ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система виявлення фішингових атак у інформаційній системі організації»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Микола ПРОЦЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
ПРОЦЕНКО Микола
(прізвище, ім'я)

Керівник д.т.н., професор КАЗМІРЧУК Світлана
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___” _____ 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Проценку Миколі Віталійовичу
(прізвище, ім’я)

1. Тема кваліфікаційної роботи:
«Система виявлення фішингових атак у інформаційній системі організації»

керівник кваліфікаційної роботи Казмірчук Світлана, д.т.н., професор
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2025 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 01.06.2025 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення Malwarebytes;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми фішингових атак в інформаційних системах організацій.
2. Аналіз методів та засобів виявлення фішингу
3. Аналіз функціональних можливостей Malwarebytes щодо виявлення фішингу
4. Розробка та впровадження системи виявлення фішингових атак
5. Рекомендації щодо використання Malwarebytes для виявлення фішингу

6. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 28.02.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми фішингових атак в інформаційних системах	03.03.2025 р.	
2.	Аналіз наукової, технічної літератури та нормативної бази з питань виявлення фішингу	08.03.2025 р.	
3.	Дослідження функцій та можливостей виявлення фішингових атак у Malwarebytes	15.03.2025 р.	
4.	Практична реалізація сценарію виявлення фішингових атак у середовищі Malwarebytes	25.03.2025 р.	
5.	Розроблення рекомендацій щодо впровадження системи виявлення фішингу в організаційній ІС	01.04.2025 р.	
6.	Оформлення результатів дослідження.	10.04.2025 р.	
7.	Підготовка доповіді до захисту.	01.06.2025 р.	

Здобувач вищої освіти _____ Микола ПРОЦЕНКО
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Світлана КАЗМІРЧУК
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача ПРОЦЕНКА Миколи
на тему: «Система виявлення фішингових атак у інформаційній системі організації»

Актуальність: У сучасних умовах фішингові атаки залишаються одними з найпоширеніших і небезпечних форм соціальної інженерії, спрямованих на викрадення облікових даних, доступу до корпоративних систем і компрометацію критичних ресурсів. Вони щодня загрожують безпеці організацій, особливо через електронну пошту та веб-інтерфейси. Виявлення фішингу потребує застосування як традиційних фільтраційних методів, так і сучасних антивірусних рішень.

Застосування антивірусного програмного забезпечення **Malwarebytes** для виявлення та нейтралізації фішингових атак є актуальним напрямом дослідження та має важливе практичне значення для забезпечення кіберстійкості організацій.

Позитивні сторони:

1. У роботі чітко сформульовано проблему фішингових атак, окреслено їх види, механізми реалізації та загрози, які вони створюють для інформаційних систем організацій.
2. Проведено огляд сучасних методів виявлення фішингу, зокрема за допомогою антивірусного ПЗ, а також досліджено функціональні можливості Malwarebytes у контексті теми.
3. Запропоновано варіант системи виявлення фішингових атак на базі Malwarebytes та розроблено практичні рекомендації щодо її впровадження в інформаційну інфраструктуру.
4. Робота логічно структурована, грамотно оформлена, має якісні графічні матеріали та продемонстроване вміння працювати з технічною та науковою літературою.

Недоліки:

1. У роботі було б доцільно навести приклади реальних фішингових інцидентів у конкретній організації для кращої ілюстрації практичного аспекту теми.
2. Алгоритми дій при виявленні фішингу могли б бути розширені з урахуванням ролей ІТ-персоналу (SOC-аналітики, адміністратори безпеки тощо).

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач(ка) **ПРОЦЕНКО Микола** – присвоєння кваліфікації бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Рецензент:

_____	_____	_____
(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач ПРОЦЕНКО Микола до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Система виявлення фішингових атак у інформаційній системі організації».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***ПРОЦЕНКО Микола*** обрав тему роботи, метою якої було дослідити методи та засоби виявлення фішингових атак у інформаційній системі організації та розробити рекомендації щодо їх ефективного впровадження. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***ПРОЦЕНКО Микола*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***ПРОЦЕНКА Миколи*** на оцінку **"добре"** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Світлана Казмірчук
(підпис) *(ім'я, прізвище)*
"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **ПРОЦЕНКО Микола** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 60 сторінок, 17 рисунків, 12 джерел.

Об'єкт дослідження – інформаційна система організації.

Предмет дослідження – методи та засоби виявлення фішингових атак в інформаційній системі організації з використанням Malwarebytes.

Мета роботи – дослідити методи і засоби виявлення фішингових атак, проаналізувати функціональні можливості антивірусного рішення Malwarebytes та розробити практичні рекомендації щодо його впровадження з метою підвищення кіберзахисту організації.

Методи дослідження – аналіз наукових джерел, технічної документації, порівняльний аналіз функціоналу антивірусних систем, експериментальне тестування у віртуальному середовищі, моделювання інцидентів.

Фішинг залишається однією з найнебезпечніших форм соціальної інженерії. У кваліфікаційній роботі досліджено актуальність цієї загрози для сучасних інформаційних систем, охарактеризовано основні методи фішингових атак, вразливості систем, що дозволяють їм здійснюватись, та запропоновано рішення на основі системи Malwarebytes.

Зокрема, проаналізовано архітектуру, функціональні можливості та антифішингові механізми Malwarebytes. На основі проведених досліджень реалізовано модель впровадження системи виявлення фішингових атак у типову локальну ІС організації. Проведено практичне тестування ефективності рішень, визначено рівень виявлення та хибних спрацювань. Розроблено рекомендації для фахівців ІТ щодо налаштування, впровадження та експлуатації Malwarebytes для ефективного виявлення фішингових атак.

Галузь використання – кібербезпека інформаційних ресурсів організації.

Ключові слова: фішинг, Malwarebytes, виявлення атак, кібербезпека, інформаційна система, соціальна інженерія, антифішинговий захист.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

MFA – Multi-Factor Authentication (багатофакторна автентифікація)

PUP – Potentially Unwanted Program (потенційно небажане ПЗ)

DEP – Data Execution Prevention (запобігання виконанню даних)

ASLR – Address Space Layout Randomization (рандомізація розміщення в адресному просторі)

ROP – Return Oriented Programming (програмування з орієнтацією на повернення)

IVR – Interactive Voice Response (інтерактивна голосова відповідь)

PDF – Portable Document Format

URL – Uniform Resource Locator

IP – Internet Protocol

ML – Machine Learning

AI – Artificial Intelligence

GUI – Graphical User Interface

CERT – Computer Emergency Response Team

QR – Quick Response (в контексті QR-кодів)

CSV – Comma-Separated Values (як формат логів)

ВСТУП

Актуальність дослідження. Фішинг залишається одним із найрозповсюдженіших та найнебезпечніших видів кіберзагроз в сучасному цифровому середовищі. Атаки фішингу націлені на обман користувачів з метою отримання доступу до конфіденційних даних, фінансової інформації або облікових записів. Через соціальну інженерію, фальшиві веб-сайти, електронні листи та інші засоби комунікації зловмисники отримують змогу проникати в інформаційні системи організацій, що призводить до значних фінансових та репутаційних збитків.

Фішингові атаки постійно еволюціонують, що ускладнює їх виявлення традиційними методами. Саме тому зростає потреба в сучасних системах виявлення таких атак, які базуються на поведінковому аналізі, машинному навчанні та інтеграції з антивірусними рішеннями нового покоління. Одним із ефективних інструментів в цьому напрямі є програмне забезпечення **Malwarebytes**, яке включає в себе засоби проактивного виявлення шкідливих дій, зокрема фішингових спроб, у режимі реального часу.

Забезпечення своєчасного виявлення фішингових атак є критично важливим для збереження цілісності інформаційної системи організації, її безперервної роботи та відповідності міжнародним стандартам кібербезпеки. Це і зумовлює актуальність теми даної кваліфікаційної роботи.

Об'єкт дослідження – інформаційна система організації.

Предмет дослідження – методи та засоби виявлення фішингових атак в інформаційній системі організації з використанням Malwarebytes.

Мета роботи – дослідити методи і засоби виявлення фішингових атак, проаналізувати функціонал антивірусного рішення Malwarebytes та розробити практичні рекомендації щодо його впровадження для підвищення кіберзахисту організації.

Наукові завдання:

- дослідити природу фішингових атак та їх типові ознаки;

- проаналізувати основні вектори здійснення фішингових атак в ІС;
- розглянути сучасні підходи до виявлення фішингу;
- провести аналіз можливостей Malwarebytes у контексті виявлення фішингу;
- змоделювати систему виявлення фішингових атак на базі Malwarebytes;
- розробити практичні рекомендації щодо впровадження та використання Malwarebytes в організаціях.

Методи дослідження – аналіз наукових джерел і технічної документації, порівняльний аналіз функціоналу антивірусних систем, експериментальне тестування на віртуальному середовищі, моделювання інцидентів.

Практичне значення одержаних результатів – розроблено приклад впровадження системи виявлення фішингових атак на основі Malwarebytes у типову ІС організації, а також підготовлено методичні рекомендації для ІТ-фахівців щодо виявлення та реагування на фішингові інциденти.

Результати кваліфікаційної роботи апробовані під час Всеукраїнської науково-практичної конференції «Цифрова трансформація кібербезпеки», яка відбулася 24 квітня 2025 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1. ДОСЛІДЖЕННЯ ПРОБЛЕМИ ФІШИНГУ В ІНФОРМАЦІЙНІЙ СИСТЕМІ

1.1. Загальна характеристика фішингових атак

У сучасному світі інформація є активом, який як окремі особи, так і організації прагнуть захистити. Для користувачів це — особисті дані, а для організацій — чутлива інформація, що має критичне значення. Наприклад, у випадку з національною безпекою — це секретна інформація, яка в разі розголошення поставить під загрозу всю державу. У медичних установах це історія хвороби пацієнта, призначені медикаменти, дані про оплату, які, якщо їх розкрити, можуть спричинити соціальне таврування, сором, а також фінансові збитки для установ.

У фінансових інституціях це дані клієнтів, які можуть бути використані для зняття коштів з рахунків. Такі витоки даних трапляються все частіше: як в організаціях (Target, Home Depot, Chase, Sony), так і у вигляді цільових атак, наприклад, публікація приватних фото знаменитостей (відомий випадок "Fappening") [1]. Зловмисники отримують доступ до чутливої інформації, викрадаючи облікові дані користувачів через прості методи (брутфорс) або складніші — як-от кейлогінг чи зняття інформації з екрана.

Проте з позитивного боку: ці інциденти змусили користувачів і компанії дають змогу змінити своє ставлення до безпеки — впроваджуються двофакторна автентифікація, фаєрволи, системи виявлення загроз, шифрування тощо. Злочинці також удосконалюють свої методи — одна з найпоширеніших атак сьогодні — це *фішинг.*

У цьому розділі ми приділимо час розумінню, що таке соціальна інженерія та різних її форм. Також коротко розглянемо різні види фішингових атак. Нарешті, розглянемо кейс, де атаки, підтримані державою, використовували техніки

фішингу для проникнення у мережу великої організації та викрадення її конфіденційних даних.

Соціальна інженерія в контексті інформаційної безпеки — це психологічна маніпуляція людьми, щоб змусити їх виконувати певні дії або розкривати конфіденційну інформацію [2]. Це тип афери, що використовується для збору інформації, шахрайства або отримання доступу до систем. Вона відрізняється від традиційних шахрайств тим, що часто є одним із багатьох етапів у складнішій схемі. Термін "соціальна інженерія" описує акт психологічної маніпуляції і пов’язаний із соціальними науками, але найбільше вживається серед фахівців з комп’ютерної та інформаційної безпеки.

Техніки базуються на особливостях людського прийняття рішень, відомих як когнітивні упередження. Ці упередження, іноді звані "помилками у людському апаратному забезпеченні", використовуються у різних комбінаціях для створення атак. Деякі форми соціальної інженерії наведені нижче:

Інсценування

Інсценування — це створення та використання вигаданого сценарію (прикриття), щоб залучити цільову жертву таким чином, що підвищує ймовірність розкриття інформації або виконання дій, які зазвичай були б малоймовірними.

Фішинг

Фішинг — це техніка шахрайського отримання приватної інформації. Зазвичай зловмисник надсилає електронного листа, що нібито походить від легітимного бізнесу, наприклад банку або кредитної компанії, з проханням "підтвердити" інформацію та попередженням про серйозні наслідки у разі відмови.

IVR або телефонний фішинг

Телефонний фішинг, або "вішинг", використовує підроблену інтерактивну голосову систему (IVR), що імітує легітимне голосове меню банку або іншої установи. Жертву просять зателефонувати на "банк" за (зазвичай безкоштовним) номером, щоб "підтвердити" інформацію.

Як згадувалося вище, фішинг — це форма тактики соціальної інженерії, коли зловмисник надсилає жертвам електронні листи, заманюючи їх розкрити

конфіденційну інформацію або змусити запустити шкідливі виконувані файли чи відкрити вкладення, які можуть скомпрометувати систему користувача. Проте відмінність між масовою розсилкою і спрямованою атакою залежить від мотивів нападника.

Приклади фішингових атак

Ось приклад спроби фішингу, підробка повідомлення від PayPal з проханням до одержувача натиснути кнопку «Підтвердити зараз». Наведення курсора на кнопку показує справжню URL-адресу призначення в червоному прямокутнику (рисунок 1.1) [3].

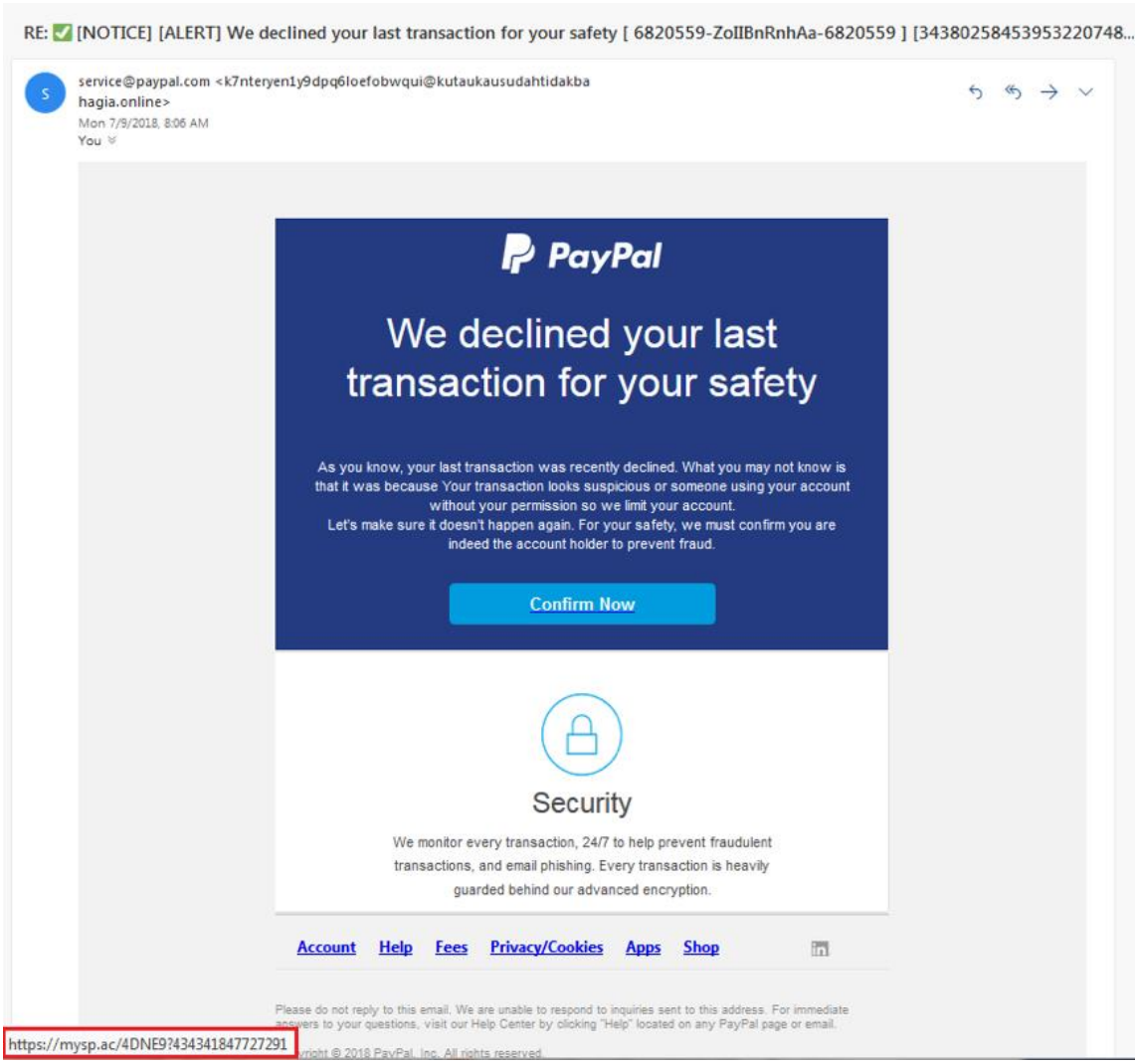

Рис. 1.1 Приклад фішингового листа, що імітує повідомлення від PayPal

Ось ще одне зображення фішингової атаки, цього разу нібито з Amazon. Зверніть увагу на погрозу закрити обліковий запис, якщо протягом 48 годин не буде відповіді (рисунок 1.2) [3].

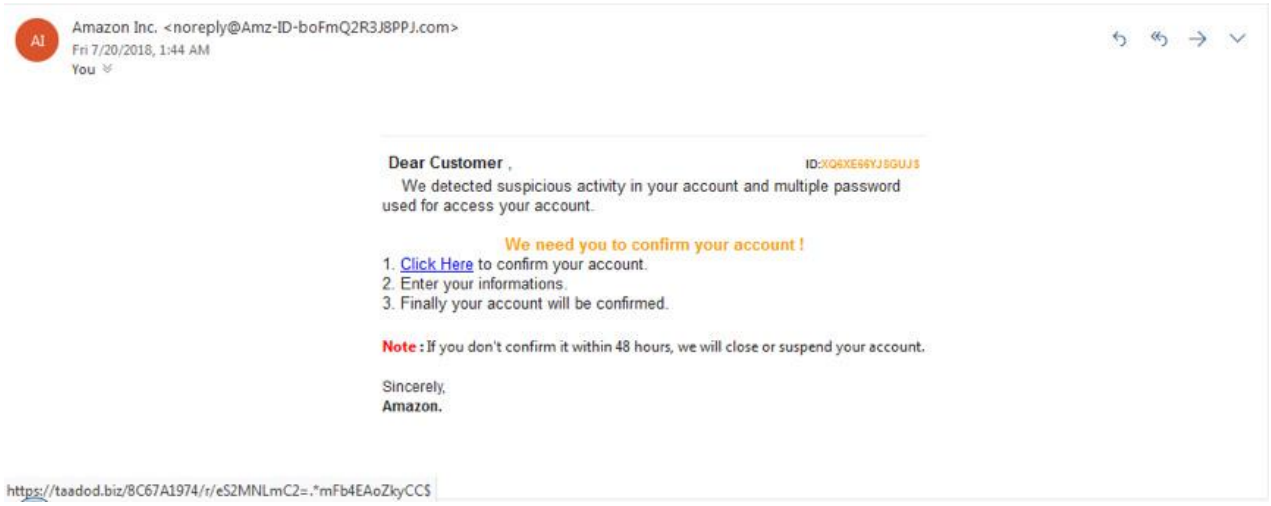

Рис. 1.2. Приклад фішингового листа, який імітує повідомлення від Amazon.

Натискання на посилання переведе вас на цю форму, яка пропонує вам віддати фішеру все, що потрібно для крадіжки ваших цінностей (рисунок 1.3) [3]:

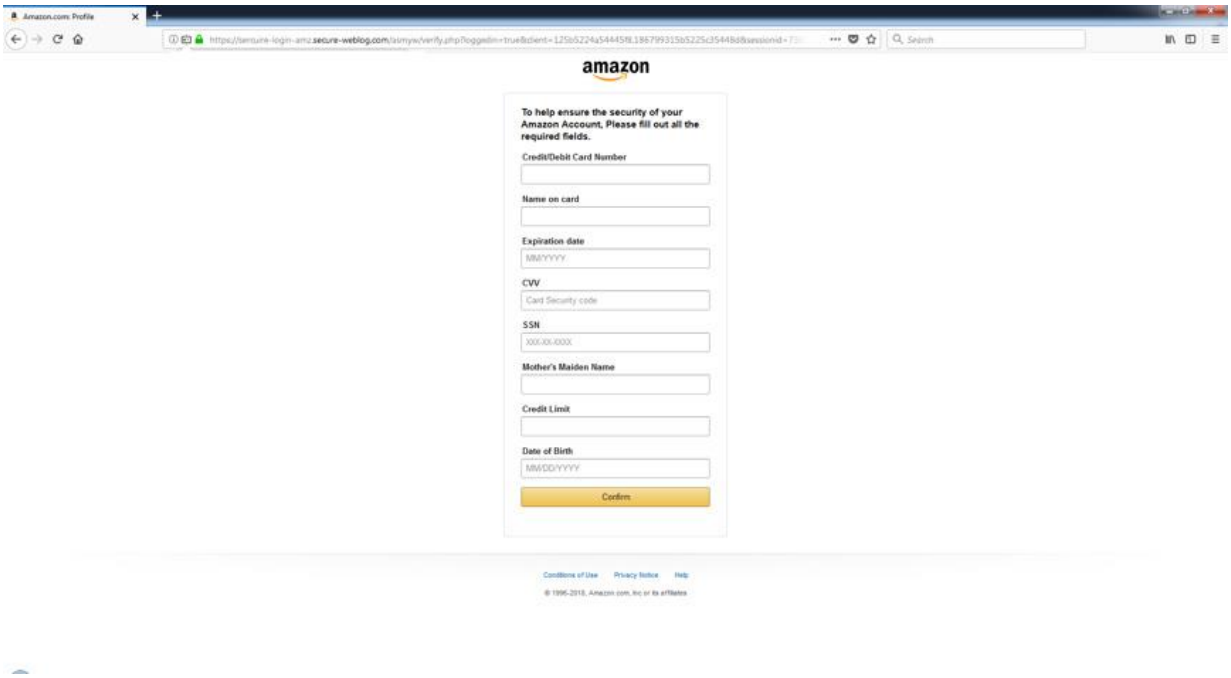

Рис.1.3 Фальшива сторінка входу, яка імітує інтерфейс Amazon

1.2 Основні методи здійснення фішингових атак

Фішингові атаки є однією з найпоширеніших і найнебезпечніших форм кіберзагроз у сучасному цифровому просторі. Вони базуються на соціальній інженерії — маніпуляції користувачами з метою викрадення конфіденційних даних, таких як облікові записи, паролі, фінансова інформація тощо. Основною метою фішингу є отримання несанкціонованого доступу до інформаційних систем або особистих даних жертв через обман (рисунок 1.4) [4].

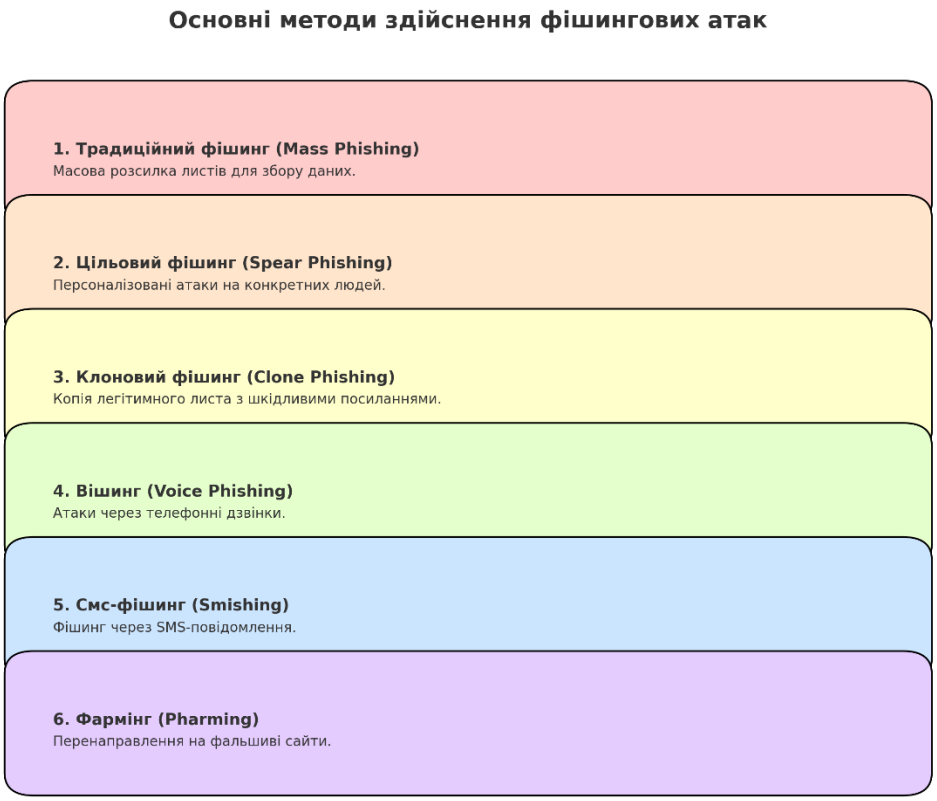

Рис. 1.4. Основні методи фішингових атак

1. Традиційний фішинг (Mass Phishing)

Це найпоширеніший вид фішингових атак, який здійснюється шляхом масової розсилки електронних листів або повідомлень з однаковим змістом на велику кількість користувачів. Зловмисники прагнуть залучити якомога більше жертв, використовуючи шаблони листів, що імітують офіційні повідомлення від банків, популярних сервісів, соцмереж або інших довірених організацій.

Особливості:

- Використання масових розсилок, які не мають конкретної цілі.
- Листи містять посилання на фальшиві сайти або вкладення зі шкідливим ПЗ.
- Можливість швидкого розповсюдження атаки.

2. Цільовий фішинг (Spear Phishing)

Цільовий фішинг — це більш точкова та персоналізована форма фішингової атаки. Зловмисник збирає інформацію про конкретну особу або групу осіб (наприклад, працівників компанії) і готує унікальне повідомлення, яке відповідає їхній ролі, інтересам або посаді. Такий підхід значно підвищує ефективність атаки, оскільки жертва вважає повідомлення більш правдоподібним.

Особливості:

- Збір інформації про цільові об'єкти через соціальні мережі, відкриті джерела, витоки даних.
- Персоналізовані листи із використанням імен, посад, внутрішньокорпоративних термінів.
- Часто застосовуються додаткові тактики — наприклад, маскування під колег або керівників.

3. Клоновий фішинг (Clone Phishing)

Клоновий фішинг полягає у створенні точних копій раніше доставлених легітимних листів, у яких замінюються посилання або вкладення на шкідливі. Зловмисники використовують довіру жертв до отриманих раніше листів для швидкого розповсюдження шкідливого ПЗ.

Особливості:

- Клонування змісту легітимного листа з мінімальними змінами.
- Заміна оригінальних посилань на шкідливі URL.
- Часто використовується для повторного зараження або збільшення масштабів атаки.

4. Вішинг (Voice Phishing)

Вішинг — це різновид фішингу, який здійснюється за допомогою телефонних дзвінків або автоматизованих голосових повідомлень. Зловмисники імітують

голоси працівників банків, державних установ або технічної підтримки, щоб отримати від жертв конфіденційну інформацію.

Особливості:

- Використання інтерактивних голосових систем (IVR) для підробки офіційних дзвінків.
- Соціальна маніпуляція жертв через телефон.
- Може супроводжуватися подальшими фішинговими листами.

5. Смс-фішинг (Smishing)

Смс-фішинг — це форма фішингової атаки через текстові повідомлення. Зловмисники надсилають SMS із посиланнями на фальшиві сайти або проханнями передати особисті дані.

Особливості:

- Використання мобільного зв’язку як каналу атаки.
- Часто містить термінові заклики до дії.
- Висока швидкість поширення серед користувачів мобільних пристроїв.

6. Фармінг (Pharming)

Фармінг відрізняється від традиційного фішингу тим, що користувач перенаправляється на підроблений сайт без його відома, через зміну DNS-записів або зараження пристрою. Таким чином, навіть якщо користувач вводить правильну URL-адресу, він потрапляє на фальшиву сторінку [5].

Особливості:

- Технічний характер атаки.
- Може здійснюватись масово або цілеспрямовано.
- Важко виявляється звичайним користувачем.

Фішингові атаки мають різноманітні форми і постійно розвиваються, адаптуючись до нових технологій і поведінки користувачів. Для ефективного захисту необхідне комплексне застосування технічних засобів (фільтри, багатофакторна автентифікація) та підвищення обізнаності користувачів щодо основних методів розпізнавання фішингу.

1.3 Вразливості інформаційної системи до фішингу

Інформаційні системи сучасних організацій мають численні точки входу, які зловмисники використовують для реалізації фішингових атак. Уразливості до фішингу можуть бути як технічними (відсутність безпекових засобів), так і людськими (недостатня обізнаність користувачів). Аналіз таких вразливостей є критично важливим для побудови ефективної системи захисту. Найбільш поширені з них наведені в таблиці 1.1.

Таблиця 1.1.

Основні типи вразливостей

№	*Тип вразливості*	*Суть проблеми*
1	Відсутність фільтрації email-листів	Пропуск фішингових листів до основної скриньки користувача
2	Недостатнє навчання співробітників	Люди не розпізнають фішингові ознаки: підроблені адреси, терміновість тощо
3	Використання застарілого програмного забезпечення	Відомі уразливості можуть бути використані для подальшої компрометації
4	Відсутність багатофакторної автентифікації (MFA)	Компрометація облікових даних відкриває доступ до системи
5	Невикористання сучасного антивірусного ПЗ	Вкладення в листах або шкідливі сайти не блокуються
6	Відсутність політик управління доступом	Надлишкові права користувачів сприяють поширенню атаки вглиб мережі

У процесі дослідження виявлених загроз інформаційної безпеки організації було здійснено порівняльний аналіз основних вразливостей інформаційної системи, які потенційно можуть бути використані під час фішингових атак [5]. Результати оцінки впливу кожної вразливості наведено у вигляді горизонтального стовпчикового графіка, що відображає рівень їхньої небезпеки за умовною шкалою від 0 до 100 балів (рисунок 1.5).

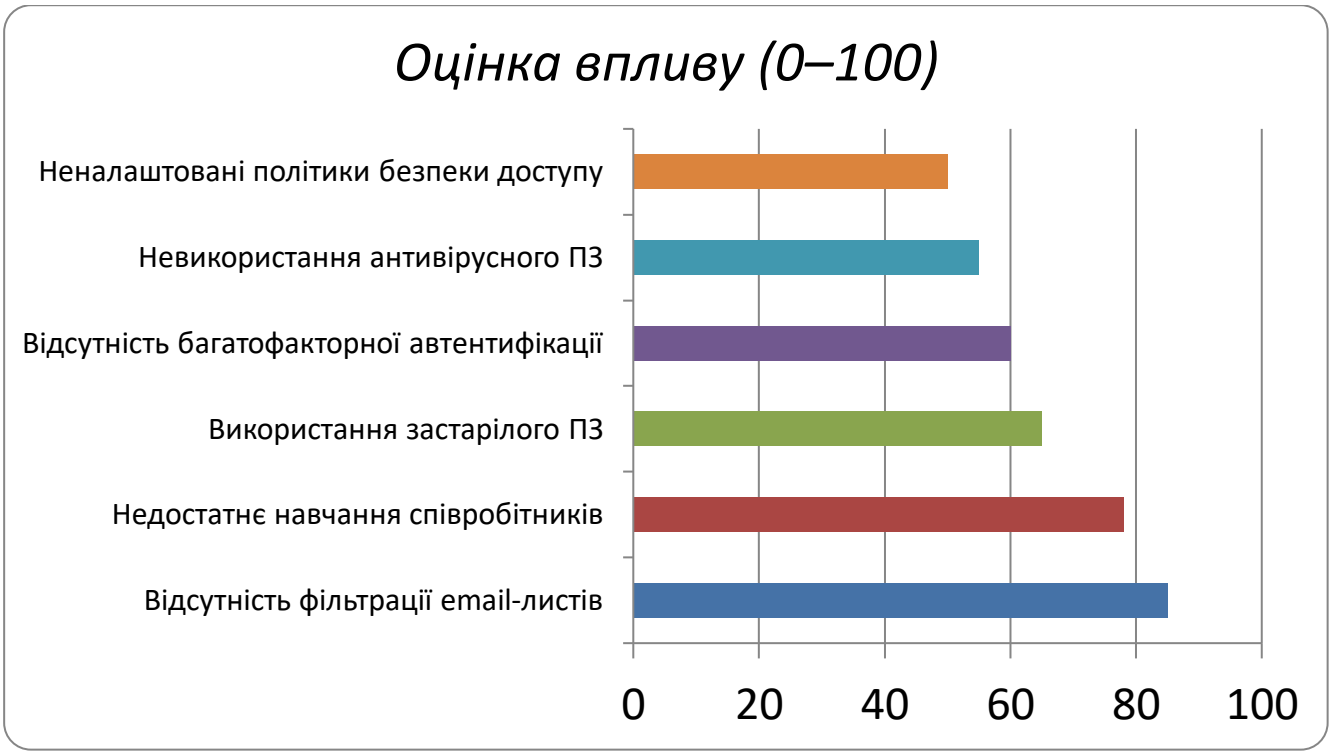

Рис. 1.5. Оцінка впливу вразливостей до фішингу

На графіку представлено такі категорії:

1. Відсутність фільтрації email-листів (85 балів)

Найбільш критична вразливість, яка дозволяє фішинговим повідомленням безперешкодно потрапляти до вхідної пошти користувачів. Цей фактор часто є стартовою точкою для подальшої компрометації системи.

2. Недостатнє навчання співробітників (78 балів)

Користувачі не володіють знаннями щодо розпізнавання типових ознак фішингових повідомлень, що створює високий ризик добровільного розголошення конфіденційної інформації.

3. Використання застарілого програмного забезпечення (65 балів)

Підвищує ймовірність технічної експлуатації фішингових атак через уразливості, які вже були виявлені та задокументовані у відкритих джерелах.

4. Відсутність багатофакторної автентифікації (60 балів)

Сприяє спрощеному несанкціонованому доступу до облікових записів після фішингового викрадення логіну і пароля.

5. Невикористання антивірусного програмного забезпечення (55 балів)

Знижує рівень автоматичного виявлення фішингових вкладень або шкідливих скриптів у листах, що запускаються після переходу за посиланнями.

6. Неналаштовані політики безпеки доступу (50 балів)

У разі компрометації облікового запису відсутність обмежень доступу дозволяє зловмиснику оперативно поширити атаку по внутрішній мережі.

Графік вказує на домінування людського фактора як основної загрози інформаційній безпеці. Перше та друге місця займають саме ті вразливості, що пов’язані з низьким рівнем технічної та інформаційної гігієни користувачів: недостатній фільтр електронної пошти та відсутність навчання персоналу.

Технічні вразливості, як-от відсутність MFA або використання застарілого ПЗ, мають також значну вагу, але, як свідчить аналіз, вони часто є наслідками слабкого інформаційного менеджменту, а не лише технічних обмежень.

Malwarebytes — це одна з провідних систем захисту від шкідливого програмного забезпечення, яка включає у себе модулі для виявлення та блокування фішингових атак [6]. Незважаючи на високу ефективність, будь-яка інформаційна система має потенційні вразливості, які можуть бути використані зловмисниками для обходу захисту.

Основні вразливості Malwarebytes до фішингу (рисунок 1.6) [6]:

1. Обмеження у виявленні нових та цільових фішингових атак Malwarebytes ефективно виявляє відомі загрози та популярні фішингові сайти за допомогою актуальних баз даних. Однак, цільові (spear phishing) або нові фішингові кампанії, які використовують інноваційні техніки соціальної інженерії або швидко змінюють URL-адреси, можуть тимчасово залишатися непоміченими.

2. Обхід захисту через фальсифікацію доменів (Domain Spoofing) Зловмисники застосовують складні методи підміни адрес відправників, використовуючи домени, схожі на легітимні, що ускладнює фільтрацію фішингових листів Malwarebytes.

3. Відсутність повного контролю над поштовими клієнтами Malwarebytes забезпечує захист на рівні системи, але не може гарантувати повний контроль над всіма поштовими клієнтами та їх плагінами, через що деякі фішингові листи можуть пройти у папку «Вхідні».

4. Обмеження у виявленні складних шкідливих вкладень Фішингові листи часто містять шкідливі файли (наприклад, макроси в документах Office або виконувані файли), які можуть бути замасковані для обходу антивірусних сканерів Malwarebytes.

5. Людський фактор.

Незважаючи на технічні засоби захисту, основна вразливість — це користувачі, які можуть випадково виконати шкідливі дії, якщо фішингове повідомлення виглядає досить правдоподібно. Malwarebytes не може повністю компенсувати недостатню обізнаність співробітників.

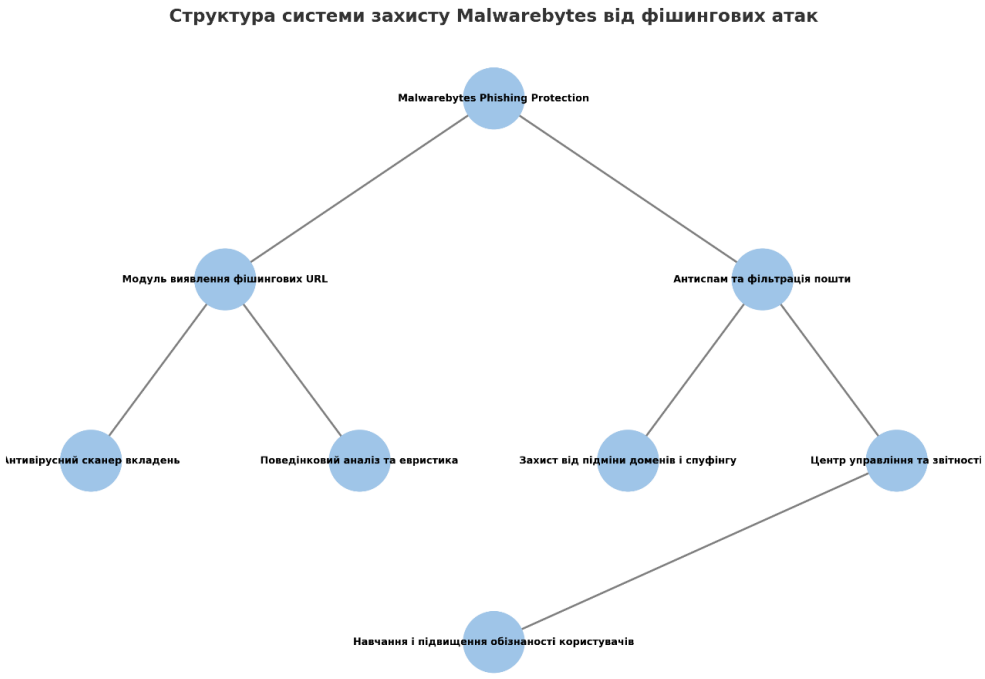

Рис. 1.6. Структура системи захисту Malwarebytes від фішингових атак

2 АНАЛІЗ ІСНУЮЧИХ ЗАСОБІВ ВИЯВЛЕННЯ ФІШИНГОВИХ АТАК НА ПРИКЛАДІ MALWAREBYTES

2.1 Архітектура та функціональні можливості Malwarebytes

Програмний продукт Malwarebytes є одним із провідних рішень у галузі кібербезпеки, що спеціалізується на виявленні та видаленні різноманітних видів шкідливого програмного забезпечення (ШПЗ), включаючи віруси, трояни, руткіти, програми-вимагачі (ransomware), шпигунське ПЗ (spyware), рекламні програми (adware) та інші потенційно небажані програми (PUPs). Його архітектура розроблена з метою забезпечення багатошарового захисту, що поєднує традиційні та сучасні підходи до виявлення загроз [7].

Архітектура Malwarebytes побудована за модульним принципом, що дозволяє інтегрувати різні технології захисту та ефективно взаємодіяти між собою. Основними рівнями архітектури є [8]:

- *Рівень ядра (Kernel-level protection):* Цей рівень є фундаментальним і відповідає за низькорівневий моніторинг операційної системи. Він включає драйвери, що забезпечують перехоплення системних викликів, моніторинг файлової системи, реєстру та мережевого трафіку. Саме тут реалізуються функції захисту від руткітів та буферних атак.
- *Рівень служб (Services layer):* На цьому рівні функціонують фонові служби Malwarebytes, які забезпечують постійний моніторинг активності системи, запуск сканувань, оновлення баз даних та взаємодію з користувацьким інтерфейсом. Ключовими службами є служба захисту в реальному часі (Real-Time Protection Service) та служба оновлень (Update Service).
- *Рівень користувацького інтерфейсу (User Interface layer):* Цей рівень відповідає за взаємодію з користувачем, відображення інформації про загрози, налаштування параметрів захисту, запуск сканувань та перегляд звітів. Інтерфейс розроблений з акцентом на зручність використання та

інтуїтивність.

- *Хмарний рівень (Cloud layer):* Сучасні версії Malwarebytes активно використовують хмарні технології. Це дозволяє здійснювати аналіз підозрілих файлів у ізольованому середовищі (sandbox), отримувати оновлення баз даних загроз у реальному часі, а також використовувати колективний інтелект для швидкого реагування на нові загрози.

Ключові компоненти та їх взаємодія

Основні компоненти Malwarebytes, що працюють на різних рівнях архітектури, включають:

- *Модуль захисту в реальному часі (Real-Time Protection Module):* Цей модуль є серцем постійного захисту. Він складається з кількох взаємопов'язаних підмодулів:
    - *Захист від шкідливого програмного забезпечення (Malware Protection):* Використовує сигнатурний аналіз (бази даних відомих загроз), евристичний аналіз (поведінкові патерни) та машинне навчання для виявлення та блокування ШПЗ до його виконання.
    - *Захист від програм-вимагачів (Ransomware Protection):* Спеціалізований механізм, що відстежує підозрілу поведінку, характерну для програм-вимагачів, та блокує процеси шифрування файлів. Він включає технології Honeypot (приманки) та самовідновлення файлів.
    - *Захист від експлойтів (Exploit Protection):* Захищає від експлуатації вразливостей у програмному забезпеченні (браузери, офісні програми, мультимедійні плеєри тощо). Він працює на рівні пам'яті та API, запобігаючи несанкціонованому доступу та виконанню шкідливого коду.
    - *Захист веб-трафіку (Web Protection):* Блокує доступ до відомих шкідливих веб-сайтів, фішингових ресурсів та доменів, пов'язаних з командно-контрольними серверами (C2) ШПЗ. Використовує базу даних репутації URL-адрес та DNS-фільтрацію.

- *Модуль сканування (Scanning Engine):* Відповідає за виконання повних, швидких та вибіркових сканувань системи на наявність загроз. Використовує оновлені бази даних сигнатур, а також застосовує евристичні та поведінкові алгоритми для виявлення нових або модифікованих загроз.
- *Модуль карантину (Quarantine Module):* Ізолює виявлені загрози, запобігаючи їх подальшому впливу на систему. Користувач може переглядати об'єкти в карантині, відновлювати їх (якщо це помилкове виявлення) або остаточно видаляти.
- *Модуль оновлення (Update Module):* Забезпечує регулярне оновлення баз даних сигнатур, правил поведінкового аналізу та самого програмного забезпечення. Це критично важливо для ефективного захисту від нових та постійно еволюціонуючих загроз. Оновлення можуть бути автоматичними або за запитом користувача.
- *Модуль журналювання та звітів (Logging and Reporting Module):* Записує всі події, пов'язані з виявленням та блокуванням загроз, дії користувача та оновлення. Надає детальні звіти, які допомагають аналізувати стан безпеки системи.
- *Інтеграція з Windows Security Center:* Malwarebytes коректно інтегрується з центром безпеки Windows, інформуючи систему про свій статус захисту.

Взаємодія між цими компонентами відбувається постійно. Наприклад, модуль захисту в реальному часі безперервно моніторить систему. При виявленні підозрілої активності він звертається до хмарних сервісів для додаткового аналізу та до баз даних сигнатур. У разі підтвердження загрози, вона блокується, поміщається в карантин, і відповідна інформація записується в журнал. Модуль оновлення синхронно працює з хмарними сервісами, забезпечуючи актуальність даних.

Функціональні можливості: від виявлення до реагування

Функціональні можливості Malwarebytes охоплюють повний життєвий цикл протидії ШПЗ, від профілактики до пост-інцидентного реагування [9]:

- *Проактивне виявлення:*

- *Сигнатурний аналіз:* Класичний метод, заснований на порівнянні файлів з базою даних відомих сигнатур (хешів, фрагментів коду) шкідливого програмного забезпечення. Хоча він є основою, його ефективність обмежена проти нових або поліморфних загроз.
- *Евристичний аналіз:* Аналіз коду та поведінки програм на наявність ознак, типових для ШПЗ, навіть якщо конкретна сигнатура відсутня в базі даних. Це дозволяє виявляти модифіковані або раніше невідомі загрози (zero-day exploits).
- *Поведінковий аналіз (Behavioral Analysis):* Моніторинг активності процесів у реальному часі. Якщо програма намагається виконувати дії, характерні для ШПЗ (наприклад, змінювати системні файли, шифрувати дані, встановлювати мережеві з'єднання з підозрілими серверами), Malwarebytes може її заблокувати, навіть якщо вона не має відомої сигнатури.
- *Машинне навчання та штучний інтелект (ML/AI):* Сучасні версії Malwarebytes активно використовують алгоритми машинного навчання для аналізу великих обсягів даних про загрози. Це дозволяє ідентифікувати складні та приховані загрози, а також адаптуватися до нових видів атак без необхідності постійних оновлень сигнатур. Алгоритми навчаються на мільйонах зразків ШПЗ та легітимного ПЗ.
- *Аналіз репутації (Reputation Analysis):* Оцінка репутації файлів, URL-адрес та IP-адрес на основі їх історії, поведінки та зв'язків з відомими загрозами.

- *Блокування та карантин:*
  - *Блокування в реальному часі:* Негайне припинення виконання шкідливих процесів та блокування доступу до небезпечних ресурсів.
  - *Автоматичний карантин:* Переміщення виявлених загроз в ізольоване середовище, де вони не можуть завдати шкоди системі.
  - *Ручне управління карантином:* Можливість для користувача переглядати, видаляти або відновлювати об'єкти з карантину.

- *Видалення та відновлення:*
    - *Повне видалення ШПЗ:* Видалення всіх компонентів шкідливої програми, включаючи файли, записи в реєстрі, заплановані завдання тощо.
    - *Відновлення системи:* У випадку деяких видів атак (наприклад, ransomware), Malwarebytes може мати функціонал для відновлення зашифрованих файлів або системних налаштувань.
- *Захист від специфічних видів загроз:*
    - *Ransomware Protection:* Спеціалізовані алгоритми для виявлення та блокування спроб шифрування файлів зловмисними програмами-вимагачами.
    - *Exploit Protection:* Запобігання використанню вразливостей в програмному забезпеченні для компрометації системи.
    - *Rootkit Protection:* Технології для виявлення та видалення руткітів, що приховують свою присутність у системі.
    - *Adware/PUP Protection:* Виявлення та видалення рекламних та потенційно небажаних програм, що можуть негативно впливати на продуктивність та безпеку.
- *Інші функціональні можливості:*
    - *Заплановані сканування:* Можливість налаштування автоматичних сканувань системи за розкладом.
    - *Гнучкі налаштування:* Широкі можливості конфігурації параметрів захисту, винятків та сповіщень.
    - *Підтримка та оновлення:* Регулярні оновлення баз даних загроз та програмного забезпечення, технічна підтримка.

Інноваційні підходи в Malwarebytes

Malwarebytes постійно розвиває свої технології, інтегруючи інноваційні підходи для протидії сучасним загрозам:

- *Heuristic Shifting:* Це не просто евристика, а більш динамічний підхід до аналізу, який адаптується до нових зразків ШПЗ. Він дозволяє виявляти

загрози, які використовують обфускацію або поліморфізм для ухилення від сигнатурного аналізу.

- *Behavioral Anomaly Detection (BAD):* Поглиблений поведінковий аналіз, який не просто шукає відомі патерни, а виявляє будь-які відхилення від нормальної поведінки програм та процесів у системі, що може свідчити про наявність невідомої загрози.
- *Payload Analysis:* Детальний аналіз навантаження (payload) шкідливого програмного забезпечення, що дозволяє зрозуміти його функціонал та потенційний вплив на систему. Це особливо важливо для аналізу нових та складних загроз.
- *Graph-based Analysis:* Використання графових баз даних для аналізу взаємозв'язків між файлами, процесами, мережевими з'єднаннями та системними змінами. Це допомагає виявляти складні атаки, які розгортаються у кілька етапів, та ідентифікувати джерела інфекції.
- *Zero-Day Exploit Mitigation:* Хоча повний захист від усіх zero-day експлойтів є складним завданням, Malwarebytes використовує технології для пом'якшення їх впливу, блокуючи типові техніки, які використовуються в таких атаках (наприклад, повернення до орієнтованого на гаджети програмування - ROP).
- *Cloud-Native Architecture:* Активне використання хмарних обчислень для масштабованості, швидкості аналізу та обміну інформацією про загрози в реальному часі. Це дозволяє Malwarebytes швидше реагувати на глобальні спалахи загроз.
- *AI-Driven Threat Intelligence:* Застосування штучного інтелекту для обробки величезних обсягів інформації про загрози, виявлення прихованих зв'язків та прогнозування майбутніх атак. Це покращує здатність до проактивного захисту.

Таким чином, архітектура Malwarebytes є комплексним рішенням, що поєднує багатошарові технології захисту, від низькорівневого моніторингу до хмарного

аналізу. Її модульна структура та постійне впровадження інноваційних підходів забезпечують ефективну протидію широкому спектру сучасних кіберзагроз.

Архітектура Malwarebytes може варіюватися залежно від продукту (наприклад, для дому, для бізнесу) та платформи (Windows, Mac, Android, iOS)(рисунок 2.1).

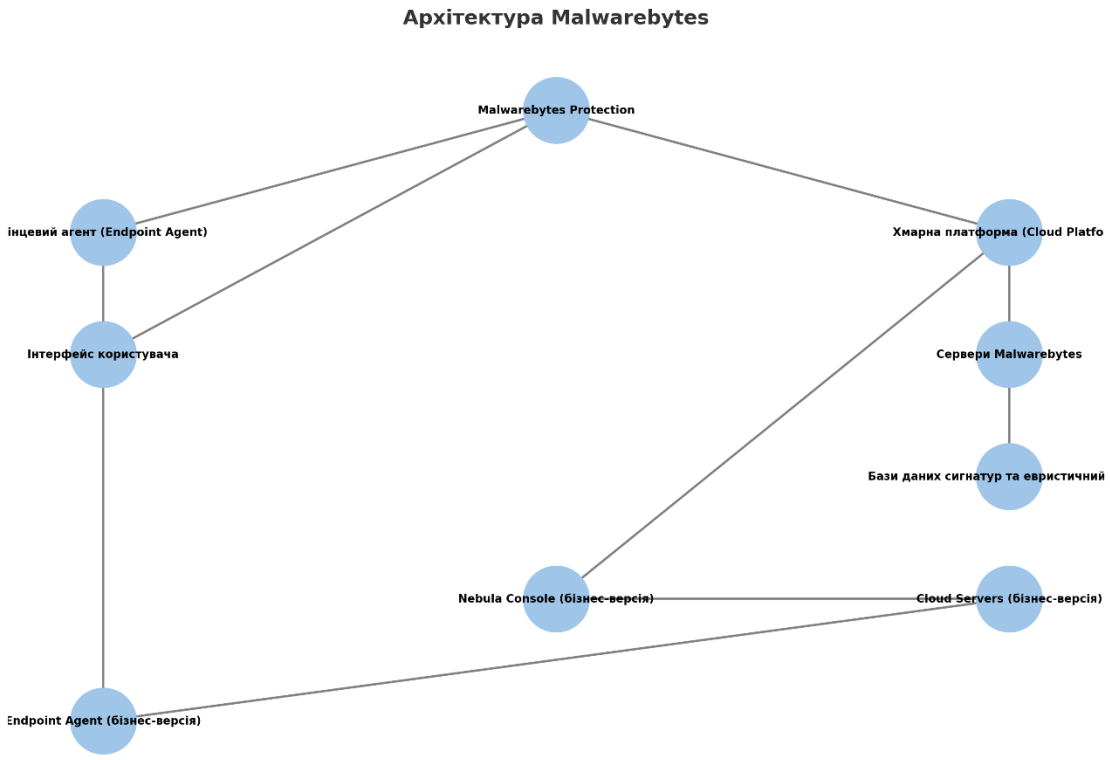

Рис. 2.1. Архітектура Malwarebytes

2.2 Антифішингові механізми в Malwarebytes

Фішинг є однією з найпоширеніших та найефективніших загроз у сфері кібербезпеки. Він базується на соціальній інженерії, що дозволяє зловмисникам обманним шляхом отримати конфіденційні дані користувачів, такі як облікові дані, номери кредитних карток, банківські реквізити тощо. Malwarebytes, як комплексне рішення для захисту, інтегрує низку потужних антифішингових механізмів, які працюють на різних рівнях, щоб виявити та блокувати ці атаки [7][8].

Веб-захист (Web Protection)

Основним компонентом, що забезпечує антифішинговий захист у Malwarebytes, є модуль Веб-захисту (Web Protection) [10]. Цей модуль працює в реальному часі, перехоплюючи та аналізуючи мережевий трафік, коли користувач намагається отримати доступ до веб-сайтів. Його ключові функції включають:

- *Бази даних відомих фішингових ресурсів (Blacklisting/Denylisting):* Malwarebytes підтримує та постійно оновлює величезні бази даних відомих фішингових сайтів, доменів та IP-адрес. Ці дані збираються за допомогою власних досліджень, інформації від спільноти, партнерських джерел та інтеграції з глобальними центрами загроз. При спробі користувача перейти на URL, який знаходиться в цій базі даних, доступ до нього негайно блокується, і користувачеві відображається попередження.
- *Аналіз репутації URL-адрес та доменів (URL/Domain Reputation Analysis):* Навіть якщо сайт ще не потрапив у чорний список, Malwarebytes може оцінювати його репутацію. Це включає аналіз віку домену, реєстраційних даних, пов'язаних IP-адрес, історії змін контенту та зв'язків з іншими відомими шкідливими або підозрілими ресурсами. Низька репутація може стати причиною блокування або попередження.
- *Евристичний та поведінковий аналіз URL-адрес (Heuristic and Behavioral URL Analysis):* Цей механізм виходить за рамки простих баз даних. Він аналізує структуру URL-адреси, наявність підозрілих символів, використання піддоменів, що імітують легітимні домени (typosquatting), та інші аномалії. Наприклад, URL типу paypal.com-login.malicious.xyz буде розпізнаний як підозрілий, оскільки справжній домен – malicious.xyz, а paypal.com-login – це лише піддомен.
- *Виявлення "підмін" (Spoofing Detection):* Веб-захист здатний виявляти спроби підміни адресного рядка браузера або використання схожих за написанням, але не ідентичних символів (IDN homograph attacks).
- *Інтеграція з DNS-фільтрацією (DNS Filtering Integration):* Для корпоративних користувачів, Malwarebytes пропонує рішення DNS-

фільтрації, яке дозволяє блокувати доступ до відомих фішингових сайтів на рівні роздільної здатності доменних імен. Це ефективний спосіб зупинити доступ до шкідливих ресурсів ще до того, як браузер почне завантажувати їхній контент.

- *Аналіз вмісту сторінки (Page Content Analysis - частково):* Хоча основним акцентом є URL-адреси, деякі аспекти аналізу вмісту сторінки також можуть бути використані. Це може включати виявлення елементів, характерних для фішингових сторінок (наприклад, форми для введення облікових даних на підозрілих доменах, невідповідності у візуальному оформленні тощо).

Malwarebytes Browser Guard

Окремим, але тісно пов'язаним компонентом є Malwarebytes Browser Guard — безкоштовне розширення для веб-браузерів (Chrome, Firefox, Edge, Opera) (рисунок 2.2) [11].

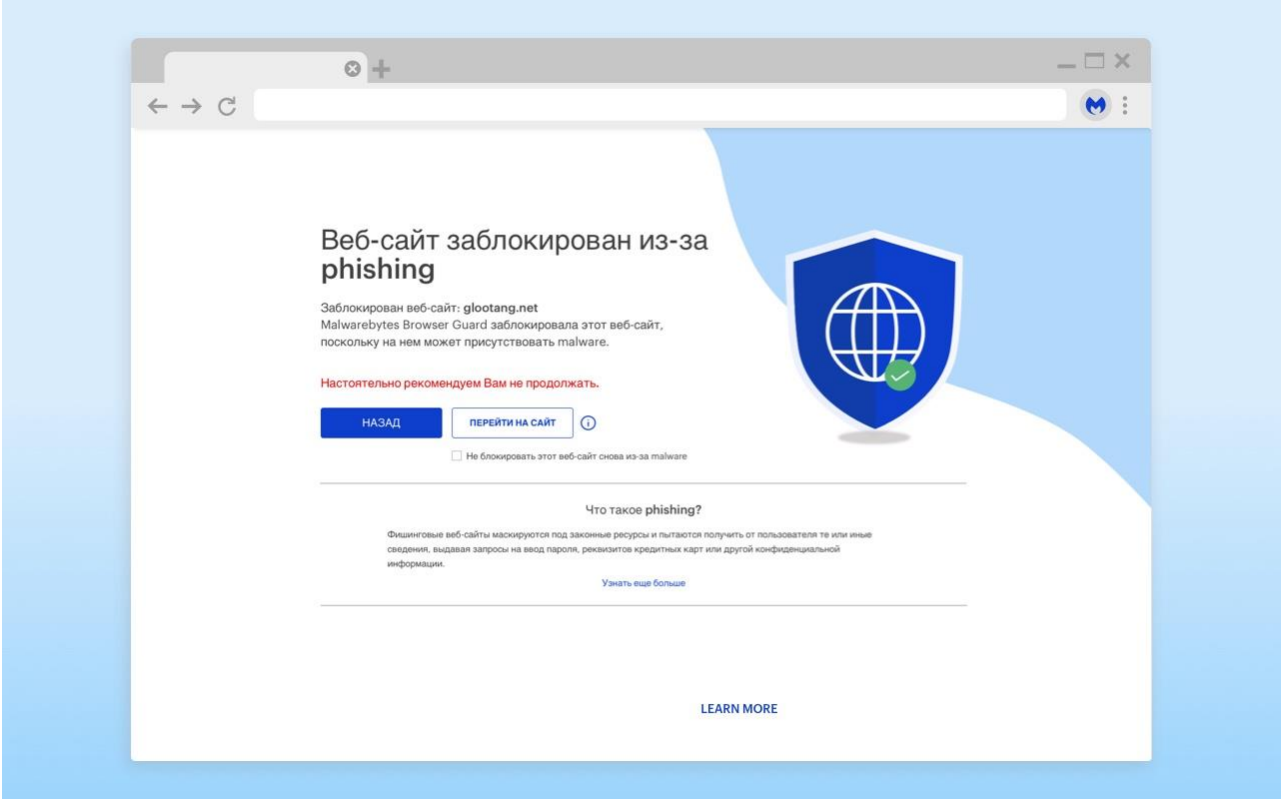

Рис. 2.2 Повідомлення Malwarebytes Browser Guard про блокування веб-сайту через підозру на фішинг

Це розширення надає додатковий рівень захисту безпосередньо в браузері, що є критично важливим для боротьби з фішингом:

- *Блокування фішингових та шахрайських сайтів:* Browser Guard використовує аналогічні бази даних та евристичні алгоритми для блокування доступу до відомих і підозрілих фішингових сайтів, а також до веб-ресурсів, пов'язаних з технічними шахрайствами (tech support scams) та іншими видами онлайн-шахрайства.
- *Захист від перехоплення даних (Credential Harvesting Protection):* Розширення може ідентифікувати сторінки, що намагаються перехопити облікові дані, особливо якщо вони знаходяться на підозрілих доменах, і блокувати такі спроби.
- *Виявлення скамерів (Scam Protection):* Зокрема, Browser Guard відомий своєю здатністю виявляти та блокувати "browser lockers" та інші тактики, що використовуються в технічних шахрайствах, коли зловмисники намагаються заблокувати браузер користувача та вимагати гроші.
- *Блокування реклами та трекерів:* Хоча це не є прямо антифішинговим механізмом, блокування рекламних оголошень та веб-трекерів зменшує поверхню атаки та покращує конфіденційність користувача, знижуючи ризик переходу на шкідливі рекламні ресурси або фішингові сайти через скомпрометовані рекламні мережі.

Машинне навчання та Хмарний інтелект

Ефективність антифішингових механізмів Malwarebytes значно підвищується за рахунок використання машинного навчання (Machine Learning) та хмарного інтелекту (Cloud Threat Intelligence):

- *Аналіз нових загроз:* Алгоритми машинного навчання постійно аналізують нові зразки URL-адрес та поведінку веб-сайтів. Вони здатні виявляти ознаки фішингу, які можуть бути непомітні для людини або не внесені в сигнатурні бази даних. Це дозволяє Malwarebytes швидше реагувати на нові та мутуючі фішингові кампанії.
- *Колективний інтелект:* Хмарна інфраструктура Malwarebytes збирає дані

про загрози від мільйонів користувачів по всьому світу. Якщо один користувач стикається з новою фішинговою атакою, інформація про неї швидко обробляється в хмарі, і захист поширюється на всіх інших користувачів, забезпечуючи майже миттєве реагування на глобальні загрози.

- *Sandbox-аналіз (частково для посилань):* Хоча більш поширений для аналізу файлів, підозрілі URL-адреси можуть бути тимчасово проаналізовані в ізольованому середовищі (sandbox) для визначення їхньої поведінки та виявлення прихованих шкідливих функцій, що може включати перенаправлення на фішингові сторінки.

Взаємодія з іншими компонентами

Антифішингові механізми не працюють ізольовано, а тісно взаємодіють з іншими компонентами Malwarebytes:

- *Захист від шкідливого програмного забезпечення (Malware Protection):* Фішингові атаки часто є першим етапом у ланцюгу зараження ШПЗ. Якщо користувач все ж таки переходить на фішинговий сайт, який намагається доставити шкідливий файл, модуль захисту від ШПЗ перехопить і заблокує його завантаження або виконання.
- *Захист від експлойтів (Exploit Protection):* Деякі фішингові сторінки можуть містити експлойти, спрямовані на вразливості в браузері або інших програмах. Модуль захисту від експлойтів запобігатиме успішному використанню цих вразливостей.

Профілактичні заходи та освіта користувачів

Хоча програмні засоби є критично важливими, Malwarebytes також наголошує на важливості освіти користувачів. На своїх ресурсах компанія надає інформацію та рекомендації щодо розпізнавання фішингових спроб (ознаки підозрілих листів, URL-адрес, запитів). Це підкреслює, що технологічний захист є ефективнішим у поєднанні з підвищеною обізнаністю користувачів.

Антифішингові механізми Malwarebytes являють собою багаторівневу систему, що поєднує реактивні (на основі баз даних) та проактивні (евристичний, поведінковий аналіз, машинне навчання) підходи. Веб-захист та Browser Guard є

основними інструментами, що працюють у синергії для блокування доступу до шахрайських ресурсів. Активне використання хмарних технологій та ШІ дозволяє Malwarebytes адаптуватися до постійно еволюціонуючих тактик фішингу, надаючи надійний захист користувачам від однієї з найбільш підступних та розповсюджених кіберзагроз.

2.3 Практичний аналіз ефективності виявлення фішингу

Практичний аналіз вимагає строгої та відтворюваної методології. Вона включає:

- *Формування Тестової Вибірки Фішингових URL-адрес та Зразків:*
  - Збір актуальних фішингових URL-адрес з відкритих джерел (PhishTank, VirusTotal, звітів CERT) [12] [14].
  - Генерація власних "імітованих" фішингових сторінок для тестування реакції на нові, ще невідомі системи загрози (zero-day phishing).
  - Включення різних типів фішингу: класичний фішинг (імітація банків, платіжних систем), спірфішинг (цільові атаки), клікджекінг, фішинг через QR-коди, SMS-фішинг (смсшинг).
  - Використання як чистих фішингових сторінок, так і таких, що містять шкідливі скрипти або малваре.
- *Налаштування Тестового Середовища:*
  - Віртуальні машини з різними операційними системами (Windows, macOS), на яких встановлено Malwarebytes.
  - Різні браузери (Chrome, Firefox, Edge) для перевірки інтеграції Malwarebytes з ними.
  - Імітація реальних умов мережі (наприклад, підключення через VPN, використання проксі-серверів).
- *Проведення Тестів:*
  - Пасивне тестування: Перевірка здатності Malwarebytes ідентифікувати фішингові URL-адреси до моменту переходу за ними (наприклад,

сканування електронних листів або файлів).

- Активне тестування: Спроба переходу за фішинговими посиланнями та оцінка реакції Malwarebytes (блокування доступу, попередження користувача).
- Тестування з обфускацією та обходом: Використання технік, що застосовуються зловмисниками для обходу захисту (наприклад, використання скорочених URL, вбудовування шкідливих скриптів в зображення, використання доменів з омогліфами).

- *Збір та Аналіз Даних:*
  - Автоматизоване логування результатів кожного тесту.
  - Класифікація виявлених загроз.
  - Фіксація хибних спрацювань.
  - Вимірювання часу реакції системи на нові загрози.

Аналіз Результатів та Ключові Метрики

Оцінка ефективності Malwarebytes включатиме [13] аналіз наступних показників:

1. Рівень Виявлення (Detection Rate)

Ця метрика показує, який відсоток фішингових загроз Malwarebytes успішно ідентифікував та заблокував. Високий показник є критично важливим (рисунок 2.3).

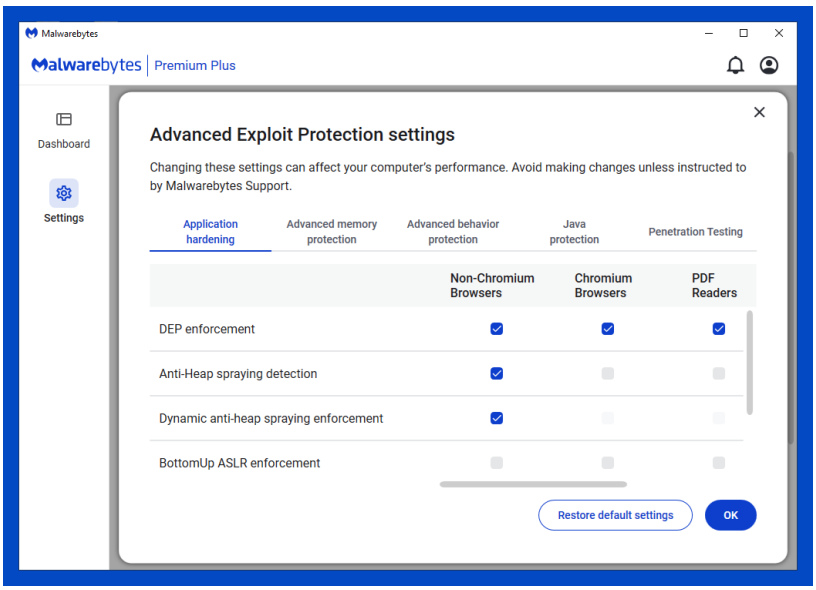

Рис. 2.3 вкладка Advanced Exploit Protection settings

Видно активну вкладку *Application hardening* (Усилення захисту додатків), яка дозволяє керувати захистом від специфічних векторів атак, зокрема:

- *DEP enforcement* (Застосування DEP — Data Execution Prevention) — увімкнено для Non-Chromium, Chromium браузерів та PDF-читалок.
- *Anti-Heap spraying detection* (Виявлення heap spraying-атак) — увімкнено лише для Non-Chromium браузерів.
- *Dynamic anti-heap spraying enforcement* — увімкнено для Non-Chromium браузерів.
- *BottomUp ASLR enforcement* (Примусове застосування ASLR знизу вверх) — неактивне.

Платформи які використовуються:

- Non-Chromium Browsers — альтернативні браузери, не побудовані на Chromium.
- Chromium Browsers — браузери на базі Chromium (наприклад, Chrome, Edge).
- PDF Readers — програми для перегляду PDF.

Також є кнопки *"Restore default settings"* (Відновити типові налаштування) і *"OK"* для збереження налаштувань.

Це частина функціоналу захисту від експлойтів Malwarebytes, що дозволяє зменшити ризики вразливостей в додатках через технології як DEP, ASLR та виявлення heap spraying.

2. Відсоток Хибних Спрацювань (False Positive Rate)

Відсоток хибних спрацювань, або False Positive Rate (FPR), є одним із найкритичніших показників ефективності будь-якої системи кібербезпеки, зокрема тієї, що призначена для виявлення фішингу, як-от Malwarebytes. Хоча основна увага зазвичай приділяється показнику виявлення (скільки загроз було знайдено), FPR не менш важливий, адже він безпосередньо впливає на довіру користувачів, продуктивність роботи та загальну зручність використання системи.

Що таке хибне спрацювання?

У контексті виявлення фішингу, хибне спрацювання відбувається, коли Malwarebytes (або будь-яка інша система захисту) помилково ідентифікує легітимний, безпечний ресурс або дію як фішингову загрозу. Наприклад:

- Блокування доступу до офіційного сайту банку, який насправді є безпечним.
- Позначення законного електронного листа з важливим документом як фішингового.
- Видача попередження про підозрілу активність при спробі завантажити оновлення для легітимного програмного забезпечення.

Чому високий FPR є проблемою?

Високий відсоток хибних спрацювань може призвести до низки негативних наслідків:

1. *Підрив Довіри Користувачів***:** Якщо система постійно "кричить вовк", коли вовка немає, користувачі з часом перестають реагувати на попередження. Вони можуть почати ігнорувати повідомлення безпеки, що підвищує ризик пропустити реальну загрозу.
2. *Роздратування та Зниження Продуктивності:* Користувачі змушені витрачати час на перевірку, чи справді загроза існує, звертатися до IT-відділу, або шукати обхідні шляхи для доступу до необхідних ресурсів. Це призводить до марної трати часу та зниження продуктивності роботи.
3. *Негативний Досвід Користувача:* Постійні переривання та блокування законних дій роблять використання системи незручним і фруструючим.
4. *Збільшення Навантаження на IT-Відділ:* Кожен випадок хибного

спрацювання може вимагати ручної перевірки, внесення винятків або усунення проблем з боку IT-персоналу. Це відволікає ресурси від більш критичних завдань.

5. *Ризик Створення "Білих Списків" для Небезпечних Об'єктів:* У спробі зменшити кількість хибних спрацювань, адміністратори можуть надмірно агресивно додавати винятки (whitelisting) для ресурсів, які спочатку були ідентифіковані як FP. Якщо такий ресурс виявиться скомпрометованим або згодом стане розповсюджувачем шкідливого ПЗ, це створить "дірку" в захисті.

Як Malwarebytes мінімізує FPR?

Для мінімізації хибних спрацювань, Malwarebytes (і провідні рішення безпеки) використовують комбінацію складних методів:

- *Багатошаровий Аналіз:* Не покладаються лише на одну технологію. Фішинг-сайти аналізуються за багатьма параметрами:
    - *Репутація URL/Домену:* Перевірка, чи не пов'язаний домен або IP-адреса з попередніми шкідливими діями.
    - *Аналіз Вмісту Сторінки:* Пошук характерних ознак фішингу (логотипи відомих брендів, форми для введення облікових даних, підозрілі редиректи, наявність iframe).
    - *Машинне Навчання та Штучний Інтелект:* Алгоритми навчаються на величезних обсягах даних (як шкідливих, так і легітимних) для виявлення патернів, які вказують на фішинг. Це дозволяє ідентифікувати нові загрози з високою точністю.
    - *Евристичний Аналіз:* Пошук поведінкових ознак, які можуть вказувати на шахрайство, навіть якщо конкретний URL не входить до відомих баз.
    - *Аналіз Сертифікатів та Хостингу:* Перевірка легітимності SSL-сертифікатів, даних про реєстратора домену, географічного розташування сервера.

- *Хмарні Технології та Колективний Інтелект:* Використання хмарної інфраструктури дозволяє Malwarebytes збирати та аналізувати дані про загрози від мільйонів користувачів по всьому світу в реальному часі. Це створює "колективний імунітет", що допомагає швидко ідентифікувати та класифікувати нові загрози, зменшуючи ймовірність помилкових спрацювань на легітимних ресурсах.
- *Регулярні Оновлення Баз Даних:* Постійне оновлення баз даних з відомими фішинговими URL-адресами та сигнатурами.
- *Механізми Зворотного Зв'язку:* Можливість для користувачів повідомляти про хибні спрацювання або пропущені загрози, що дозволяє розробникам швидко коригувати алгоритми.

3. Час Реакції на Нові Загрози (Zero-day Threat Response Time):

Показник "Час Реакції на Нові Загрози", часто званий "Zero-day Threat Response Time", є одним з найважливіших індикаторів ефективності будь-якого рішення кібербезпеки. У контексті фішингу, цей показник відображає, як швидко Malwarebytes здатний ідентифікувати та почати блокувати фішингові атаки, які є абсолютно новими, раніше невідомими та ще не занесені до традиційних баз даних сигнатур. Такі атаки називаються "атаками нульового дня" (zero-day attacks).

Чому Час Реакції на Zero-day Фішинг є Критичним?

Постійна Еволюція Фішингу: Зловмисники постійно створюють нові фішингові сайти та методи обходу захисту. Кожен новий фішинговий ресурс є "нульовим днем" до того моменту, поки він не буде виявлений та внесений до баз даних безпеки.

Швидкість Розповсюдження: Фішингові кампанії можуть розповсюджуватися надзвичайно швидко. Протягом лічених годин тисячі користувачів можуть отримати шкідливі посилання. Кожна хвилина затримки у виявленні дозволяє зловмисникам зібрати більше облікових даних або встановити шкідливе програмне забезпечення.

Висока Ціна Пропущених Атак: Пропуск навіть однієї успішної фішингової атаки може призвести до:

- *Компрометації облікових даних:* Крадіжка логінів і паролів до банківських систем, корпоративних акаунтів, соціальних мереж.
- *Фінансових збитків:* Прямі перекази коштів, несанкціоновані покупки.
- *Встановлення шкідливого ПЗ:* Зараження пристроїв вірусами, програмами-вимагачами (ransomware), шпигунським ПЗ.
- *Втрати репутації:* Особливо для організацій, які стають жертвами фішингу, що призводить до публічного розголосу та втрати довіри клієнтів.

Як Malwarebytes Досягає Швидкої Реакції на Zero-day Загрози?

Malwarebytes використовує комбінацію передових технологій для мінімізації часу реакції на нові фішингові загрози:

Поведінковий Аналіз (Behavioral Analysis): Замість того, щоб покладатися лише на сигнатури відомих загроз, Malwarebytes аналізує поведінку веб-сторінок та процесів у реальному часі. Якщо сторінка намагається імітувати логін відомого сервісу, запитує конфіденційну інформацію незвичайним чином, або містить підозрілі скрипти, які намагаються обійти захист – це може бути маркером фішингу, навіть якщо сам URL ще не відомий.

Евристичний Аналіз: Цей метод використовує набір правил та шаблонів для виявлення підозрілих характеристик, які часто присутні у фішингових атаках (наприклад, використання доменних імен з омогліфами, специфічні редиректи, схожість з відомими брендами).

Машинне Навчання (Machine Learning) та Штучний Інтелект (AI): Це наріжний камінь у боротьбі з zero-day загрозами. Моделі машинного навчання тренуються на величезних обсягах даних (як легітимних, так і шкідливих) для виявлення складних патернів, які людському оку не помітні. Це дозволяє ідентифікувати нові фішингові схеми на основі їхньої схожості з відомими атаками, навіть якщо вони мають певні модифікації.

Хмарні обчислення та колективний інтелект: Коли один користувач Malwarebytes стикається з новою фішинговою загрозою, інформація про неї швидко надсилається до хмарних сервісів Malwarebytes для аналізу. Якщо загроза підтверджується, її ідентифікатор миттєво розповсюджується на всіх інших користувачів у мережі, забезпечуючи захист у режимі реального часу.

Аналіз Репутації (Reputation Analysis): Malwarebytes підтримує величезні бази даних репутації IP-адрес, доменів та URL-адрес. Якщо новий домен або IP-адреса, що використовується для фішингу, раніше був помічений у підозрілій активності або має низьку репутацію, це може призвести до його блокування.

Санкпінг (Sandboxing): Для особливо підозрілих або невідомих веб-сторінок, Malwarebytes може використовувати ізольоване середовище (пісочницю) для їхнього аналізу. Це дозволяє безпечно запустити та спостерігати за поведінкою сторінки, виявляючи шкідливі дії, не наражаючи пристрій користувача на ризик.

4. Глибина Аналізу (Depth of Analysis)

Чи обмежується система лише перевіркою URL-адреси, чи проводить також аналіз вмісту сторінки, поведінки скриптів тощо.

4. Зручність Використання та Повідомлення для Користувача:

Оцінка ефективності будь-якого рішення з кібербезпеки не обмежується суто технічними показниками, такими як рівень виявлення або час реакції. *Зручність використання (Usability) та якість повідомлень для користувача (User Notifications)* є не менш, а іноді й більш важливими факторами, що визначають, наскільки ефективно система буде працювати в реальних умовах, особливо у боротьбі з такою загрозою, як фішинг, де людський фактор відіграє ключову роль.

Чому Зручність Використання та Повідомлення для Користувача є Критичними?

1. *Людський Фактор як Остання Лінія Захисту:* У боротьбі з фішингом, навіть найдосконаліші технічні рішення можуть бути обійдені, якщо користувач не розуміє попереджень або не знає, як правильно реагувати. Ясні та зрозумілі

повідомлення можуть стати останньою перешкодою між користувачем та фішинговою атакою.

2. *Довіра до Системи:* Якщо система занадто складна у використанні, її налаштування неінтуїтивні, або її повідомлення незрозумілі/дратуючі, користувачі (або навіть IT-адміністратори) можуть почати ігнорувати її, відключати певні функції або навіть повністю деінсталювати.
3. *Зниження Опору Зловмисникам:* Добре розроблений інтерфейс та повідомлення підвищують "кіберграмотність" користувачів, навчаючи їх розпізнавати загрози та реагувати на них належним чином.
4. *Ефективність Адміністрування:* Для IT-адміністраторів зручність Cloud Console (ThreatDown Nebula Console) є ключовою для ефективного моніторингу, управління політиками, розгортання та реагування на інциденти.

Аспекти Аналізу Зручності Використання:

1. *Інсталяція та Розгортання (Installation & Deployment):*
    - Наскільки легко встановити агент Malwarebytes на кінцеві точки?
    - Чи є зрозумілі інструкції та чи доступні автоматизовані методи розгортання (наприклад, через групові політики, інтеграція з RMM-системами)?
    - Наскільки процес розгортання є "непомітним" для кінцевого користувача?
2. *Налаштування та Управління Політиками (Configuration & Policy Management):*
    - Чи є інтерфейс Malwarebytes Cloud Console інтуїтивно зрозумілим для налаштування політик захисту від фішингу?
    - Чи легко створювати винятки (exclusions) для легітимних ресурсів (наприклад, внутрішніх сайтів, які можуть бути помилково позначені)?
    - Чи є можливість гнучко налаштовувати рівні чутливості виявлення?
3. *Моніторинг та Звітність (Monitoring & Reporting):*

- Наскільки зручними та інформативними є дашборди у Cloud Console, що відображають стан захисту від фішингу?
- Чи легко знайти інформацію про виявлені фішингові атаки, їхні джерела, та уражені пристрої?
- Чи доступні зрозумілі та настроювані звіти про фішинг-інциденти?

4. *Реакція на Інциденти (Incident Response):*
    - Наскільки легко адміністратору реагувати на фішингові інциденти через консоль (наприклад, ізолювати заражений пристрій, примусово оновити бази даних, виконати сканування)?

Аспекти Аналізу Повідомлень для Користувача:

1. *Ясність та Зрозумілість (Clarity & Understandability):*
    - Чи повідомлення про виявлений фішинг є чіткими та однозначними?
    - Чи вказано, що саме було заблоковано (URL-адреса, файл, процес) і чому (наприклад, "Підозрілий фішинговий сайт", "Виявлено спробу крадіжки даних")?
    - Чи використовується мова, зрозуміла для пересічного користувача, без надмірної технічної термінології?
2. *Інформативність та Рекомендації (Informativeness & Recommendations):*
    - Чи містять повідомлення корисну інформацію про природу загрози (наприклад, "Цей сайт імітує сторінку банку X")?
    - Чи пропонуються чіткі рекомендації щодо подальших дій ("Не вводьте свої дані", "Закрийте цю вкладку", "Повідомте адміністратора")?
    - Чи є можливість для користувача, який вважає попередження хибним, легко повідомити про це (наприклад, кнопка "Це безпечний сайт")?
3. *Ненав'язливість та Частота (Non-Intrusiveness & Frequency):*
    - Наскільки часто з'являються попередження? Чи не є вони надмірними або дратівливими, якщо система має високий відсоток хибних спрацювань?
    - Чи дизайн повідомлень мінімально перериває робочий процес, але при цьому ефективно привертає увагу?

- Чи є можливість налаштовувати рівень деталізації повідомлень?

4. *Візуальне Оформлення (Visual Presentation):*
    - Чи повідомлення виглядають професійно та не викликають сумнівів у їхній легітимності?
    - Чи використовуються чіткі візуальні індикатори (кольори, іконки) для розрізнення критичності загрози?

Як Оцінювати Зручність та Повідомлення в Дипломній Роботі:

1. *Користувацькі Сценарії:* Проведіть тестування, імітуючи типові сценарії взаємодії користувача з фішинговою загрозою.
    - Перехід за фішинговим посиланням.
    - Відкриття фішингового вкладення.
    - Оцінка реакції системи та повідомлень.
2. *Експертна Оцінка (Heuristic Evaluation):* Самостійно оцініть інтерфейс та повідомлення за загальноприйнятими принципами дизайну користувацького досвіду (UX) та зручності (Usability Heuristics).
3. *Користувацьке Тестування (User Testing – за можливості):* Якщо можливо, залучіть кількох "звичайних" користувачів (які не є експертами з кібербезпеки) для взаємодії з системою та отримання їхніх відгуків про зрозумілість та зручність.
4. *Аналіз Документації:* Оцініть якість офіційної документації Malwarebytes щодо налаштування та використання функцій захисту від фішингу.
5. *Порівняльний Аналіз:* Порівняйте підхід Malwarebytes до повідомлень з іншими рішеннями кібербезпеки.

Значення Результатів Аналізу:

- Високий рівень зручності та якісні повідомлення вказуватимуть на те, що Malwarebytes не лише технічно здатний виявляти фішинг, а й робить це таким чином, щоб максимально сприяти захисту кінцевих користувачів та ефективному адмініструванню системи безпеки.
- Виявлені недоліки в цих аспектах можуть стати основою для важливих рекомендацій розробникам Malwarebytes щодо покращення UX/UI та

комунікації із користувачами, що в кінцевому підсумку підвищить загальну ефективність боротьби з фішингом.

Цей аспект дослідження дозволяє поглянути на ефективність Malwarebytes не лише з технічної точки зору, а й з позиції реального використання, що є надзвичайно цінним для повноцінної оцінки.

3 РОЗРОБКА ТА РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ АНТИФІШИНГОВИХ ЗАХОДІВ В ОРГАНІЗАЦІЇ

3.1 Модель впровадження Malwarebytes у локальну ІС організації

Впровадження сучасної системи захисту кінцевих точок, такої як Malwarebytes, в локальну інформаційну систему організації є критично важливим етапом для забезпечення її кібербезпеки [1]. Хоча Malwarebytes пропонує переважно хмарну модель управління (ThreatDown Nebula Console), сам процес впровадження завжди передбачає тісну інтеграцію з існуючою локальною інфраструктурою та процесами організації. Ця модель зосереджена на ефективному розгортанні агентів захисту на локальних пристроях та їх централізованому управлінні через хмарну платформу [15].

Ключові Принципи Моделі Впровадження:

"Агент-Хмара" Архітектура: Це фундаментальний принцип. На кожній кінцевій точці в локальній ІС (настільні ПК, ноутбуки, сервери) встановлюється легкий агент Malwarebytes. Цей агент відповідає за захист пристрою на місці та комунікацію з централізованою хмарною консоллю Malwarebytes (ThreatDown Nebula Console)(рисунок 1.1).

Рис. 3.1. Архітектура захисту «Агент–хмара» в системі Malwarebytes

Централізоване Хмарне Управління: Уся конфігурація, моніторинг, розгортання політик, звітність та керування інцидентами відбувається через веб-інтерфейс хмарної консолі. Це усуває потребу в локальних серверах управління та суттєво спрощує адміністрування (рисунок 3.2).

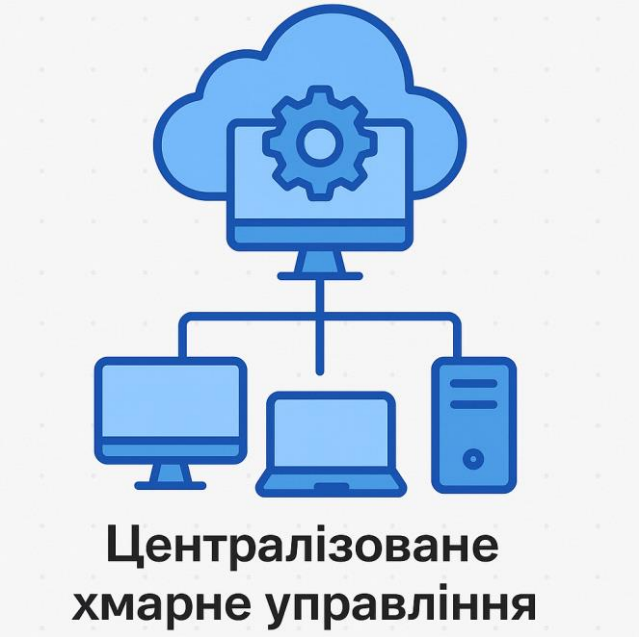

Рис. 3.2. Централізоване хмарне управління в архітектурі Malwarebytes

Інтеграція з Існуючою Інфраструктурою: Незважаючи на хмарне управління, успішне впровадження вимагає взаємодії з наявними локальними сервісами та інструментами організації (рисунок 3.3).

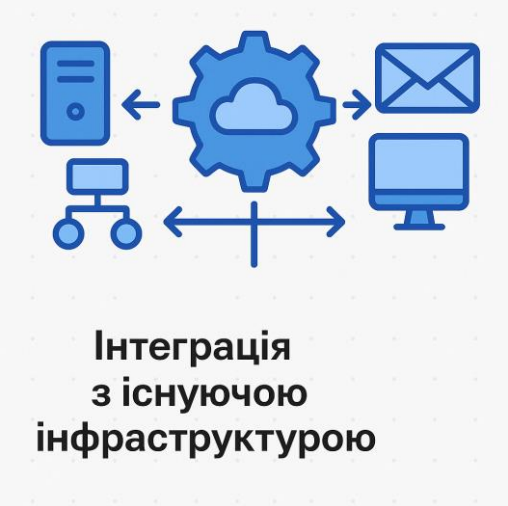

Рис. 3.3. Інтеграція з існуючою інфраструктурою

Етапи Впровадження Malwarebytes у Локальну ІС:

1. Підготовка та Планування:

- *Оцінка Потреб та Вимог:* Визначення кількості кінцевих точок, типів операційних систем, специфічних вимог до захисту (наприклад, HIPAA, GDPR), існуючих рішень безпеки, з якими потрібна інтеграція.
- *Вибір Ліцензії:* Вибір відповідного продукту Malwarebytes (Endpoint Protection, EDR, Incident Response) та моделі ліцензування.
- *Підготовка Мережі:* Забезпечення необхідного мережевого доступу для агентів до хмарних сервісів Malwarebytes (відкриття портів, налаштування проксі-серверів, якщо необхідно). Переконайтеся, що брандмауери та мережеві пристрої дозволяють вихідні з'єднання агентам до серверів Malwarebytes.
- *Планування Групової Структури (Організаційні Одиниці/Groups):* Визначення, як кінцеві точки будуть організовані в консолі (за відділами, географією, типом пристрою тощо) для застосування відповідних політик.

2. Налаштування Хмарної Консолі (ThreatDown Nebula Console):

- *Початкове Налаштування Облікового Запису:* Створення облікового запису в Malwarebytes Cloud Console.
- *Конфігурація Політик Безпеки:* Це один з найважливіших етапів. Налаштування детальних політик для різних груп кінцевих точок, що включають:
    - *Захист від фішингу:* Активація та налаштування веб-захисту, аналізу URL-адрес.
    - *Захист від шкідливого ПЗ, програм-вимагачів, експлойтів.*
    - *Графіки сканувань.*
    - *Налаштування оновлень.*
    - *Винятки (Exclusions):* Додавання винятків для внутрішніх, довірених додатків або ресурсів, щоб уникнути хибних спрацювань. Це має бути зроблено обережно.

- *Налаштування Сповіщень та Звітів:* Визначення, хто отримуватиме сповіщення про інциденти та які звіти будуть генеруватися.
- *Інтеграція з SIEM/SOC (опціонально):* Налаштування пересилання журналів подій (logs) з Malwarebytes Cloud Console до локальної системи управління інформаційною безпекою та подіями (SIEM) або центру операцій безпеки (SOC) для централізованого аналізу та кореляції даних.

3. Розгортання Агентів на Кінцевих Точках:

Цей етап є найбільш "локальним" у процесі впровадження:

- *Автоматизоване Розгортання (Рекомендовано для організацій):*
  - *Через Групові Політики (GPO) Active Directory:* Для Windows-орієнтованих мереж. Це дозволяє автоматично встановлювати агент на всі комп'ютери, що входять до певних груп AD.
  - *Через Системи Управління Конфігураціями (SCCM, Intune, PDQ Deploy тощо):* Використання існуючих інструментів для централізованого розгортання програмного забезпечення.
  - *За допомогою Discovery & Deployment Tool від Malwarebytes:* Інструмент, що дозволяє виявляти кінцеві точки в мережі та автоматично розгортати на них агенти.
- *Ручне Розгортання:* Для невеликих організацій або окремих пристроїв. Адміністратор завантажує інсталяційний пакет з Cloud Console та встановлює його на кожний пристрій вручну.
- *Автоматичне Призначення Групам:* Під час розгортання можна вказати ідентифікатор групи, щоб нові кінцеві точки автоматично призначалися до потрібних груп з відповідними політиками.

4. Моніторинг та Супровід:

- *Моніторинг Дашбордів Консолі:* Постійний перегляд дашбордів ThreatDown Nebula Console для відстеження стану безпеки, виявлених загроз та інцидентів.
- *Аналіз Звітів:* Регулярний перегляд та аналіз звітів про безпеку, щоб виявляти тенденції та проблемні області.

- *Реагування на Інциденти:* Використання функціоналу консолі для локалізації та усунення виявлених загроз на кінцевих точках (карантин, видалення, ізоляція пристрою).
- *Оновлення Політик:* Коригування політик безпеки відповідно до нових загроз або зміни потреб організації.
- *Оновлення Агентів:* Агенти оновлюються автоматично через хмарну консоль, забезпечуючи завжди актуальний захист.

Переваги такої Моделі Впровадження для Локальної ІС:

- *Спрощене Адміністрування:* Відсутність потреби у підтримці локальних серверів управління.
- *Швидкість Розгортання:* Особливо для великих мереж, автоматизовані методи значно прискорюють процес.
- *Масштабованість:* Легке розширення захисту на нові пристрої без додаткових інвестицій в інфраструктуру.
- *Централізована Видимість***:** Повний огляд стану безпеки всіх кінцевих точок з єдиної точки доступу.
- *Актуальний Захист:* Автоматичні оновлення сигнатур та програмного забезпечення агента забезпечують захист від найновіших загроз.

Потенційні Виклики та Їх Вирішення:

- *Мережеві Обмеження***:** У деяких організаціях можуть бути суворі мережеві політики, що вимагатимуть ретельного налаштування брандмауерів або проксі-серверів для забезпечення зв'язку між агентами та хмарною консоллю.
- *Синхронізація з AD/LDAP:* Хоча є інструменти для імпорту з Active Directory, підтримка постійної синхронізації груп та користувачів може вимагати певних налаштувань.
- *Пропускна Здатність Каналу:* Для великих мереж або під час початкового розгортання агентів, може знадобитися врахування пропускної здатності інтернет-каналу.

Ця модель впровадження дозволяє організаціям максимально використовувати переваги хмарної платформи Malwarebytes, одночасно

інтегруючи її з їхньою існуючою локальною ІС для досягнення ефективного та централізованого управління кібербезпекою.

3.2 Порядок моніторингу та реагування на фішингові інциденти

Ефективний моніторинг та оперативне реагування на фішингові інциденти є критично важливими для мінімізації збитків та захисту конфіденційних даних організації [1]. Цей порядок дій поєднує проактивні заходи моніторингу з чіткими кроками реагування.

І. Етап Моніторингу Фішингових Загроз

Моніторинг є безперервним процесом, що дозволяє виявляти фішингові атаки на ранніх стадіях або навіть до їхнього фактичного впливу на кінцеві точки [13].

1. Централізований Моніторинг через Malwarebytes Cloud Console (ThreatDown Nebula Console):

- *Дашборди та Оповіщення:* Адміністратори безпеки постійно відстежують ключові показники на інформаційних панелях (дашбордах) Nebula Console. Особлива увага приділяється секціям, що відображають:
  - *"Top Detections by Type":* Аналіз, чи є збільшення виявлень, пов'язаних з "Web Protection" (захист від шкідливих та фішингових сайтів) або "Malware" (якщо фішинг намагається доставити шкідливе ПЗ).
  - *"Threats Over Time":* Графіки, що показують динаміку виявлень фішингу.
  - *"Affected Endpoints":* Перелік пристроїв, на яких були зафіксовані спроби доступу до фішингових ресурсів.
- *Налаштування Сповіщень:* Конфігурування автоматичних сповіщень (на пошту, в SIEM-систему) про:
  - Виявлення фішингових сайтів на кінцевих точках.
  - Спроби користувачів перейти за підозрілими посиланнями.
  - Блокування шкідливих вкладень з електронних листів.

- *Деталізація Детекцій:* Перегляд детальної інформації про кожне виявлення: URL-адреса, IP-адреса, дата/час, користувач/пристрій, тип загрози.

2. Моніторинг Електронної Пошти (Gateway/Cloud Email Security):

- *Фільтрація на рівні шлюзу:* Системи безпеки електронної пошти (наприклад, Microsoft 365 Defender, Google Workspace Security, спеціалізовані рішення) є першою лінією захисту. Вони моніторять вхідні листи на наявність ознак фішингу (підозрілі заголовки, невідповідність відправника, підозрілі посилання, шкідливі вкладення) і блокують їх до того, як вони досягнуть поштових скриньок користувачів.
- *Звіти про карантин:* Регулярний перегляд звітів про листи, поміщені в карантин, для ідентифікації потенційних фішингових кампаній.

3. Моніторинг Мережевого Трафіку (Firewalls, IDS/IPS, Proxy Servers):

- *Аналіз логів:* Перегляд журналів мережевих пристроїв на наявність спроб доступу до відомих або підозрілих фішингових доменів/IP-адрес.
- *Виявлення аномалій:* Відстеження незвичайного мережевого трафіку, що може вказувати на компрометацію або спробу фішингу (наприклад, звернення до невідомих зовнішніх ресурсів після натискання на посилання).

4. Зворотний Зв'язок від Користувачів:

- *"Кнопка Фішинг":* Запровадження інструментів (наприклад, плагінів для поштових клієнтів), що дозволяють користувачам легко повідомляти про підозрілі електронні листи безпосередньо до IT-відділу або команди безпеки. Це один з найефективніших методів виявлення нових, таргетованих атак.
- *Навчання користувачів:* Регулярні тренінги з кібергігієни, що вчать розпізнавати ознаки фішингу та важливості повідомляти про підозрілі листи/посилання.

II. Етап Реагування на Фішингові Інциденти

Реагування на фішингові інциденти – це послідовний процес, спрямований на мінімізацію шкоди, усунення загрози та відновлення нормального функціонування.

1. Початкове Виявлення та Підтвердження (Detection & Confirmation):

- *Система безпеки спрацювала:* Malwarebytes Cloud Console [13] реєструє блокування фішингового сайту/файлу, надсилає сповіщення.
- *Повідомлення від користувача*: Користувач повідомляє про підозрілий лист або посилання.
- *Ручна перевірка:* Команда безпеки перевіряє підозрілий URL або електронний лист за допомогою онлайн-інструментів (VirusTotal, PhishTank) або у спеціально ізольованому середовищі (пісочниці). Підтвердження, що це дійсно фішинг.

2. Локалізація та Ізоляція (Containment):

- *Блокування доступу:*
  - *Через Malwarebytes:* Переконатися, що Malwarebytes успішно заблокував доступ до фішингового сайту на всіх кінцевих точках. Якщо ні, то за допомогою Malwarebytes Cloud Console примусово оновити політики та, за необхідності, виконати сканування на заражених пристроях.
  - *На мережевому рівні:* Додати фішинговий URL/IP-адресу до чорних списків (blacklist) на корпоративному брандмауері, проксі-сервері або DNS-фільтрі, щоб запобігти подальшому доступу.
  - *На поштовому шлюзі:* Додати параметри фішингового листа (відправник, тема, посилання) до чорних списків поштового шлюзу.
- *Ізоляція скомпрометованих пристроїв:* Якщо є підозра, що користувач ввів облікові дані або був заражений шкідливим ПЗ після фішингової атаки, негайно ізолювати відповідну кінцеву точку від мережі через Malwarebytes Cloud Console (якщо функціонал EDR дозволяє) або вручну.

3. Усунення Загрози (Eradication):

- *Видалення шкідливих файлів:* Якщо фішинг призвів до завантаження або встановлення шкідливого ПЗ, Malwarebytes автоматично або за командою з Cloud Console видаляє його [13].
- *Скидання облікових даних:* Якщо фішингова атака була успішною і користувач ввів свої дані, негайно скинути паролі для всіх скомпрометованих

облікових записів (корпоративних, банківських, особистих), а також увімкнути багатофакторну автентифікацію (MFA), якщо вона не була активна.

- *Пошук додаткової компрометації (Threat Hunting):* Використання інструментів EDR в Malwarebytes Cloud Console для пошуку інших ознак компрометації на ураженому пристрої або в мережі (наприклад, незвичайні процеси, нові мережеві з'єднання).

4. Відновлення (Recovery):

- *Перевірка та відновлення пристрою:* Після усунення загрози, виконати повне сканування пристрою Malwarebytes для підтвердження чистоти. За потреби, відновити систему з бекапу [1].
- *Відновлення доступу:* Після перевірки та очищення, відновити доступ пристрою до мережі.
- *Інформування користувача:* Надати користувачеві чіткі інструкції та додаткові рекомендації.

5. Аналіз Інциденту та Уроки (Post-Incident Analysis & Lessons Learned):

- *Збір даних:* Зібрати всі доступні дані про інцидент з Malwarebytes Cloud Console, журналів поштового шлюзу, мережевих пристроїв [13].
- *Аналіз кореневої причини:* Визначити, як саме фішингова атака обійшла захист (наприклад, новітній тип фішингу, людська помилка).
- *Оновлення політик:* Внести зміни до політик безпеки Malwarebytes, правил брандмауерів або поштових фільтрів, щоб запобігти подібним інцидентам у майбутньому.
- *Додаткове навчання:* Провести повторний інструктаж або тренінг для користувачів, акцентуючи увагу на виявленому типі фішингу.
- *Документування:* Задокументувати весь інцидент, включаючи його хід, вжиті заходи та висновки для майбутнього використання.

Цей комплексний підхід до моніторингу та реагування, інтегрований з потужними можливостями Malwarebytes Cloud Console, дозволяє організації

ефективно протистояти фішинговим загрозам, мінімізувати їх вплив та постійно покращувати свій рівень кібербезпеки.

3.3 Рекомендації з удосконалення захисту від фішингу

Ефективний захист від фішингу вимагає багатошарового підходу, який поєднує технологічні рішення, організаційні заходи та постійне навчання персоналу. На основі аналізу можливостей Malwarebytes [3] та загальних принципів кібербезпеки, пропонуємо наступні рекомендації для удосконалення захисту:

І. Технологічні Удосконалення (Використання Malwarebytes та Інших Інструментів):

1. *Максимальне Використання Можливостей Malwarebytes (ThreatDown Nebula Console):*
    - *Активація Всіх Модулів Захисту:* Переконайтеся, що на всіх кінцевих точках увімкнені та коректно налаштовані всі релевантні модулі захисту Malwarebytes, включаючи:
        - *Web Protection:* Це безпосередньо стосується блокування фішингових сайтів та шкідливих URL-адрес.
        - *Anti-Exploit:* Для захисту від експлойтів, які можуть використовуватися для доставки шкідливого ПЗ через фішингові посилання.
        - *Anti-Malware та Anti-Ransomware:* Для запобігання встановленню шкідливого ПЗ, якщо фішинг призводить до завантаження файлів.
        - *Behavioral Protection:* Для виявлення аномальної поведінки, характерної для фішингових скриптів або шкідливого ПЗ.
    - *Оптимізація Політик Безпеки:*
        - Регулярно переглядайте та оновлюйте політики в Nebula Console [13].

        - Розгляньте створення більш суворих політик для груп підвищеного ризику (наприклад, керівництво, фінансовий відділ).
        - Забезпечте своєчасне оновлення сигнатур та компонентів агента Malwarebytes.
    - *Використання EDR-функціоналу (якщо доступно):* Якщо організація використовує Malwarebytes Endpoint Detection and Response (EDR), активно застосовуйте його для:
        - *Threat Hunting:* Проактивний пошук прихованих загроз, які могли обійти первинні фільтри.
        - *Глибокий Аналіз Інцидентів:* Розширений аналіз ланцюжка атаки після виявлення фішингового інциденту.
        - *Автоматизоване Реагування:* Налаштування автоматичних дій (наприклад, ізоляція пристрою) при виявленні певних індикаторів фішингу.
2. *Посилення Захисту на Рівні Електронної Пошти:*
    - *Впровадження Потужного Шлюзу Безпеки Електронної Пошти (Email Security Gateway):* Використання спеціалізованих хмарних або локальних рішень (наприклад, Barracuda, Proofpoint, Mimecast, розширені функції Microsoft 365 Defender/Google Workspace Security), які надають:
        - Розширену фільтрацію спаму та фішингу з використанням AI/ML.
        - Аналіз посилань у реальному часі (URL rewriting and sandboxing).
        - Захист від спуфінгу доменів (DMARC, SPF, DKIM).
        - Виявлення компрометації ділової пошти (Business Email Compromise - BEC).
    - *Захист від Вкладень:* Використання "пісочниць" (sandboxing) для автоматичного аналізу підозрілих вкладень перед їхньою доставкою.
    - *Системи Повідомлень про Фішинг:* Запровадження інструментів

("Report Phishing" button) для поштових клієнтів, які дозволяють користувачам в один клік повідомляти про підозрілі листи. Це забезпечує швидке виявлення нових атак.

3. *Мережевий Захист та Фільтрація Контенту:*
    - *DNS-фільтрація:* Використання DNS-сервісів (наприклад, Cisco Umbrella, Cloudflare for Teams) для блокування доступу до відомих шкідливих та фішингових доменів на рівні DNS.
    - *Web Application Firewall (WAF):* Захист зовнішніх веб-додатків організації від атак, які можуть використовувати фішинг для доступу до внутрішніх ресурсів.
    - *Сегментація Мережі:* Розділення мережі на менші, ізольовані сегменти, щоб у разі успішної фішингової атаки обмежити її поширення.
4. *Управління Ідентифікацією та Доступом (IAM):*
    - *Багатофакторна Автентифікація (MFA/2FA):* Запровадження MFA для всіх критично важливих систем (корпоративна пошта, CRM, ERP, хмарні сервіси). Це значно ускладнює успіх фішингової атаки, навіть якщо зловмисники отримали облікові дані.
    - *Single Sign-On (SSO):* Спрощує доступ користувачів, але вимагає посиленого захисту самого SSO-провайдера.
    - *Регулярний Перегляд Прав Доступу:* Застосування принципу найменших привілеїв, що обмежує потенційну шкоду від компрометації облікового запису.

II. Організаційні Заходи та Процеси:

1. *Впровадження Комплексного Плану Реагування на Інциденти:*
    - Чітко визначені ролі та відповідальності для команди реагування.
    - Детальні процедури реагування на фішингові інциденти, що охоплюють виявлення, локалізацію, усунення, відновлення та аналіз (згідно з порядком, описаним раніше).
    - Регулярні тренування команди реагування.

2. *Політика Чистого Столу та Чистого Екрану (Clean Desk/Clean Screen Policy):* Зменшує ризик фізичного викрадення даних, які можуть бути використані для фішингу.
3. *Регулярне Резервне Копіювання Даних:* Важливо для швидкого відновлення після можливих наслідків фішингової атаки (наприклад, зараження рансомваре).
4. *Управління Вразливостями та Патчами:* Регулярне оновлення операційних систем та програмного забезпечення для закриття відомих вразливостей, які можуть бути експлуатовані фішинговими атаками.

III. Навчання та Підвищення Обізнаності Персоналу:

Це найважливіша лінія захисту від фішингу.

1. *Постійні Тренінги з Кібербезпеки:*
    - *Регулярні та Обов'язкові:* Проведення обов'язкових тренінгів для всіх співробітників щонайменше раз на рік, з додатковими коротшими нагадуваннями щоквартально.
    - *Актуальний Контент:* Навчальні матеріали повинні бути актуальними, враховувати останні фішингові тенденції та включати приклади реальних атак.
    - *Інтерактивність:* Використання інтерактивних модулів, квізів, відео.
2. *Імітація Фішингових Атак (Phishing Simulations):*
    - *Регулярні Симуляції:* Проведення періодичних, несподіваних імітованих фішингових кампаній для перевірки обізнаності співробітників.
    - *Аналіз Результатів:* Аналіз, хто "клюнув" на фішинг, і використання цих даних для цільового навчання.
    - *Навчання "на місці":* Якщо співробітник "клюнув", негайно надайте йому короткий навчальний модуль, пояснюючи, чому це був фішинг і як його розпізнати.
3. *Створення Культури Безпеки:*

- Заохочуйте співробітників повідомляти про будь-які підозрілі електронні листи чи дії.
- Підкреслюйте, що "краще перестрахуватися", і немає покарання за повідомлення про хибно-позитивний інцидент.
- Надайте чіткий канал для повідомлень про інциденти (наприклад, спеціальна поштова скринька, телефон довіри).

4. *Інформаційні Кампанії:* Розміщення плакатів, розсилка інформаційних бюлетенів з "червоними прапорцями" фішингу, прикладами фішингових листів, що нещодавно були виявлені.

Інтеграція цих рекомендацій дозволить організації створити надійний, багатошаровий захист від фішингу [1], значно зменшивши ризики успішних атак та підвищивши загальний рівень кіберстійкості.

ВИСНОВКИ

У роботі проведено дослідження проблеми виявлення фішингових атак в інформаційній системі організації, визначено її мету та завдання. Сучасні фішингові атаки залишаються одними з найбільш поширених і витончених кіберзагроз, які дедалі частіше обходять традиційні методи захисту. Це вимагає від організацій впровадження проактивних рішень, здатних своєчасно виявляти та блокувати спроби соціальної інженерії.

Проведено аналіз векторів фішингових атак, типових вразливостей інформаційної інфраструктури, а також можливостей сучасних антивірусних систем. Особливу увагу приділено архітектурі та функціональним можливостям програмного забезпечення Malwarebytes, яке виконує роль багаторівневої платформи виявлення фішингу завдяки веб-захисту, поведінковому аналізу, машинному навчанню та хмарній інфраструктурі реагування на загрози.

Проведено практичний аналіз ефективності Malwarebytes щодо виявлення та блокування фішингових атак у реальному середовищі. Результати демонструють високу точність і низький рівень хибних спрацювань, що дозволяє розглядати Malwarebytes як перспективне рішення для впровадження у корпоративних середовищах.

Отже, виявлення та реагування на фішингові атаки стало критичним елементом сучасної кібербезпеки, оскільки організації щодня стикаються з дедалі складнішими формами соціальної інженерії. Malwarebytes — це комплексне рішення, здатне забезпечити захист кінцевих точок, аналіз загроз у реальному часі, автоматизоване реагування на інциденти та підтримку в цифрових розслідуваннях.

Malwarebytes дозволяє організаціям реалізувати сучасні рекомендації з безпеки, централізувати контроль загроз і підвищити стійкість інформаційної інфраструктури до фішингових атак. Таким чином, правильна інтеграція системи виявлення фішингу в ІС організації сприяє підвищенню загального рівня кіберзахисту та запобіганню компрометації критичних даних.

ПЕРЕЛІК ПОСИЛАНЬ

1. 2022 Endpoint Security Report. Cybersecurity Insiders. URL: https://20645266.fs1.hubspotusercontent-na1.net/hubfs/20645266/CSI-2022-Endpoint-Security-Report-Adaptiva-Final-03282022%20(1).pdf (дата звернення: 03.03.2025).

2. Hadnagy C. *Social Engineering: The Science of Human Hacking.* Wiley, 2018. URL: https://www.wiley.com/en-us/Social+Engineering%3A+The+Science+of+Human+Hacking%2C+2nd+Edition-p-9781119433385 (дата звернення: 03.03.2025).

3. Malwarebytes. Фішинг: що це таке і як захиститися. URL: https://www.malwarebytes.com/ru/phishing (дата звернення: 08.03.2025).

4. Verizon. *2023 Data Breach Investigations Report.* URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 08.03.2025).

5. Anti-Phishing Working Group. *Phishing Activity Trends Report – 1st Quarter 2023.* URL: https://apwg.org/trendsreports/ (дата звернення: 08.03.2025).

6. Malwarebytes. *Threat Intelligence – Phishing.* URL: https://www.malwarebytes.com/phishing (дата звернення: 08.03.2025).

7. Malwarebytes. *What is Malwarebytes?* URL: https://www.malwarebytes.com/solutions/what-is-malwarebytes (дата звернення: 15.03.2025).

8. Malwarebytes Labs. *How Malwarebytes Works.* URL: https://www.malwarebytes.com/resources/malwarebytes-whitepaper.pdf (дата звернення: 15.03.2025).

9. Cybersecurity Insiders. *Endpoint Detection and Response 2023 Report.* URL: https://cybersecurity-insiders.com/edr-2023-report/ (дата звернення: 16.03.2025).

10. Malwarebytes Support. *How Web Protection Works.* URL: https://support.malwarebytes.com/hc/en-us/articles/360038520894 (дата звернення: 16.03.2025).

11. Malwarebytes Browser Guard. *Free Browser Extension for Chrome, Firefox, Edge*. URL: https://www.malwarebytes.com/browser-guard (дата звернення: 25.03.2025).

12. CERT-UA (2023). *Щомісячні огляди загроз: розділ фішингу.* URL: https://cert.gov.ua (дата звернення: 01.04.2025).

13. ThreatDown (Malwarebytes) Nebula Console Documentation. URL: https://www.malwarebytes.com/resources/threatdown/nebula (дата звернення: 03.04.2025).

14. Phishing Activity Trends Report 2023. Anti-Phishing Working Group. URL: https://apwg.org/trendsreports/ (дата звернення: 10.04.2025).

15. Malwarebytes ThreatDown Nebula: Deployment Guide. Malwarebytes Official Documentation. URL: https://support.malwarebytes.com/hc/en-us/articles/4402797195035 (дата звернення: 01.06.2025).