системи, мережева розвідка, Nessus Essentials , OpenVAS, локальна мережа, конфігурація, оптимізація, активи, безпека. 45 с., 2 табл., 27 рис., 41 джерел.

ANNOTATION

Garder O.S. Determination of optimal configuration parameters of information systems in the conditions of network intelligence. Specialty 125 «Cybersecurity». Vasyl Stus Donetsk National University, Vinnytsia, 2024.

In the qualifying (bachelor's) work, the optimal parameters of the configuration of information systems in the conditions of network intelligence were investigated, in particular, on the example of a local network. The main information assets of the network were analyzed, the methodology for setting up and optimizing the configuration of information systems using OpenVAS and Nessus Essentials was developed. An example of using OpenVAS and Nessus Essentials for scanning network nodes, detecting vulnerabilities, and determining optimal configuration parameters to ensure increased network security and

efficiency is given.

Keywords: information systems, network intelligence, Nessus Essentials, OpenVAS, local network, configuration, optimization, assets, security. 45 pp., 2 tables, 27 figures, 41 sourse.

ЗМІСТ

ВСТУП

У сучасному світі інформаційні системи стають дедалі важливішими для функціонування різних галузей економіки, державного управління та оборони. З початком повномасштабного вторгнення кожен з нас хоча б раз чув про загрози, пов'язані з мережевою розвідкою та кібератаками. Часто з телевізійних новин попереджають про необхідність забезпечення захисту інформаційних систем, оскільки ці системи є привабливими цілями для країни-агресора. Але що саме розуміється під оптимальною конфігурацією інформаційних систем та як забезпечити їх захист від мережевої розвідки?

Інформаційні системи складаються з різноманітних складових, які є надзвичайно важливими, оскільки їх пошкодження або некоректне використання може вплинути на національні інтереси.

На сьогоднішній день існує чимало методів та засобів, які мають функціонал допомогти забезпечити безпеку в інформаційних системах. Це можуть бути програмні засоби антивірусного захисту, технології захисту від технічної розвідки та спеціалізовані системи оборони інформації. До засобів захисту також відносяться методи шифрування даних, використання брандмауерів, а також системи виявлення вторгнень.

Особливо актуальним питанням у період війни є забезпечення оптимальної конфігурації інформаційних систем для запобігання мережевій розвідці. Використання спеціалізованого програмного забезпечення, такого як OpenVAS та Nessus Scanner , дозволяє моделювати та визначати оптимальні параметри конфігурації інформаційних систем, що підвищить їх стійкість до кібератак та забезпечує безпеку даних.

Актуальність: В умовах постійного зростання ефективності кібератак особливо важливими є питання розробки та моделювання оптимальних параметрів конфігурації інформаційних систем в умовах мережевої розвідки, що дозволить знизити кількість вразливостей.

Мета дослідження: розробка підходів до моделювання оптимальних параметрів конфігурації інформаційних систем з використанням OpenVAS та

Nessus Scanner для вдосконалення їх захисту в умовах мережевої розвідки.

Для досягнення поставленої мети потрібно виконати наступні завдання:

1. Аналіз інформаційних систем та необхідність їх захисту від мережевої розвідки.

2. Проектування конфігурації інформаційних систем, визначення загальних правил проектування.

3. Визначення оптимальних параметрів конфігурації інформаційних систем в умовах мережевої розвідки.

4. Моделювання оптимальної конфігурації інформаційної системи з використанням OpenVAS та Nessus Essentials для визначення вразливостей, та найбільш ефективних заходів захисту.

Об’єкт дослідження – інформаційні системи та їх конфігурація в умовах мережевої розвідки.

Предмет дослідження – оптимальні параметри конфігурації інформаційних систем, методи та засоби їх захисту від мережевої розвідки з використанням OpenVAS та Nessus Scanner.

Практична значимість: результати дослідження можуть бути використані для підвищення рівня безпеки інформаційних систем у різних галузях економіки, державного управління та оборони. Визначення оптимальних параметрів конфігурації інформаційних систем дозволить зменшити вразливості та підвищити стійкість до кібератак, що є особливо актуальним в умовах війни. Використання спеціалізованого програмного забезпечення, такого як OpenVAS та Nessus Scanner, забезпечить ефективне виявлення та усунення потенційних загроз.

РОЗДІЛ І. АНАЛІЗ ЗАГРОЗ ТА ВИМОГ ДО ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

1.1. Огляд існуючих методів та засобів захисту інформаційних систем

Досліджуючи проблему інформаційних систем, було проаналізовано класифікацію вхідних даних і алгоритмів їх обробки (рис. 1.1).

Всі алгоритми, які може виконувати інформаційна система, можна поділити на чотири класи:

1. Алгоритми, що реалізують методи захисту інформації, і використовуються для:

а) обробка помилок інформаційної системи;

б) блокування даних, яка може включати в себе: установку захисних екранів, знищення (знешкодження) джерела інформації що може завдати шкоди системі;

в) перевірка коду або "психоаналіз" для виявлення прихованих програм та/або їх початкових причин [1].

2. Алгоритми, що відповідають за модифікацію існуючих програм і створення додаткових програм для обробки вхідних послідовностей [1].

3. Алгоритми, які можуть порушити нормальну роботу, тобто вивести систему з допустимого стану, що в більшості випадків рівносильно пошкодженню аж до руйнування. На додаток до алгоритмів, які система також може пошкодити, до цього класу належать так звані "несертифіковані" алгоритми (програми), які не пройшли якісного тестування. У самонавчальних системах постійно з'являються такі програми, в яких можуть виконуватися алгоритми другого сорту [1].

4. Всі інші алгоритми [1].

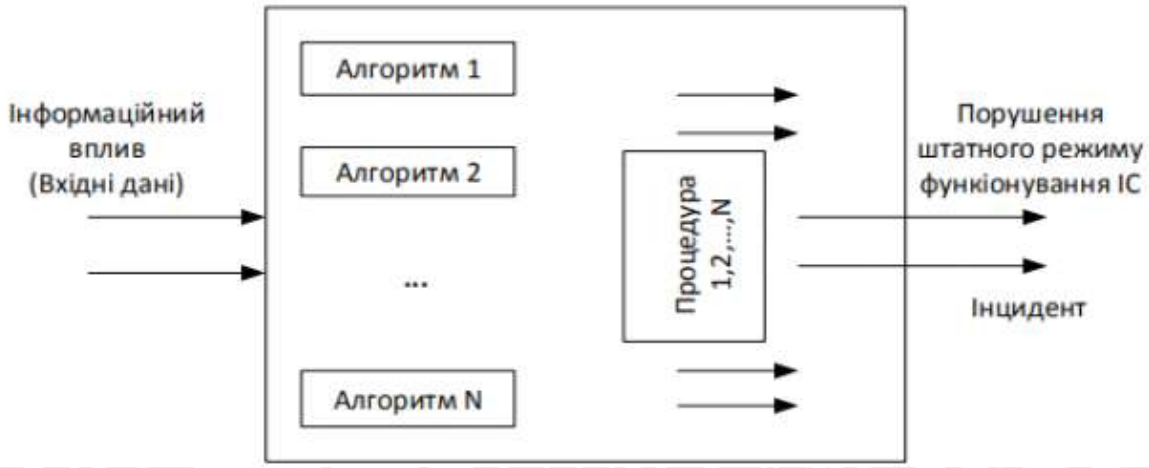

Рисунок 1.1 - Множина алгоритмів, які здатні виконувати ІС [2][15]

1.2. Характеристика об'єктів інформаційних систем, які потребують захисту

Метою інформаційної розвідки є активація алгоритмів, відповідальних за порушення нормального режиму роботи, тобто за виведення ІР з дозволеного стану.

Джерело впливу може бути як внутрішнім, так і зовнішнім (рис. 1.2).

Причини зовнішнього впливу в разі цілеспрямованого інформаційного нападу сховані у війні конкуруючих інформаційних систем за спільні ресурси, які забезпечують прийнятний режим існування для системи.

Причинами внутрішніх впливів є поява багатьох елементів всередині системи, підструктур, для яких нормальна робота стала неприйнятною в силу ряду обставин [2].

Таким чином, інформаційний вплив - це вхідні дані, призначені для активації алгоритмів в ІС, відповідальних за порушення нормального режиму роботи [1].

Класифікуємо впливи. Зовнішні і внутрішні впливи поділяються на свідомі (дійсні) і несвідомі (приховані) впливу (рис.1.2) [3].

Рисунок 1.2 - Класифікація впливів [8]

Очевидний вплив зазвичай направлено на порушення нормального функціонування системи. Однак немає значення, як система сприймає це, є важливим, щоб, якщо IP-адреса сприймає вхід як вплив, це чітко вказує на те, що вплив є очевидним[2].

Етапи обробки експліцитного впливу:

1. Система приймає дані.

2. Система оцінює надані дані. Чи впливають вхідні дані на результат? Якщо так, перейдіть до кроку Z, інакше перейдіть до кроку 1 [6].

3. Система проводить оцінку реальності. Якщо наслідки реальні, ми переходимо до пункту 4, інакше повертаємося до пункту 1 [2].

4. Система аналізує, чи є в неї здатність організувати захист і оцінити розмір власного збитку в разі втрати. У випадку організації захисту, якщо шкода оцінюється як менша (моральна, матеріальна тощо), ніж шкода, заподіяна внаслідок впливу, перейдіть до пункту 5, інакше - до пункту 7 [3].

5. Активація алгоритмів, які реалізують методи захисту інформації. Якщо цього буде недостатньо, тоді потрібно включити алгоритми, відповідальні за пошук нових нестандартних рішень даної проблеми [7].

6. Система проводить оцінку результатів інформаційної війни. У разі успіху перейдіть до кроку 1, інакше перейдіть до кроку 7 [5].

7. Під час виконання робот, які відповідають вимогам інформаційних зловмисників. Якщо система залишається зберігає статус

"працездатна", повертаємось до пункту 1, поки система продовжує функціонувати. [6].

З точки зору України Джерела інформаційних впливів, їх походження і внутрішня природа можна поділити на три категорії[8].

До першої категорії входять джерела зовнішнього впливу:

- зовнішні атаки;
- зміна потоків інформації зовні та всередині країни;
- ослаблення політичної, економічної та військової ролі України як у регіоні, так і у світі [6];
- підтримка та позитивне ставлення до дестабілізуючих сил в Україні;
- інтерес до інформаційних ресурсів України та прагнення встановити контроль над ними [4].

Друга категорія складається з таких джерел:

- зовнішні умови, які діють за межами України та не мають прямих ознак інформаційного впливу на країну;
- підвищення витрат на інформаційні операції та протидію дезінформації;
- соціальна напруга і політична нестабільність всередині країни [2].

Третя категорія включає в себе внутрішні чинники, що впливають на безпеку інформації в Україні:

- недостатній рівень захищеності інформації;
- недостатня фінансова підтримка заходів з інформаційної безпеки
- соціально-політична та морально-психологічна криза, викликана інформаційною війною.

Всі ці категорії впливають на інформаційну безпеку держави і, як наслідок, посилюють умови для інформаційної війни [9].

1.3. Вимоги до конфігурації інформаційних систем для забезпечення їх захисту

Розробка стратегій та тактик у інформаційних конфліктах ускладнюється внаслідок неоднозначного розуміння терміну "інформація". Згідно з законодавством України, "інформація" розглядається як документована чи публічно розголошена інформація про події та явища, що відбуваються в суспільстві, державі і оточуючому середовищі [9]. У той же час, у філософському аспекті "інформація" розглядається як система ідеальних уявлень про об'єкти, процеси і явища навколишнього світу, що виникають у свідомості людини. Однак ці визначення можуть не враховувати роль інформації як засобу впливу, що може обмежувати розмах інформаційної боротьби [10].

Зважаючи на різноманітність знань про інформацію, яка випливає на складність самого об'єкта дослідження, а також різних форм і методів його теоретичного розгляду, можна визначити один аспект, який виокремлюється і не обмежується іншими - філософський аспект [12].

Філософський підхід до проблематики, який розглядає взаємовідносини між суб'єктами та об'єктами, дає можливість розглядати інформацію як об'єкт боротьби і визначити сфери, в яких вона проводиться. Цей підхід сприяє створенню системи загальних і конкретних категорій інформаційної боротьби, що характеризуються відповідними об'єктами та засобами впливу, а також методами та формами їх застосування [11]. Розгляд загальних і індивідуальних категорій інформаційної війни може бути представлений за таким підходом (рис. 1.3) [15].

Термін "інформація" є основою для розуміння процесів, які відбуваються під час інформаційної війни.

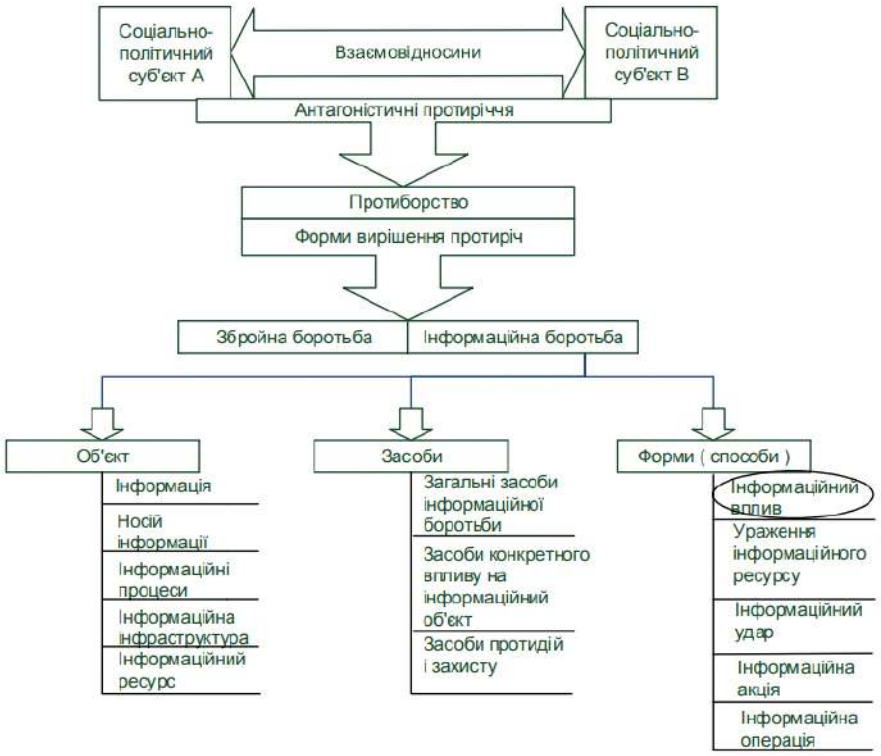

Рисунок 1.3 - Побудова загальних і окремих категорій інформаційної боротьби [19][21]

Проблема інформації в сучасній науці розглядається з різних точок зору. Загальний об'єкт дослідження "інформації" розглядається фахівцями в різних галузях знань кожним з свого погляду. Наприклад, фахівець у галузі теорії передачі інформації зосереджується на кількісних параметрах інформації, методах кодування, впливі шуму, перешкод і інших аспектах, що стосуються передачі та обробки інформації. [17].

Тут є тільки один об'єкт дослідження-інформація. Однак, оскільки інформація вивчається в різних галузях науки з різними темами, сама інформація може бути розглянута з різних точок зору в залежності від конкретної наукової галузі, що призводить до різного освітлення її сутності та значення [12].

Спочатку термін "інформація" мав виключно соціальне значення, пов'язане з комунікацією між людьми [13]. Це підтверджується аналізом етимології слова "інформація", яке вперше з'явилося в латинській мові. Вперше в Російській імперії це слово з'явилося під час правління Петра I.

Н.А. Смирнов стверджує, що це слово потрапило в російську мову через польське "інформація", яке, своєю чергою, походить з латини. На той час "інформація" означала "ідея, наука" [20].

З цього випливає, що "інформація" — це набір образів та взаємозв'язків між ними в певній системі [14]. Це дає можливість визначити друге непряме значення терміна "інформація", яке акцентує на тому, що інформація є сукупністю властивостей, притаманних об'єктам, процесам і явищам матеріального світу, що формують ідеальні образи [15].

Це дає змогу зрозуміти, що інформація дозволяє ідентифікувати джерела та виявляти об'єкти, що зазнають впливу протягом інформаційних війн [24].

Джерела інформації включають самі об'єкти, процеси та явища, які створюють коливання і хвилі, випускають потоки заряджених частинок, а також центральну нервову систему (мозок) людини [23].

Розуміння сутності та природи інформації дозволяє осягнути природу і зміст інформаційних процесів, які передають інформацію у часі та просторі [21]. Спочатку важливо зосередитися на простих інформаційних процесах, таких як отримання, обробка, передача та збереження інформації, які можна визначити як:

- отримання (сприйняття) - виділення розпізнаної інформації з усього різноманіття навколишнього світу [26].
- обробка - зміна інформації відповідно до заздалегідь визначеного алгоритму, з метою отримання нової суб'єктивної інформації [25].
- передача - переміщення незмінної інформації у просторі та часі. Під час передачі властивості зображень можуть змінюватися, зберігаючи їх семантичний зміст [25].
- зберігання - передача інформації у часі, а не у просторі, тобто відтворення образів (знаків) об'єкта у потрібний момент часу [26].

Сукупність елементарних інформаційних процесів формує такі типи, як інформаційні ланцюжки та інформаційні мережі [22]. У неживих природних

об'єктах відображення відбувається у формі накопичення внутрішнього різноманіття структури матерії.

Розвиток живих систем до найвищого рівня призвів до виникнення всіх форм елементарних процесів: сприйняття, обробки, передачі та зберігання, а також до деяких видів інформаційних процесів [23]. Високоорганізована система, такою як суспільство та сама людина, характеризується всіма формами і типами інформаційних процесів.

У структурі світу матеріального, технологія знаходиться на проміжному рівні між природою неживою і суспільством, виступаючи як складова штучної природи неживої. Це пояснюється тим, що людина, розробляючи технічні пристрої, прагнула покращити свої можливості та взаємодію з навколишнім світом [20].

Джерело інформації — це сукупність самої інформації, її носіїв, технологій та інфраструктури, що є відправною точкою для інформаційних процесів [18]. Інформаційна боротьба спрямована на цілеспрямований вплив на джерела інформації для ураження або зменшення їхньої ефективності [18].

Інформаційний вплив може бути навмисним або ненавмисним, здійснюється на активні або пасивні джерела. Активні впливи змінюють ознаки, порушують стійкість інформаційних процесів та комунікації. Пасивні впливи не змінюють ознак і не порушують комунікацію [19].

Основні види інформаційного впливу включають інформаційно-пропагандистський, психологічний, технічний та кібернетичний вплив [27].

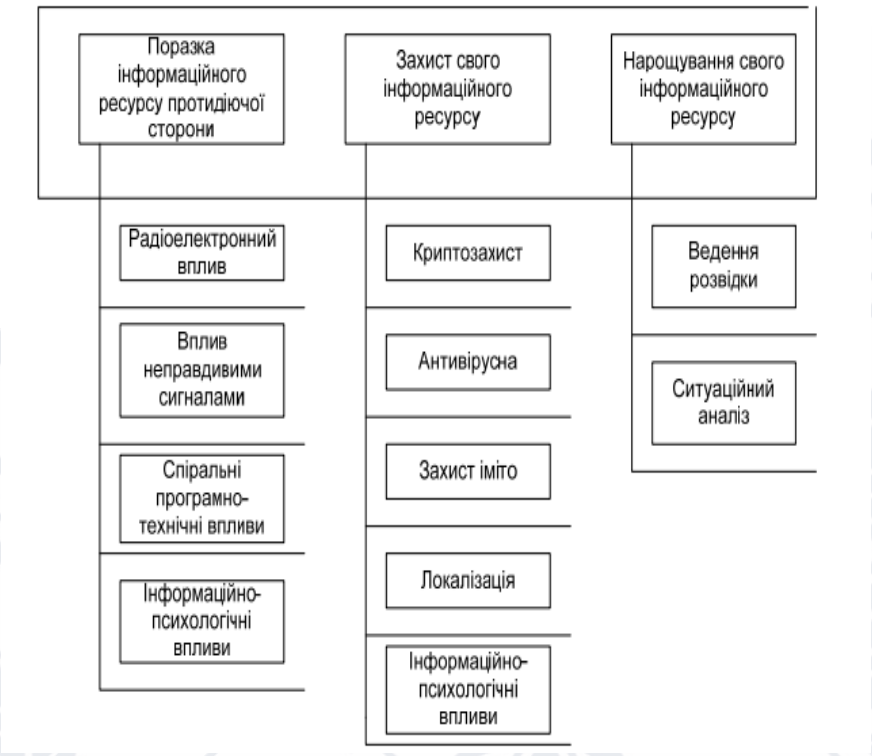

Рисунок - 1.4 Види інформаційних впливів [34][38]

Сучасний підхід до моделювання впливу на інформаційні системи полягає в виділенні вхідних та вихідних даних за кожним критерієм, описі основних операцій, а також визначенні їх переваг та недоліків (табл.1.2).

Висновок до розділу 1

У даному розділі було розглянуто поняття інформації та її значення в сучасному світі, важливість інформаційних процесів у високоорганізованих системах, таких як суспільство та людина. Також розглянуто поняття "інформаційний ресурс" як сукупність інформації, носіїв, технологій та інфраструктури.

Було розглянуто значення інформаційної боротьби, види інформаційних впливів. У другому розділі буде розглянуто параметри конфігурації інформаційних систем з точки зору їх впливу на безпеку, виокремлено ключові аспекти, та самі конфігуруванні системи.

РОЗДІЛ ІІ. МЕТОДОЛОГІЯ ВИЗНАЧЕННЯ ОПТИМАЛЬНИХ ПАРАМЕТРІВ КОНФІГУРАЦІЇ

2.1. Принципи розробки безпечних інформаційних систем

Більшість розробників обізнані про важливість безпеки інформаційних систем і дбають про неї. Однак, як стверджують Джордж Ву [28] та Макбет [29], іноді їм не вдається висловити свої занепокоєння під час впровадження спеціальних заходів управління. Дослідження Чарльза Вуда [30] показує, що це часто зумовлено браком фінансування, нестачею кваліфікованих розробників і досвідчених спеціалістів із інформаційної безпеки, а також інших осіб, які знають, як встановити контрольні елементи на етапі розробки системи. Основна причина цього - обмежені знання про принципи проектування захищених інформаційних систем, які можна застосовувати при розробці контролю доступу. Використання таких принципів може сприяти ефективному впровадженню заходів безпеки, як зазначено в публікації Алана Клаба [31].

За відомостями, що надали Чарльз Вуд [30] і Філіп Кропаткін [32], можна розглянути ключові засади створення захищених інформаційних систем. Принцип простоти стверджує, що зменшення складності інструменту управління зменшує необхідні зусилля для всіх процесів від його розробки до експлуатації.

Користувачі і менеджери бажають зосередитися на виконанні своєї роботи, а не витрачати час на контроль. Чим ефективніше контролюється ситуація, тим менше необхідної втручання людей у реальному часі. У більшості випадках простіші елементи керування є ефективнішими, ніж складні, оскільки їх можна легше зрозуміти та протестувати.

Засада найменших привілеїв стверджує, що лише ті, хто можуть аргументувати свої комерційні або професійні інтереси, мають мати доступ до інформації, можливість запускати певні програми та користуватися

іншими системними привілеями [32].

Незалежність контролю вимагає, щоб особа, що відповідає за розробку, впровадження та керування контролем, не збігалася з особою, яка піддається цьому контролю. В іншому випадку може виникнути ситуація конфлікту інтересів, оскільки та сама особа, що впроваджує систему контролю, буде контролюватися цією ж системою [32].

Підзвітність є одним із найважливіших принципів внутрішнього контролю за безпекою інформаційних систем. Це означає, що принаймні одна особа повинна нести відповідальність за правильне функціонування системи управління. [32].

Суть принципу найменшого загального механізму полягає в зменшенні впливу недоступних компонентів центральної системи на її роботу [32].

Принцип участі людини стверджує, що потрібно забезпечити присутність людини, яка буде перевіряти або приймати критичні або важливі рішення. Навіть при використанні передових технологій, таких як штучний інтелект, експертні системи або нейронні мережі, необхідно мати людину, яка перевірить або затвердить вихідні результати. Це важливо, оскільки комп'ютерні системи не завжди можуть врахувати всі можливі обставини та відповісти адекватно у всіх ситуаціях. Тому необхідно, щоб завжди була присутня людина, яка здійснить контроль за системою [32].

Принцип аудиту вимагає, щоб засоби контролю надавали достатні докази їх належного функціонування, такі як протоколи, контрольні записи або звіти. Наприклад, системи контролю доступу на основі паролів можуть створювати журнали входів, виходів, запусків програм або запитів доступу. Без достатніх доказів керівництво не може бути впевненим у належному функціонуванні системи [32].

Хоча не всі ці принципи застосовуються до кожної системи, їх розуміння може підвищити рівень безпеки. Розробник, який розуміє ці принципи, зможе створити більше ідей для поліпшення безпеки [31]. Якщо розробник залишається відкритим до принципів контролю, він може

зрозуміти, як різні елементи управління можуть співпрацювати для підвищення безпеки [32].

Рисунок 2.1 - Проектування захищених інформаційних систем [2]

2.2. Параметри конфігурації інформаційних систем, що впливають на безпеку

Конфігурація інформаційних систем має великий вплив на їх безпеку, оскільки різні налаштування можуть представляти як загрози, так і захист. Основні параметри конфігурації, що впливають на безпеку інформаційних систем, можна проілюструвати за допомогою OpenVAS:

Права доступу до системи: Правильно налаштовані права доступу є основою безпеки. Неналежні права можуть призвести до несанкціонованого доступу до системи або її компонентів.

Налаштування інструментів мережевої безпеки, таких як брандмауери та системи виявлення та запобігання вторгненням (IDS / IPS), має вирішальне значення для виявлення та запобігання мережевим атакам [33].

Оновлення програмного забезпечення: уразливості програмного забезпечення становлять загрозу безпеці. Не оновлене програмне

забезпечення може містити вразливості, які можуть бути використані зловмисниками. OpenVAS допоможе вам виявити такі вразливості шляхом сканування вашої системи.

Налаштування мережевої безпеки:неправильні налаштування мережі можуть зробити систему вразливою до мережевих атак. Правильне налаштування мережевої безпеки, таке як VPN та бездротові мережі, має вирішальне значення.

Контроль ідентифікації та доступу:слабкі або неправильно налаштовані механізми аутентифікації та авторизації можуть надати доступ неавторизованим користувачам.

Налаштування конфіденційності: Захист конфіденційних даних має вирішальне значення для безпеки системи. Потрібне належне шифрування та контроль доступу до даних [34].

Ці параметри слід розглядати як ключові компоненти для налаштування інформаційних систем з точки зору їх безпеки (рис.2.2). Використання таких інструментів, як OpenVAS, дозволяє виявляти та виправляти потенційні проблеми безпеки шляхом сканування та аналізу вразливостей.

Рисунок 2.2 - Параметри конфігурації інформаційних систем, що впливають на безпеку [15]

2.3. Методи моделювання та аналізу параметрів конфігурації

Алгоритми оптимізації конфігурації інформаційних систем у контексті мережевої розвідки використовуються для забезпечення ефективності та безпеки системи, наприклад, за допомогою такого програмного забезпечення, як OpenVAS (відкрита система оцінки вразливостей). OpenVAS-це програмне забезпечення з відкритим кодом, яке використовується для пошуку вразливостей у комп'ютерних системах та мережах.

Деякі з можливих алгоритмів оптимізації конфігурації для забезпечення оптимальної ефективності та безпеки системи можуть включати:

Ви можете використовувати їх для налаштування параметрів сканування та налаштування правил сканування. Такі параметри, як час очікування між запитами, ступінь використання сканування та інші, можуть бути змінені для забезпечення ефективності та зниження впливу на продуктивність мережі.

Використання машинного навчання та інших методів штучного інтелекту може допомогти системі самостійно розробити оптимальні стратегії сканування та реагування на виявлені вразливості [35].

Методи оптимізації на основі даних: аналіз історичних даних про вразливість, збір даних про мережевий трафік та інші мережеві характеристики можуть бути використані для налаштування оптимальних параметрів сканування.

Розробка алгоритмів, заснованих на великій кількості правил безпеки та експертних знань, може допомогти визначити стратегії сканування та реагування на виявлені вразливості [35].

При оптимізації конфігурації інформаційних систем в середовищі мережевої аналітики за допомогою OpenVAS важливо враховувати особливості мережі, типи потенційних загроз, а також вимоги до продуктивності і безпеки (рис.2.3). У будь-якому випадку може знадобитися

індивідуальний підхід та комбінація різних методів оптимізації для досягнення найкращих результатів.

Рисунок 2.3 - Методи оптимізації конфігурації інформаційних систем за допомогою OpenVAS

Висновок до розділу 2

У даному розділі було розглянуто важливість оновлення програмного забезпечення та налаштування захисту мережі, висвітлено важливість керування ідентифікацією і доступом, а також захисту даних, що підкреслює необхідність належного контролю над доступом до системи та конфіденційністю даних. Зазначені методи оптимізації, такі як аналіз історичних даних та розробка алгоритмів прийняття рішень, допомагають визначити оптимальні стратегії сканування та реагування на вразливості.

На основі даної інформації у третьому розділі будуть обрані програми, які є ключовими для аудиту та забезпечення безпеки мережі.

РОЗДІЛ ІІІ. МОДЕЛЮВАННЯ ОПТИМАЛЬНОЇ КОНФІГУРАЦІЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

В сучасному світі, де інформаційні технології відіграють ключову роль у всіх сферах життя, забезпечення безпеки інформації стає вкрай важливою задачею. Інформаційні системи піддаються різноманітним загрозам, включаючи кібератаки, вразливості програмного забезпечення та несанкціонований доступ.

Метою даного розділу є дослідження та моделювання оптимальної конфігурації інформаційної системи з точки зору забезпечення безпеки. У цьому контексті ми розглядаємо стратегії побудови систем безпеки, методи аудиту безпеки мережі та виявлення потенційних вразливостей.

Для досягнення цієї мети, в рамках даного дослідження використовуються дві важливі програми - OpenVAS та Nessus Scanner. Ці програмні засоби надають можливість проведення аудиту безпеки мережі, виявлення вразливостей та надання рекомендацій з їх усунення.

У подальших розділах цього відділу ми детально розглянемо процес використання цих програмних засобів, а також проаналізуємо їх ефективність та вплив на оптимальну конфігурацію інформаційних систем на локальній мережі.

Таблиця 3.1 - Характеристика обладнання

Характеристика	**Значення**
Ім'я	DESKTOP-413CVQC
Процесор	12th Gen Intel(R) Core(TM) i5-12600KF
Частота процесора	3.70 GHz
Оперативна пам'ять	32,0 ГБ (доступно: 31,8 ГБ)
Операційна система	Windows 10 Pro
Версія Windows	22H2

Дата встановлення	15.04.2023
Версія ПЗ	0.9.1 3.16 v0283.0 Build 180619 Rel.56190n
Версія обладнання	TL-WR845N v4 00000004
Жорсткий диск	KINGSTON SKC3000S1024G
Відеоадаптер	NVIDIA GeForce RTX 3050
Мережеве обладнання	Bluetooth Device (Personal Area Network), Famatech Radmon VPN Ethernet Adapter, Hyper-V Virtual Ethernet Adapter, Realtek PCIe 2/5GbE Family Controller, VirtualBox Host-Only Ethernet Adapter, WAN Miniport (IKEv2), WAN Miniport (IP), WAN Miniport (IPv6), WAN Miniport (L2TP), WAN Miniport (Network Monitor), WAN Miniport (PPPOE), WAN Miniport (PPTP), WAN Miniport (SSTP).
Інші компоненти	USB 3.0 порти
Діапазон IP адрес	192.168.0.1-192.168.255.254

3.1. Використання програми OpenVAS для аудиту мережі

Одними із відомих комерційних сканерів є -Nessus, GFI LANguard та Spider.

На відміну від інших, OpenVAS безкоштовний, працює без обмежень і може бути корисним як адміністраторам мережі, так і фахівцям з інформаційної безпеки для виявлення поточних проблем в їх інфраструктурі.

OpenVAS заснований на постійно оновлюваній колекції тестів безпеки мережевих відеореєстраторів (яких вже налічується понад 30 000) і підключенні до бази даних CVE, що описує відомі уразливості. Запустивши тести NVT, можна визначити вразливість, CVE надасть опис проблеми та її вирішення.

На адресі localhost: 9392, вводимо своє ім'я користувача та пароль та переходимо до консолі управління Rainbow Security Assistant (рис.3.1).

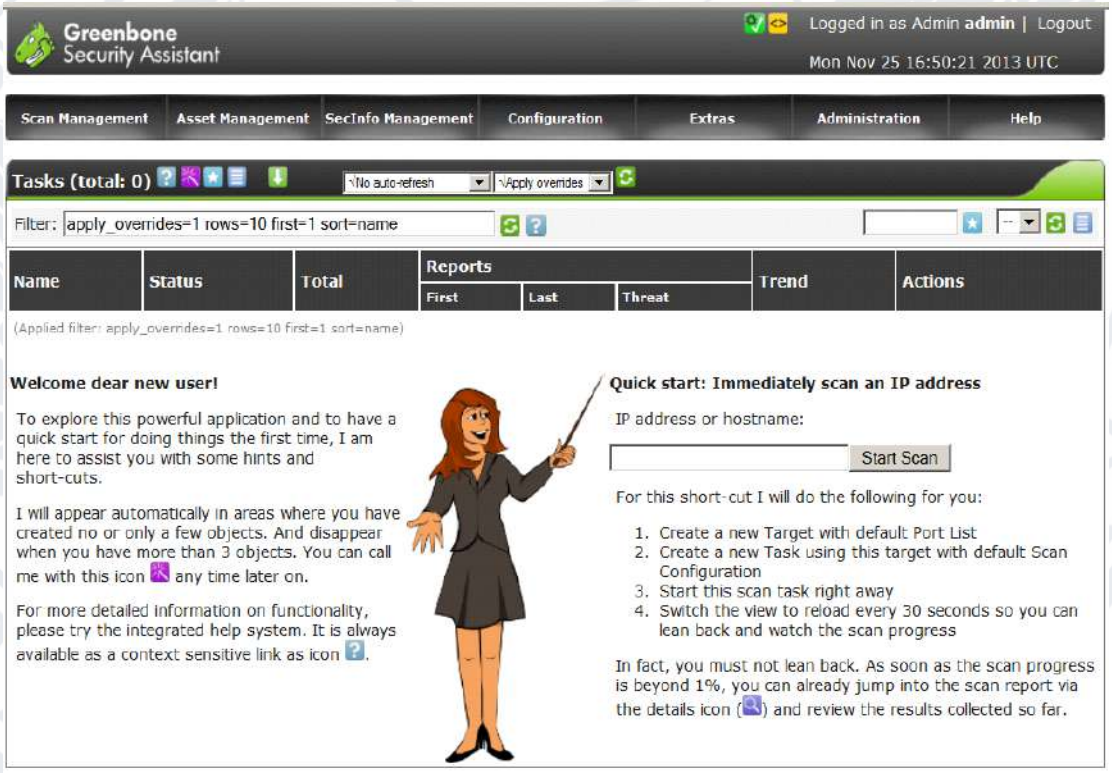

Рисунок 3.1 - Структура ПЗ “OpenVAS”

Далі ми розглянемо приклад роботи з Openvas для сканування внутрішньої області мережі. Основні налаштування налаштовані на оптимальну швидкість тестування кожного хоста.

Виберіть конфігурацію сканування.

Переходимо до розділу Configuration-Scan Configurations.

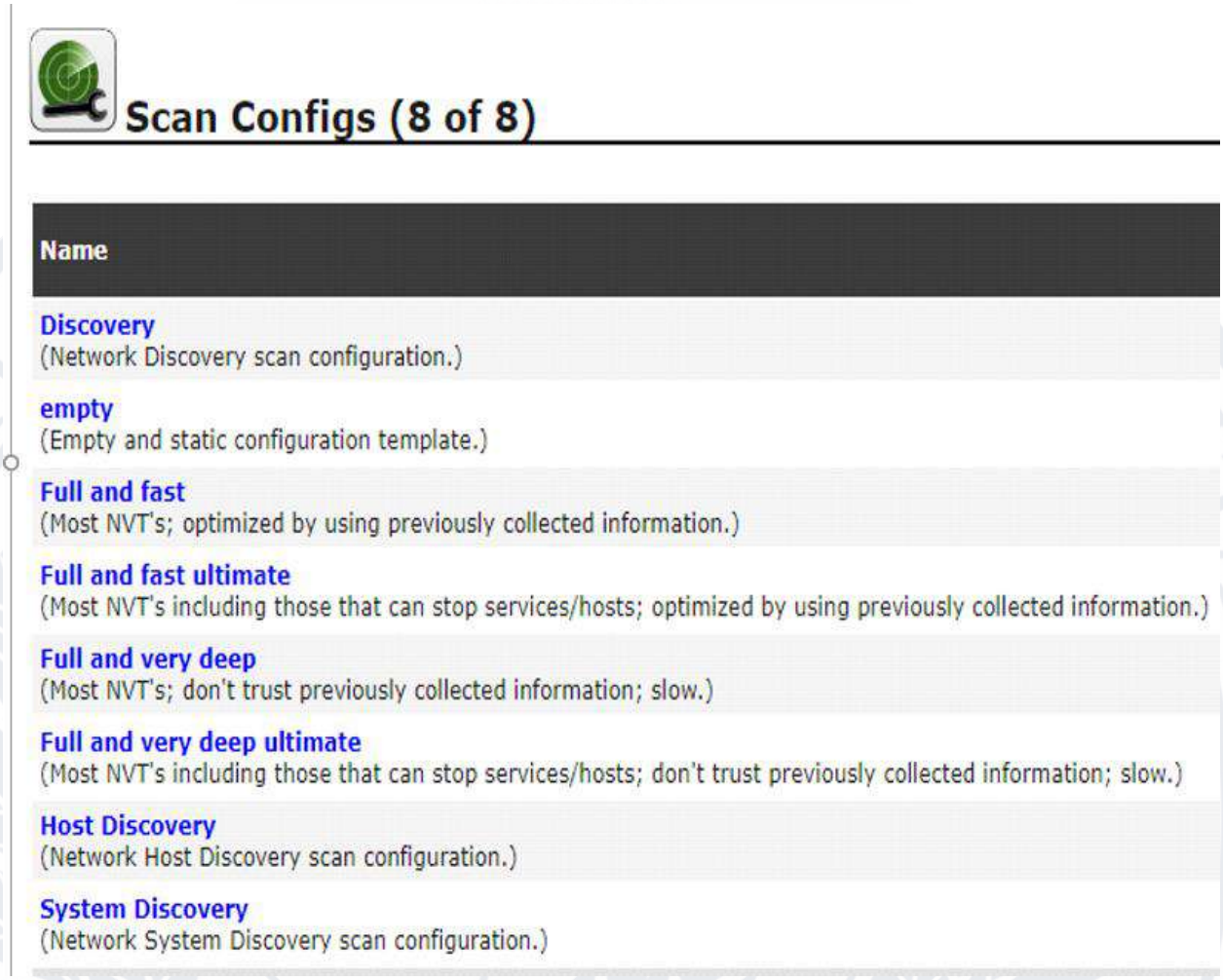

Рисунок 3.2 - Інтерфейс користувача ПЗ “OpenVAS” у режимі роботи “Configuration-Scan”

Як видно на Рисунку 3.2 ПЗ складається з 4 стандартних політик та 1 порожньою.

Рекомендації діляться на дві групи – швидкі і глибокі.

Принципова відмінність полягає в тому, що робота кожного попереднього скрипта по перевірці і збору інформації заново не враховується.

Для підвищення швидкості потрібно вибрати директиву Full і fast ultimate і клонувати її, натиснувши на значок овечки .

Тепер для клону є варіанти редагування, далі потрібно натиснути на значок ключа .

Варіантів багато, кілька сотень, але це тільки початок. Всі параметри згруповані за тестовими підрозділами NVT з різних типів операційних систем і мережевого обладнання, з налаштувань різних підключаються утиліт, таких як nmap, nobody і т. д. всі параметри згруповані за розділами тестування NVT з різних типів ОС і мережевого обладнання, з налаштувань різних підключаються утиліт, таких як nmap (рис.3.3.)

Edit Network Vulnerability Test Families

Family	NVTs selected
AIX Local Security Checks	1 of 1
Amazon Linux Local Security Checks	748 of 748
Brute force attacks	9 of 9
Buffer overflow	562 of 562
CISCO	647 of 647
CentOS Local Security Checks	2528 of 2528
Citrix Xenserver Local Security Checks	30 of 30
Compliance	7 of 7
Databases	556 of 556
Debian Local Security Checks	3101 of 3101
Default Accounts	245 of 245
Denial of Service	1384 of 1384
F5 Local Security Checks	125 of 125
FTP	174 of 174
Fedora Local Security Checks	10917 of 10917
Finger abuses	6 of 6
Firewalls	18 of 18
FortiOS Local Security Checks	34 of 34
FreeBSD Local Security Checks	437 of 437

Рисунок 3.3 - Вікно форми “Типи протоколів для сканування”

Називаємо нову політику MOMO_GreeM (рис.3.4.)

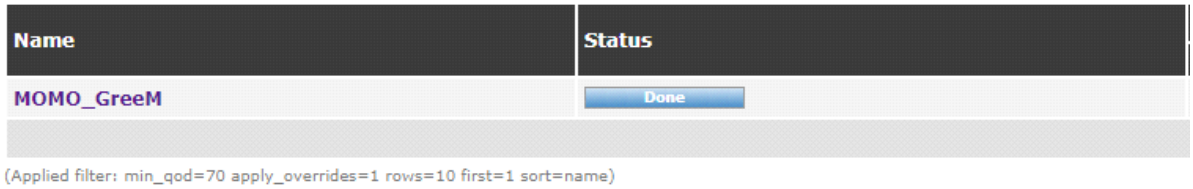

Рисунок 3.4 - Вікно форми стану та назви процесу сканування “Інформаційний блок”

Включення опції safe_check дозволить запускати потенційно небезпечні тести NVT, що можуть призвести до аварійного відключення тестованого хоста. Перемикач optimize_test встановлює режим сканування - швидкий або глибокий.

Перед налаштуванням опцій PingHost необхідно врахувати ці параметри (рис.3.5).

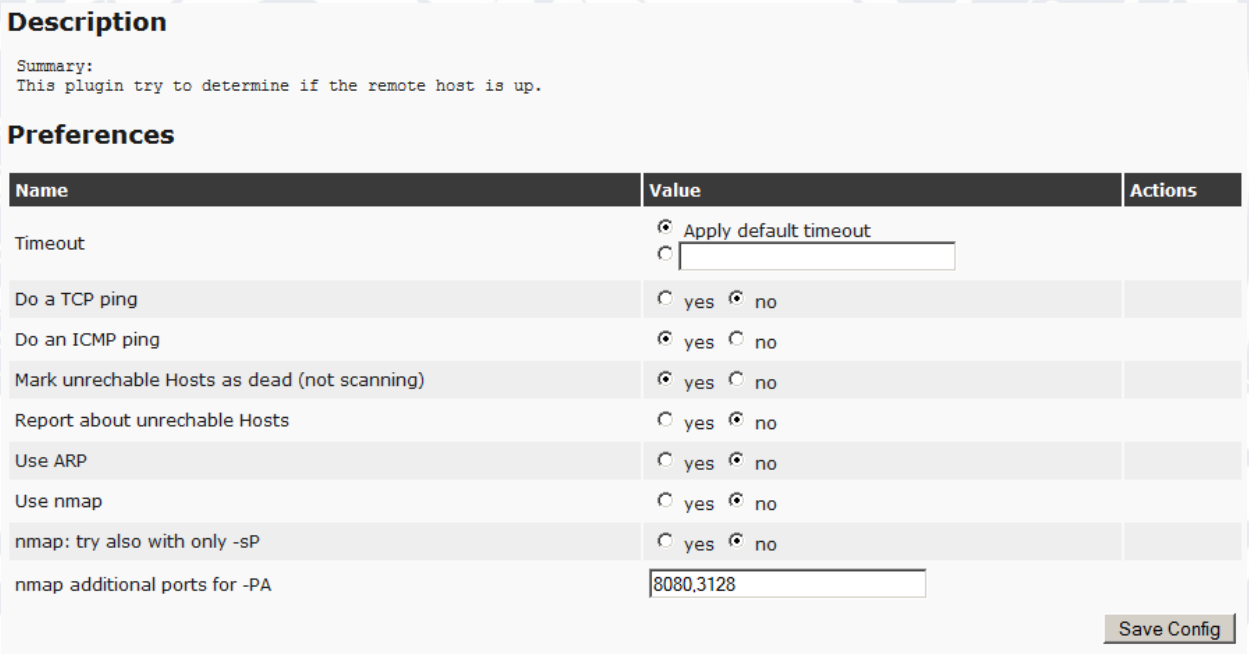

Рисунок 3.5 - Вікно форми списку довідника “PingHost”

Після активації цього компонента, OpenVAS буде автоматично сканувати кожен пристрій, перевірятиме встановлені програми, аналізуватиме налаштування локальної безпеки та висилатиме сповіщення у випадку виявлення проблем.

Це збільшує час сканування.

Якщо не налаштувати його, Openvas буде обмежений віддаленими

перевірками.

Нижче наведено розділ Configuration-Credentials.

Далі для створеня нового запису, потрібно натиснути значок зірочки.

На мережі Windows у домені присутній користувач GreeM, який має привілеї локального адміністратора на відповідних комп'ютерах. Цей сценарій можна побачити у вигляді, представленому на рисунку 3.6.

Рисунок 3.6 - Вікно форми списку довідника “Configuration-Credentials”

В розділі "Configuration – Target" необхідно створити нову ціль, натиснувши на значок зірочки. Ім'ям цієї цілі буде "Test" (див. рис.3.7).

Після цього потрібно вказати діапазон IP-адрес для сканування і визначитися з набором портів, які Openvas буде перевіряти.

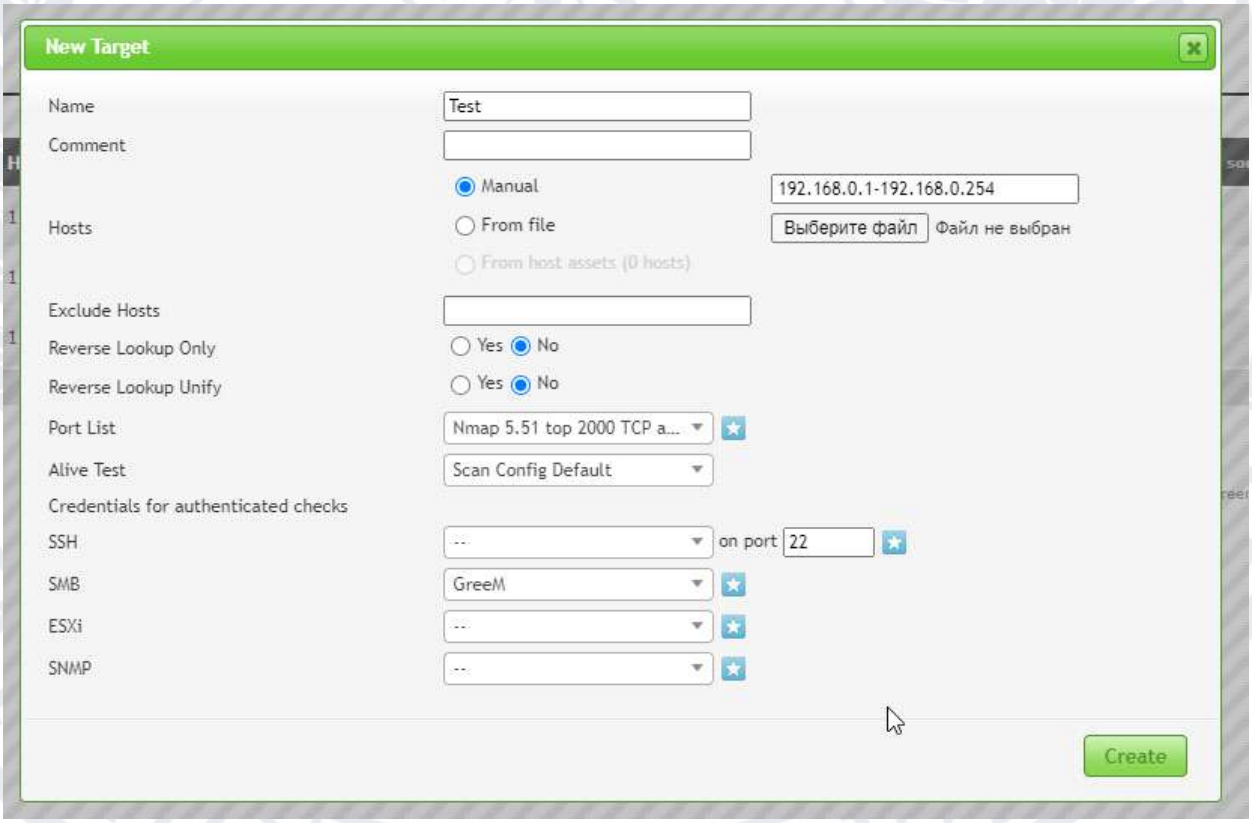

Рисунок 3.7 - Вікно форми списку довідника “Configuration –Target”

У розділі SMB необхідно налаштувати підключення для вже створеного користувача для проведення перевірок.

У розділі PortList встановлюється діапазон портів, який включає

популярні порти, які рекомендовано для сканування Nmap. Вибір такого діапазону здійснюється з метою оптимізації процесу сканування.

У розділі Хости потрібно вказати діапазон IP-адрес. В розділі ScanManagement - Task. Створюємо нове завдання, натиснувши значок зірочки (рис.3.8.).

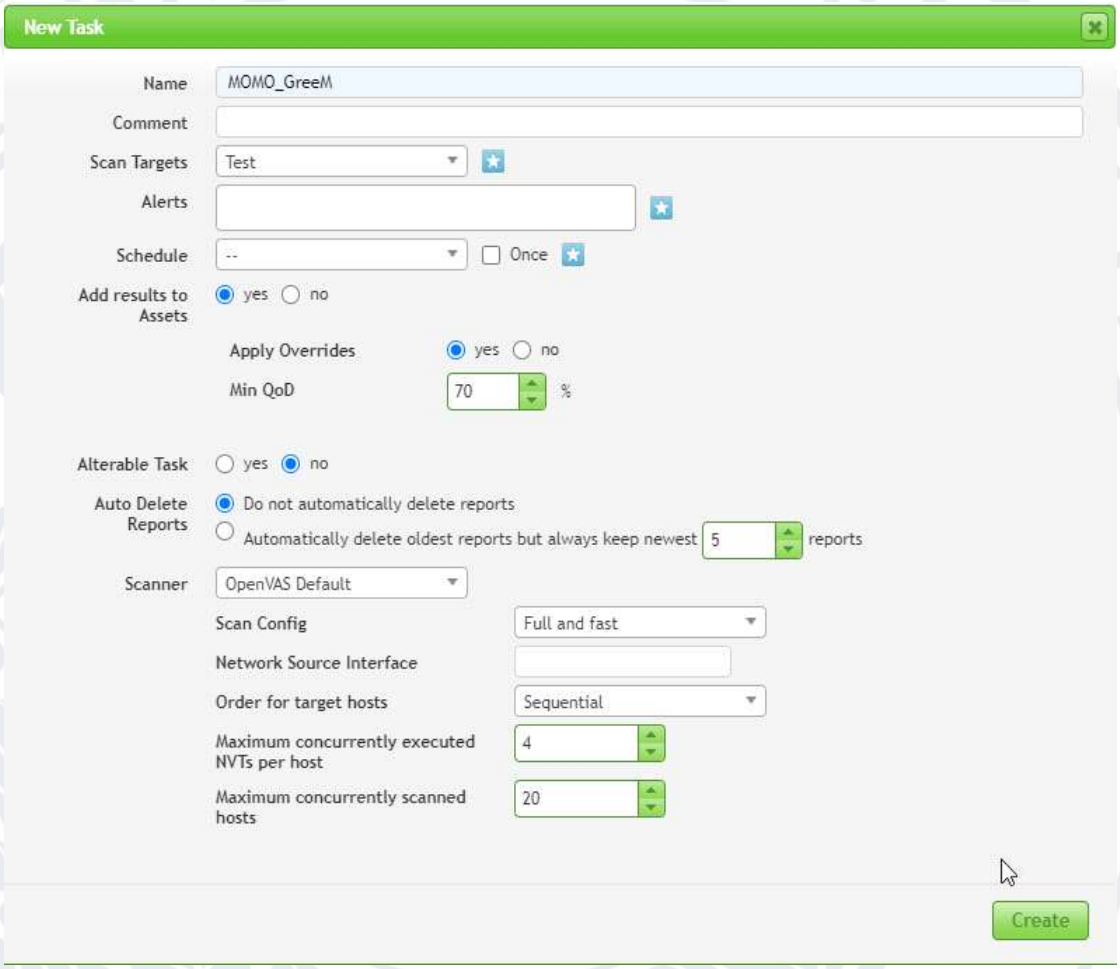

Рисунок 3.8 - Вікно форми списку довідника “ScanManagement - Task”

Запуск (рис.3.9.).

Рисунок 3.9 - Вікно форми стану та назви процесу сканування “Інформаційний блок”

Після завершення процесу є можливість натиснути на значок лупи та переглянути всі виявлені проблеми. Цей функціонал зображений на рисунку 3.10.

Рисунок 3.10 - Вікно форми стану та назви процесу сканування “Оцінка вразливостей”

Типовий алерт (рис.3.11).

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: 49664/tcp

      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:192.168.0.103[49664]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access

      UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
      Endpoint: ncacn_ip_tcp:192.168.0.103[49664]
      Annotation: Ngc Pop Key Service

      UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
      Endpoint: ncacn_ip_tcp:192.168.0.103[49664]
      Annotation: Ngc Pop Key Service

      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:192.168.0.103[49664]
      Annotation: KeyIso

Port: 49665/tcp

      UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
      Endpoint: ncacn_ip_tcp:192.168.0.103[49665]

Port: 49666/tcp

      UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
      Endpoint: ncacn_ip_tcp:192.168.0.103[49666]
      Annotation: Event log TCPIP

Port: 49667/tcp

      UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
      Endpoint: ncacn_ip_tcp:192.168.0.103[49667]

      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
      Endpoint: ncacn_ip_tcp:192.168.0.103[49667]

Port: 49668/tcp

      UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
      Endpoint: ncacn_ip_tcp:192.168.0.103[49668]

      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.0.103[49668]
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
```

Рисунок 3.11 - Вікно форми списку довідника “Вразливість”

Періодично необхідно підкачувати актуальні відомості про вразливості та тести, що їх виявляють.

Робиться це або з браузера розділу Administration. (По черзі у всіх 3-х розділах: nvt,scap,cert) (рис.3.12).

Рисунок 3.12 - Вікно форми списку довідника “NVT feed Management”

3.2. Використання програми Nessus Essentials для сканування мережі

Nessus Essentials — безкоштовна версія інструмента для сканування вразливостей від Tenable. Вона дозволяє виявляти вразливості в системах, додатках та мережах, проводити аудит безпеки та оцінювати ризики. Обмежена до 16 IP-адрес, Nessus Essentials підходить для малого бізнесу, студентів та ентузіастів безпеки.

Інструмент забезпечує аудит конфігурацій, перевіряючи налаштування системи на відповідність найкращим практикам безпеки. Інтуїтивно зрозумілий веб-інтерфейс дозволяє легко запускати сканування, переглядати звіти та керувати налаштуваннями. Користувачі мають доступ до регулярно оновлюваної бази даних вразливостей, що забезпечує актуальність сканувань. Генерація детальних звітів про знайдені вразливості з рекомендаціями щодо їх усунення є важливою функцією Nessus Essentials.

Коли Nessus завершить оновлення, вас зустріне такий екран, як показано нижче. Для початку сканування потрібно натиснути "New Scan" (рис.3.13).

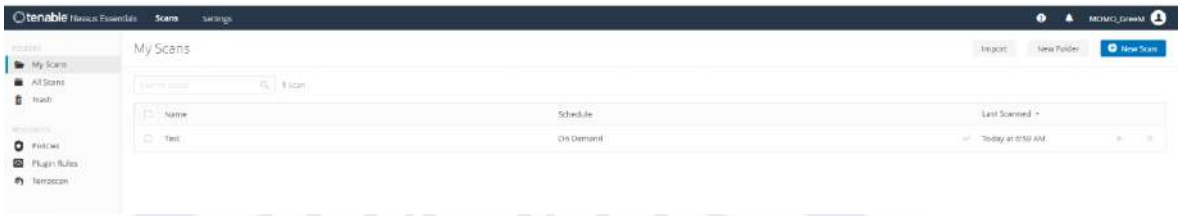

Рисунок 3.13 - Інтерфейс користувача ПЗ “Nessus Essentials” у режимі роботи “Історія сканування”

Після відкриття нової сторінки, можна вибрати тип сканування, там завжди містяться найактуальніші моделі загроз.

Далі потрібно натиснути "Basic Network Scan" (рис.3.14).

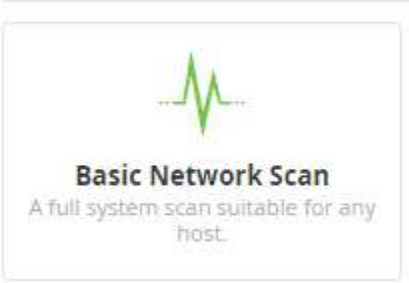

Рисунок 3.14 - Вікно довідника “Basic Network Scan”

Відкриється сторінка, на якій попросять вказати ім'я вашого сканування. Також необхідно буде вказати вузли, які буде просканово (рис.3.15.).

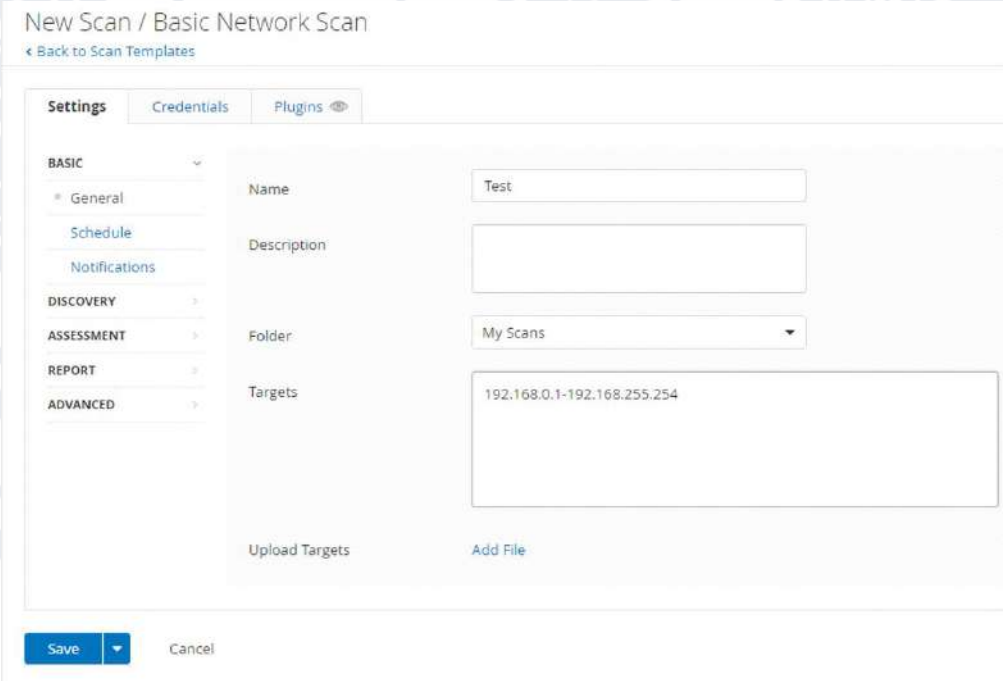

Рисунок 3.15 - Вікно форми списку довідника “New Scan - Basic Network Scan”

Далі потрібно натиснути кнопку "Launch", щоб запустити сканування вразливостей (рис.3.16).

Рисунок 3.16 - Вікно форми списку довідника “My Scans”

За результатами сканування ми отримуємо список IP-адрес та пов'язані з ними ризики. Ризики мають колірне кодування (рис.3.17).

Рисунок 3.17 - Вікно форми списку довідника “Результат(и) сканування”

Натискаємо "vulnerabilities" у верхньому меню, щоб відобразити уразливості, виявлені в мережі (рис.3.18).

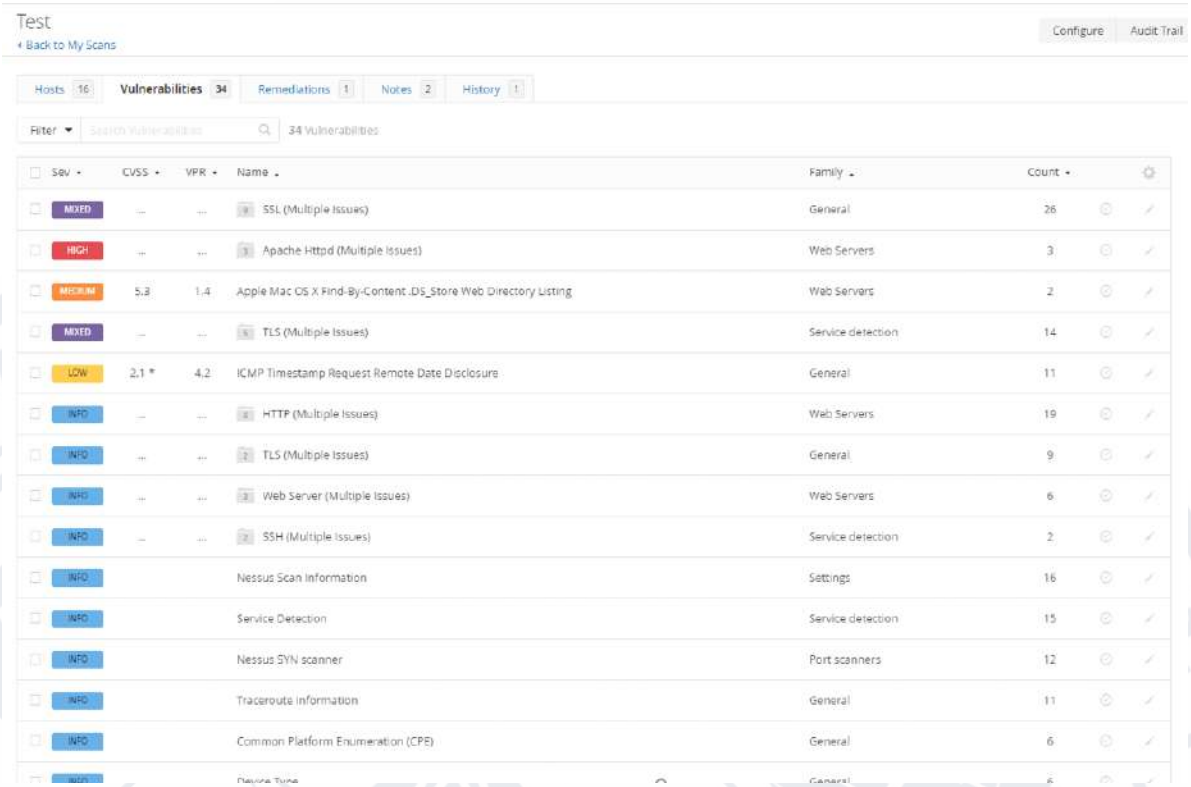

Рисунок 3.18 - Вікно форми списку довідника “Vulnerabilities”

Якщо натиснути на конкретну вразливість, можна отримати більш детальну інформацію. Нижче наведено приклад уразливості "Apache 2.4.x < 2.4.59 Multiple Vulnerabilities" (рис.3.19).

Поміж описом вразливості в звіті також присутній розділ рішення, який включає в себе методи виправлення та закриття цієї вразливості (розділ Solution).

Рисунок 3.19 - Вікно форми списку довідника “Apache 2.4.x < 2.4.59

Multiple Vulnerabilities”

Результат(и) можна зберегти у різних форматах. На вкладці "Експорт" вибрати формат файлу звіту (рис.3.20):

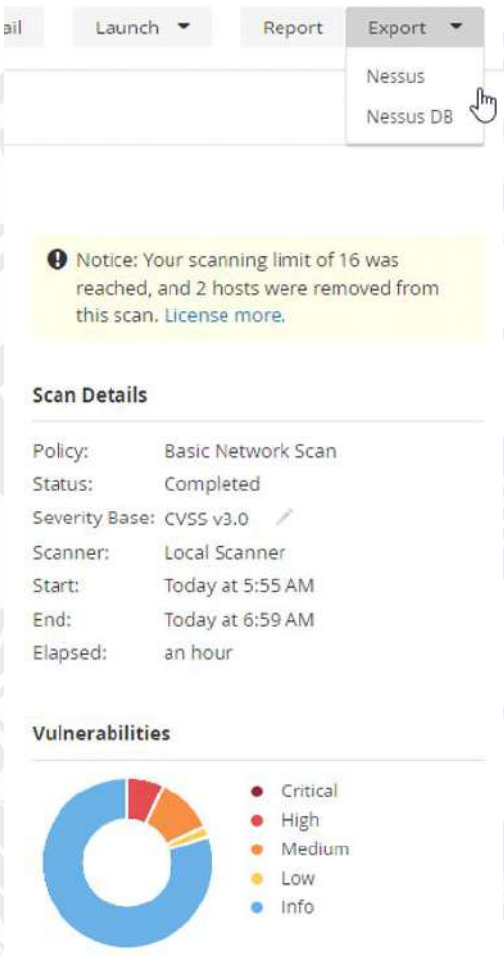

Рисунок 3.20 - Вікно форми списку довідника “Export”

Висновок до розділу 3

Використання програм OpenVAS та Nessus Essentials є ключовим для аудиту та забезпечення безпеки мережі. OpenVAS, завдяки своїм безкоштовним можливостям та широкому спектру тестів безпеки, надає зручний інструмент для виявлення вразливостей у мережевій інфраструктурі. Його використання забезпечує доступ до різноманітних тестів безпеки та бази CVE для ідентифікації потенційних загроз.

Спрощене використання Nessus Scanner також є ефективним засобом

для сканування мережі та ідентифікації вразливостей. Встановлення та налаштування Nessus дозволяє здійснювати швидке та точне сканування мережі, а отримані результати забезпечують детальну інформацію щодо виявлених проблем та можливі шляхи їх виправлення.

Загальна ефективність обох програм залежить від правильного конфігурування та регулярного оновлення баз даних вразливостей. Використання обох програм дозволяє забезпечити безпеку мережі та зменшити ризики кібератак і несанкціонованого доступу до систем.

ВИСНОВКИ

Під час виконання кваліфікаційної (бакалаврської роботи) було проаналізовано існуючі методи та інструменти для оцінки вразливостей інформаційних систем. Деякі з них включають систему правил для моделювання критеріїв оптимальності та застосування методу диференціальної гри для оптимізації параметрів інформаційних систем. Також розглянуті методи оптимізації систем захисту інформації та шляхи їх удосконалення з урахуванням параметрів системи безпеки. У ході виконання бакалаврської роботи було розроблено методи оцінки вразливостей та їх вплив на інформаційні системи. Крім того, досліджено різноманітні алгоритми та програмне забезпечення, такі як OpenVAS та Nessus Essentials, які використовувалися для впровадження розроблених методів.

Розроблені інструменти підходять для навчання, тестування та базової оцінки безпеки в невеликих мережах, дозволяючи користувачам отримати досвід роботи з інструментами для сканування вразливостей та зрозуміти основи управління ризиками в інформаційній безпеці.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Алексеев А. Управление рисками. Метод CRAMM / А. Алексеев // IT Expert. – Электрон. дан. – М. : ЗАО “ИТ Эксперт”, 2010.

2. Андреєв В.І. Основи інформаційної безпеки / Андреєв В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є. – К.: Вид. ДУІКТ, 2009. – 292 с.

3. Астахов А. Актуальные вопросы вявления сетевых атак. Jet Info №3 (106), 2002.

4. Астахов А. Анализ защищенност корпоративных систем//Оперативные системы. №07-08/2002.

5. Буравльов Є.П. Глобалізація: проблеми безпеки / Буравльов Є.П. – К.: Ін-т проблем нац. безпеки, 2007 – 160 с.

6. Голубенко А.Л. Информационные технологии и киберпреступность / Голубенко А.Л., Хорошко В.А., Петров А.С., Белозеров Е.В. // Вісник СНУ ім. В. Даля, №9 (103), 2006. – С. 7-10.

7. Захаров А.И. Информационные системы: оценка рисков / А.И. Захаров // Information Security (Информационная безопасность) – 2005. – №6

8. Петренко С.А. Политика информационной безопасности / Петренко С.А., Курбатов В.А. – М.: Компания Ай Ти, 2006. – 400 с.

9. Волобуев С.В. О систематизации выявления и анализа каналов утечки. Прямые и косвенные носители информации / Волобуев С.В. // Вопросы защиты информации, №1, 2000. – С. 26-37.

10. Астахов А.М. Искусство управления информационными рисками / Астахов А.М. – М : ДМК Пресс, 2010. – 314 с.

11. Берж К. Теория графов и ее применение. – М.: ИЛ, 1962. – 308 с.

12. Будько М.М. Визначення залишкового ризику при оцінці захищеності інформації в інформаційно-обчислювальних системах / Будько М.М. // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні, Вип. 8, 2004. – С. 20-26.

13. К.: Ін-т проблем нац. безпеки, 2007 – 160 с.

14. Коменюк В.Б. Элементы теории целевой оптимизации / Коменюк В.Б. – М. : Наука, 1983. – 288 с.

15. Ленков С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А. – К.: Арий, 2008.

16. Майника Є. Алгоритмі оптимизации на сетях и графах. – М.: Мир, 1981. – 323 с.

17. Мину М. Математическое программирование. Теория и алгоритмы / Мину М. – М.: Наука, 1990. – 488 с.

18. Габович А.Г. Методика оцінки рівня безпеки інформації / Габович А.Г., Горобець А.Ю., Горобець А.Ю., Хорошко В.О. // Вісник НУ «Львівська політехніка», №551, Автоматика, вимірювання та керування, 2006. – С. 48-53.

19. Хорошко В.А. Виды информационных воздействий / Хорошко В.А., Чередниченко В.С. // Захист інформації, Спец. випуск, 2007 – С 6-8.

20. Николаев Ю.А. Оборонная достаточность: критерии и методы оценки / Николаев Ю.А. // Военная мысль, 1992, №4-5. – С. 47-52.

21. Ковтун И.А. Виды информационных воздействий / Ковтун И.А., Мухан В.И., Набока Ю.И. // Вопросы защиты информации, 2001, №1 (52). – С. 2-7.

22. Коменюк В.Б. Элементы теории целевой оптимизации / Коменюк В.Б. – М. : Наука, 1983. – 288 с.

23. Майника Є. Алгоритмі оптимизации на сетях и графах. – М.: Мир, 1981. – 323 с.

24. Нейман Дж. Теория игр и экономическое поведение / Дж. Нейман, О. Моргенштерн; пер. с англ. – М. : Наука, 1970. – 707 с.

25. Николаев Ю.А. Оборонная достаточность: критерии и методы оценки / Николаев Ю.А. // Военная мысль, 1992, №4-5. – С. 47-52.

26. Нэш Д. Бескоалиционные игры. В кн.: Матричные игры / Нэш Д. – М. : Физматгиз, 1961. – С. 42-59.

27. Оре О. Теория графов. – М.: Наука, 1980. – 336 с.

28. Джордж Ву. Інформаційні та комунікаційні технології для цілей сталого розвитку: сучасний стан, потреби та перспективи / Джордж Ву. - IEEECcommun. Опитування Tuts., вип. 20, № 3, стор. 2389– 2406, 3 квартал, 2019.

29. С. Макбет, Самоорганізуюче управління даними та знаннями, створеними користувачами / С. Макбет. - IEEECcommun, вип. 30, № 3, стор. 237–264, травень 2018 р.

30. Чарльз Крессон Вуд. Процедура захисту корпоративних інформаційних систем / Чарльз Вуд – Лондон: Комп’ютери і безпека, 2015.

31. Алан Е. Бріл. Вбудовування засобів керування в структуровані інформаційні системи / Алан Е. Бріл. – Нью-Йорк: Yourdon Press, 2016.

32. Філіп Кропаткін. Принципи управління для захисту активів / Філіп Кропаткін, Річард П. Куссеров. – Нью-Йорк: Yourdon Press, 2015.

33. Стратегія управління інформаційною безпекою / В. І. Андрєєв, В. Д. Козюра, Л. М. Скачек, В. О. Хорошко. – К. : ДУІКТ, 2007. – 272 с.

34. Терейковський І.А. Нейронні мережі в засобах захисту комп'ютерної інформації / І.А. Терейковський. – К.: ПоліграфКонсилтинг. – 2007. – 209 с.

35. Феллер В. Введение в теорию вероятностей и ее приложения. В 2-х томах / Феллер В. – М.: Мир, 1967.

36. Мухин В.Е. Комплексная система мониторинга безопасности на основе анализа целей субъектов компьютерных систем и сетей / В.Е. Мухин, А.Н. Волокита // Управляющие системы и машины. – К.: УСиМ, 2006. - №5. – С. 85-92.

37. Девянин В.Д. Модели безопасности компьютерных систем / В.Д. Девьянин. – М.: Издательский центр "Академия", 2005. – 144 с.

38. Терейковський І.А. Нейронні мережі в засобах захисту комп'ютерної інформації / І.А. Терейковський. – К.: ПоліграфКонсилтинг. – 2007. – 209 с.

39. Тиснина Е.О. Абсолютная устойчивость положения равновесия системы поддержки принятия решений в системе защиты информации / Тиснина Е.О., Хорошко В.А. // Сучасний захист інформації, №4, 2010. – С. 74-79.

40. Грищук Р.В. Теоретичні основи моделювання процесів нападу на інформацію методами теорії диференційних ігор та диференційних перетворень: Монографія / Р.В. Грищук. – Житомир: Рута, 2010. – 280 с.

41. Воронин А.Н. Векторная оптимизация динамических систем / А.Н. Воронин, Ю.К. Зиатдинов, А.И. Козлов, В.С. Чабанюк; под ред. А.Н. Воронина. – К.: Техніка, 1999. – 284 с.

ДОДАТОК А

Таблиця 1.1 Огляд методологій моделювання впливу на інформаційні системи

№	Назва	Вхідні параметри	Вихідні параметри	Основні дії	Позитивні сторони	Негативні аспекти
1	Модель Мухіна-Волокіти [36]	Статистика вибраних даних	Лічильник загроз які впливають на інформацію	Оцінка від експерта, вплив на інформацію	Висока точність	Потребує статистику даних, і компетентного експерта
2	Модель Бела-Лападули та модель Біба[36]	Множини об’єктів, суб’єктів, сторонні стани, і запити	Визначення порушення цілісності	Теорія множин, булева алгебра	Простота реалізація, і контроль цілісності	Враховує лише цілісність, є можливість створення двосторонніх потоків інформації і необхідність

						створення довірених потоків
3	Модель Хартсона [37]	Моніторинг ресурсів та їх стану	Безпека системи	Декарти добутка множин	Отримання оцінки ІС	Теоретична формалізація процесу атаки
4	Модель на основі нейронних ланцюгів Маркова [38]	Дані для навчання нейромереж	Виявлення вірусів, спаму, та різні атаки на Web-сервіси	Теорія нейронних мереж	Адаптація	Потреба у статистичних даних
5	Модель мереж Петрі-Маркова [39]	Стан системи	Можливість проведення тестування	Теорія мереж Петрі та теорія Маркова	Оцінка з урахуванням часу	Надання розрахунків для практичних реалізацій
6	Диференціально	Моніторинг	Оптимальна	Теорія графів,	Здійснення	Не відображ

	ігрова однокритеріальна графова модель[40]	стану ІС	стратегія захисту	диференціальна-ігрове моделювання	розподілу інформаційних ресурсів	ає загальну динаміку впливу
7	Диференціально-ігрові спектральні однокритеріальні моделі[40]	Моніторинг стану ІС	Оптимальна стратегія захисту	Диференціально-ігрове моделювання	Низька обчислювальна складність	Не точний процес впливу на ІС
8	Диференціальна-ігрова нетейлорівська модель[40]	Інтенсивність потоку захисту і атаки	Траєкторія	Диференціальні перетворення нетоейлорівського типу	Опис процесу атаки на ІС	Висока обчислювальна складність, низький рівень технічних досліджень
9	Гібридна диферен	Показує ступінь	Оптимальний	Диференціально	Врахування	Точність досягає

	ціально-ігрова модель[40]	надійності та захищеності, ймовірність загрози	розподіл ресурсів для захисту	ігрове моделювання	показників якості СЗІ, висока точність	ься тільки при певному застосуванні математичних методів
10	Неперервна дискретна диференціально-ігрова модель[40]	Скінченна множина станів	Оптимальний розподіл ресурсів для захисту ІС	Числово-аналітичне моделювання, диференціальне перетворення	Можливість розширення діапазону моделювання впливу на ІС, низка обчислювальна здатність	Не враховує всі критерії
11	Багатокритеріальна диференціально-	Противоборча стратегія сторін	Стратегія оптимальних гравців	Диференціально-ігрове моделювання	Захист в умовах конфлікту у частинни	Обмеження на критеріях якості

	ігрова модель з основою інтегральної оптимальності[40]				х критеріїв та несанкціонованого розподілу ресурсів атакуючої сторони	
12	Багатокритеріальна диференціально-ігрова модель на основі нелінійної схеми компромісів[41]	Розподіл потокових ресурсів протиборчих сторін	Оптимальність стратегій протиборчих сторін	Диференціальні перетворення	Проста в реалізації, адаптивність	Значних недоліків немає