Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Захарова Володимира Володимировича

на здобуття ступеня вищої освіти магістра

Метод організації системи захисту корпоративної інформації
на основі технології Honeynet

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека та захист інформації
Освітня програма Кібербезпека та захист інформації

Шифр КРМКБЗІ.2301138.23.01.09 ПЗ

Виконав студент 2 курсу група КБЗІм-23-1 Володимир ЗАХАРОВ
Керівник канд. техн. наук, доцент Віктор ЧЕШУН
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

16 12 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Магістр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Освітня програма Кібербезпека та захист інформації

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

2 09 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Захарову Володимиру Володимировичу

1 Тема роботи Метод організації системи захисту корпоративної інформації на основі технології Honeynet

Керівник роботи канд.техн.наук, доцент Віктор ЧЕШУН

Затверджено наказом ректора університету від 26 08 2024 № 60

2 Строк подання студентом кваліфікаційної роботи на кафедру 27.11.2024р.

3 Вихідні дані до роботи Дослідити можливості технологій мережевих приманок для організації ефективної системи захисту корпоративної інформації, визначити концептуальні положення методу організації системи захисту корпоративної інформації на основі технології Honeynet

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Дослідження вразливостей та способів захисту корпоративної інформації. Огляд технологій реалізації мережевих пасток в системах захисту. Вибір технології реалізації методу захисту корпоративної інформації. Визначення принципів організація системи захисту корпоративної інформації на основі технології Honeynet. Практична реалізація системи захисту корпоративної інформації на основі технології Honeynet. Політики безпеки системи захисту корпоративної інформації на основі технології Honeynet

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

–

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 2 09 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Ґрунтовне ознайомлення та дослідження предметної галузі	15.09.2024	Виконано
Визначення змісту, структури кваліфікаційної роботи	22.09.2024	Виконано
Підготовка першого розділу кваліфікаційної роботи	29.09.2024	Виконано
Підготовка другого розділу кваліфікаційної роботи	10.10.2024	Виконано
Підготовка третього розділу кваліфікаційної роботи	20.10.2024	Виконано
Підготовка статті/тези за темою кваліфікаційної роботи	4.11.2024	Виконано
Підготовка четвертого розділу кваліфікаційної роботи	17.11.2024	Виконано
Підготовка та оформлення ілюстративного матеріалу	24.11.2024	Виконано
Оформлення кваліфікаційної роботи	24.11.2024	Виконано
Попередній захист кваліфікаційної роботи	27.11.2024	Виконано
Захист кваліфікаційної роботи на засіданні ЕК	19.12.2024	Виконано

Студент Володимир ЗАХАРОВ

Керівник кваліфікаційної роботи Віктор ЧЕШУН

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод організації системи захисту корпоративної інформації на основі технології Honeynet

Автор роботи: Захаров Володимир Володимирович

Керівник роботи: канд. техн. наук, доц. Чешун Віктор Миколайович

Загальний обсяг роботи: 99 сторінок, 8 рисунків, 6 таблиць, 2 додатки, 68 посилань.

Ключові слова: захист інформації, корпоративна інформація, мережеві приманки, технологія Honeynet.

Кваліфікаційна робота присвячена визначенню базових теоретичних положень, способів і засобів реалізації методу організації системи захисту корпоративної інформації на основі технології Honeynet.

В роботі здійснено ідентифікацію та класифікацію технології застосування мережевих пасток в системах захисту, визначено концепцію організації системи захисту корпоративної інформації на основі технології Honeynet, за результатами теоретичних та практичних досліджень здійснено розробку методу, орієнтованого на вдосконалення і розширення можливостей системи захисту корпоративної інформації за рахунок комплексного застосування можливостей технології Honeynet; визначено принципи організації системи захисту корпоративної інформації на основі технології Honeynet для комплексного захисту ресурсів корпоративної комп'ютерної мережі, вебзастосунків і систем моніторингу та управління.

Для впровадження і ефективної реалізації запропонованого методу розроблено політики безпеки використання системи захисту корпоративної інформації на основі технології Honeynet для захисту ресурсів корпоративної комп'ютерної мережі, вебзастосунків і систем моніторингу та управління.

25.11.2024 _____

ANNOTATION

Theme of qualification work: The method of organization of the protection system for corporate information based on Honeynet technology

Author of the work: Zakharov Volodymyr Volodymyrovych

Mentor: Ph.D. Cheshun Viktor Mykolaiovych

Total volume of work: 99 pages, 8 figures, 6 tables, 2 appendices, 68 links.

Keywords: information protection, corporate information, network decoys, Honeynet technology.

The qualification work is devoted to defining the basic theoretical provisions, methods and means of implementing the method of organizing a corporate information protection system based on Honeynet technology.

The work identifies and classifies the technology of using network traps in protection systems, defines the concept of organizing a corporate information protection system based on Honeynet technology, and based on the results of theoretical and practical research, develops a method focused on improving and expanding the capabilities of the corporate information protection system through the comprehensive use of Honeynet technology capabilities; defines the principles of organizing a corporate information protection system based on Honeynet technology for comprehensive protection of corporate computer network resources, web applications, and monitoring and management systems.

For the implementation and effective implementation of the proposed method, security policies for using a corporate information protection system based on Honeynet technology for protecting corporate computer network resources, web applications, and monitoring and management systems have been developed.

25.11.2024 _____

ЗМІСТ

ВСТУП

У сучасних умовах масштабної цифровізації всіх сфер життя та бізнесу кількість кібератак на корпоративні інформаційні системи невпинно зростає. Це пов’язано зі зростанням обсягу й цінності даних, які компанії зберігають і обробляють[1]. Сучасні кібератаки стають дедалі витонченішими: багато з них організовуються злочинними угрупуваннями або навіть підтримуються державними структурами, що ускладнює їх виявлення та нейтралізацію. З кожним новим вектором атак ризики для компаній підвищуються [1,2]. Неналежний рівень захисту може призвести до втрати даних, значних фінансових збитків та пошкодження репутації [1,3].

У відповідь на зростаючі загрози кібербезпеки технології захисту розвиваються стрімкими темпами. Це стимулює наукові дослідження та впровадження інноваційних рішень для боротьби з кіберзлочинністю.

Важливим напрямом стало створення класифікацій типів атак [4-6] на корпоративні ресурси, що дозволяє ефективніше розробляти стратегії захисту. Увага науковців також приділяється методам виявлення аномального трафіку та контролю мережевої активності для захисту корпоративних систем [7,8].

Додатково, безпека фінансових операцій підтримується технологіями, такими як блокчейн, електронні підписи та системи електронного банкінгу [9-11]. Використання штучного інтелекту та машинного навчання стало невід'ємною частиною систем кіберзахисту, спрямованих на виявлення та запобігання як відомим, так і новим загрозам [12-14].

Незважаючи на значний прогрес у захисті бізнес-інформаційних систем від зовнішніх загроз, проблема внутрішніх ризиків, зумовлених людським фактором, залишається недостатньо уваги [1]. Дії співробітників, як навмисні, так і випадкові, часто стають джерелом серйозних проблем для інформаційної безпеки компаній. Ці ризики наразі є одними з найактуальніших і становлять значну загрозу для корпоративних інформаційних систем.

Для зменшення впливу внутрішніх загроз організації впроваджують політики

безпеки та розробляють системи контролю доступу [8]. Такі системи розглядаються як ключовий елемент забезпечення сучасних потреб кібербезпеки [15] . Контроль доступу реалізується через різні моделі, включаючи дискреційний, мандатний і рольовий підходи. Крім того, постійно з'являються нові моделі контролю доступу, які адаптуються до зростаючих вимог у сфері інформаційних технологій [16,17].

Одним із основних способів забезпечення безпеки корпоративних ресурсів в умовах сьогодення стає використання мережевих приманок і технологій омани зловмисників [18].

Актуальність роботи зумовлена постійним і незупинним зростання кількості кіберзагроз корпоративним інформаційним ресурсам, що актуалізує розробку, впровадження і вдосконалення систем захисту інформації на основі сучасних і інноваційних технологій, до числа яких відносяться технології мережевих приманок і омани зловмисників, зокрема, технології Honeynet.

Ця кваліфікаційна робота присвячена визначенню базових теоретичних положень та алгоритмічній реалізації методу організації системи захисту корпоративної інформації на основі технології Honeynet.

Мета кваліфікаційної роботи полягає у вдосконаленні захисту корпоративної інформації за рахунок застосування технології Honeynet для організації комплексного захисту ресурсів корпоративної інформаційної системи.

Об'єктом дослідження є процеси захисту корпоративної інформації на основі технологій мережевих приманок.

Предметом дослідження є методи і технології розгортання Honeynet для захисту корпоративної інформації у різних підсистемах корпоративної інформаційної системи.

Щоб реалізувати програму досліджень необхідно:

а) дослідити вразливості та способи захисту корпоративної інформації і технології застосування мережевих пасток в системах захисту;

б) дослідити можливості сучасних засобів реалізації технології Honeynet для організації системи захисту корпоративної інформації;

в) обґрунтувати вибір технології реалізації методу захисту корпоративної інформації;

г) визначити концепцію організації системи захисту корпоративної інформації на основі технології Honeynet;

д) запропонувати рішення щодо організації системи захисту корпоративної інформації на основі технології Honeynet;

є) обґрунтувати вибір платформи для практичної реалізації системи захисту корпоративної інформації на основі технології Honeynet;

ж) розробити політики безпеки використання системи захисту корпоративної інформації на основі технології Honeynet.

В основі методів дослідження лежать базові положення інформаційної безпеки, теорії і практики виявлення вразливостей і вторгнень, теорії реалізації мережевих пасток.

Наукова новизна отриманих результатів:

1. Визначено принципи організації системи захисту корпоративної інформації на основі технології Honeynet для комплексного захисту ресурсів корпоративної комп'ютерної мережі, вебзастосунків і систем моніторингу та управління.

2. Запропоновано спосіб застосування Honeytoken у мережі Honeynet_для виявлення складних Ransomware і APT атак.

Практична значимість отриманих результатів полягає у розробці рішень щодо застосування технології Honeynet, спрямованих на захист від атак на ресурси різних підсистем корпоративної інформаційної системи, наданні рекомендацій щодо вибору платформи для комплексного розгортання Honeynet та визначенні положень політик безпеки для кожного із запропонованих варіантів застосування Honeynet.

Публікації. За темою магістерської роботи опубліковано 3 тези за результатами доповідей на міжнародній і Всеукраїнських науково-практичній конференціях.

1 ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ТА СПОСОБІВ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ І ТЕХНОЛОГІЙ РЕАЛІЗАЦІЇ МЕРЕЖЕВИХ ПАСТОК В СИСТЕМАХ ЗАХИСТУ

1.1 Корпоративна інформація як об’єкт атак і захисту

Захист корпоративної інформації є критично важливим аспектом сучасного бізнесу, адже витік конфіденційних даних або компрометація систем може призвести до значних фінансових втрат, пошкодження репутації компанії та навіть до порушення законодавства [1].

Корпоративні дані включають комерційні таємниці, інформацію про клієнтів, фінансові звіти, стратегії компанії та іншу критично важливу інформацію [1,2]. Будь-яка несанкціонована діяльність, спрямована на викрадення чи компрометацію цих даних, може призвести до суттєвих збитків і навіть паралізувати роботу компанії.

Ефективний захист корпоративної інформації також є обов’язковою умовою для дотримання міжнародних стандартів та регламентів, таких як GDPR [19] і ISO/IEC 27001 [20], а також цілого ряду законів України [21-25], що забезпечують довіру клієнтів і партнерів.

Вразливості та сучасні загрози корпоративної інформації – одна з головних проблем, з якими стикаються організації в цифровому середовищі. З поширенням дистанційної роботи, використанням хмарних технологій та зростанням кількості IoT-пристроїв, корпоративні мережі стають більш уразливими до атак зловмисників. Захист корпоративної інформації сьогодні вимагає комплексного підходу, що включає як технічні, так і організаційні заходи безпеки.

Аналіз типових вразливостей корпоративної інформації дозволяє визначити типові загрози її безпеці.

Найбільшою вразливістю корпоративних інформаційних ресурсів залишаються їх користувачі, оскільки фітингові атаки, соціальна інженерія та банальна необачність можуть зумовити інформаційні витоки. Традиційна лінь і необачність людини, що має наслідком слабкі паролі, використання одного і того

ж пароля для кількох сервісів або випадкове відкриття підозрілих файлів катастрофічно збільшують ризики. Надання співробітникам доступу до корпоративної інформації, яка не є необхідною для їх роботи, збільшує ризики втрат.

Співробітники або колишні працівники можуть стати джерелом витоку інформації через невдоволення, фінансові стимули або банальну необачність. Інсайдерські загрози є особливо небезпечними, оскільки інсайдери часто мають доступ до критично важливої інформації.

І ще одна вада лінощів людського фактору – використання застарілого програмного забезпечення або несвоєчасне встановлення оновлень, що створює вразливості, які можуть бути використані зловмисниками для несанкціонованого доступу до корпоративних мереж. Використання незахищених протоколів передачі даних, таких як FTP, або відсутність шифрування на рівні маршрутизаторів і точок доступу, може призвести до перехоплення даних та атак типу «людина посередині» (MITM).

Загрозу корпоративній інформації несе відсутність сегментації мережі. Коли корпоративна мережа не розділена на сегменти, зловмисники можуть отримати доступ до всієї мережі в разі успішного злому хоч одного вузла. Нерозділена мережа збільшує ризик поширення загрози у разі компрометації одного з компонентів. Наприклад, якщо кіберзлочинці отримають доступ до одного сервера або комп’ютера, відсутність сегментації дозволить їм переміщуватися мережею і отримати доступ до більш критичних ресурсів. Відсутність сегментації також ускладнює відстеження та ізоляцію загроз.

Характерною позитивною властивістю сучасного бізнес-середовища є використання хмарних сервісів, оскільки хмара дозволяє компаніям зберігати великі обсяги даних, але при цьому належний захист хмарних ресурсів не завжди забезпечується. Часто компанії покладаються на базові налаштування безпеки, які можуть бути вразливими до атак, якщо не налаштовані відповідним чином.

Позитивним, але ризикованим є використання в мережі компанії незахищених пристроїв інтернету речей, оскільки такі пристрої часто мають слабкий захист або стандартизовані паролі, які легко зламати. Зловмисник може

використати такі пристрої в якості точки доступу проникнення в мережу.

Використовуючи подібні вразливості зловмисники здійснюють різноманітні атаки з метою отримати доступ до корпоративної інформації. Одним з найпоширеніших методів проникнення до корпоративних систем залишається фішинг [26-28]. Сучасні фішингові атаки стають дедалі більш таргетованими і складними, наприклад, spear phishing [29], де зловмисники атакують конкретних співробітників з використанням персоналізованих повідомлень.

Ще одна критична загроза корпоративної інформації – Ransomware-атаки. Програми-вимагачі, такі як WannaCry або Petya [30], блокують доступ до файлів компанії, вимагаючи викуп за їх розблокування. Ransomware стає дедалі складнішим, здатним атакувати резервні копії даних і навіть шифрувати цілі системи, залишаючи компанію без критичної інформації.

Через співпрацю з численними постачальниками компанії стають вразливими до атак на сторонніх підрядників або постачальників ПЗ, відомих як атаки на ланцюг постачання (Supply Chain Attacks). Це дозволяє зловмисникам проникнути в корпоративні мережі через надійних партнерів, використовуючи легітимні сертифікати або навіть підробляючи оновлення програмного забезпечення. Атака на ланцюжок поставок програмного забезпечення характеризується впровадженням шкідливого коду в пакет програмного забезпечення з метою скомпрометувати залежні системи далі по ланцюжку. Останніми роками спостерігалася низка атак на ланцюги поставок, які використовують все більш широке використання відкритого коду під час розробки програмного забезпечення, чому сприяють менеджери залежностей, які автоматично виявляють, завантажують і встановлюють сотні пакетів з відкритим кодом протягом життєвого циклу програмного забезпечення [31-32].

У атаках типу «людина посередині» (MITM) зловмисники перехоплюють дані, що передаються між двома сторонами, несанкціоновано втручаючись у комунікацію. Вразливою корпоративну інформацію до подібних атак робить відсутність шифрування, слабкі паролі або загальна мережа Wi-Fi компанії [33] .

Зловмисне програмне забезпечення (Malware) – це шкідливе програмне

забезпечення, яке може включати трояни, віруси, кейлогери та інші засоби, призначені для крадіжки корпоративної інформації або руйнування корпоративних інформаційних систем [35]. Malware може проникати в корпоративні системи через файли, завантажені з інтернету, через електронні листи тощо [36].

На сьогодні існують і широко використовуються різноманітні класичні методи захисту від подібних загроз [34].

Розподіл мережі на окремі сегменти дозволяє обмежити розповсюдження загроз, якщо зловмисники отримали доступ до одного з вузлів, а також спрощує моніторинг мережевої активності та допомагає швидше ідентифікувати загрози.

Використання багатофакторної автентифікації – додатковий рівень захисту корпоративної інформації, який ускладнює завдання зловмисникам навіть у разі, якщо вони зламали пароль.

Для зменшення ризиків перехоплення корпоративної інформації є критично важливим захист через шифрування цієї інформації. Навіть якщо зловмисник отримав доступ до корпоративних ресурсів, шифрування інформації як у спокої, так і під час передачі забезпечує належний рівень захисту. Ненадійне шифрування або його відсутність призводить до того, що дані, які зберігаються або передаються без належного шифрування, можуть бути перехоплені зловмисниками. Відсутність шифрування або використання слабких алгоритмів робить малоефективним захист корпоративної інформації у разі несанкціонованого доступу.

Використання систем виявлення та запобігання загрозам (IDS/IPS-систем) для моніторингу активності в мережі дозволяє оперативно виявляти та реагувати на аномалії та підозрілі дії. Це особливо важливо для захисту від складних атак, таких як APT (Advanced Persistent Threat). IDS (Intrusion Detection Systems) і SIEM (Security Information and Event Management) системи дозволяють виявляти атаки на ранніх стадіях і попереджати про загрози. Недостатній моніторинг та відсутність систем виявлення вторгнень має критичні наслідки. Відсутність постійного моніторингу мережевої активності та систем виявлення вторгнень знижує можливість своєчасного реагування на аномалії або підозрілу активність у системі.

Без регулярних тестувань систем на вразливості (penetration testing) компанії

можуть не знати про потенційні слабкі місця у своїй інфраструктурі. Пентести дозволяють виявляти можливі вразливості та усувати їх до того, як вони будуть використані зловмисниками.

Ну і практичне навчання з кібербезпеки допомагає співробітникам розпізнавати фішингові атаки та уникати підозрілих файлів або повідомлень, вчасно оновлювати програмне забезпечення тощо, тим самим знижуючи людський фактор як вразливість.

Вразливості та сучасні загрози корпоративної інформації постійно змінюються, вимагаючи від організацій застосування комплексних заходів захисту. Оскільки зловмисники використовують нові тактики та техніки, компанії мають дотримуватися проактивного підходу до кібербезпеки, інвестуючи в технологічні рішення, навчання співробітників і систематичне вдосконалення захисту корпоративної інформації.

З проведеного аналізу можна зробити висновки, що корпоративна інформація є постійним об’єктом атак і має велику цінність. Захист корпоративної інформації вимагає комплексного підходу, виявлення та усунення слабких місць значно знижує ризики атак, допомагаючи створити надійну систему кіберзахисту, що відповідає сучасним вимогам та загрозам.

1.2 Технології мережевих приманок і їх потенціал в захисті корпоративної інформації

Сучасні кіберзагрози стають дедалі складнішими і підходять до атак з використанням новітніх технологій, тому традиційних методів захисту, як-от міжмережеві екрани та антивіруси, уже недостатньо. У цьому контексті інноваційні технології, такі як мережеві приманки, забезпечують додатковий рівень захисту, дозволяючи перехоплювати та аналізувати атаки на ранніх стадіях.

Технології приманок у мережі (Deception technology) – це спеціальний метод відволікання кіберзлочинців від реальних ресурсів компанії, спрямовуючи їх

приманкою у заздалегідь створені пастки. Ці приманки імітують справжні сервери, програми та дані, створюючи у зловмисників ілюзію доступу до критично важливих активів організації, хоча насправді вони взаємодіють із фальшивими об'єктами. Цей підхід допомагає зменшити шкоду від кібератак та забезпечити захист корпоративної інформації [37].

У боротьбі між хакером і кіберзахисником загальноприйнято вважати, що правопорушник має перевагу: кіберзахисники мають переконатися, що все належним чином обслуговується та запобігати вторгненням у кожній точці, тоді як хакерам просто потрібно скористатися однією вразливістю для порушення захисту . У той же час зловмисники завжди можуть отримати інформацію про цільову систему або мережу за допомогою різноманітних тактик розвідки та виявлення, тоді як захисникам зазвичай не вистачає інформації про своїх противників. Очікується, що такі асиметричні недоліки для кіберзахисту будуть перебалансовані шляхом використання оборонного обману, який, як очікується, матиме кардинальний вплив на те, як протистояти загрозам [38].

Стратегія захисту на основі периметра з використанням звичайних заходів безпеки, таких як брандмауери, засоби контролю автентифікації та системи запобігання вторгненням, виявилася слабкою проти проникнення. Навіть із стратегією поглибленого захисту Міністерства внутрішньої безпеки США (2016) [39], де кілька рівнів звичайних засобів контролю безпеки розміщено по всій цільовій мережі, кіберзахисникам усе ще важко запобігати та виявляти складні атаки, такі як APT. Такі цілеспрямовані атаки зазвичай використовують уразливості нульового дня, щоб закріпитися на цільовій мережі та залишити дуже мало слідів своєї зловмисної діяльності для виявлення. Крім того, звичайні рішення для виявлення аномалій, такі як системи виявлення вторгнень і сканери зловмисного програмного забезпечення на основі поведінки, як правило, викликають переважну кількість хибно-позитивних сповіщень, що завдає шкоди кіберзахисникам і знижує їхню ефективність у виявленні справжніх атак і реагуванні на них. Захисний обман, який характеризується здатністю виявляти вразливості нульового дня та низьким рівнем помилкових тривог завдяки чіткій

межі між законною діяльністю користувача та зловмисною взаємодією, може діяти як додатковий рівень захисту для пом’якшення проблем[38].

Замість того, щоб зосереджуватися на діях зловмисників, технологія мережевих приманок працює на їхньому сприйнятті, затьмарюючи поверхню атаки. Мета полягає в тому, щоб приховати цінну корпоративну інформацію від зловмисників і заплутати або ввести їх в оману, тим самим збільшуючи ризик їх виявлення, змушуючи їх неправильно спрямовувати або витрачати ресурси, затримуючи ефект атак і передчасно викриваючи торговельні дії противника . Іншими словами, захисний обман допомагає встановити активну позицію кіберзахисту, де ключовими елементами є передбачення атак до того, як вони відбудуться, збільшення витрат супротивника та збір нових даних про загрози для запобігання подібним атакам.

Технологія мережевих приманок має на меті ввести зловмисників в оману, змушуючи їх вважати, що вони успішно проникли в систему. Наприклад, хакери можуть думати, що виконують атаку з розширенням привілеїв, тоді як насправді вони взаємодіють лише з фальшивими інструментами, не отримуючи реального доступу до привілейованих прав чи впливу на інфраструктуру.

Приманка у мережах імітує законні сервери, програми та дані, щоб зловмисник обманом був змушений повірити, що він проник і отримав доступ до найважливіших активів підприємства, хоча насправді це не так. Стратегія використовується для мінімізації збитків і захисту справжніх активів організації.

Одним із ризиків цієї технології є те, що сучасні атаки стають дедалі масштабнішими та складнішими, і сервер обману разом із фіктивними активами може виявитися недостатньо потужним, щоб впоратися з ними. До того ж досвідчені кіберзлочинці можуть швидко зрозуміти, що їх обманюють, адже приманки та фальшиві ресурси можуть видатися їм підозрілими. У такому випадку вони можуть припинити атаку та повернутися з новими, ще витонченішими методами.

Для ефективності технологія мережевих приманок повинна залишатися непомітною не лише для кіберзлочинців, але й для співробітників компанії, підрядників і клієнтів. Її механізм полягає у створенні імітованих цифрових

активів, схожих на реальні ресурси, що є в інфраструктурі організації. Коли хакери намагаються взаємодіяти з цими фальшивими елементами, вони фактично потрапляють у пастку, не завдаючи шкоди критично важливим системам.

Зазвичай технологія мережевих приманок не є основною складовою кібербезпеки, однак її використовують для реагування на можливі загрози. Її мета – запобігти несанкціонованому доступу, перенаправивши зловмисників на фіктивні дані. Це дозволяє забезпечити безпеку справжніх ресурсів підприємства.

Крім того, технологія мережевих приманок є ефективним інструментом для вивчення поведінки кіберзлочинців. Аналіз їх дій під час проникнення та взаємодії з фальшивими даними дозволяє спеціалістам з кібербезпеки глибше розуміти методи атак. Деякі організації навіть розгортають спеціалізовані сервери обману, які фіксують усі дії зловмисників – від моменту вторгнення до їхніх маніпуляцій з приманкою. Такий підхід допомагає відстежувати вектори атак і надавати цінну інформацію для вдосконалення системи безпеки та попередження подібних загроз.

Іншим важливим елементом технології мережевих приманок є система сповіщень, яка дозволяє фіксувати активність зловмисника в реальному часі. Як тільки сервер отримує відповідне сповіщення, він починає записувати всі дії хакера в зоні, на яку спрямована атака. Це забезпечує можливість глибокого аналізу методів і тактик, що використовуються кіберзлочинцями, надаючи цінну інформацію для вдосконалення засобів захисту.

Однією з ключових переваг технологій мережевих приманок є їх здатність виявляти активи, які найбільше приваблюють зловмисників. Наприклад, можна припустити, що бази даних із чутливою інформацією, такою як платіжні реквізити, особисті дані чи номери соціального страхування, є основними цілями хакерів. Однак за допомогою технологій обману можна точно підтвердити, які саме активи найчастіше стають об'єктами атак.

Більше того, технологія мережевих приманок дозволяє визначати конкретні типи даних, які цікавлять зловмисників. ІТ-команди можуть створювати симульовані середовища з різними типами підробленої інформації, наприклад бази даних, що містять вигадані номери соціального страхування, імена, адреси чи

навіть облікові дані керівників компанії. Спостерігаючи за тим, до яких саме активів отримують доступ хакери, можна зробити висновки щодо їхніх цілей та пріоритетів.

Технологія мережевих приманок має низку переваг і залишається важливим компонентом сучасних стратегій кібербезпеки. Однією з ключових переваг є здатність значно скоротити час перебування зловмисника в мережі. Це досягається завдяки використанню активів-приманок, які виглядають достатньо переконливо, щоб хакери прийняли їх за реальні. Проте, коли атака починає поширюватися, IT-фахівці можуть втрутитися, обмежуючи доступ зловмисників до мережі.

У певний момент хакери можуть зрозуміти, що мають справу із симульованими активами, і усвідомити, що всі справжні ресурси організації залишаються поза їхнім доступом. Це може змусити їх припинити атаку та залишити мережу, визнавши операцію невдалою. Завдяки цьому якісна реалізація технологій приманок сприяє не лише збору цінних даних про атаки, а й зменшенню шкоди, яку може завдати зловмисник.

Хоча зломи завжди є небажаними, аналіз точок входу та поведінки кіберзлочинців під час атаки забезпечує цінні дані для аналітиків. Зібрана інформація допомагає не лише зміцнити мережеву інфраструктуру, а й розробити більш ефективні стратегії захисту від майбутніх атак. Чим переконливіше налаштовані приманки, включаючи сервери, програми та підроблені дані, тим довше триває симульована атака. Це збільшує обсяг отриманих даних, необхідних для вдосконалення захисту.

Технологія мережевих приманок дозволяє IT-командам детально досліджувати поведінку зловмисників під час атак на приманні активи. Завдяки ресурсам, які зосереджуються на аналізі цих атак, такі інциденти розглядаються як важливі місії. Це дає змогу швидко реагувати на несанкціонований доступ або аномальну активність у мережі. Як результат, технологія обману скорочує середній час виявлення та нейтралізації загроз.

Одним із ключових викликів кібербезпеки є велика кількість сповіщень, які можуть перевантажити IT-команду. Використовуючи технологію мережевих приманок, команда отримує лише цільові сповіщення, коли зловмисники

перетинають периметр захисту та взаємодіють із приманками. Такі сповіщення містять важливу інформацію про поведінку атакуючих і дозволяють відстежувати їхні подальші дії.

Масштабування технології приманок є відносно простим та економічно вигідним процесом. Один сервер-приманку можна багаторазово використовувати, а створення фальшивих даних, таких як вигадані облікові записи чи паролі, не потребує значних ресурсів. Крім того, автоматизовані інструменти, що використовуються в інших елементах кіберзахисту, можуть бути інтегровані й у технологію обману.

Ще однією перевагою цієї технології є її сумісність із застарілими системами та новітніми рішеннями типу інтернету речей. Кіберзлочинці часто атакують застарілі системи, вважаючи їх менш захищеними через відсутність оновлень. Використання приманок у таких середовищах дозволяє не лише виявляти атаки, але й збирати важливі дані для посилення кіберзахисту.

1.3 Огляд технологій реалізації мережевих приманок і пасток

Технологія мережевих приманок набули широкого поширення і різноманітних реінкарнацій. Як правило, ці реінкарнації пов’язані терміном Honey як натяк на солодку привабливість приманки для зловмисника.

Серед сучасних модифікацій мережевих приманок можна відзначити:

– Honeypot;
– Honeynet;
– Honeytoken;
– Honeydoc;
– Honeywall.

Дослідимо зазначені технології як потенційні інструменти захисту корпоративної інформації.

1.3.1 Технологія Honeypot

Технологія Honeypot є найбільш відомою і широко популяризованою серед Honey-приманок.

Honeypot або «горщик з медом» є прототипом сучасних технологій кіберобману, що з’явився на межі 1980-90-х років [40].

Це спеціально створений мережевий об’єкт, основна мета якого – привабити зловмисника та стати об’єктом атаки. У межах мережі Honeypot не виконує жодних легітимних функцій і не взаємодіє з іншими компонентами системи. Будь-яка активність, що фіксується Honeypot, є ознакою спроби злому. Під час атаки Honeypot записує всі дії зловмисника, що дозволяє дослідникам аналізувати його поведінку, шляхи проникнення та тактики [40].

Honeypot може бути операційною системою, що імітує робоче місце працівника, сервер або окремий сервіс. Це робить Honeypot привабливим і реалістичним об'єктом для атак [41].

Використання Honeypot є важливим елементом стратегії кібербезпеки, що дозволяє не лише захистити систему, а й проактивно досліджувати нові загрози.

Відволікаючи увагу злочинця на вивчення хибного ресурсу, Honeypot затримує просування останнього мережею, що дає службі безпеки виграш у часі для реагування на інцидент атаки.

На відміну від типових корпоративних вебсерверів або поштових серверів, які мають великий обсяг легітимного трафіку, Honeypot практично немає законної активності. Це означає, що сутність зафіксованих даних є явною атакою. Весь вхідний і вихідний трафік Honeypot повинен ретельно аналізуватися, щоб своєчасно виявляти атаки та усувати уразливості. Завдяки цьому легше аналізувати активність зловмисників, розуміти їхні наміри та дії [42].

Honeypot рекомендується розміщувати на IP-адресах, суміжних із критично важливими серверами, але без надання очевидних імен або доменів [43]. Це зумовлено тим, що більшість атак здійснюється через IP, а не через DNS-записи.

Розміщення Honeypot поряд із реальними серверами компанії (корпоративним вебсервером або поштовим сервером тощо) дозволяє отримувати

цінні дані про характер атак. Для підвищення ефективності Honeypot можна налаштувати так, щоб він повністю повторював конфігурацію захищеної системи, включаючи операційну систему, встановлені патчі та програмні пакети. Використання ідентичних налаштувань Honeypot із системами, які захищаються, дозволяє отримати найбільш релевантну інформацію про методи злому. Якщо зловмисник зламає Honeypot, це дасть чітке уявлення про потенційні загрози для реального сервера.

Сучасні наукові дослідження охоплюють широкий спектр застосувань Honeypot, включаючи захист інтернету речей, промислових мереж та адаптивні моделі для змінних умов кібератак.

В роботі [44] розглядається використання індустріальних Honeypot-систем, які базуються на глибоких нейронних мережах, для захисту від кібератак у промислових мережах. Це дозволяє виявляти та моделювати поведінку зловмисників більш точно, а також адаптувати захист до нових типів загроз, характерних для критичної інфраструктури.

Група дослідників пропонує [45] описує високорівневі Honeypot-системи для промислових контролерів , що використовуються в SCADA-системах. Вони допомагають досліджувати специфічні атаки на промислові середовища, такі як Stuxnet, і вивчати методи захисту від загроз у галузі управління виробничими процесами.

Авторами роботи [46] запропоновано динамічні моделі Honeypot, які дозволяють адаптуватися до змінюваних умов атаки. Публікація зосереджена на побудові Honeypot-систем для захисту від різнорідних загроз у корпоративних мережах підприємств та інтернету речей.

Хоча Honeypot ефективно виявляють загрози й надають цінні дані в різних реалізаціях, застосування вони мають обмежене. Honeypot корисні лише в разі, якщо зловмисник взаємодіє саме з приманкою. Honeypot не замінюють комплексну систему захисту, а лише доповнюють її, забезпечуючи глибше розуміння поведінки зловмисника в корпоративному кіберпросторі [40].

1.3.2 Технологія Honeynet

Одним із найбільш захоплюючих досягнень у сфері мережевих приманок є створення віртуальних Honeynets – цілих мереж віртуальних комп'ютерів, які можуть функціонувати на одному фізичному хості завдяки технологіям віртуалізації (наприклад, на VMware чи User-Mode Linux). Такий підхід дозволяє одночасно запускати декілька (зазвичай від чотирьох до десяти) віртуальних систем на одному фізичному сервері.

Honeynet є розширеним варіантом Honeypot і імітує складну корпоративну інфраструктуру.

Для Honeynet характерними є властивості [47]:

– Honeynet включає симуляцію серверів, додатків та служб, які виглядають привабливими для зловмисників;

– Honeynet використовує спеціалізовані інструменти для відстеження дій атакуючих, надаючи аналітикам цінні дані про методи та стратегії кібератак;

– у Honeynet немає авторизованих користувачів чи дозволених дій і будь-яка взаємодія з мережею автоматично вважається атакою.

Віртуальні Honeynet можна розміщувати поряд із робочими системами, імітуючи конфігурацію корпоративної мережі. Це робить псевдо-мережі цінною ціллю для атакуючих і дозволяє службі захисту корпоративної інформації вивчати моделі поведінки зловмисників. Завдяки можливості збереження та аналізу вхідного й вихідного трафіку, такі системи стають ефективним інструментом для запобігання атакам на корпоративну інформацію.

Віртуалізація зменшує витрати на апаратне забезпечення, фізичний простір та обслуговування систем. Це також спрощує управління мережами Honeynet, оскільки всі дані знаходяться на одній хост-системі. Оскільки «диски» віртуальних комп'ютерів є файлами на хості, фахівцям легко виявляти внесені зловмисником зміни та швидко відновлювати систему до початкового стану.

У роботі [48] досліджується комбінована модель Honeynet, що використовує віртуальні та реальні пристрої. Такий підхід підвищує реалізм мережі-приманки, дозволяючи точніше імітувати структуру захищених мереж і досліджувати тактики

атакуючих.

Honeynet може служити приманкою, що утримує увагу зловмисників від критичних інформаційних ресурсів корпоративної мережі. Навмисно створені вразливості дозволяють хакерам проникати в Honeynet, відкриваючи шлях для дослідження їхніх стратегій і тактик. Honeynet може ефективно використовуватись для збору великих обсягів даних і дослідження складних атак на корпоративні системи [49]. Це допомагає спеціалістам із кібербезпеки зміцнити захист реальних систем, оскільки на основі зібраних даних розробляються стратегії захисту від майбутніх атак.

Завдяки функціям «призупинення» та «відновлення» можна зберегти стан скомпрометованого комп'ютера Honeynet, що дозволяє детально вивчати поведінку зловмисників в корпоративному кіберпросторі, відкриті з'єднання TCP/IP та інші параметри.

Технології Honeynet перебувають у постійному розвитку.

Дослідження [51] зосереджене на застосуванні Honeynet у промислових системах управління (інтернет речей , промисловий Інтернет речей і кіберфізичні системи (CPS), які стали важливими для нашого повсякденного життя в таких контекстах, як наші будинки, будівлі, міста, здоров’я, транспорт, виробництво, інфраструктура, і сільське господарство). Розробка включає емуляцію фізичних процесів та інтеграцію протоколів, які широко використовуються у SCADA-системах.

У статті [50] пропонується архітектура Honeyfactory (рисунок 1.1), яка використовує контейнеризацію для створення Honeynet, що імітують бізнес-мережі.

Архітектура Honeyfactory дозволяє підвищити ефективність збору даних про загрози завдяки новим моделям кіберобману, базованим на прихованих Марківських моделях. Архітектура спрямована на захист від складних атак у хмарних і програмно-визначених мережах.

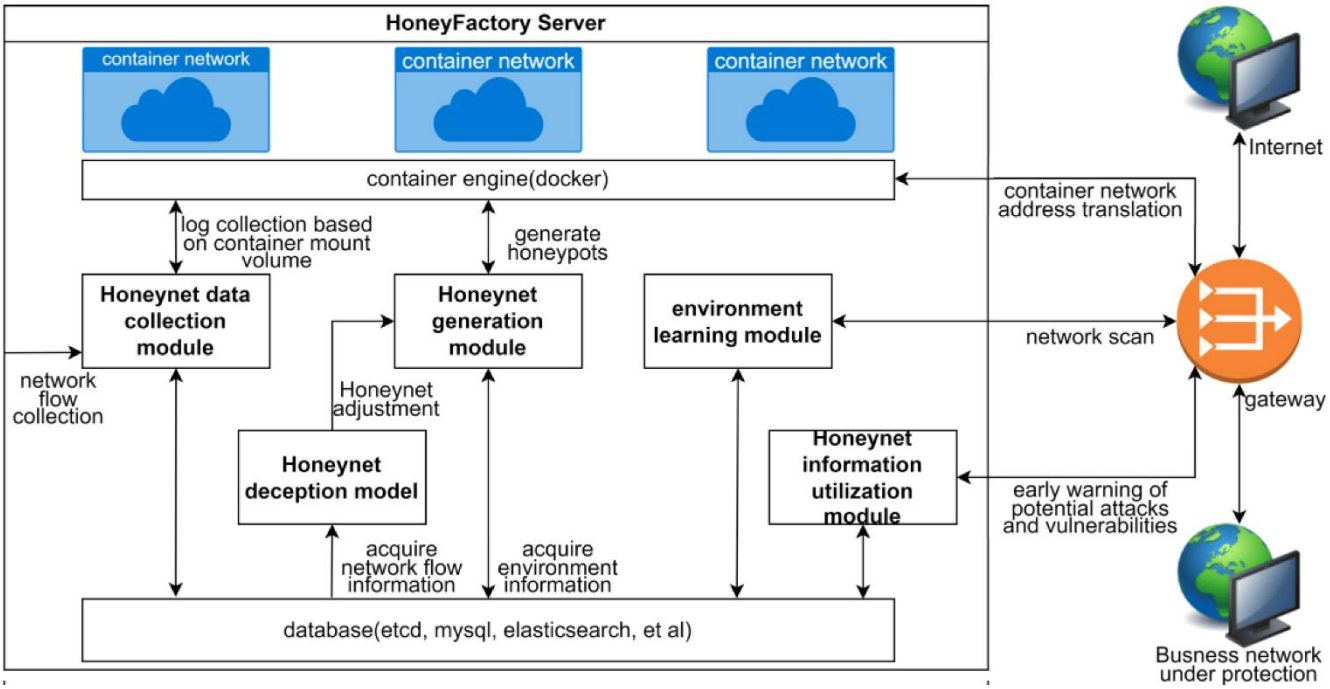

Рисунок 1.1 – Honeynet-архітектура Honeyfactory [50]

1.3.3 Технологія Honeytoken

Honeytoken – це фальшиві дані (облікові записи, файли, API-ключі), які розміщуються в системах з метою привернення уваги зловмисників. Вони допомагають виявляти несанкціонований доступ і запобігати загрозам, таким як витік даних або атаки інсайдерів. На відміну від більш складних Honeypots, вони простіше у розгортанні та використанні, що робить їх зручним інструментом для швидкого реагування на загрози [52,53].

Існує кілька типів Honeytoken, включаючи фальшиві облікові записи, записи в базах даних і помилкові файли. Вони можуть бути інтегровані з інструментами управління подіями безпеки (SIEM) для автоматичної генерації тривог доступу до них. Це дозволяє ефективно моніторити спроби проникнення та знижувати помилкові спрацьовування [54,55]. У статті CrowdStrike [55] обговорюється як Honeytoken допомагають привертати увагу атакуючих і генерувати тривоги при спробі доступу до них. Наведено рекомендації щодо їх розміщення, інтеграції з системами безпеки та моніторингу активності для виявлення загроз.

Правильне розміщення Honeytoken у цільових системах та їх інтеграція з існуючою інфраструктурою безпеки є ключем до їх ефективності. Важливо також

регулярно оновлювати ці «пастки», щоб вони залишалися актуальними та надійними. Найкращі практики використання Honeytoken у Microsoft Defender for Identity обговорюються у статті [54], де наведено приклади впровадження, включаючи створення підроблених облікових записів, PowerShell-скриптів та інтеграцію з SIEM-системами, такими як Microsoft Sentinel. Основну увагу приділено виявленню атак та моніторингу дій зловмисників. Робота [56] досліджує методи створення та керування Honeytoken для підвищення їх непомітності та складності виявлення зловмисниками. Детально розглядається впровадження Honeytoken у корпоративні системи для моніторингу активності атакуючих.

Honeytoken можуть використовуватися для виявлення як зовнішніх загроз, так і внутрішніх, таких як атаки фішинга або несанкціоноване використання облікових даних. Наприклад, підроблені облікові записи в Active Directory або помилкові API-ключі часто застосовуються для моніторингу та виявлення атак [53,55].

Публікація [57] містить практичну реалізацію прототипу Honeytoken, який базується на Remote Template Injection і Azure Function App.

Рішення базується на трьох різних блоках (рисунок 1.2):

– медовий документ (файл docx). Файл docx повідомляє веб-серверу за допомогою Remote Template Injection, коли його відкривають;

– додаток Azure Function, написаний на Powershell, – це серверна частина коду, яка очікує на вихід honey-docx. Коли він отримує запит GET від honey-docx, він пересилає ці події до робочої області Log Analytics в Azure;

– правило в Sentinel, яке виявляє події, що надходять із програми Azure Function у робочу область Log Analytics.

Дії, позначені червоними стрілками, запускаються, коли хтось відкриває документ. Зображення представляє сценарій відкриття вкраденого документа на машині зловмисника, який вкрав файл. Дії на синіх стрілках – це звичні дії. Ці дії проводяться для налаштування та моніторингу середовища.

Відкликання та відновлення «скомпрометованих» ключів і документів також є частиною звичайної діяльності, але вони не показані на схемі.

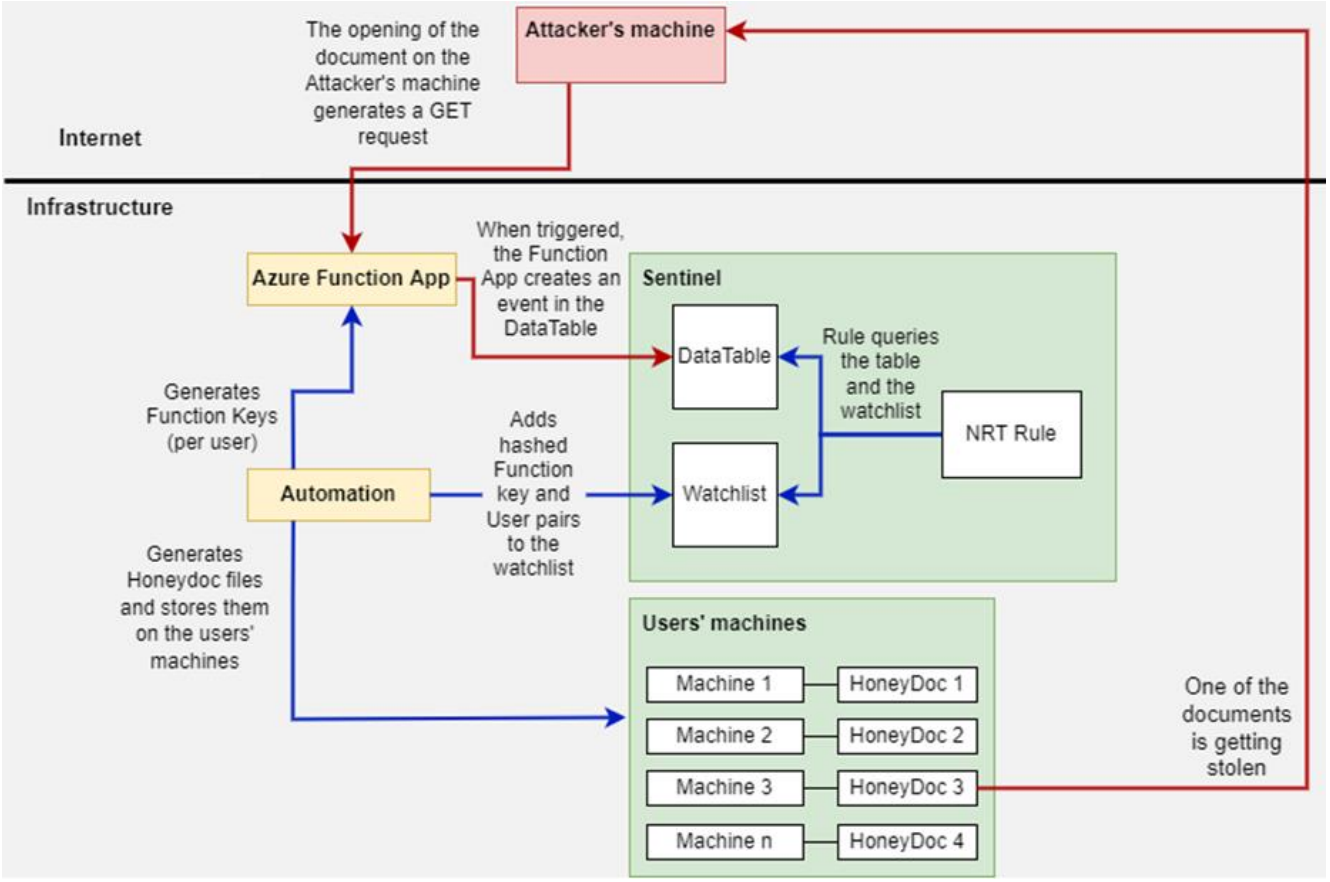

Рисунок 1.2 – Прототипу Honeytoken з файлами Honeydoc (файли docx) [57]

Окрім основних блоків використано логіку автоматизації, яка допомагає створювати ключі у програмі Function App і синхронізувати ці дані зі списком спостереження, щоб мати можливість диференціювати та ідентифікувати різних користувачів і комп'ютери. Такі самі кроки автоматизації необхідні для відкликання ключів після їх зламу. Цей крок не є основною функціональністю, рішення працює навіть без нього, але він потрібен, щоб усунути ручну роботу та мати можливість розрізняти користувачів.

1.3.4 Технологія Honeywall

Honeywall – це спеціалізоване рішення, розроблене для забезпечення безпеки в кіберпросторі. Воно є програмно-апаратним комплексом, який використовується для моніторингу, аналізу та захисту від загроз, що виходять від потенційних зловмисників. Основне призначення Honeywall полягає у підтримці роботи пасток Honeypot та забезпеченні їхньої безпеки [58].

Honeywall виступає в ролі шлюзу між зовнішнім світом і Honeypot. Усі дані,

які проходять через нього, контролюються та аналізуються. Цей підхід гарантує, що реальні системи залишаються захищеними навіть якщо атакуючий захопить Honeypot.

Honeywall є важливим елементом сучасної кібербезпеки, дозволяючи організаціям не лише захищатись від атак, але й активно вивчати та прогнозувати нові загрози.

Основними функціями Honeywall [58] є фільтрація трафіку, збір інформації, знешкодження загроз, здійснення аналізу і формування звітності.

Honeywall перехоплює весь вхідний та вихідний трафік, що спрямовується до Honeypot, для запобігання небажаним атакам на інфраструктуру та збору даних про дії атакуючих. Він фіксує дії зловмисників, включаючи спроби сканування портів, експлуатацію вразливостей та інші методи злому. Це допомагає організаціям зрозуміти природу загроз та розробити контрзаходи.

Honeywall ізолює шкідливу активність, запобігаючи поширенню загроз усередині мережі, та надає інструменти для аналізу даних про зломи та створення звітів для подальшого вивчення атак та покращення кіберзахисту.

Honeywall забезпечує покращену поінформованість про кіберзагрози. З його допомогою можна отримати детальну інформацію про методи та інструменти, які використовуються хакерами. Honeywall забезпечує ізоляцію атакуючих, запобігаючи впливу на реальні сервіси, тим самим досягається мінімізація ризиків для основної інфраструктури.

Застосування Honeywall [59]:

– компанії використовують Honeywall для вивчення активності кіберзлочинців та тестування вразливостей у своїх системах.

– дослідницькі центри аналізують загрози та розробляють нові методи захисту.

– правоохоронці використовують дані Honeywall для розслідування кіберзлочинів.

Реалізація Honeywall передбачає низку технічних етапів, які забезпечують

безпеку, аналіз трафіку та збір інформації про загрози.

Honeywall зазвичай реалізується у вигляді програмно-апаратного комплексу або віртуального пристрою, що працює у мережевому середовищі.

Основні компоненти [60]:

– мережевий фільтр – виконує аналіз вхідного та вихідного трафіку.

– модуль ізоляції – забезпечує, щоб шкідлива активність залишалася в межах Honeypot і не поширювалася мережею.

– інструменти журналювання та логування – фіксують всі дії атакуючого для подальшого аналізу.

– модуль аналітики – аналізує зібрані дані для ідентифікації вразливостей та схем атак.

Honeywall може бути реалізований за допомогою наступних технологій [61]:

– Linux-платформи з інтеграцією модулів на основі iptables для фільтрації трафіку;

– контейнеризація (Docker, Kubernetes) для створення ізольованого середовища, яке легко масштабувати;

– мережеві монітори, такі як Snort або Suricata, які забезпечують аналіз мережевого трафіку.

Щоб уникнути компрометації самого Honeywall, важливо [60]:

– використовувати ізольоване середовище;

– захищати доступ до системи (використання SSH, двофакторної аутентифікації);

– регулярно оновлювати програмне забезпечення.

Honeywall дозволяє проводити моніторинг атак у режимі реального часу:

– перегляд підозрілих підключень;

– фіксація атакуючих IP-адрес;

– аналіз типів атак (використання експлойтів, методи перебору паролів тощо).

Honeywall може бути інтегрований із SIEM-системами, хмарними платформами безпеки або іншими засобами аналізу для зручності автоматизації

процесів.

На етапі розгортання необхідно перевірити, як Honeywall реагує на змодельовані атаки. Використовуються такі інструменти, як Metasploit або Nmap, для тестування ефективності системи.

Реалізація Honeywall потребує глибоких знань у сфері мережевої безпеки, але правильно налаштована система забезпечує ізоляцію загроз та надає цінну інформацію для вдосконалення захисних механізмів.

1.3.5 Технологія Honeydoc

Honeydoc – це інноваційна архітектура *Honeypot*-пасток для зловмисників , яка створена для вдосконалення захисту кіберсистем і збору розширених даних про атаки [62]. Її основна мета – зробити пастки більш переконливими для атакуючих, одночасно вирішуючи технічні та практичні проблеми, що виникають у класичних Honeypot-системах.

Для досягнення цієї мети в Honeydoc реалізовані інноваційні рішення [62, 63].

Honeydoc підтримує динамічний контроль за поведінкою атакуючих. Honeydoc інтегрує прозорі проксі, що дозволяє змінювати конфігурацію пастки в реальному часі. Це робить систему менш вразливою до виявлення і збільшує ймовірність збору детальної інформації про атаку.

В Honeydoc розв’язано проблему "ідентичного відбитка". Однією з основних проблем традиційних Honeypot є те, що зловмисники можуть розпізнати їх за унікальними відбитками-сигнатурами. Honeydoc використовує динамічне підлаштування, щоб замаскувати свої характеристики і зменшити ризик виявлення.

В Honeydoc наявна інтеграція з SDN (Software-Defined Networking). Використання SDN дозволяє гнучко управляти мережевими потоками, змінюючи поведінку пастки залежно від типу загрози. Це робить Honeydoc ефективним рішенням для динамічних середовищ.

Система підтримує розподілений підхід, де декілька вузлів Honeydoc працюють разом для збору даних про атаку. Це покращує масштабованість і дозволяє вивчати атаки в складних мережах.

У Honeydoc реалізовані автоматизовані механізми аналізу, які

використовують алгоритми машинного навчання та поведінкову аналітику. Ці інструменти дозволяють ідентифікувати нові види атак і генерувати докладні звіти про дії зловмисників.

Honeydoc забезпечує повну ізоляцію атакуючого від реальних систем. Використання контейнеризації (наприклад, Docker) дозволяє розгорнути пастку в окремому середовищі, яке повністю захищене від впливу атак.

У порівнянні з класичними Honeypot, Honeydoc спроєктований для оптимізації використання ресурсів. Завдяки розподіленій архітектурі і гнучким мережам, його можна ефективно впроваджувати навіть у малих організаціях[62].

Як особливі застосування Honeydoc, не властиві Honeypot, визначаються [64]:

– аналіз атак типу zero-day;
– дослідження нових видів експлойтів;
– виявлення ботнетів і вразливостей у реальних мережах;
– покращення засобів реагування на інциденти.

Honeydoc представляє собою значний крок уперед у технології Honeypot, надаючи інструменти для більш глибокого вивчення атак і захисту від сучасних кіберзагроз.

1.4 Постановка задачі

З проведеного аналізу можна зробити висновки, що корпоративна інформація є постійним об’єктом атак і має велику цінність. Захист корпоративної інформації вимагає комплексного підходу, виявлення та усунення слабких місць значно знижує ризики атак, допомагаючи створити надійну систему кіберзахисту, що відповідає сучасним вимогам та загрозам.

Мета кваліфікаційної роботи полягає у вдосконаленні і розширенні можливостей системи захисту корпоративної інформації за рахунок комплексного застосування можливостей технології Honeynet.

Щоб реалізувати програму досліджень необхідно:

а) дослідити можливості сучасних засобів реалізації технології Honeynet для організації системи захисту корпоративної інформації;

б) обґрунтувати вибір технології реалізації методу захисту корпоративної інформації;

в) визначити концепцію організації системи захисту корпоративної інформації на основі технології Honeynet;

г) запропонувати рішення щодо організації системи захисту корпоративної інформації на основі технології Honeynet;

д) обґрунтувати вибір платформи для практичної реалізації системи захисту корпоративної інформації на основі технології Honeynet;

є) розробити політики безпеки використання системи захисту корпоративної інформації на основі технології Honeynet.

2 ВИЗНАЧЕННЯ ТЕХНОЛОГІЙ РЕАЛІЗАЦІЇ МЕТОДУ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ

2.1 Класифікація технологій мережевих приманок

В першому розділі нами було здійснено огляд технологій мережевих приманок та їх характерних властивостей. Основною метою цього аналізу було визначення ефективності різних типів Honey-технологій для захисту корпоративної інформації. Наступним кроком є вибір конкретної технології для реалізації мережевих приманок та обґрунтування цього вибору.

При реалізації будь-якого наукового чи практичного проєкту завжди доцільно обирати прості, але ефективні рішення, які можуть забезпечити досягнення поставлених цілей. Такі рішення зазвичай є гнучкими, легко налаштовуються під конкретні потреби та дозволяють масштабувати проєкт за необхідності. Відповідно, аналітичне дослідження мережевих Honey-технологій і обґрунтування вибору базової технології реалізації методу захисту корпоративної інформації здійснимо не в історичному аспекті, а в порядку ускладнення Honey-технологій:

– Honeytoken;
– Honeypot;
– Honeywall;
– Honeynet;
– Honeydoc;
– Honeyfactory.

На рисунку 2.1 наведена ієрархічна схема класифікації Honey-технологій, реалізована на підставі здійснених аналітичних досліджень і класифікації зазначених технологій мережевих приманок.

Першим рівнем є Honeytoken. Це найпростіший тип мережевої приманки, який представляє собою фальшиві об’єкти, наприклад, підроблені файли, посилання, облікові дані або API-ключі. Вони використовуються для виявлення несанкціонованого доступу, оскільки будь-яка взаємодія з Honeytoken є підозрілою

і сигналізує про потенційну загрозу. Honeytoken часто впроваджують на реальних корпоративних ресурсах: робочих станціях, фізичних та програмно-реалізованих серверах, вебсайтах або в базах даних тощо. Їхньою перевагою є легкість впровадження, а також можливість інтеграції з існуючими системами безпеки.

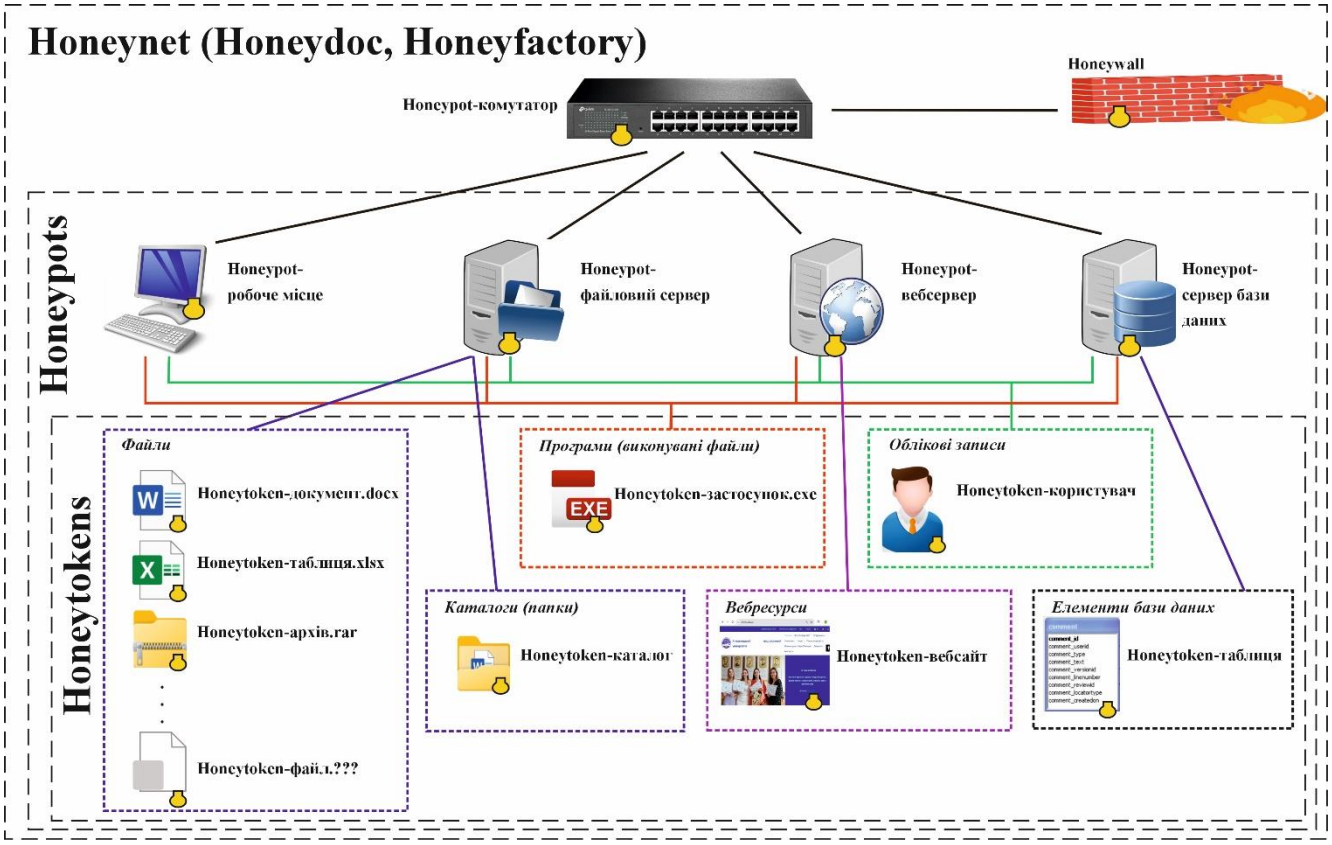

Рисунок 2.1 – Ієрархічна схема класифікації Honey-технологій

Другим рівнем є Honeypot. Це віртуальні або фізичні сервери, які імітують реальні мережеві вузли, щоб залучити зловмисників. Вони дозволяють не лише виявити атаки, але й отримати інформацію про методи атакуючих. Honeypot забезпечує більш складний рівень захисту, ніж Honeytoken, і є основою для побудови більш складних Honey-технологій. В реальній корпоративній мережі Honeypot можуть імітувати робочі станції, сервери або інші мережеві ресурси, а також можуть включати до свого складу різні види Honeytoken для створення ілюзії реального мережевого ресурсу.

Третім рівнем ускладнення є Honeywall. Це типовий елемент в складі

Honeynet. Honeywall використовується як інструмент для моніторингу трафіку між зловмисником і Honeypot, а також для управління цим трафіком. Honeywall може здійснювати фільтрацію та обмеження взаємодій, дозволяючи захищати основну інфраструктуру навіть у разі активної роботи зловмисників із Honeypot. Тобто, Honeywall вже є складовою не реальної корпоративної мережі, а мережі Honey-технологій. Honeywall розділяє простір Honeynet і простір корпоративної мережі, забезпечуючи захист ресурсів корпоративної мережі від атак і проникнення зловмисників з простору мережі приманок Honeynet.

Наступним повноформатним рівнем є рівень Honeynet. Honeynet є комплексною системою, що включає кілька взаємопов’язаних Honeypot-серверів, які створюють реалістичну імітацію мережі. Honeynet є потужним інструментом для аналізу загроз, оскільки дозволяє досліджувати дії зловмисників у складному мережевому середовищі. Така система ідеально підходить для захисту корпоративних мереж й інформації в них, де важливо відстежувати спроби проникнення і вивчати поведінку атакуючих.

Стосовно Honeynet слід відзначити, що існують вдосконалення цієї технології – Honeydoc і Honeyfactory.

Honeydoc спроєктований для оптимізації використання ресурсів. Завдяки розподіленій архітектурі і гнучким мережам, його можна ефективно впроваджувати навіть у малих організаціях. У Honeydoc реалізовані автоматизовані механізми аналізу, які використовують алгоритми машинного навчання та поведінкову аналітику. Ці інструменти дозволяють ідентифікувати нові види атак і генерувати докладні звіти про дії зловмисників. В Honeydoc розв’язано проблему "ідентичного відбитка" (типових сигнатур Honeypot). Honeydoc використовує динамічне підлаштування, щоб замаскувати свої характеристики і зменшити ризик виявлення.

Найвищим рівнем складності є HoneyFactory. Це системи, які генерують велику кількість різноманітних Honey-елементів, таких як Honeypot і Honeytoken й автоматично інтегрують їх у мережу. Вони надають масштабованість та ефективність у великих корпоративних системах.

2.2 Аналітичне дослідження і порівняльний аналіз можливостей технологій Honeytoken і Honeypot

Отже, Honeytoken є найпростішим представником з наведених Honey-технологій.

Проведений в попередньому розділі огляд публікацій про Honeytoken дозволяє зробити наступні висновки про цю технологію.

Honeytoken – це підроблений або «мітковий» об'єкт, такий як документ, файл, обліковий запис або дані, створений для ідентифікації несанкціонованого доступу чи використання. Він зазвичай не має фізичного чи мережевого компоненту, працюючи як пастка на рівні даних.

Призначення Honeytoken:

– виявлення витоків інформації або несанкціонованого доступу;

– виявлення і відстеження зловмисників, які намагаються викрасти або використовувати ці дані.

Приклади використання Honeytoken:

– вставка фальшивих даних у базу даних, щоб ідентифікувати зловмисників, які її сканують;

– використання підроблених облікових записів у хмарних службах для моніторингу спроб доступу.

Переваги Honeytoken:

– простота реалізації та низькі витрати;

– не потребує великих ресурсів чи складної інфраструктури.

Обмеження Honeytoken:

– застосовується лише для захисту даних або визначення точкових загроз;

– не взаємодіє з атакуючими, обмежуючи можливості для аналізу.

Наведені факти свідчать, що Honeytoken можуть використовуватись як елементи системи захисту корпоративної інформації, але не є самодостатньою технологією для створення ефективної системи відповідного призначення і не може бути основною в реалізації створюваного методу.

Наступним рівнем Honey-технологій є Honeypot. Аналітичне дослідження Honeypot дає такі висновки.

Honeypot – це фізична або віртуальна система, яка імітує реальний сервер, додаток або вразливу мережу, щоб привабити зловмисників і зафіксувати їхні дії. Це активна пастка, яка бере участь у взаємодії з атакуючими.

Призначення Honeypot:

– імітація конкретного активу (сервера, бази даних, веб-додатку);

– виявлення кіберзагроз;

– аналіз вразливостей системи;

– вивчення методів атак;

– збір інформації про поведінку зловмисників:

– відволікання уваги зловмисників від справжніх корпоративних інформаційних ресурсів.

Приклади використання Honeypot:

– імітація баз даних, веб-серверів або систем входу для виявлення вторгнень;

– елемент для створення реалістичних Honeynet.

Типи Honeypot :

– Low-interaction Honeypot – проста емуляція базових функцій;

– High-interaction Honeypot – складна симуляція, що максимально імітує реальну систему.

Функціональність Honeypot:

– працює як ізольований компонент;

– локальний захист або тестування окремих вразливостей;

– пропонує певні сервіси, які приваблюють зловмисників, наприклад, відкриті порти або фальшиві дані;

– взаємодіє з зловмисником для фіксації його дій;

– може бути низької (імітація лише деяких сервісів) або високої взаємодії (повноцінна симуляція реальних систем).

Приманки Honeypot із низьким рівнем взаємодії забезпечують зловмисників лише базовим доступом до системи. Вони зазвичай імітують лише початкові етапи

роботи певних протоколів, таких як HTTP, FTP або SSH, але не дозволяють розширеної взаємодії. Емуляція працює через прив'язку до окремих портів, імітуючи стандартні протоколи. Важливим аспектом є точність такої імітації, оскільки недостатній рівень деталізації може викликати підозру у зловмисників, змусивши їх припинити атаку. Завдяки своїй простоті та легкості у розгортанні, ці приманки часто використовують у великій кількості для обману атакуючих.

Honeypot із високим рівнем взаємодії є складнішими системами, які забезпечують повноцінну взаємодію. Вони працюють на основі реальних операційних систем і включають справжні сервіси, що робить їх привабливими цілями для зловмисників. Такі приманки оснащені спеціалізованими інструментами моніторингу, які відстежують всі взаємодії в системі. Це дозволяє отримати більш глибоку інформацію про методи атак і спостерігати за багатоступеневими загрозами. Завдяки реалістичності вони довше утримують увагу зловмисників, захищаючи реальні робочі системи від атак.

В таблиці 2.1 наведено дані порівняння Honeypot і Honeytoken.

Таблиця 2.1 – Аналітичне порівняння Honeypot і Honeytoken

Параметр	Honeytoken	Honeypot
Рівень реалізації	Логічний (дані)	Фізичний/віртуальний (система/мережа)
Ціль	Виявлення витоків даних	Аналіз загроз і поведінки зловмисників
Складність	Низька	Висока
Взаємодія	Пасивна	Активна
Область застосування	Захист даних	Захист інфраструктури та аналіз атак

Переваги Honeypot:

– надає детальну інформацію про дії атакуючих;

– може бути інтегрований у складні мережі.

Обмеження Honeypot:

– застосовується лише для моніторингу окремих загроз;

– не дає уявлення про взаємодію між компонентами мережі;

– вимагає значних ресурсів для розгортання та моніторингу;

– великий ризик того, що зловмисник зрозуміє, що система є приманкою.

Хоча технологія Honeypot і є значно потужнішою за Honeytoken, вона все ще не є самодостатньою для реалізації методу організації системи захисту корпоративної інформації.

2.3 Аналітичне дослідження і порівняльний аналіз можливостей технологій Honeywall і Honeypot

Окремим класом Honey-технологій є Honeywall. Аналітичне дослідження Honeywall дає такі висновки.

Honeywall – це спеціалізований шлюз для моніторингу та управління мережею Honeynet. Він виконує роль фільтруючого пристрою між Honeynet і зовнішнім середовищем.

Призначення Honeywall:

– контроль та ізоляція трафіку між Honeynet і мережею;

– запобігання витоку інформації з Honeynet у реальну мережу;

– логування та аналіз трафіку для розуміння тактики атакуючих.

Функціональність Honeywall:

– моніторинг всього трафіку до і з Honeynet;

– обмеження вихідного трафіку, щоб уникнути використання Honeynet для подальших атак;

– інструмент збору даних для аналізу безпечності мережі.

Особливості Honeywall:

– Honeywall є частиною проєкту Honeynet Project і часто використовується в поєднанні з Honeynet;

– підтримує різні рівні фільтрації трафіку, включаючи повну ізоляцію, модерацію або прозоре перенаправлення.

Обмеження Honeywall:

– фокусується лише на мережевому рівні, без можливості детального аналізу внутрішньої роботи системи.

– не працює як окремий засіб без Honeynet.

В таблиці 2.2 наведено дані порівняння Honeypot і Honeywall.

Таблиця 2.2 – Аналітичне порівняння Honeypot і Honeywall

Параметр	Honeypot	Honeywall
Призначення	Імітація системи для аналізу атак	Контроль і моніторинг трафіку Honeynet
Тип взаємодії	Активна взаємодія з атакуючим	Пасивний моніторинг і обмеження трафіку
Функціональність	Імітація серверів, додатків, мереж	Логування та ізоляція мережевого трафіку
Область застосування	Аналіз поведінки зловмисників	Забезпечення безпеки Honeynet

З даних таблиці 2.2 можна зробити висновок, Honeypot і Honeywall як інструменти є частиною стратегії кіберобману та використовуються для виявлення та аналізу загроз. Вони ефективні при роботі в комплексі: Honeypot створює середовище для атаки, а Honeywall контролює і фільтрує трафік, що надходить до цього середовища і з нього. Honeywall не є самодостатньою технологією, а застосовується разом з Honeypot як складова технології Honeynet і відокремлено не може бути базою методу організації системи захисту корпоративної інформації.

2.4 Аналітичне дослідження і порівняльний аналіз можливостей технологій Honeynet і Honeypot

Наступним рівнем Honey-технологій є Honeynet. Аналітичне дослідження Honeynet дає такі висновки.

Honeynet – це мережа, що складається з кількох Honeypot, які працюють разом для імітації реального корпоративного середовища або складної інфраструктури. Honeynet може включати імітовані сервери, додатки та інші компоненти корпоративної мережі.

Призначення Honeynet:

– створення повноцінної мережевої архітектури для вивчення складних атак;

– виявлення складних загроз та аналіз атак на взаємодію між системами в мережі;

– дозволяє аналізувати атаки, які зачіпають взаємодію різних систем.

Особливості Honeynet:

– акцент на моделюванні повноцінної мережевої структури;

– зазвичай включає високовзаємодіючі Honeypot, які максимально імітують справжню систему.

Функціональність Honeynet:

– Honeynet є комплексною системою, яка включає інструменти моніторингу, ізоляції трафіку (наприклад, Honeywall) і аналітики;

– здатна взаємодіяти із зловмисниками в реальному часі та збирати багатошарові дані.

Архітектура Honeynet:

– складається з фізичних чи віртуальних серверів і мережевих компонентів;

– використовує інструменти моніторингу, такі як Honeywall, для аналізу трафіку та ізоляції системи.

Переваги Honeynet:

– підходить для дослідження взаємодій між різними частинами мережі;

– допомагає виявляти комплексні багатошарові атаки;

– може бути інтегрована з традиційними мережевими системами.

Область застосування Honeynet:

– дослідження складних атак, таких як атаки на корпоративні або промислові мережі (SCADA, IoT);

– у великих організаціях;

– для наукових досліджень.

Обмеження Honeynet:

– високі витрати на налаштування та підтримку;

– вимагає значних технічних ресурсів і кваліфікованого персоналу.

В таблиці 2.3 наведено дані порівняння Honeypot і Honeynet.

Таблиця 2.3 – Аналітичне порівняння Honeypot і Honeynet

Параметр	Honeypot	Honeynet
Складність	Мережевий компонент	Складна мережа з кількома компонентами
Призначення	Локальний моніторинг загроз	Аналіз складних атак на рівні мережі
Область	Захист окремих серверів чи додатків	Дослідження атак на інфраструктуру
Функціональність	Ізольована система	Взаємодія між декількома системами
Тип загроз	Точкові атаки	Комплексні атаки на мережеві середовища

З проведеного аналізу і за даними таблиці 2.3 можна зробити висновки, що Honeynet є самодостатньою технологією для організації системи захисту корпоративної інформації на основі Honey-технологій.

2.5 Аналітичне дослідження і порівняльний аналіз можливостей технологій Honeynet, Honeydoc і Honeyfactory

Наступним рівнем і представником Honey-технологій в нашому переліку є Honeydoc. Аналітичне дослідження Honeydoc дає такі висновки.

В Honeydoc наявна інтеграція з SDN (Software-Defined Networking). Використання SDN дозволяє гнучко управляти мережевими потоками, змінюючи поведінку пастки залежно від типу загрози. Це робить Honeydoc ефективним рішенням для динамічних середовищ.

Система підтримує розподілений підхід, де декілька вузлів Honeydoc працюють разом для збору даних про атаку. Це покращує масштабованість і дозволяє вивчати атаки в складних мережах.

Honeydoc забезпечує повну ізоляцію атакуючого від реальних систем і підтримує динамічний контроль за поведінкою атакуючих. Honeydoc інтегрує прозорі проксі, що дозволяє змінювати конфігурацію пастки в реальному часі. Це робить систему менш вразливою до виявлення і збільшує ймовірність збору детальної інформації про атаку. Використання контейнеризації (наприклад, Docker) дозволяє розгорнути пастку в окремому середовищі, яке повністю захищене від впливу атак.

Слід відзначити неоднозначність і малу розповсюдженість терміну Honeydoc. В роботі [57] як Honeydoc розглядаються Honeytoken – файли docx, тобто назва визначена з розширення Honeytoken-файлу. У роботах [62, 63] Honeydoc розглядається як інноваційні рішення і вдосконалення Honeynet, а сам термін Honeydoc в цьому варіанті може походити від використання засобу контейнеризації Docker.

Більш розповсюдженим і однозначним терміном інноваційної Honeynet є Honeyfactory.

Honeyfactory та Honeynet представляють дві концепції в області кібербезпеки, пов’язані з технологією Honeypot, проте вони мають різні рівні складності, структури та підходи до реалізації. Архітектура Honeyfactory є

важливим кроком у розвитку технологій кіберобману (зокрема, Honeynet), що адаптуються до складних умов сучасної кібербезпеки.

Honeyfactory – це сучасна архітектура Honeynet, яка використовує контейнеризацію для створення гнучких і масштабованих мереж кіберобману. Вона була розроблена для підвищення ефективності виявлення та аналізу складних кібератак у сучасних мережах, спрямована на моделювання складних мережевих середовищ із використанням сучасних технологій. Основна ідея полягає в імітації мережі, яка виглядає як реальне корпоративне середовище, але призначена для збору інформації про поведінку зловмисників.

Архітектура Honeyfactory:

– базується на контейнерах (наприклад, Docker), що імітують різні компоненти мережі;

– містить модулі для автоматизації, управління, збору даних і моніторингу загроз.

Архітектура дозволяє симулювати багатошарові атаки на мережі, які охоплюють різні сегменти, зокрема хмарні сервіси, IoT і традиційні корпоративні системи.

Honeyfactory складається з декількох модулів, які працюють разом для забезпечення повної емуляції мережі. Це включає:

– відстеження трафіку;

– моніторинг взаємодій зловмисників;

– автоматичне відновлення систем після атак;

– моделювання складних атак:

Зібрані дані про атаки використовуються для вдосконалення захисту реальних мереж. Honeyfactory також підтримує використання прихованих Марківських моделей для аналізу обману.

Honeyfactory використовується для:

– тестування та вдосконалення систем кіберзахисту.

– вивчення поведінки зловмисників у реальних умовах.

– аналізу нових методів атак для запобігання загрозам.

Особливості Honeyfactory:

– гнучкість у створенні складних мереж із низькими витратами;

– використовує приховані Марківські моделі для аналізу поведінки зловмисників;

– підтримує хмарні сервіси, IoT та програмно-визначені мережі (SDN).

Переваги Honeyfactory відносно Honeynet:

– більш економічна та адаптована до сучасних умов кібербезпеки;

– легко масштабується завдяки контейнеризації;

– легко налаштовується під конкретні потреби організації;

– може імітувати як прості системи, так і складні корпоративні мережі;

– забезпечує раннє виявлення та аналіз нових видів атак;

– можливість швидкого відновлення після компрометації систем;

– низька затримка зв’язку та висока швидкість обробки трафіку.

Обмеження:

– вимагає високого рівня технічної експертизи для налаштування;

– орієнтована на використання сучасних технологій, що може бути складним для традиційних мереж.

Використання технологій контейнерів (наприклад, Docker) дозволяє створювати окремі віртуальні системи, які імітують різні сервіси й ресурси корпоративної мережі. Кожен контейнер може бути окремим Honeypot із власними параметрами. Завдяки контейнерній архітектурі Honeyfactory має високу продуктивність, забезпечуючи низьку затримку зв’язку і високу швидкість обробки трафіку.

В таблиці 2.4 наведено дані порівняння Honeyfactory і Honeynet.

З проведеного аналізу і за даними таблиці 2.4 можна зробити висновки, що Honeyfactory є більш сучасною та гнучкою реалізацією Honeynet, орієнтованою на сучасні технології та вимоги кібербезпеки, але Honeynet, у свою чергу, забезпечує глибший аналіз взаємодій, хоча є менш адаптивною для новітніх технологічних платформ.

Таблиця 2.4 – Аналітичне порівняння Honeyfactory і Honeynet

Параметр	Honeyfactory	Honeynet
1	2	3
Суть	Сучасна архітектура Honeynet, яка використовує контейнеризацію для побудови мереж кіберобману	Мережа Honeypot, що імітує корпоративну інфраструктуру для аналізу атак та поведінки зловмисників
Основне призначення	Дослідження та швидке реагування	Дослідження складних атак
Мета	Розширене виявлення складних атак через динамічну контейнеризацію та гнучке моделювання мереж	Виявлення атак та вивчення взаємодії зловмисників з імітованою мережею
Архітектура	Контейнерна, сучасна архітектура. Використовує контейнеризацію (Docker тощо), яка дозволяє створювати модульні та гнучкі систем	Традиційна мережа Honeypot. Базується на віртуальних машинах або фізичних системах Honeypot
Технології	Контейнери, HMM, SDN	Фізичні та віртуальні сервери
Адаптивність	Легко адаптується під сучасні вимоги	Менш гнучка
Масштабованість	Висока. Легко масштабована завдяки використанню контейнерів	Обмежена масштабованість через складнощі управління фізичними чи віртуальними Honeypot

Кінець таблиці 2.4

Параметр	Honeyfactory	Honeynet
Глибина взаємодії	Підтримує як низько-, так і високорівневу взаємодію з атакуючими	Зазвичай реалізує високорівневу взаємодію, але може бути менш адаптивною.
Моніторинг трафіку	Підтримує сучасні інструменти аналізу та ізоляції трафіку для виявлення атак	Включає інструменти моніторингу, такі як Honeywall, але може бути менш інтегрованою з новими технологіями
Автоматизація	Висока. Honeyfactory підтримує автоматичне налаштування мереж і швидке відновлення після атак	Менша автоматизація. Потрібні значні ручні налаштування для управління мережею
Типи загроз	Орієнтована на складні загрози, включаючи атаки на IoT, хмарні мережі та SCADA-системи	Підходить для класичних атак, таких як злом серверів, баз даних та інших мережевих ресурсів
Галузі використання	Підходить для великих інфраструктур, включаючи хмарні середовища, IoT та промислові мережі	Частіше застосовується для локальних або корпоратив-них мереж стандартного рівня складності
Використання в дослідженнях	Застосовується для глибокого аналізу багатошарових атак	Використовується для накопичення даних і їх подальшого аналізу
Ціна	Низька завдяки контейнеризації	Висока

На користь використання Honeynet в даній роботі свідчить наявність великої кількості платформ реалізації мережевих приманок, що можуть бути ефективно використані при реалізації методу організації системи захисту корпоративної інформації на основі технології Honeynet.

2.6 Висновки

Обираючи технологію реалізації мережевих приманок, необхідно враховувати специфіку корпоративної мережі, її розмір, рівень загроз і наявність ресурсів для впровадження та підтримки. Найбільш оптимальним вибором для комплексного захисту є Honeynet, оскільки вона забезпечує високий рівень інтерактивності, дозволяє детально аналізувати дії зловмисників і надає широкі можливості для дослідження методів атак. Водночас, для розширення можливостей Honeynet доцільно інтегрувати Honeytoken як додаткові компоненти, що забезпечують виявлення витоків даних та спроби компрометації облікових даних.

Комплексне впровадження технологій Honeynet з Honeypot, доповнене Honeytoken, дозволяє створити багаторівневу систему захисту корпоративної інформації, яка ефективно протидіє сучасним кіберзагрозам і сприяє підвищенню загальної кіберстійкості організації.

3 ОРГАНІЗАЦІЯ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ТЕХНОЛОГІЇ HONEYNET

У сучасних умовах масштабної цифровізації всіх сфер життя та бізнесу кількість кібератак на корпоративні інформаційні системи невпинно зростає. Це пов’язано зі зростанням обсягу й цінності даних, які компанії зберігають і обробляють[1]. Сучасні кібератаки стають дедалі витонченішими: багато з них організовуються злочинними угрупуваннями або навіть підтримуються державними структурами, що ускладнює їх виявлення та нейтралізацію. З кожним новим вектором атак ризики для компаній підвищуються [1,2]. Неналежний рівень захисту може призвести до втрати даних, значних фінансових збитків та пошкодження репутації [1,3].

Для ефективної організації системи захисту корпоративної інформації на основі будь-якої технології включно із Honeynet необхідно дослідити об’єкт захисту, тобто, визначити основні складові корпоративних інформаційних систем і наявні типові загрози для цих складових. За результатами такого аналізу визначаються вимоги щодо організації і функціональних можливостей системи захисту корпоративної інформації.

Проведений аналіз складових цифрових технологій корпоративного середовища обробки і підтримки інформації дозволяє в загальному декомпонувати їх на три види підсистем:

– класичні інформаційні технології корпорації (тобто, сама корпоративна інформаційна система або ж корпоративна комп’ютерна мережа з усіма її складовими);

– корпоративні інтернет-ресурси (вебзастосунки з усіма їх складовими та засобами підтримки);

– корпоративні системи моніторингу технологічних процесів і оперативного управління (SCADA-системи).

Відповідну організацію ,інформаційної системи ілюструє рисунок 3.1.

Рисунок 3.1 – Складові сучасної корпоративної інформаційної системи

Для забезпечення комплексного підходу в реалізації системи захисту корпоративної інформації на основі технології Honeynet нам потрібно проаналізувати і визначити принципи застосування зазначеної технології у захисті всіх трьох підсистем.

3.1 Організація системи захисту корпоративної інформації на основі технології Honeynet для протидії атакам на мережеві ресурси

Атаки на корпоративні мережеві ресурси з метою заволодіння цінною інформацією або нанесення шкоди володільцю (розпоряднику тощо) інформації через втрату цілісності або доступності критично важливої інформації є сьогодні надзвичайно розповсюдженими і різноманітними.

Загальний огляд і класифікація атак на корпоративні інформаційні ресурси здійснені в першому розділі цієї кваліфікаційної роботи, тому повертатися до аналізу всіх можливих атак не будемо. У першому розділі зроблено висновок, що різних видів атак є дуже багато і вони весь час оновлюються, тому розглянути детально протидію кожній зловмисній технології в межах однієї роботи не вийде. Крім того, більшість платформ Honeynet орієнтовані на типові атаки і їх впровадження в типових конфігураціях за рекомендаціями розробника автоматично знімає питання налаштування пасток, оскільки діє принцип «встановлюй і використовуй».

Зупинимось на визначенні принципів організації системи захисту корпоративної інформації на основі технології Honeynet для протидії найскладнішим атакам на мережеві ресурси, які розглядалися в першому розділі і потребують розгортання Honeynet з урахуванням саме специфіки цих атак. Такі атаки здійснюються з використанням зловмисного програмного забезпечення, є тривалими і замаскованими, не містять характерних ознак дій людини-зловмисника, а тому виявлення подібних атак є найскладнішим.

Отже, здійснюємо організацію системи захисту корпоративної інформації на основі технології Honeynet для протидії атакам програм-вимагачів та розширеної постійної загрози (APT).

3.1.1 Організація системи Honeynet для захисту корпоративної інформації від атак програм-вимагачів (Ransomware-атак)

Ransomware-атаки або атаки програм-вимагачів (WannaCry, Petya, REvil, NotPetya тощо [30]) блокують доступ до файлів компанії, вимагаючи викуп за їх розблокування. Програми-вимагачі не мають за мету нанесення удару по цілісності інформації, адже лише за збережену інформацію можна отримати викуп. Акцент робиться саме на втраті доступності.

Прості Ransomware-атаки здійснюються через блокування доступу на рівні операційної системи або носіїв інформації, вони орієнтовані на малодосвідчених користувачів інформаційних технологій, їх наслідки легко усуваються фахівцями відділів підтримки інформаційних ресурсів компанії.

Але атаки програм-вимагачів стають дедалі складнішими, здатними атакувати резервні копії даних і навіть шифрувати цілі системи, залишаючи компанію без критичної інформації. Вимагач використовує складні алгоритми шифрування (наприклад, AES або RSA), щоб заблокувати доступ до файлів користувача. Розшифрування криптографічно закритих даних може займати час, не сумісний з потребами володільця інформації. Крім того, існують атаки програм-вимагачів, які не є класичними і знищують цілісність інформації не передбачаючи її відновлення навіть після отримання викупу (NotPetya [30]). Саме на протидію таким атакам, які шифрують або руйнують файли даних,

орієнтуємо нашу Honeynet систему захисту корпоративної інформації.

Для виявлення та аналізу програм-вимагачів Honeynet має бути налаштована як мережа із цілеспрямованими вразливостями, які провокують програм-вимагачів використовувати свої інструменти для атак.

Першочергово доцільно зробити в мережі компанії «темний простір», в якому розгортається мережа Honeynet з усіма її елементами: серверами, робочими станціями, файловою структурою та сховищами даних тощо.

Темний простір (Dark Space) – це частина корпоративного IP-адресного простору, яка не використовується в реальній корпоративній мережі . Вона є видимою для зовнішніх зловмисників, але приховується для легітимних користувачів і будь-який трафік до таких адрес зазвичай свідчить про сканування, помилкову конфігурацію або зловмисну активність.

Темний простір може бути використаний у великих масштабах, що дає змогу створювати реалістичні і складні Honeynet для збору детальних даних. Темний простір дозволяє виявити спроби сканування портів, ботнет-активність або атаки з використанням відомих експлойтів.

В рамках темного простору нам потрібно розгорнути Honeynet – мережу Honeypot, яка буде виглядати як корпоративна чи критично важлива інфраструктура. Це дозволить спостерігати за складними багатоступеневими атаками, що включають сканування, експлуатацію вразливостей та злом систем.

Уся активність у темному просторі фіксується. Це може бути корисним для дослідження різних типів атак, вивчення поведінки ботнетів чи виявлення автоматизованих атак та атак програм-вимагачів.

Наприклад, у великій організації може бути виділений діапазон IP-адрес у темному просторі, де розгортається Honeynet, яка імітує вебсервери, бази даних із фальшивими даними, SCADA-системи або IoT-пристрої тощо.

Розгортання темного простору Honeynet може здійснюватися на різноманітних платформах і широко презентоване в багатьох роботах.

Для відсікання темного простору від реальної корпоративної мережі можуть використовуватись Fierwall, Honeywall відокремлені сервери керування

та VPN-тунелі для передачі даних.

Водночас, темний простір не є панацеєю від програм вимагачів, а, швидше, використовується як інструмент виявлення різноманітних відомих атак і додатковий полігон для виявлення програм-вимагачів.

Темний простір не може гарантувати, що зловмисне програмне забезпечення поширилось лише в його межах або взагалі не проігнорувало розгорнуту в ньому Honeynet, і не проникло в реальну корпоративну мережу.

,Отже, протидію для програм-вимагачів необхідно реалізувати реальній корпоративній мережі компанії.

Мішенями програм-вимагачів є документи, бази даних, фото та навіть резервні копії таких файлів, тому об’єкт-приманку слід обирати з цієї категорії, а краще реалізувати декілька типів приманок. Як було визначено в огляді-аналізі технологій мережевих приманок, об’єкт-приманку такого типу класифікують як Honeytoken.

Одним із підходів до виявлення програм-вимагачів є створення спільного файлу в мережі, який містить фіктивні дані. Цей Honeytoken-файл (а краще – Honeytoken-файли) приховується від користувачів, але зіставляється з усіма клієнтськими пристроями, щоб збільшити ймовірність виявлення атак програм-вимагачів, коли вони намагаються зашифрувати новий ресурс.

Пропоноване рішення для захисту корпоративної інформації від програм-вимагачів з використанням Honeytoken-файлу як складової у Honeynet-технології представлене на рисунку 3.3 .

Таке «фальшиве» мережеве сховище Honeytoken можна реалізувати з допомогою сервісів Samba на хості з Linux, налаштувавши файл samba.conf для ввімкнення модуля повного аудиту, або у Windows, використовуючи політику аудиту файлової системи в налаштуваннях локальної безпеки.

Схема ілюструє заходи для виявлення та протидії атакам програм-вимагачів, які шифрують файли та вимагають викуп. Основний підхід базується на використанні Honeytoken-файлів як пасток для зловмисників та моніторингу активності у файловій системі.

,

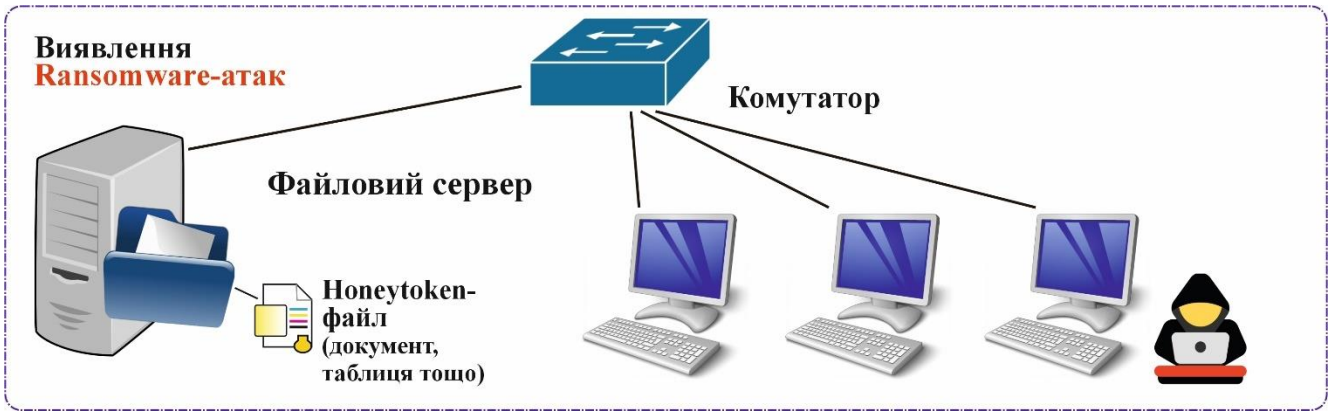

Рисунок 3.3 – Організація захисту від програм-вимагачів у Honeynet корпоративної мережі

Для зменшення кількості зареєстрованих подій доступу до Honeytoken-файлу слід конфігурувати таким чином, щоб фокусуватися лише на операціях запису, які є обов'язковими після внесення змін у файл (його шифрування тощо). Це дозволяє виявляти активність програм-вимагачів, які, зазвичай, шифрують десятки файлів одночасно. Також доцільно зробити цей файл прихованим від легітимних користувачів, хоча заборона на доступ до невідомих файлів і внесення змін в них повинна бути передбачена політикою безпеки.

Файловий сервер в схемі є центральним сховище корпоративних файлів, яке стає основною мішенню програм-вимагачів.

Сервер містить як реальні дані, так і спеціально створені Honeytoken-файли, що використовуються для виявлення загроз.

Honeytoken-файли (файли-пастки) які виглядають як цінна інформація (наприклад, документи, таблиці з конфіденційними даними), але створені виключно для виявлення спроб несанкціонованого доступу або шифрування. Спроба шифрування чи модифікації таких файлів при записі змін у файл одразу генерує сигнал тривоги, що дозволяє виявити дії програм-вимагачів, які шифрують файли, або іншого зловмисника ще на ранньому етапі атаки.

На схемі зображено зловмисника, який використовує програму-вимагача для шифрування файлів на сервері та вимагання викупу. Потенційним вектором атаки через соціальну інженерію (фішинг) або використання уразливостей є реальні

користувачі (їхні дії логуються та аналізуються для виявлення підозрілої активності). Програма-вимагач часто поширюється через заражені електронні листи, шкідливі посилання або незахищені мережеві ресурси.

Комутатор забезпечує зв’язок між файловим сервером та користувачами, може використовуватися для моніторингу трафіку та виявлення аномальної активності, пов’язаної з великим обсягом змін файлів, характерним для атак програм-вимагачів. Мережевий комутатор може допомогти обмежити доступ підозрілого пристрою до інших ресурсів мережі.

Honeytoken-файли розміщуються у важливих каталогах файлового сервера. Система виявлення загроз (наприклад, SIEM або спеціалізовані інструменти моніторингу) відстежує операції із файлами на сервері. Будь-яка спроба зчитування, модифікації чи шифрування цих файлів автоматично фіксується як підозріла активність.

Підозріла активність як масове шифрування файлів, одразу блокується. Якщо Honeytoken-файл зазнає змін, сервер негайно відключає користувача чи пристрій, що ініціював операцію, для запобігання подальшому поширенню атаки. Ізоляція підозрілого пристрою запобігає поширенню шкідливого ПЗ по всій мережі.

Уся підозріла активність детально фіксується для подальшого аналізу. Ці дані використовуються для покращення правил захисту та виявлення атак. Усі операції фіксуються та передаються до центральної системи моніторингу для візуалізації.

Такий підхід дозволяє реалізувати:

– реєстрацію активності на рівні файлових операцій;

– моніторинг змін у файловій системі;

– фіксацію операцій читання й запису, що здійснюються на мережевих ресурсах.

– виявлення активності програм-вимагачів, коли вони починають шифрувати (змінювати, пошкоджувати) файли.

Зазначимо, що пропонована стратегія є одним із способів підвищення безпеки та оперативного виявлення загроз, хоча ефективної профілактики програм-

вимагачів поки не існує. Діяльність програм-вимагачів можна зафіксувати лише після початку шифрування.

3.1.2 Організація системи Honeynet для захисту корпоративної інформації від розширеної постійної загрози (APT-атак)

Ймовірно, APT сьогодні є однією з найсерйозніших загроз для компаній і їхніх критично важливих активів. APT не лише тривалий час залишаються непоміченими в мережі, але й активно збирають інформацію про її структуру та топологію, готуючись до подальшого бокового переміщення. APT можуть залишатися у системі протягом значного часу, перш ніж досягнуть своєї мети – викрадення цінних даних або порушення роботи мережі.

Виявлення таких дій є критично важливим для запобігання подальшому поширенню загрози та мінімізації шкоди, завданої мережею APT. Оскільки APT в мережі надзвичайно небезпечні, то дуже важливо виявити їх присутність якомога швидше.

Пропонований сценарій виявлення зосереджений на моменті, коли APT починають рухатися мережею, переміщуючи облікові дані користувачів між клієнтськими машинами. Ці облікові дані не співвідносяться з реальними обліковими записами у домені, що є ключовою ознакою компрометації. На клієнтських машинах з операційною системою Windows зловмисники часто зчитують збережені облікові дані з процесу LSASS (Local Security Authority Subsystem Service) і використовують їх для автентифікації. Цей метод, відомий як «передача хешу» (Pass-the-Hash), є одним із найбільш поширених способів бокового руху в скомпрометованих мережах. У цьому сценарії передбачається, що зловмисник вже проникнув в одну з машин і встановив бекдор для збереження доступу.

На рисунку 3.3 представлена схема розміщення Honeytoken у корпоративній мережі як елемента організації системи захисту корпоративної інформації на основі технології Honeynet.

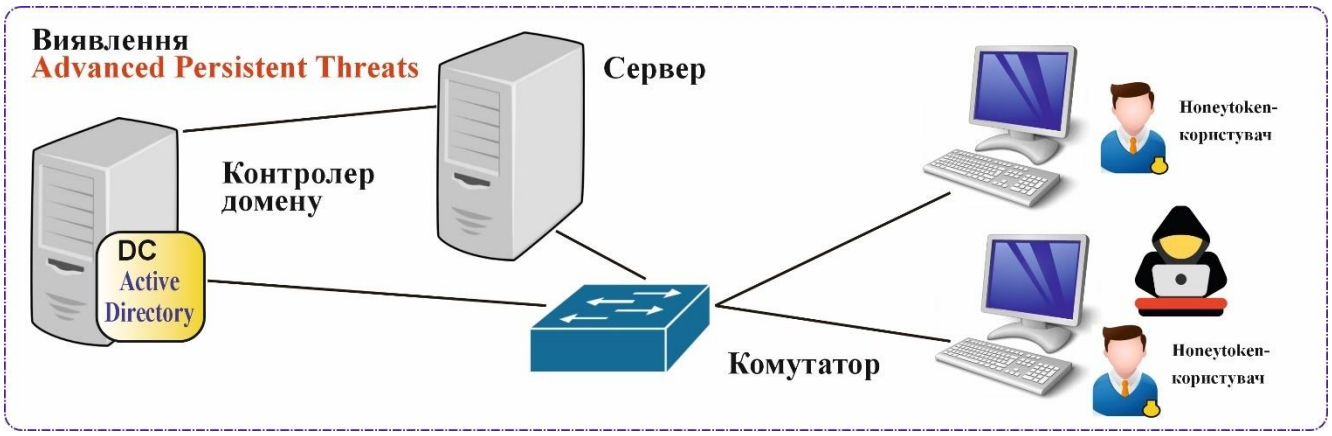

Рисунок 3.3 – Організація захисту від APT-атак у Honeynet корпоративної мережі

Ця схема демонструє, як використання сучасних технологій захисту (зокрема, Honeytoken) може забезпечити ефективне виявлення та нейтралізацію розширених постійних загроз для корпоративної інформаційної системи. Система захисту побудована на основі контролю доменної інфраструктури, інтеграції Honeytokens та відстеження аномальної активності.

Honeytoken створюють пастки для атакуючих. Honeytoken створюються у вигляді облікових записів користувачів, які не мають реальних функцій, але виглядають привабливими для зловмисників (наприклад, облікові записи з правами адміністратора чи доступом до конфіденційних корпоративних інформаційних ресурсів). Наприклад, облікові записи з іменами, які виглядають цінними для зловмисника ("admin_backup" або "HR_secrets" тощо). Будь-яка спроба взаємодії з такими обліковими записами сигналізує про потенційне проникнення до мережі, а будь-яка спроба авторизації чи доступу з допомогою цих облікових записів реєструється як потенційна загроза APT.

Контролер домену (DC Active Directory) відповідає за аутентифікацію та авторизацію користувачів у корпоративній мережі. Контролер домену дозволяє централізовано керувати політиками доступу.

Серед інших механізмів безпеки, як інструмент для виявлення APT-атак в мережі розглядається Honeynet-приманка середнього рівня взаємодії OpenCanary. OpenCanary має достатні потужності для виявлення фази вторгнення та експлуатації APT, виявлення аномального руху в мережевому просторі.

Розглянемо сценарій використання Honeynet користувача OpenCanary.

Для виявлення APT пропонується використовувати мережу, побудовану на основі Active Directory, яка включає щонайменше один контролер домену. Контролер домену виконує автентифікацію користувачів у домені, використовуючи орієнтований на клієнт-серверну архітектуру мережевий протокол Kerberos. Клієнтські машини в мережі мають можливість підключатися до контролера домену, отримуючи доступ до спільних ресурсів, таких як файли та сервери.

Для моніторингу та виявлення загроз APT створюється спеціальний обліковий запис користувача OpenCanary, дані якого розповсюджуються на всі клієнтські машини мережі. У домені Windows це можна зробити за допомогою команди: runas /user:<Domain>\<User>. Ця команда надсилає хеш-комбінацію «ім'я користувача»+NTLM у пам’ять, не підключаючись до контролера домену.

Відстеження використання облікового запису OpenCanary потребує налаштування аудиту подій входу в систему через політику домену. Це включає увімкнення аудиту подій входу та фільтрацію помилок у подіях входу (подія #533).

Журнали подій контролера домену передаються на центральний сервер для централізованого моніторингу. Синтаксичний аналізатор файлу журналу збирає події аудиту, пов’язані з помилками, і передає їх через протокол Hpfeeds. Відповідний канал Hpfeeds має бути підписаний центральним сервером керування.

Якщо зловмисник застосовує інструменти для отримання хешів, наприклад, Mimikatz, облікові дані користувача OpenCanary можуть бути зчитані та використані для атаки. У випадку їх використання для автентифікації, центральний інтерфейс повинен:

– відображати IP-адресу або ім’я хоста скомпрометованої машини;
– показувати IP-адресу, до якої відбувається рух бокового доступу;
– візуалізувати використаний NTLM-хеш і відповідне ім’я користувача.

Інформація, зібрана системою Honeynet, передається оператору. Він аналізує дані для визначення джерела компрометації та сценаріїв руху APT у мережі. Отримані дані використовуються для ініціювання роботи групи реагування на

інциденти (CERT), яка досліджує, яким чином зловмисник проникнув у мережу, та запобігає подальшому поширенню загрози.

3.2 Організація системи захисту корпоративних вебзастосунків на основі технології Honeynet

Сьогодні кожна велика фірма або компанія має потребу бути представленою в Інтернеті. Презентувати компанію може окремий статичний вебзастосунок або динамічний вебресурс з необхідною інформацією та сервісами.

Публічні корпоративні домени вебзастосунків є доступними всім бажаючим, а тому стикаються щоденно з значною кількістю атак. Оскільки публічні корпоративні домени легкодоступні, вони потребують якісної ізоляції від інших ресурсів мережі для запобігання намірам можливих зловмисників скомпрометувати корпоративну мережу загалом.

Застосування методу захисту корпоративної інформації на основі технології Honeynet для захисту корпоративних вебзастосунків має за мету реєстрацію і подальший аналіз атак щоб сформувати уявлення про те, яким чином зловмисники намагаються скомпрометувати ресурси корпоративної мережі, які є доступними із Інтернету, і щоб потім виявити та усунути вади організації системи захисту корпоративних вебзастосунків.

На нашу думку, кращу ізоляцію хибних корпоративних вебзастосунків Honeynet можна досягти, помістивши вебзастосунок-приманку в демілітаризовану зону.

Демілітаризована зона є сегментом мережі, ізольованим від внутрішньої корпоративної мережі організації. Ця зона слугує буфером для захисту внутрішніх ресурсів від зовнішніх атак, забезпечуючи безпечний доступ до публічних сервісів, таких як вебзастосунки чи поштові сервери. Використання демілітаризованої зони у поєднанні з технологіями Honeynet створює додатковий рівень безпеки для виявлення та аналізу потенційних загроз.

Якщо вебсервери, що надають послуги вебзастосунків для зовнішніх

користувачів, розміщуються до демілітаризованої зони, то це дозволяє ізолювати їх від основної корпоративної мережі, знижуючи ризики отримання доступу зловмисників до корпоративної інформації. Трафік між Інтернетом, демілітаризованою зоною і внутрішньою мережею контролюється міжмережевими екранами. Це дозволяє обмежити доступ до певних портів і протоколів, що використовуються вебзастосунками.

У разі компрометації серверів у демілітаризованій зоні зловмисники не отримають доступу до інформації і ресурсів внутрішньої корпоративної мережі.

Honeynet у демілітаризованій зоні слугує додатковим інструментом для моніторингу та аналізу дій зловмисників. Основна ідея – створити приманку, яка виглядає як критичний сервіс або частина вебзастосунку, але насправді служить виключно для виявлення та вивчення атак.

У демілітаризованій зоні розгортають Honeypot або Honeynet, які імітують реальні вебсервери чи інтерфейси API, що дозволяє притягувати увагу зловмисників до Honey-приманки та відволікати від справжніх серверів, а головне – накопичувати інформацію про дії зловмисників і вивчати її, адже спеціалізовані інструменти в Honeynet записують усі дії зловмисників, такі як спроби сканування портів, ін'єкції SQL або експлуатація відомих вразливостей вебзастосунків.

На рисунку 3.4 представлена схема розміщення Honeynet у демілітаризованій зоні як елемента організації системи захисту корпоративної інформації на основі технології Honeynet.

Honeynet, представлений на схемі, є багатокомпонентною системою, організованою для виявлення, аналізу та протидії атакам на корпоративні вебзастосунки. Основною метою цієї Honeynet є створення інтерактивного середовища, яке привертає увагу потенційних зловмисників, дозволяючи фіксувати їх дії та мінімізувати ризики для реальних ресурсів компанії.

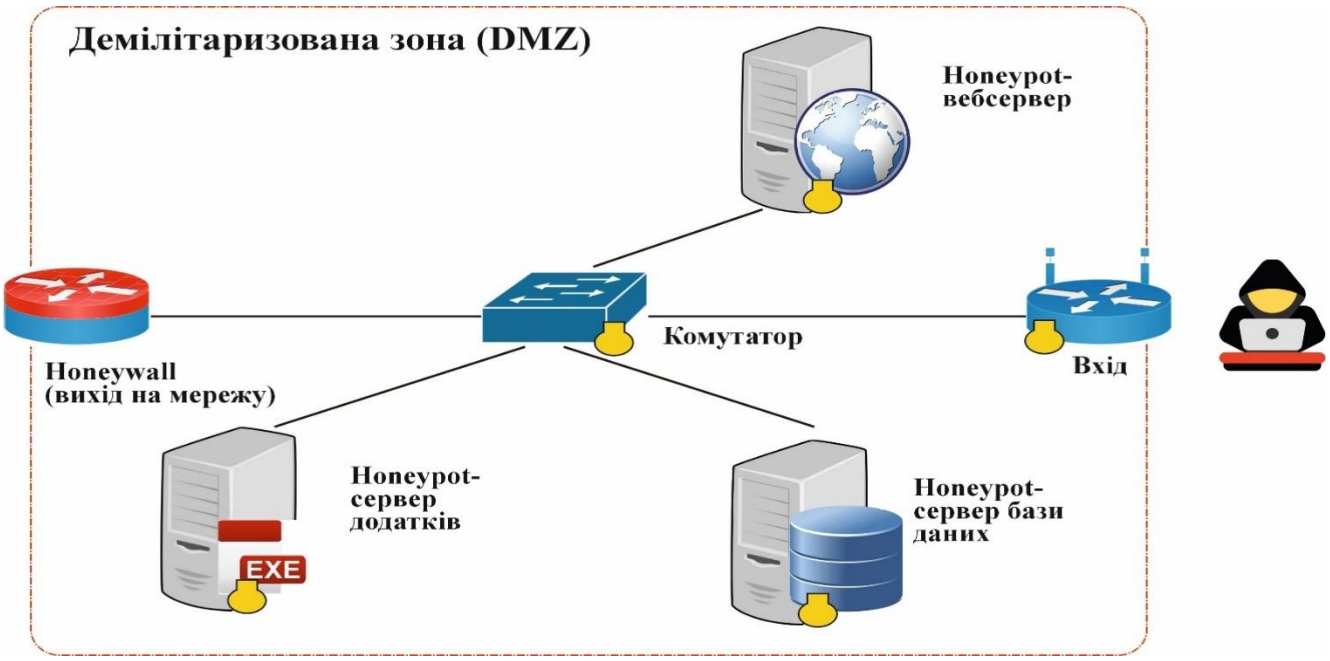

Рисунок 3.4 – Honeynet у демілітаризованій зоні для організації системи захисту інформації корпоративних вебзастосунків

Honeynet розташована в демілітаризованій зоні (DMZ), яка відокремлює зовнішню мережу від внутрішньої корпоративної інфраструктури. Це забезпечує безпеку реальних систем навіть у разі компрометації елементів Honeynet.

В демілітаризованій зоні Honeynet розміщується типова конфігурація для інтерактивного вебзастосунку корпорації, що містить Honeypot-приманки серверного рівня:

– вебсервер;
– сервер додатків;
– сервер бази даних.

Honeynet-сервери призначені для обслуговування запитів клієнтів (зловмисників).

База даних Honeynet містить фальшиві облікові записи.

Сервер керування системи розміщується поза демілітаризованою зоною у корпоративній мережі. Важливо забезпечити надійний захист зв’язку між сервером і демілітаризованою зоною, щоб зловмисник не зміг проникнути з демілітаризованої зони у внутрішню мережу. Для цього потрібно: використання

Honeywall на виході демілітаризованої зони у внутрішню корпоративну мережу, якісне налаштування фаєрволів внутрішньої мережі на з’єднанні з демілітаризованою зоною та бажаною є реалізація взаємодії між сервером керування та демілітаризованою зоною через VPN-тунель.

Усередині демілітаризованої зони лише Honeynet-вебзастосунок може з’єднуватися з базою даних. Всі приманки надсилають статистичні дані про атаки через Honeywall (або VPN тощо) на сервер керування.

Основні компоненти Honeynet мають таке призначення.

Honeypot-вебсервер імітує типову конфігурацію корпоративного вебзастосунку, включаючи вразливості, які можуть зацікавити зловмисників. Вебсервер слугує основною приманкою для хакерів, залучаючи їх спробами проникнення через уразливості вебдодатків, такі як SQL-ін’єкції, XSS або RCE.

Honeypot-сервер додатків імітує роботу серверів бізнес-логіки, які забезпечують виконання програм корпоративних систем. Він створює ілюзію реальних бізнес-процесів, що може стимулювати зловмисника виконувати глибший аналіз або атакувати даний вузол.

Honeypot-сервер бази даних імітує базу даних, яка містить "чутливу інформацію". Наприклад, фіктивні облікові записи, фінансові дані чи іншу інформацію, яка може зацікавити зловмисника. Завдяки цьому стає можливим відстеження спроби SQL-ін’єкцій чи інших методів доступу до бази даних.

Honeywall контролює весь вхідний та вихідний трафік у Honeynet. Він відповідає за реєстрацію підозрілої активності, фільтрацію шкідливих дій та недопущення виходу небажаного трафіку з Honeynet у реальну корпоративну мережу. Honeywall є бар'єром, що забезпечує ізоляцію Honeynet і захист корпоративних ресурсів та інформації від проникнення зловмисників з демілітаризованої зони.

Комутатор використовується для з’єднання всіх елементів Honeynet. Його завдання – забезпечувати правильну маршрутизацію даних між різними вузлами Honeynet без порушення загальної ізоляції DMZ.

Зовнішній шлюз (вхід) до Honeynet створює точку входу для зловмисників, імітуючи підключення до реальної корпоративної мережі. Через нього потенційні

атакуючі отримують доступ до Honeynet і взаємодіють з його компонентами.

На схемі ілюстровано зловмисника, що намагається проникнути до корпоративної мережі через вразливості Honeynet. Цей компонент символізує джерело атак. Якщо зловмисник здійснює спроби отримати доступ до вебзастосунку або до бази даних, його дії фіксуються для подальшого аналізу.

Завдяки інтеграції Honeynet в такій системі захисту корпоративної інформації можна спостерігати за складними сценаріями атак на корпоративну інформацію, що включають експлуатацію декількох уразливостей для досягнення доступу до систем.

Навіть якщо зловмисник успішно атакує Honeypot у демілітаризованій зоні, доступ до внутрішніх ресурсів корпоративної мережі залишається заблокованим через ізоляцію цієї зони.

Серед переваг такого підходу до захисту корпоративної інформації вебзастосунків із розміщенням Honeynet в демілітаризованій зоні відзначимо:

– демілітаризована зона забезпечує фізичну та логічну ізоляцію внутрішньої мережі, ускладнюючи доступ до реальних ресурсів;

– Honeynet дає змогу виявляти нові вразливості у вебзастосунках і методи атак;

– Honeynet-приманки у демілітаризованій зоні збільшують час атак, який зловмисники витрачають на неефективні дії;

– зібрані дані можуть і мають використовуватись для вдосконалення корпоративної політики інформаційної безпеки, щоб посилювати захист реальних систем обробки і зберігання корпоративної інформації.

У Honeynet також можуть бути реалізовані Honeytoken (на рисунку відсутні, але потенційно можливі) – спеціальні маркери у вигляді фіктивних даних чи файлів, які виглядають привабливими для зловмисників:

– псевдодокументи з конфіденційною інформацією;

– фіктивні облікові дані чи API-ключі;

– лог-файли з видимими "слабкими місцями".

Будь-який доступ або використання Honeytoken також є сигналом про компрометацію та дозволяє виявити дії зловмисників.

Щодо засобів реалізації такої підсистеми захисту корпоративної інформації можна надати такі рекомендації.

Для реалізації серверної частини Honeynet рекомендується використовувати інструменти SNARE і TANNER. SNARE є приманкою-датчиком для вебзастосунків, який орієнтований на приваблення зловмисників з Інтернету. TANNER є службою для віддаленого аналізу й класифікації даних з метою оцінки HTTP-запитів і формування висновків, які потім обслуговуються SNARE. Сумісне використання SNARE і TANNER деталізується в [65]: «SNARE визначає площину атак та надсилає запити до TANNER, який оцінює їх і визначає, як SNARE має відповідати на запити. TANNER, як інструмент аналізу та класифікації, аналізує та оцінює HTTP-запити, що обслуговуються SNARE, і створює динамічну відповідь за допомогою механізму емуляції».

Для утворення приманки бази даних рекомендуємо приманку середнього рівня взаємодії OpenCanary, яка може імітувати роботу системи управління базами даних.

Дані статистики від запропонованої конфігурації Honeynet міститимуть фіксацію експлойтів веб-додатків (впровадження SQL, XSS, локальне/віддалене включення файлів), а також і дані про багатоетапні атаки із приманки веб-додатків і спрямовані на базу даних. Оскільки багатоетапні стабільні атаки до бази даних є значно шкідливішими за непостійні атаки на веб-сервер, це є важливим при захисті корпоративної інформації вебзастосунків. Крім того, OpenCanary накопичує дані про всі види експлойтів проти бази даних, які можуть не фіксуватись SNARE і TANNER.

Така організація Honeynet дозволяє не лише запобігати атакам на реальні вебзастосунки, а й аналізувати методи зловмисників, розуміти їхні стратегії та вдосконалювати системи захисту корпоративної інформації. Демілітаризована зона гарантує ізоляцію Honeynet від критичних ресурсів, а застосування декількох рівнів приманок підвищує ефективність виявлення атак.

Щоб збільшити потужність Honeynet і заманити якнайбільше зловмисників, приманки необхідно популяризувати. Розкрутити вебзастосунок-приманку можна додаванням DNS-записів або IP-адрес для Honeynet, інтеграцією посилання на

Honeynet до робочого сайту або іншими методами популяризації. Спрямування множини IP-адрес на один Honeynet-вебзастосунок збільшує ймовірність знаходження приманки зловмисниками. Збільшити ефективність покриття системи захисту корпоративної інформації можна за рахунок збільшення кількості запропонованих реалізацій приманок.

3.3 Організація захисту корпоративних систем моніторингу і управління на основі технології Honeynet

Supervisory Control and Data Acquisition (SCADA) або корпоративні системи моніторингу технологічних процесів і оперативного управління використовуються для контролю промислових процесів у реальному часі.

Такі підсистеми є складовими далеко не кожної корпоративної інформаційної системи, але за наявності певної системи моніторингу технологічних процесів і оперативного управління її важливість важко переоцінити. SCADA сьогодення забезпечують централізоване керування об’єктами критичної інфраструктури, такими як енергетика, водопостачання, транспорт, виробничі підприємства та об'єкти зв'язку.

В корпоративних системах, що розглядаються в цій роботі і які можуть розгортатися на об'єктах критичної інфраструктури, SCADA може виконувати типові функції:

– моніторинг процесів у реальному часі;

– збір даних із сенсорів, контролерів та інших пристроїв на об’єктах;

– відображення поточного стану систем (тиск, температура, напруга тощо);

– керування процесами;

– автоматизація регулювання параметрів, таких як швидкість насосів, відкриття клапанів або перемикання електромереж;

– віддалений контроль, що дозволяє зменшити потребу в фізичній присутності персоналу;

– збереження даних для подальшого аналізу, оптимізації роботи систем та виявлення несправностей;

– здійснення статистичного аналізу та формування звітності;

– попередження аварій (система сповіщення про аномалії дозволяє оперативно реагувати на загрози, наприклад, витік хімічних речовин чи перевантаження електромережі).

За цими функціями можна навести приклади застосування корпоративних систем моніторингу і управління в різних галузях:

– енергетика – для контролю електростанцій, трансформаторних підстанцій та розподільчих мереж, для виявлення перевантажень або обривів ліній електропередач;

– водопостачання та водовідведення – для управління насосними станціями, очисними спорудами, а також для забезпечення сталого тиску та якості води;

– нафтогазова галузь – для моніторингу трубопроводів, резервуарів і компресорних станцій, а також для виявлення витоків газу чи нафти;

– транспорт – для управління літаками в польотах, рухом залізничного транспорту, метро, автотранспорту магістралями, для контролю систем світлофорів.

SCADA-системи є критично важливими для управління об’єктами інфраструктури, забезпечуючи стабільну роботу ключових галузей.

Аварійне вимкнення критичних корпоративних систем моніторингу і управління може призвести до серйозних наслідків для об'єктів критичної інфраструктури. Наприклад, вірус Stuxnet, який уразив іранські центрифуги, призвів до краху ядерної програми цілої держави [45].

Водночас, розвиток корпоративних систем моніторингу і управління залежить від удосконалення безпеки, інтеграції новітніх технологій та адаптації до сучасних вимог. Ресурси корпоративних системи моніторингу і управління часто стають мішенню для кібератак, а особливо в умовах війни з росією і намірів агресора максимально уразити об’єкти критичної інфраструктури України.

Як показали проведені дослідження, технологія Honeynet може бути ефективним інструментом виявлення й аналізу атак, спрямованих на системи

моніторингу і управління, завдяки створенню приманок, які імітують реальні інфраструктури SCADA-системи.

Honeynet може бути налаштована для симуляції типових компонентів SCADA-систем, що дозволяє вивчати дії зловмисників, які намагаються експлуатувати специфічні протоколи, такі як Modbus, DNP3 або IEC-60870-5-104. Приманка збирає дані про атаки, включаючи IP-адреси, використовувані інструменти та методи, які можуть бути використані для покращення захисту. Аналіз дій зловмисників забезпечує глибоке розуміння використовуваних технік. Також Honeynet дозволяє виявити спроби несанкціонованого доступу, зловживання вразливостями або застосування експлойтів.

Загальний сценарій використання Honeynet:

– у Honeynet розгортається для емуляції SCADA-системи з відкритим доступом до протоколу Modbus;

– зловмисник здійснює сканування мережі, намагаючись виявити вразливі системи;

– приманка реєструє дії зловмисника, включаючи команди управління, IP-адресу та методи атаки;

– зібрані дані аналізуються для розробки оновлень систем захисту.

Для організації захисту корпоративних систем моніторингу і управління на основі технології Honeynet першочергово потрібно розібратися зі складовими цих систем та їх роллю в системі.

SCADA-системи є критично важливими для управління промисловими процесами в енергетиці, водопостачанні, транспорті та інших галузях. Через їхню важливість вони часто стають мішенню кіберзлочинців, що робить питання їхнього захисту першочерговим. Основні компоненти SCADA-систем, які разом забезпечують автоматизацію, моніторинг і управління промисловими процесами, це програмований логічний контролер (ПЛК; Programmable Logic Controller – PLC), віддалений термінальний пристрій (ВТП; Remote Terminal Unit – RTU) й людино-машинний інтерфейс (ЛМІ; Human-Machine Interface – HMI). Усі три компоненти є ключовими елементами SCADA-систем і працюють разом для реалізації функцій

системи, вони взаємодіють один із одним через мережу, передаючи дані між пристроями, центральним сервером SCADA та оператором.

Хоча їхні функції взаємопов'язані, кожен компонент виконує окремі завдання.

Програмований логічний контролер локально керує пристроями, такими як насоси, двигуни чи клапани, виконує завдання на основі запрограмованих алгоритмів.

Віддалений термінальний пристрій збирає дані з віддалених сенсорів і передає їх у SCADA-систему, а також може виконувати обмежені команди управління.

Людино-машинний інтерфейс забезпечує взаємодію між оператором і системою через екрани, де відображаються графіки, стан процесів і тривоги.

Їх взаємозв’язок і взаємодію можна пояснити наступним чином. ПЛК виконує локальні завдання, а ВТП передає інформацію з ПЛК та сенсорів у SCADA. ВТП забезпечує передачу даних у SCADA, яка через ЛМІ надає оператору візуалізацію процесів. Оператор через ЛМІ може надсилати команди до ПЛК, щоб змінювати параметри роботи обладнання.

В таблиці 3.1 наведено порівняльну характеристику ПЛК, ВТП і ЛМІ.

Створення імітацій ВТП, ПЛК і ЛМІ, які виглядають як реальні системи, дозволяє утворити якісну Honeynet-структуру системи моніторингу і управління для заманювання зловмисників.

Для вирішення цієї задачі можна використовувати платформу Conpot.

Conpot – одна з найбільш популярних open-source платформ для створення Honeynet-систем для моделювання промислових середовищ (ICS/SCADA). Conpot особливо корисний для моделювання атак на інфраструктуру критичного значення, як-от енергетика, водопостачання чи транспорт.

Conpot підтримує ключові протоколи, такі як Modbus, SNMP, HTTP, BACnet, і S7comm, що дозволяє імітувати промислові пристрої різних типів. Це робить його ідеальним для аналізу потенційних атак на системи моніторингу і управління.

Таблиця 3.1 – Порівняльний аналіз елементів систем SCADA

Характеристика	Програмований логічний контролер	Віддалений термінальний пристрій	Людино-машинний інтерфейс
Функція	Локальний контроль та автоматизація	Збір і передача даних, управління на відстані	Інтерфейс для взаємодії оператора із системою
Призначення	Виконання програмованих інструкцій для контролю локальних пристроїв (клапанів, моторів)	Збір даних із сенсорів і віддалене управління обладнанням	Візуалізація даних і командний контроль
Розташування	Встановлюється локально, поряд із обладнанням	Встановлюється віддалено для збору даних і управління	Розташовується в операторському центрі
Мережеві протоколи	Modbus, Ethernet/IP, Profinet	Modbus, DNP3, IEC 60870	Не використовує власних протоколів, отримує дані з SCADA
Рівень інтеграції	Нижній рівень (ближче до обладнання)	Проміжний рівень між сенсорами і SCADA	Верхній рівень, інтегрований з SCADA
Особливості	Виконує швидкі, повторювані дії для локальних процесів	Орієнтований на дистанційні об’єкти та несприятливі умови	Призначений для користувачів: графіки, звіти, управління
Приклади використання	Контроль руху конвеєра, управління насосами	Збір даних із віддалених свердловин, підстанцій	Контроль оператором енергоспоживання або стану насосів

Conpot може бути розгорнутий як на окремих машинах, так і у вигляді складних Honeynet-мереж, що складаються з кількох вузлів. Це дає змогу досліджувати різні сценарії атак.

Завдяки оптимізації, Conpot може працювати на пристроях із низькою потужністю, таких як Raspberry Pi, що робить його доступним для широкого кола дослідників. Використовуючи XML-файли, користувачі можуть налаштувати поведінку Honeypot, додаючи власні параметри, сервіси або протоколи. Це дозволяє створити індивідуалізовані середовища для моделювання.

Conpot записує всі взаємодії зловмисників із системою, що дозволяє детально аналізувати їхні дії, виявляти нові методи атак та вдосконалювати реальні системи захисту. Завдяки простоті налаштування, підтримці багатьох протоколів і широким можливостям для збору даних, Conpot дозволяє створювати реалістичні моделі промислових систем. Conpot є потужним і гнучким інструментом для імітації ВТП, ПЛК і ЛМІ в контексті Honeynet.

Пристрої ВТП, що використовуються для збору даних із сенсорів і передачі їх до центральної системи керування, за допомогою Conpot можна імітувати з підтримкою таких функцій:

– прийом і обробка запитів через протоколи Modbus або DNP3;

– відповідь на запити для імітації реальних даних (температура, тиск, стан пристроїв тощо);

– імітація мережевої взаємодії між ВТП і SCADA-системою.

Використання Conpot дозволяє досліджувати типи атак, спрямовані на ВТП, включаючи атаки "людина посередині", спроби переписування даних сенсорів або відключення зв'язку між ВТП і SCADA.

ПЛК є основним компонентом систем моніторингу і управління, відповідальним за виконання алгоритмів управління виробничими процесами. Моделювання ПЛК дозволяє аналізувати спроби злому, зміни програмного забезпечення чи логіки управління, що особливо важливо для розуміння кіберзагроз у промисловості. Conpot може імітувати ПЛК завдяки підтримці протоколів, які часто використовуються у цих системах:

– Modbus TCP – найпоширеніший протокол для обміну даними між ПЛК і SCADA. Conpot дозволяє імітувати відповіді ПЛК на команди зчитування або запису регістрів;

– S7comm – протокол, специфічний для контролерів Siemens. Імітація ПЛК через S7comm допомагає досліджувати атаки, спрямовані на маніпуляцію логікою контролера;

– OPC UA – сучасні протоколи, все частіше використовуються в автоматизації.

Використовуючи Conpot, можна створити ілюзію робочого людино-машинного інтерфейсу ЛМІ, який буде "відображати" дані, отримані з ВТП або ПЛК. Така імітація дозволяє зрозуміти методи компрометації ЛМІ, які можуть включати викрадення облікових даних, зміну відображених даних або запуск шкідливого програмного забезпечення. Приманка включає:

– вебінтерфейси (через HTTP/HTTPS), які часто використовуються в сучасних ЛМІ;

– симуляцію отримання даних через OPC UA, Modbus чи інші протоколи;

– записи дій зловмисників, які намагаються взаємодіяти з імітованою ЛМІ.

Honeynet, побудований на Conpot, може включати кілька вузлів, кожен із яких імітує різні пристрої. Це дозволяє створювати складніші сценарії, наприклад, взаємодію ВТП, ПЛК і ЛМІ у єдиній мережі. Підтримка реальних протоколів забезпечує реалістичну взаємодію між зловмисниками та імітованими пристроями. Це збільшує шанси залучити кіберзлочинців для подальшого аналізу їхніх дій.

Conpot записує всі дії зловмисників, що дає змогу аналізувати їхню поведінку, техніки та методи атак. Зібрані дані використовуються для вдосконалення захисних заходів у реальних системах.

Це відкриває нові можливості для дослідження кібератак, навчання персоналу та підвищення загальної кіберстійкості систем моніторингу і управління.

Honeynet модель мережі SCADA проєктуємо для імітації роботи традиційних протоколів і вузлів систем моніторингу та управління (рисунок 3.5). Основна мета Honeynet–SCADA системи полягає у створенні середовища для відстеження дій зловмисників, аналізу їхніх методів та моделювання потенційних загроз.

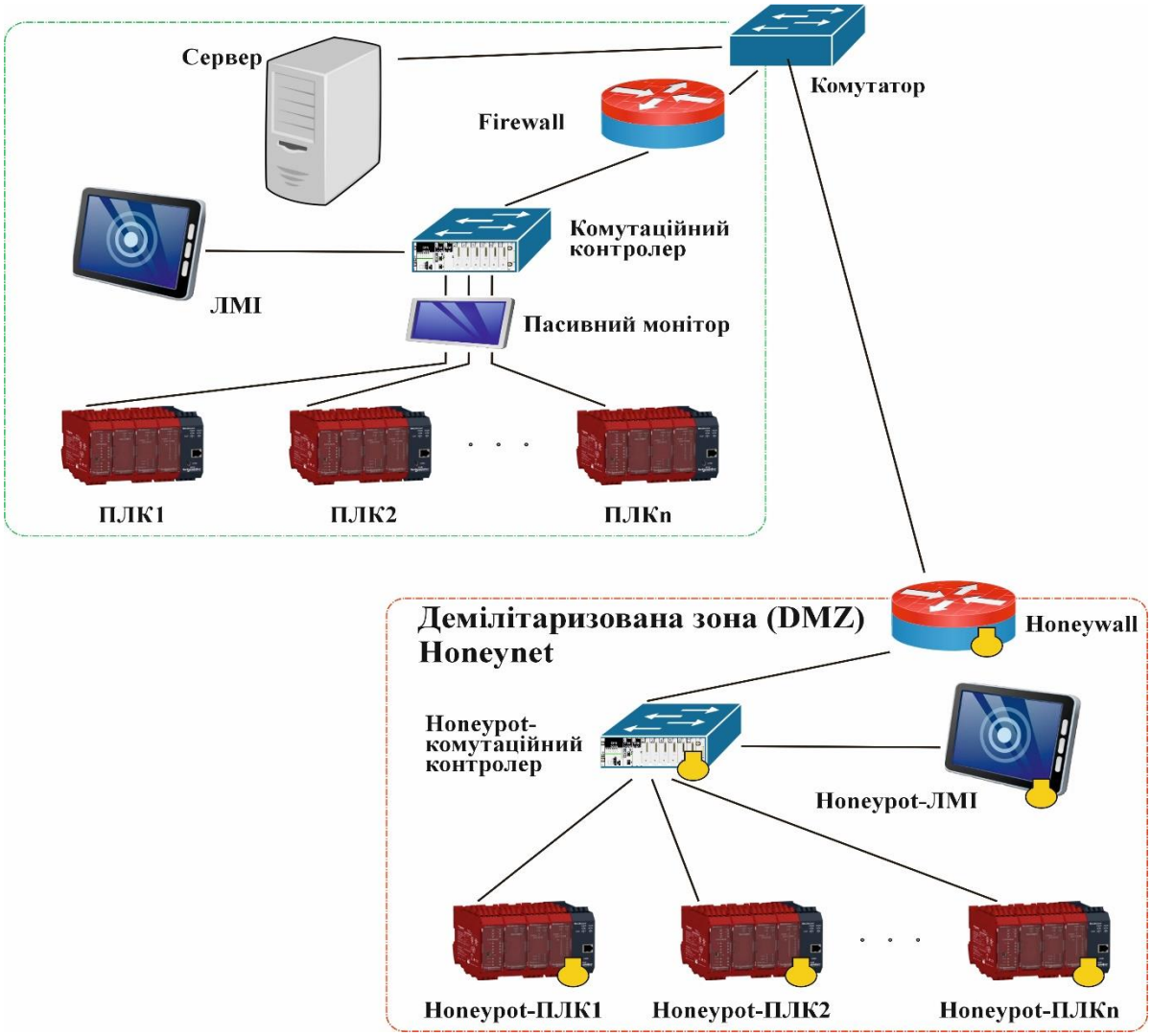

Рисунок 3.5 – Honeynet для захисту Організація захисту від APT-атак у корпоративної мережі

Ключовими елементами, які необхідно імітувати в Honeynet, є програмовані логічні контролери ПЛК та людино-машинний інтерфейс ЛМІ. Саме ці компоненти взаємодіють один із одним та виконують центральну роль у функціонуванні SCADA-систем, а тому є обов'язковими при проєктуванні Honeynet–SCADA.

Для створення ефективної Honeynet–SCADA мережі необхідно включити декілька імітацій ПЛК і хоча б один інтерфейс ЛМІ. Людино-машинний інтерфейс забезпечує взаємодію оператора з системою, надаючи можливість контролювати стан кожного з вузлів. Імітація цих компонентів має бути максимально реалістичною, щоб привернути увагу потенційного зловмисника та змусити його взаємодіяти із системою, вважаючи її справжньою.

Honeynet–SCADA мережа має бути відокремленою від реальних мережевих ресурсів, щоб уникнути ризиків для корпоративної мережі. Розташування такої мережі у демілітаризованій зоні є критично важливим. Демілітаризована зона створює ізольоване середовище, яке забезпечує жорсткі правила фільтрації трафіку за допомогою фаєрвола. Ці заходи дозволяють захистити основну інфраструктуру від потенційних загроз, що можуть виникнути під час роботи зі сторони Honeynet. Крім того, доступ до інтерфейсу ЛМІ, який підключено до імітованих контролерів ПЛК, також має здійснюватися через демілітаризовану зону. Це гарантує, що взаємодія з Honeynet буде повністю контрольованою.

При розробці Honeynet–SCADA мережі необхідно враховувати особливості реальної корпоративної мережі системи моніторингу та управління. Доцільно створити модель, яка максимально відображає існуючу інфраструктуру, або навіть удосконалити її, щоб вона здавалася більш привабливою для зловмисників. Такий підхід сприяє глибшому аналізу атак, дозволяючи зловмисникам проявляти свої методи в реалістичних умовах. Ідеалізована модель також може сприяти виявленню нових векторів загроз, які потенційно можуть бути спрямовані на реальну систему.

Для підвищення рівня безпеки реальної системи доцільно включити до її складу вузол пасивного моніторингу мережевої активності. Такий вузол є абсолютно «прозорим» для інших компонентів SCADA-системи, тобто, не впливає на їхню роботу, але він забезпечить можливість виявляти аномальні дії. Наприклад, якщо один із контролерів ПЛК починає розсилати керуючі інструкції іншим контролерам, це може свідчити про його компрометацію.

Функція пасивного моніторингу дозволяє фіксувати таку активність і сигналізувати про потенційно небезпечну поведінку. Це особливо важливо, оскільки компрометація одного вузла Honeynet може бути спрямована на компрометацію інших, що створює ризик ескалації атаки. Завдяки впровадженню вузла пасивного моніторингу адміністратори отримують інструмент для аналізу подій, ідентифікації шкідливих дій і розробки відповідних заходів захисту.

Оскільки Honeynet–SCADA мережа є ізольованою і розташовується в

демілітаризовану зону, будь-яка активність у ній повинна трактуватися як підозріла. Це дає змогу своєчасно ідентифікувати несанкціоновані дії та виявляти потенційні атаки.

3.4 Висновки

В розділі запропонована організація захисту корпоративної мережі для виявлення та протидії Advanced Persistent Threats (APT) – складних атак, які можуть тривати довгий час, спрямованих на викрадення чи компрометацію корпоративних даних. Система захисту побудована на основі контролю доменної інфраструктури, інтеграції Honeytokens та відстеження аномальної активності.

Захист від програм-вимагачів базується на запобіганні шифруванню важливих даних через моніторинг активності у файловій системі та використання Honeytoken-файлів. Такий підхід забезпечує ефективне виявлення та протидію атакам ще на ранніх етапах.

Організація Honeynet вебпростору дозволяє не лише запобігати атакам на реальні вебзастосунки, а й аналізувати методи зловмисників, розуміти їхні стратегії та вдосконалювати системи захисту корпоративної інформації. Демілітаризована зона гарантує ізоляцію Honeynet від критичних ресурсів, а застосування декількох рівнів приманок підвищує ефективність виявлення атак.

Honeynet–SCADA мережа з використанням імітацій ПЛК і ЛМІ має стати ефективним інструментом для аналізу кіберзагроз і підвищення безпеки SCADA-систем. Її ізольованість, реалістичність і можливість моніторингу забезпечують високий рівень захисту та дозволяють оперативно реагувати на потенційні атаки, спрямовані на критичну інфраструктуру. Розгортання Honeynet у демілітаризованій зоні є ефективним рішенням для захисту SCADA-систем. Це дозволяє ізолювати потенційні загрози, забезпечуючи безпеку основної мережі та виявлення атак у режимі реального часу.

4 ПРАКТИЧНА РЕАЛІЗАЦІЯ І ПОЛІТИКИ БЕЗПЕКИ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ТЕХНОЛОГІЇ HONEYNET

4.1 Обґрунтування вибору засобів практичної реалізації системи захисту корпоративної інформації на основі технології Honeynet

Для реалізації технологій Honeypot і Honeynet розроблено досить велику кількість платформ. До формулювання положень концепції реалізації методу захисту корпоративної інформації на основі технології Honeynet є потреба здійснити дослідження можливостей і обґрунтування вибору засобів реалізації Honeynet-системи захисту корпоративної інформації.

Дослідимо найбільш поширені і популярні платформи.

Аналіз почнемо з фреймворка Honeybrid.

Honeybrid – це передова гібридна платформа-пастка для зловмисників, яка поєднує в собі переваги низької та високої взаємодії honeypot-систем. Основною метою Honeybrid є ефективне виявлення та аналіз атак на інформаційні системи з оптимальним балансуванням між продуктивністю системи і глибиною дослідження поведінки зловмисників.

Платформа має модульну структуру, яка дозволяє інтегрувати різні honeypot-рішення, аналізатори мережевого трафіку та інші інструменти безпеки. Це робить Honeybrid універсальним інструментом, адаптованим до потреб різних організацій.

Honeybrid є важливим інструментом для дослідників кібербезпеки, державних установ та компаній, що працюють над захистом своєї інфраструктури. Він дозволяє швидко реагувати на загрози, аналізувати атаки в реальному часі та збагачувати базу даних загроз для майбутнього використання.

Для швидкого виявлення аномальної активності та відсівання нешкідливого трафіку Honeybrid використовує режим низької взаємодії У разі підозрілої активності зловмисника Honeybrid перенаправляє його до високовзаємодійного середовища для детальнішого аналізу. Таке поєднання низької та високої взаємодії дозволяє мінімізувати витрати ресурсів на постійний моніторинг і одночасно

забезпечувати високий рівень деталізації під час аналізу складних атак.

Завдяки високовзаємодійним середовищам Honeybrid може детально вивчати дії зловмисників, отримуючи дані про їхні методи роботи, використовувані інструменти та цілі.

Однією з ключових функцій Honeybrid є здатність динамічно перемикати підозрілий трафік між різними honeypot-середовищами. Це забезпечує гнучкість і ефективність при виявленні різноманітних атак.

Honeybrid може стати ключовим інструментом для захисту корпоративної інформації.

Використовуючи Honeybrid, компанія створює відволікаючі пастки, які імітують реальні корпоративні системи. Це дозволяє перенаправити увагу зловмисників від цінних ресурсів корпоративної інформації до фіктивних, захищаючи конфіденційні дані. Застосування Honeybrid сприяє збагаченню корпоративної бази даних про загрози. Отримані дані допомагають розробляти стратегії захисту від нових типів атак та підвищувати загальну кіберстійкість компанії.

Honeybrid здатний ефективно ідентифікувати підозрілу активність у корпоративній мережі. Honeybrid забезпечує оперативний моніторинг мережевого трафіку та швидке реагування на загрози. Завдяки динамічній маршрутизації платформа може гнучко адаптуватися до змін у поведінці нападників.

Завдяки поєднанню технологій низької та високої взаємодії, Honeybrid пропонує корпоративним службам захисту інформації широкий спектр можливостей для виявлення, аналізу та запобігання загрозам, спрямованим на інформаційну інфраструктуру компаній, а також оптимізує використання ресурсів компанії. Більшість стандартного трафіку обробляється системами з низькою взаємодією, а глибокий аналіз проводиться лише для потенційно небезпечної активності. Використовуючи низьковзаємодійні honeypot-системи, платформа фільтрує великий обсяг трафіку, виявляючи потенційні загрози ще до того, як вони досягнуть критично важливих систем.

Під час перенаправлення зловмисника до високовзаємодійного honeypot-

середовища Honeybrid проводить детальне вивчення його дій. Це дозволяє з'ясувати, які інструменти використовуються, які вразливості атакуються, та які кінцеві цілі в корпоративному середовищі переслідує зловмисник.

За результатами аналізу властивостей Honeybrid можна запропонувати сценарії використання платформи у системах захисту корпоративної інформації:

– побудова реалістичних сценаріїв тестування систем безпеки та виявлення вразливостей у внутрішній інфраструктурі;

– захист від цілеспрямованих атак (наприклад, APT), які спрямовані на викрадення конфіденційної інформації;

– виявлення та аналіз дій інсайдерів, які можуть становити загрозу для компанії;

– моніторинг та аналіз атак у хмарних середовищах, які активно використовуються сучасними компаніями.

Ще один потужний інструмент захисту корпоративних інформаційних ресурсів – SURFcert IDS.

SURFcert IDS (Intrusion Detection System) – рішення для виявлення та запобігання кіберзагрозам, яке здатне ефективно захистити корпоративну інформацію. Завдяки адаптивним алгоритмам і широким можливостям інтеграції, система допомагає організаціям виявляти загрози, аналізувати інциденти та посилювати свої заходи безпеки.

SURFcert IDS забезпечує безперервний моніторинг мережевого трафіку для виявлення підозрілих дій. Система фіксує такі загрози, як:

– сканування портів;

– атаки типу DDoS;

– впровадження шкідливого програмного забезпечення;

– підбір паролів.

Це дозволяє виявити спроби доступу до корпоративних ресурсів ще на ранніх етапах.

SURFcert IDS ідентифікує вторгнення, спрямовані на крадіжку критичних

даних, таких як фінансова, комерційна та персональна інформація. Система блокує підозрілі дії, запобігаючи витоку даних.

SURFcert IDS легко інтегрується з іншими засобами кібербезпеки, такими як брандмауери, SIEM-системи, антивірусне програмне забезпечення та honeypot-мережі. Це створює комплексну систему захисту корпоративної інформації.

Система збирає інформацію про всі підозрілі події, що дозволяє проводити глибокий аналіз атак. Отримані дані допомагають зрозуміти методи зловмисників і розробити заходи для запобігання подібним інцидентам у майбутньому.

SURFcert IDS використовує сучасні алгоритми для виявлення аномальної поведінки в мережі, включаючи невідомі раніше типи атак. Це знижує ризик компрометації корпоративних систем.

SURFcert IDS може бути налаштована для роботи у локальних, хмарних або гібридних інфраструктурах, що робить її придатною для компаній будь-якого масштабу.

Переваги SURFcert IDS для систем захисту корпоративної інформації:

– система оперативно виявляє загрози, дозволяючи уникнути серйозних наслідків;

– SURFcert IDS захищає від спроб викрадення даних та інших атак, чим досягається зменшення ризиків витоку інформації;

– автоматизація виявлення та аналізу інцидентів знижує навантаження на команди IT-безпеки;

– система генерує інформативні звіти про інциденти, що допомагає керівництву приймати обґрунтовані рішення щодо кібербезпеки.

Сфери застосування SURFcert IDS в корпоративному бізнесі:

– захист транзакцій, облікових записів клієнтів та конфіденційної фінансової інформації;

– безпечне управління даними клієнтів, партнерів і внутрішніми документами компанії;

– забезпечення безпеки великих мереж і конфіденційних даних у

дослідницьких проєктах;

– захист критичної інфраструктури та забезпечення інформаційної безпеки.

Заслуговує уваги як Honey-платформа захисту корпоративної інформації також інноваційна платформа для кібербезпеки CyberTrap.

CyberTrap – це сучасна пастка для зловмисників (honeypot), розроблена для виявлення, аналізу та нейтралізації кіберзагроз у корпоративних та державних інформаційних системах. Ця платформа забезпечує високий рівень захисту завдяки своїй здатності обманювати нападників, виявляти їхню активність та отримувати цінну інформацію про їхні дії.

CyberTrap створює реалістичні імітації корпоративної інфраструктури, які приваблюють кіберзлочинців. Це дозволяє перенаправити їхню увагу з реальних систем на підроблені, зберігаючи конфіденційні дані та критично важливі інформаційні ресурси компанії. Платформа швидко ідентифікує підозрілу активність, дозволяючи командам безпеки негайно реагувати на можливі загрози.

CyberTrap стає особливо корисним для раннього виявлення цілеспрямованих атак (APT) та шкідливого ПЗ. CyberTrap створює фальшиві ресурси, які виглядають як реальні частини корпоративної інфраструктури, зокрема бази даних, сервери чи облікові записи користувачів. Це дозволяє швидко виявити зловмисників, які намагаються отримати доступ до конфіденційної інформації, перш ніж вони досягнуть справжніх даних. Платформа CyberTrap здатна дезорієнтувати нападників, скеровуючи їх до симуляційних середовищ. Це дає змогу компанії виграти час для аналізу загрози та запобігання подальшим атакам, мінімізуючи потенційні ризики.

Завдяки інтерактивному середовищу CyberTrap досліджує методи, інструменти та стратегії нападників. Зібрана інформація використовується для розробки ефективних механізмів захисту та підвищення кіберстійкості.

CyberTrap легко інтегрується в різні мережеві середовища, включаючи локальні мережі, хмарні сервіси та гібридні інфраструктури. Це дозволяє компаніям будь-якого масштабу адаптувати платформу до своїх потреб і робить платформу

універсальним рішенням для підприємств різного розміру. Інтеграція CyberTrap із наявними системами захисту дозволяє створити багаторівневий підхід до безпеки. Платформа доповнює традиційні інструменти, такі як брандмауери, системи виявлення вторгнень (IDS) та антивіруси, забезпечуючи додатковий рівень захисту.

CyberTrap допомагає ідентифікувати дії інсайдерів, які можуть становити небезпеку для корпоративних даних. Це особливо актуально для великих організацій, де контроль за доступом до даних є складним завданням.

Серед переваг CyberTrap як інструменту захисту корпоративної інформації можна відзначити:

– ефективно запобігає доступу до справжніх даних, спрямовуючи атакуючих у фальшиві середовища;

– автоматично сповіщає команди безпеки про підозрілу активність;

– дозволяє здійснювати виявлення інсайдерських загроз (допомагає ідентифікувати підозрілу активність з боку співробітників або партнерів компанії);

– платформа надає командам безпеки аналітику, яка прискорює процес реагування та ліквідації наслідків атак;

– зібрана інформація про методи нападників дозволяє покращувати захисні стратегії компанії та створювати більш ефективні системи безпеки.

Заслуговує уваги як Honey-платформа захисту корпоративної інформації також T-Pot.

T-Pot –інтегрована honeypot-платформа, яка пропонує сучасні можливості для захисту корпоративної інформації. Її головна перевага у здатності імітувати різні системи та сервіси, залучаючи зловмисників і забезпечуючи захист реальної інфраструктури організації. T-Pot є багатофункціональним рішенням, яке ефективно поєднує в собі виявлення загроз, їх аналіз і запобігання атакам.

Завдяки інтеграції кількох honeypot-рішень, таких як Cowrie, Dionaea та ConPot, T-Pot створює реалістичні копії корпоративних сервісів і систем. Це дозволяє відволікти увагу зловмисників від реальної інфраструктури компанії, захищаючи конфіденційну інформацію.

Використовуючи фальшиві сервери, T-Pot запобігає спробам викрадення реальних корпоративних даних, забезпечуючи додатковий рівень безпеки для фінансової, комерційної та клієнтської інформації.

T-Pot забезпечує моніторинг мережевої активності, миттєво виявляючи сканування портів, спроби впровадження шкідливого ПЗ чи підбір паролів. Це дає змогу реагувати на потенційні загрози ще до того, як вони можуть завдати шкоди.

Платформа автоматично збирає та зберігає інформацію про поведінку зловмисників у honeypot-середовищі. Ці дані є ресурсом для аналізу методів і інструментів нападників, що дозволяє вдосконалювати стратегії кіберзахисту.

Завдяки інтеграції з ELK Stack (Elasticsearch, Logstash, Kibana), T-Pot надає зручний інструмент для аналізу зібраної інформації. Це дозволяє візуалізувати атаки, створювати детальні звіти та відслідковувати тренди загроз.

T-Pot підтримує розгортання у хмарних середовищах, локальних мережах і віртуальних інфраструктурах. Завдяки своїй гнучкості платформа може бути адаптована до потреб компаній різного масштабу.

Переваги використання T-Pot для корпоративної безпеки:

– автоматично фіксує підозрілу активність, зменшуючи ризик пропуску атак;

– інтеграція кількох honeypot-систем в одній платформі знижує витрати на розгортання окремих рішень;

– платформа дозволяє тестувати сценарії атак і навчати співробітників реагувати на кіберзагрози;

– дозволяє організаціям збирати дані про нові методи атак для покращення своєї безпеки;

– завдяки підтримці ConPot, платформа імітує промислові SCADA/ICS системи управління, що дозволяє захищати їх від атак;

– забезпечує захист від сканування портів, атак на SSH або Telnet, атак на хмарні сервіси та інші загрози завдяки обновлюваним компонентам, T-Pot завжди готовий до протидії новим типам атак.

В таблиці 4.1 наведено порівняльну характеристику можливостей розглянутих платформ для реалізації Honeynet.

Таблиця 4.1 – Порівняльний аналіз платформ для реалізації Honeynet

Функція захисту	Платформа для реалізації Honeynet та її можливості					
	Honeybrid	Honeywall	T-Pot	SURFcert IDS	CyberTrap	MHN
Темний простір	–	*	–	–	+	*
Виявлення програм-вимагачів	–	*	–	–	+	*
Виявлення APT	–	–	–	–	*	*
Захист вебзастосунків	+	+	+	+	+	+
Моніторинг APT	+	+	+	+	*	+
Захист SCADA	–	*	+	–	–	+
Пасивний монітор	–	–	–	–	+	*

В таблиці використано позначки: «+» – платформа підтримує відповідну функцію захисту повністю; «*» – платформа може бути адаптована на відповідну функцію захисту із використанням додаткових інструментів; «–» – платформа не підтримує відповідну функцію захисту і не може бути адаптована із використанням додаткових інструментів;

На підставі оцінки різних систем управління Honeynet, зведеної до таблиці 4.1, платформа MHN (Modern Honey Network) виявилася найбільш гнучким і придатним рішенням для використання при реалізації методу організації системи захисту корпоративної інформації на основі технології Honeynet.

4.2 Політики безпеки системи захисту корпоративної інформації на основі технології Honeynet

В умовах сучасних кіберзагроз при захисті корпоративної інформації за допомогою Honeynet надзвичайно актуальним є визначення і дотримання політики безпеки. Політика безпеки, розроблена для роботи з Honeynet, може розглядатися як ключові положення, які визначають правила використання цієї технології в корпоративному інформаційному середовищі та діяльності різних категорій користувачів цього середовища.

Політика безпеки для роботи з Honeynet має забезпечити контрольоване середовище для виявлення зловмисної активності, захистити реальні ресурси від проникнень і запобігти компрометації корпоративних даних. Актуальність дотримання політики безпеки також полягає у запобіганні помилок, які можуть призвести до витоків даних або експлуатації вразливостей у самій Honeynet. Чітко визначені правила доступу, ізоляція фальшивих серверів та моніторинг усіх підозрілих дій гарантують, що система буде працювати ефективно, без ризику порушення конфіденційності або компрометації реальних мереж.

Таким чином, впровадження Honeynet разом із ретельно продуманою політикою безпеки є стратегічно важливим елементом сучасного кіберзахисту.

Оскільки метод організації системи захисту корпоративної інформації на основі технології Honeynet розглядає корпоративну інформаційну систему як сукупність корпоративних інформаційних ресурсів, до складу яких може входити корпоративна комп’ютерна мережа з усіма її складовими, корпоративні інтернет-ресурси (вебзастосунки з усіма їх складовими та засобами підтримки і корпоративні системи моніторингу технологічних процесів і оперативного управління (SCADA-системи), а кожна з цих підсистем має специфіку організації системи захисту корпоративної інформації на основі технології Honeynet, то і політику безпеки доцільно деталізувати для кожної підсистеми.

4.2.1 Політика безпеки організації захисту інформації корпоративної

комп’ютерної мережі на основі технології Honeynet

Розроблена Honeynet-система захисту ресурсів корпоративної комп’ютерної мережі є інтерактивною захисною інфраструктурою, яка дозволяє виявляти атаки з боку зловмисників, таких як програми-вимагачі (ransomware) і цільові тривалі атаки (APT) тощо.

Ця політика спрямована на забезпечення правильного використання Honeynet для захисту інформаційних ресурсів внутрішньої корпоративної мережі.

4.2.1.1 Призначення системи захисту і політики безпеки:

– забезпечення виявлення та ізоляції кіберзагроз, включаючи APT-атаки та програми-вимагачі;

– аналіз методів зловмисників для створення ефективних механізмів протидії;

– запобігання несанкціонованому доступу до критичних корпоративних інформаційних ресурсів.

4.2.1.2 Принципи експлуатації Honeynet:

– ізоляція Honeynet. Цей принцип передбачає, що Honeynet-система повинна бути повністю ізольованою від внутрішніх інформаційних ресурсів компанії;

– використання Honeytoken. Цей принцип передбачає, що Honeytoken-користувачі та Honeytoken-файли використовуються для створення «приманок», які імітують реальні об'єкти корпоративної мережі. Honeytoken мають бути максимально реалістичними (наприклад, облікові записи співробітників, документи з фінансовими або юридичними даними);

– реалістичність і прозорість для зловмисників. Цей принцип передбачає, що Honeynet повинна виглядати як частина реальної корпоративної мережі. Необхідно симулювати активність користувачів (логіни, збереження файлів, звернення до серверів тощо).

4.2.1.3 Управління доступом:

– доступ до Honeynet мають лише співробітники корпоративного відділу інформаційної безпеки;

– всі підключення проходять через сегмент демілітаризованої зони із

багаторівневим міжмережевим екраном;

– заборонено пряме підключення Honeynet до реальної корпоративної мережі;

– всі зміни конфігурації Honeynet повинні бути затверджені керівництвом ІТ-відділу, відділу інформаційної безпеки та директоратом компанії;

– усі дії в Honeynet мають логуватися для подальшого аналізу;

– зберігання логів повинно здійснюватися не менше 12 місяців.

4.2.1.4 Збір даних та моніторинг:

– весь трафік і дії у Honeynet повинні відслідковуватись у реальному часі;

– для аналізу вхідного та вихідного трафіку використовувати системи виявлення вторгнень (IDS);

– для обмеження вихідного трафіку, щоб уникнути передачі інформації зловмисникам використовувати Honeywall ;

– інформація про дії зловмисників (спроби доступу, поширення шкідливого ПЗ) зберігається для подальшого аналізу.

4.2.1.5 Політика реагування на інциденти:

– Honeytoken-файли, розташовані на файлових серверах, дозволяють виявляти спроби шифрування даних. У разі виявлення активності програм-вимагачів відповідальний співробітник корпоративного відділу інформаційної безпеки негайно блокує відповідний сегмент мережі;

– аналіз дій Honeytoken-користувачів дозволяє виявити довгострокову активність атакуючих, таких як збір даних або спроби розширення привілеїв. У разі виявлення підозрілої активності співробітникам корпоративного відділу інформаційної безпеки необхідно провести аналіз маршруту зловмисника та блокування його доступу;

– після інциденту обов’язковим є проведення розслідування, щоб зрозуміти методику атаки;

– після інциденту обов’язковим є аналіз потреб та, за потреби, оновлення правил безпеки корпоративної мережі (Firewall, IDS/IPS).

4.2.1.6 Технічний супровід Honeynet:

– періодичне тестування Honeynet (не рідше 1 разу на квартал) на відповідність сучасним загрозам, виправлення виявлених вразливостей у конфігурації Honeynet;

– регулярне оновлення Honeytoken-файлів і облікових записів для уникнення підозр з боку зловмисників;

– щорічний аудит Honeynet із залученням незалежних експертів.

4.2.1.7 Заборони:

– заборонено використовувати Honeynet для тестування реального ПЗ чи збереження корпоративних даних;

– заборонено надавати стороннім особам доступ до конфігурацій Honeynet;

– забороняється виведення даних із Honeynet без їх попереднього аналізу експертами корпоративного відділу інформаційної безпеки.

4.2.1.8 Відповідальність та звітність:

– адміністратори Honeynet відповідають за правильну конфігурацію системи та її роботу;

– корпоративний відділ інформаційної безпеки відповідає за моніторинг і реагування на інциденти;

– корпоративний відділ інформаційної безпеки здійснює підготовку звітів про роботу Honeynet, які включають виявлені інциденти та рекомендації для покращення системи.

Ця політика є обов’язковою для виконання всіма співробітниками, які залучені до експлуатації Honeynet. Її дотримання дозволяє знизити ризики кіберзагроз та забезпечити захист інформаційних ресурсів корпоративної мережі.

4.2.2 Політика безпеки організації захисту інформації корпоративних вебзастосунків на основі технології Honeynet

Honeynet-система, зображена на схемі, є частиною багаторівневого підходу до захисту корпоративних вебзастосунків. Вона призначена для виявлення та ізоляції загроз, таких як експлойти вебдодатків, SQL-ін'єкції, атак на сервери баз даних, та інших кіберзагроз.

4.2.2.1 Призначення системи захисту і політики безпеки:

– забезпечення моніторингу та виявлення загроз у демілітаризованій зоні Honeynet-системи;

– створення фальшивих сервісів (Honeypot-серверів), які імітують реальні компоненти корпоративної мережі.

– запобігання компрометації реальних вебсервісів та даних.

4.2.2.2 Принципи експлуатації Honeynet:

Honeynet розташовується виключно в демілітаризованій зоні та не має доступу до основної мережі

– всі Honeypot-сервіси повинні бути фізично та логічно ізольовані від реальних серверів компанії.

– Honeypot-системи мають бути налаштовані так, щоб виглядати максимально реалістично, що включає використання реальних доменних імен, структур URL та відповідей сервера;

– Honeypot-вебсервер імітує корпоративний вебсайт або API і використовується для виявлення атак, спрямованих на вебсервіси;

– Honeypot-сервер баз даних імітує базу даних, щоб виявляти SQL-ін'єкції, атаки на облікові дані тощо;

– Honeypot-сервер додатків симулює роботу серверних компонентів застосунків (обробка виконуваних файлів, логіка бізнес-процесів);

– Honeywall захищає вихідний трафік, забезпечуючи контрольовану ізоляцію системи.

4.2.2.3 Управління доступом:

– доступ до конфігурації Honeynet дозволений лише уповноваженим співробітникам корпоративного відділу інформаційної безпеки;

– реальні IP-адреси honeypot-серверів не повинні розголошуватись зовнішнім та внутрішнім користувачам;

– всі підключення до Honeynet логуються та передаються у систему моніторингу безпеки;

– журнали подій мають зберігатися не менше 12 місяців у зашифрованому вигляді.

4.2.2.4 Збір даних та моніторинг:

– вхідний та вихідний трафік Honeynet повинен аналізуватись у реальному часі за допомогою системи виявлення вторгнень (IDS);

– виявлені аномалії автоматично повідомляються співробітникам корпоративного відділу інформаційної безпеки;

– дані для аналізу: способи проникнення зловмисників, використані вразливості вебзастосунків та серверів, стратегії обходу безпекових механізмів.

4.2.2.5 Політика реагування на інциденти:

– у разі виявлення спроби атаки Honeynet негайно блокує підозрілий трафік за допомогою Honeywall;

– експерт корпоративного відділу інформаційної безпеки аналізує активність зловмисника та розробляє контрзаходи (оновлення правил брандмауера, виправлення вразливостей у реальних вебсервісах);

– після інциденту обов’язковим є проведення розслідування, щоб зрозуміти методику атаки, з подальшим складанням звіту;

– після інциденту обов’язковим є аналіз потреб та, за потреби, внесення змін до архітектури Honeynet та налаштувань безпеки вебзастосунків.

4.2.2.6 Технічний супровід Honeynet:

– Honeypot-сервери мають бути періодично обновлювані відповідно до нових загроз і уразливостей.

– періодично (не рідше 1 разу на 3 місяці) використовувати тестові атаки для перевірки надійності Honeynet;

– облікові дані та адреси Honeynet-серверів мають періодично змінюватись, щоб уникнути їх розпізнавання зловмисниками;

– всі журнали роботи Honeynet мають бути систематизовані та аналізовані для побудови профілів загроз.

4.2.2.7 Заборони:

– забороняється використовувати Honeynet як платформу для тестування власних корпоративних застосунків;

– заборонено надавати доступ до Honeynet стороннім підрядникам без

письмового дозволу керівництва;

– забороняється видалення журналів подій без аналізу.

4.2.2.8 Відповідальність та звітність:

– адміністратори системи відповідають за коректність конфігурації Honeynet;

– команда корпоративного відділу інформаційної безпеки відповідає за своєчасне виявлення атак та відповідь на інциденти;

– технічна команда корпоративного відділу інформаційної безпеки зобов’язана підтримувати актуальність компонентів Honeynet.

Політика є обов'язковою до виконання всіма співробітниками, які працюють із системами захисту вебзастосунків. Вона гарантує надійний захист інформаційних ресурсів, сприяє аналізу атакуючих стратегій та формуванню ефективного кіберзахисту.

4.2.3 Політика організації безпеки захисту інформації корпоративних систем моніторингу та управління на основі технології Honeynet

Для ефективного застосування Honeynet-системи в захисті SCADA-систем корпорації необхідно впровадити чітко регламентовану політику безпеки. Вона визначає правила використання, моніторингу, адміністрування та реагування на загрози. Нижче наведені основні аспекти такої політики.

4.2.3.1 Призначення системи захисту і політики безпеки:

– раннє виявлення загроз передбачає виявлення атак на SCADA-систему до того, як вони вплинуть на критичні компоненти;

– збір інформації про атаки, що передбачає отримання даних про техніки, тактики і методи зловмисників;

– ізоляція атак через захист основної мережі шляхом перенаправлення атакуючої активності на Honeynet.

– використання результатів аналізу для вдосконалення засобів кіберзахисту.

4.2.3.2 Принципи експлуатації Honeynet:

– забороняється використання реальних даних чи доступу до основних SCADA-компонентів у Honeynet;

– Honeynet повинна бути фізично та логічно ізольована від основної мережі;

– забороняється прямий доступ до Honeynet з основної корпоративної мережі;

– всі операції в Honeynet повинні бути задокументовані;

– використання Honeywall для фільтрації та контролю всього вхідного/вихідного трафіку;

– інформація, зібрана Honeynet, може використовуватись для оновлення політик міжмережевого екрану (Firewall) та систем виявлення вторгнень (IDS/IPS).

4.2.3.3 Управління доступом: доступ до Honeynet дозволяється виключно кваліфікованим адміністраторам безпеки корпоративного відділу інформаційної безпеки.

4.2.3.4 Збір даних та моніторинг:

– пасивний монітор та Honeywall повинні постійно реєструвати весь трафік, що проходить через Honeynet;

– записи повинні зберігатися не менше 6 місяців для додаткового відтермінованого аналізу;

– використовувати автоматизовані системи аналізу трафіку для виявлення підозрілої активності;

– реагувати на будь-яку несанкціоновану взаємодію з Honeynet у реальному часі;

– негайне повідомлення відповідальних осіб про критичні атаки;

– щомісячна звітність про виявлені загрози та інциденти.

4.2.3.5 Політика реагування на інциденти:

– інциденти повинні класифікуватися за рівнем ризику: низький, середній, високий, критичний;

– рівень ризику визначається на основі впливу на Honeynet і потенційної загрози основній мережі;

– при виявленні атаки активність зловмисника не повинна припинятися, доки не буде зібрано достатньо даних;

– після збору інформації зловмисна активність ізолюється через Honeywall

або інші засоби;

– всі зібрані дані про атаку повинні бути ретельно проаналізовані;

– висновки аналізу включають: тип атаки (наприклад, DDoS, експлуатація вразливостей PLC, фішинг тощо); використані техніки зловмисників; потенційні шляхи покращення безпеки.

4.2.2.6 Технічний супровід Honeynet:

– регулярно оновлювати симулятори (Honeypot-ПЛК, Honeypot-ЛМІ) для імітації нових технологій і систем;

– перевіряти відповідність Honeynet актуальним загрозам;

– використовувати інформацію з Honeynet для оновлення: політик міжмережевих екранів; конфігурацій систем виявлення вторгнень; алгоритмів моніторингу трафіку;

– періодично проводити тестування Honeynet для перевірки її готовності до роботи в умовах реальних атак.

4.2.2.7 Заборони:

– забороняється використовувати Honeynet для цілей, не пов’язаних із кібербезпекою (наприклад, для тестування інших продуктів);

– забороняється об’єднувати реальні та симульовані компоненти, що може призвести до компрометації реальної інфраструктури.

4.2.2.8 Відповідальність та звітність:

– відповідальність та контроль за виконанням політики Honeynet покладається на корпоративний відділ інформаційної безпеки

– у разі порушення політики винні особи притягаються до дисциплінарної відповідальності.

Політика є обов'язковою до виконання всіма співробітниками, які працюють із системами моніторингу та управління. Реалізація цієї політики гарантує безпечне використання Honeynet та підвищує рівень захисту SCADA-системи в умовах сучасних кіберзагроз.

4.3 Висновки

В розділі здійснене обґрунтування вибору засобів практичної реалізації системи захисту корпоративної інформації на основі технології Honeynet. Для цього здійснено аналіз можливостей ряду популярних у подібних застосунках платформ, а саме Honeybrid, Honeywall, T-Pot, SURFcert IDS, CyberTrap, MHN, з метою визначення їх придатності до вимог методу організації системи захисту корпоративної інформації на основі технології Honeynet.

На підставі дослідження і порівняльної оцінки різних систем управління Honeynet найбільш гнучким і придатним рішенням для використання при реалізації методу організації системи захисту корпоративної інформації на основі технології Honeynet визнана платформа MHN (Modern Honey Network), яку і рекомендовано для реалізації напрацьованих рішень комплексного захисту корпоративної інформації внутрішньої мережі, вебзастосунків і систем моніторингу та управління.

В розділі також описано політики безпеки для організації комплексного захисту інформації Політика безпеки системи захисту інформації корпоративної комп’ютерної мережі, корпоративних вебзастосунків та корпоративних систем моніторингу та управління на основі технології Honeynet.

ВИСНОВКИ

В роботі за результатами теоретичних та практичних досліджень здійснено розробку методу, орієнтованого на вдосконалення і розширення можливостей системи захисту корпоративної інформації за рахунок комплексного застосування можливостей технології Honeynet; визначено принципи організації системи захисту корпоративної інформації на основі технології Honeynet для комплексного захисту ресурсів корпоративної комп'ютерної мережі, вебзастосунків і систем моніторингу та управління.

Для реалізації програми досліджень виконано наступні роботи:

– досліджено вразливості та способи захисту корпоративної інформації і технології застосування мережевих пасток в системах захисту;

– проаналізовано можливості сучасних засобів реалізації технології Honeynet для організації системи захисту корпоративної інформації;

– обґрунтовано вибір технології Honeynet для реалізації методу захисту корпоративної інформації;

– визначено концепцію організації системи захисту корпоративної інформації на основі технології Honeynet;

– запропоновані рішення щодо організації системи захисту корпоративної інформації на основі технології Honeynet для комплексного захисту ресурсів корпоративної комп'ютерної мережі, вебзастосунків і систем моніторингу та управління;

– обґрунтовано вибір платформи Modern Honey Network для практичної реалізації системи захисту корпоративної інформації на основі технології Honeynet;

– розроблено політики безпеки використання системи захисту корпоративної інформації на основі технології Honeynet для захисту ресурсів корпоративної комп'ютерної мережі, вебзастосунків і систем моніторингу та управління.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Чубаєвський В. І. Корпоративна інформаційна безпека: монографія. Київ : Держ. торг.-екон. ун-т, 2022. 272 с.

2. Saha B., Anwar Z. A Review of Cybersecurity Challenges in Small Business: The Imperative for a Future Governance Framework. Journal of Information Security. №15. 2024. P.24-39.

3. Kala E. The Impact of Cyber Security on Business: How to Protect Your Business. Open Journal of Safety Science and Technology. 2023. №13. P. 51-65.

4. Safitra M. F., Lubis M., Fakhrurroja H. Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability. 2023. Vol. 15(18). P. 1-32.

5. A Systematic Review on classification of Cyber Attacks and its Prevention techniques to improve Cyber Security / P. Nirmala et al. 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India. 2023. P. 1-6.

6. Bala B., Behal S. AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges. Computer Science Review. 2024. Volume 52.

7. Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model / Luuk Bekkers et al. Computers & Security. 2023. Volume 127. P. 99-103.

8. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53. Revision 5. 2020.

9. Sulillari J., Nasto K. E-banking services knowledge and usage, the case of Korca city, Albania. International journal of new economics and social sciences (IJONESS). 2020. Vol. 12, №2. P. 9-22.

10. Chien-Hua Tsai, Dah-Kwei Liou, Hsiu-Li Lee. Blockchain-supported online banking scheme. Egyptian Informatics Journal. 2024. Volume 27. ISSN 1110-8665.

11. Safe Decentralized Applications Development Using Blockchain Technologies / V. Cheshun et al. 10th International Conference on Advanced Computer

Information Technologies (ACIT), Deggendorf, Germany, 2020. P. 800-805.

12. Examining the Role of Artificial Intelligence in Cyber Security (CS): A Systematic Review for Preventing Prospective Solutions in Financial Transactions / Faraji Mahfujur Rahman et al. International Journal of Religion. 2024. Volume 5. P. 4766-4782.

13. A hybrid EMD - Neuro-fuzzy model for financial time series analysis / A. Vlasenko et al. Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020. 2020. P. 112–115.

14. Karpiuk R., Kokovska Y., Venherskyi P. Development of a Universal High-Performance Machine Learning Framework for Finding Cybersecurity Anomalies in Big Data. In book: Digital Ecosystems: Interconnecting Advanced Networks with AI Applications. 2024. P.289-300.

15. Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN / Lewis Golightly et al. Cyber Security and Applications. 2023. Volume 1. P.1-20.

16. A systematic literature review for authorization and access control: definitions, strategies and models. A.K.Y.S. Mohamed et al. International Journal of Web Information Systems. 2022. Vol. 18, №. 2/3. P. 156-180.

17. Aljuaid Turkea Ayedh M, Ainuddin Wahid Abdul Wahab, Mohd Yamani Idna Idris. Systematic Literature Review on Security Access Control Policies and Techniques Based on Privacy Requirements in a BYOD Environment: State of the Art and Future Directions. Applied Sciences. 2023. №13(14): 8048.

18. Опірський І. Р. Василишин С.І., Піскозуб А.З. Аналіз використання програмних приманок як засобу забезпечення інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2020. №2(10). С. 88-97.

19. General Data Protection Regulation GDPR. URL: https://gdpr-info.eu/ (date of access: 09.11.2024).

20. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/ru/standard/27001 (date of access: 09.11.2024).

21. Про захист персональних даних : Закон України від 01.06.2010 № 2297-

VI : Редакція від 27.04.2024. URL: http://surl.li/mhodoi (дата звернення: 11.11.2024).

22. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : Редакція від 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 11.09.2024).

23. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : Редакція від 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 11.11.2024).

24. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII : Редакція від 30.10.2024. URL: http://surl.li/uswvto (дата звернення: 11.11.2024).

25. Про банки і банківську діяльність : Закон України від 07.12.2000 № 2121-III : Редакція від 8.11.2024. URL: http://surl.li/splfwz (дата звернення: 12.11.2024).

26. Модель аналізу стратегій при динамічній взаємодії учасників фішингових атак / В. Лахно та ін. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2023. №4(20). С. 124–141.

27. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. Підприємництво, господарство і право. 2019. №5. С. 304–307.

28. Коршикова Т. В. Розслідування шахрайства, з використанням електро-обчислювальної техніки : дис. док. філ. 2021. 255 с.

29. Гринько Л. П. Фішинг як спосіб вчинення шахрайства у мережі інтернет. Полтавський правовий часопис. № 4 (2022). С. 16-39.

30. Шеремета Д. Вірус Petya схожий на WannaCry, але складніший - Європол. Главком. URL: http://surl.li/otwkmz (дата звернення: 11.11.2024).

31. Advanced Persistent Threats: Attack Stages, Examples, and Mitigation. Hacker One Attack Resistance Platform. URL: http://surl.li/yptkjz (дата звернення: 3.11.2024).

32. What are the different types of cyber threat actors? Sophos 2024 Threat Report. URL: http://surl.li/jflrdc (дата звернення: 7.11.2024).

33. Knife Collection: A Review of Open Source Software Supply Chain Attacks / M. Ohm et al. Detection of Intrusions and Malware, and Vulnerability Assessment, 2020 Jun 11;12223. P. 23–43.

34. Дослідження системи на уразливість до MITM-атаки за допомогою

створення FAKE AP / С. Кривенко та ін. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2021. №1(13). С. 29–38.

35. Evolution of Malware Threats and Techniques: A Review / Alenezi Mohammed et al. International Journal of Communication Networks and Information Security. 2020. P. 326-337. Vol. 12, № 3.

36. Analyzing and comparing the effectiveness of malware detection: A study of machine learning approaches / M. Azeem et al. Heliyon. 2023. № 10(1):e23574. P. 1-19.

37. Жилін А., Шевчук О. Архітектура та класифікація Deception Technology. Information Technology and Security. 2021. Vol. 9, Iss. 2 (17). P. 165–175.

38. Li Zhang, Vrizlynn L.L. Thing. Three decades of deception techniques in active cyber defense - Retrospect and outlook. Computers & Security. 2021. Volume 106. P. 1-19.

39. Abdelghani Tschroub. Implementation of Defense in Depth Strategy to Secure Industrial Control System in Critical Infrastructures. American Journal of Artificial Intelligence. 2020. № 3. P. 17-22.

40. Гапоненко О. І., Марченко В.В., Гайдур Г.І. Переваги та недоліки Honeypot–приманки для хакерів. Сучасний захист інформації. 2020. № 2(42). С. 59-63.

41. Honeypot allocation for cyber deception under uncertainty / A.H. Anwaret al. IEEE Trans. Netw. Serv. Manag. 2022. № 19 (3). P. 3438-3452.

42. Anwar A.H., Kamhoua C., Leslie N. Honeypot allocation over attack graphs in cyber deception games. 2020 International Conference on Computing, Networking and Communications (ICNC). IEEE. 2020. P. 502-506.

43. Multi-cloud integration security framework using honeypots / T. Alyas et al. Mob. Inf. Syst. 2022. P. 1-13.

44. NeuralPot: An Industrial Honeypot Implementation Based On Deep Neural Networks / Siniosoglou et al. 2020 IEEE Symposium on Computers and Communications (ISCC). Rennes, France. 2020. P. 1-7.

45. HoneyPLC: A Next-Generation Honeypot for Industrial Control Systems / Morales Efren et al. Cyber Deception. 2022. P. 145-181.

46. Dowling S., Schukat M., Barrett E. New framework for adaptive and agile honeypots. ETRI Journal. 2020. №42. DOI: 10.4218/etrij.2019-0155.

47. A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems / J. Franco et al. IEEE Communications Surveys & Tutorials. 2021. P. 2351-2383.

48. , M. Yufeng, W. Bo and Q. Zhang, "A Dynamic Deceptive Honeynet System with A Hybrid of Virtual and Real Devices / Z. Minjiao et al. 5th International Conference on Computing and Big Data (ICCBD), Shanghai, China. 2022. P. 113-117.

49. A HoneyNet Environment for Analyzing Malicious Actors / Gisolfi Daniel et al. Conference: 2018 IEEE MIT Undergraduate Research Technology Conference. P. 1-5.

50. Yu T, Xin Y, Zhang C. HoneyFactory: Container-Based Comprehensive Cyber Deception Honeynet Architecture. Electronics. 2024. №13(2):361. P. 1-27.

51. A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems / Franco Javier et al. IEEE Communications surveys and tutorials. 2021. Vol.23 (4). p.2351-2383.

52. What Are HoneyTokens? Fortinet. URL: http://surl.li/qorwpl (дата звернення: 11.11.2024).

53. What are Honeytokens in Cybersecurity? SentinelOne. URL: http://surl.li/rfohof (дата звернення: 11.11.2024).

54. From Detection to Deceotion: Honepots and Honeytokens in Modern Cybersecurity. URL: https://tinyurl.com/4pf25tw8 (дата звернення: 11.11.2024).

55. What are Honeytokens? CrowdStrike. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/honeytokens/ (дата звернення: 11.11.2024).

56. Honeysweeper: Towards Stealthy Honeytoken Fingerprinting Techniques / Msaad et al. Secure IT Systems. NordSec 2022. Lecture Notes in Computer Science. 2022. Vol 13700. Springer, Cham. P.101-119.

57. Sandor Tokesi. HoneyDoc with Azure and Remote Template Injection. 2022. URL: https://shorturl.at/Z6t53 (дата звернення: 12.11.2024).

58. Sharma Navita, Sran Sukhwinder. Detection of threats in Honeynet using Honeywall. International Journal on Computer Science and Engineering. 2011. №3. P. 3332-3336.

59. Lackner P. How to Mock a Bear: Honeypot, Honeynet, Honeywall Honeytoken: A Survey. In Proceedings of the 23rd International Conference on

Enterprise Information Systems (ICEIS 2021). 2021. Volume 2. P. 181-188.

60. Abnormal network packets identification using header information collected from Honeywall architecture / Nguyen K. V. et al. Journal of Information and Telecommunication, Vol. 37(4). P. 437–461.

61. Mohssen Mohammed, Mohamed Abdalla Nour, Mohamed Elhoseny. Detecting Zero-day Polymorphic Worms Using Honeywall. Journal of Cybersecurity and Information Management (JCIM). 2025. Vol. 15. № 01. P. 34-49.

62. HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design / Fan Wenjun et al. IEEE Journal on Selected Areas in Communications. 2019. №37. P. 683-697.

63. The Therapeutic Mechanisms of Honey in Mitigating Toxicity from Anticancer Chemotherapy Toxicity: A Review / D. Bose et al. Journal of Xenobiotics. 2024. Vol. 14(3). P. 1109-1129.

64. Dowling S., Schukat M., Barrett E. New framework for adaptive and agile honeypots. ETRI Journal, 2020. Vol. 42. P. 965-975.

65. Gupta Rajat, Madhu V., Manikandan K. An Innovative Security Strategy using Reactive Web Application Honeypot. International Journal of Innovative Technology and Exploring Engineering. 2020. № 9(5). P.2092-2097.

66. Захаров В.В., Рижий Я.О., Філюк Є.В., Чешун В.М. Рольова декомпозиція технології атрибутивного цифрового підпису. Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп’ютерних наук АПКН-2024». Хмельницький. 2024. С.237-241.

67. Захаров В.В., Чешун В.М. Технологія HONEYNET в захисті корпоративної інформації від кіберзагроз. Військова освіта і наука: сьогодення та майбутнє : зб. тез доповідей XX Міжнародної НПК. Київ : Військовий інститут Київського національного університету імені Тараса Шевченка, 2024. С.44.

68. Захаров В.В., Чешун Д.В., Чешун В.М. Виявлення загроз Advanced Persistent Threats з допомогою Honeynet-приманки середнього рівня взаємодії OpenCanary. VII Всеукраїнська НПК студентів, аспірантів та молодих вчених "Сучасні інформаційні системи та технології". 29 листопада 2024 року, Херсонський національний технічний університет. (в стадії видання).

Військова освіта і наука: сьогодення та майбутнє : зб. тез доповідей XX Міжнародної науково-практичної конференції, м. Київ, 29 листопада 2024 р. Київ : Військовий інститут Київського національного університету імені Тараса Шевченка, 2024. 532 с.

Рекомендовано до друку Вченою радою Військового інституту Київського національного університету імені Тараса Шевченка
(протокол від 21.11.2024 № 3).

У збірнику тез доповідей друкуються матеріали виступів наукових і науково-педагогічних працівників, курсантів (студентів) Військового інституту Київського національного університету імені Тараса Шевченка та інших вищих військових та закладів вищої освіти України.

У публікаціях розглядаються: технічні проблеми озброєння і військової техніки та технології подвійного призначення; актуальні проблеми лінгвістичного забезпечення Збройних Сил України; актуальні питання військової психології та соціальної роботи; інформаційна та психологічна боротьба у воєнній сфері; інформаційно-медійне забезпечення МОУ та ЗСУ в умовах правового режиму воєнного стану; фінанси; актуальні проблеми військового права в умовах воєнного стану; актуальні проблеми геопросторової підтримки військ в умовах ведення російсько-української війни; наукові проблеми воєнної політології та морально-психологічного впливу; аналіз бойового застосування частин (підрозділів) Сухопутних військ Збройних Сил України у сучасному загальновійськовому бою (тактичних діях)

Захаров В.В. (ХмНУ)
к.т.н., доц. Чешун В.М. (ХмНУ)

ТЕХНОЛОГІЯ HONEYNET В ЗАХИСТІ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ ВІД КІБЕРЗАГРОЗ

Вразливості та сучасні загрози корпоративній інформації постійно змінюються, вимагаючи від організацій застосування комплексних заходів захисту. Оскільки зловмисники використовують нові тактики та техніки, компанії змушені дотримуватися проактивного підходу до кібербезпеки, інвестуючи в технологічні рішення, навчання співробітників і систематичне вдосконалення захисту корпоративної інформації.

Одним із прогресивних підходів до захисту корпоративної інформації від кіберзагроз є технологія Honeynet.

Корпоративні Honeynet-системи включають типові ключові компоненти: фальшиві сервери та бази даних, які імітують справжні сервери, бази даних та інші ресурси, надаючи зловмисникам доступ до неіснуючих даних; моніторингова інфраструктура, яка дозволяє відстежувати всі дії зловмисників;

Засоби збору та збереження даних для подальшого аналізу, що дозволяє зібрати детальну інформацію про тактики та техніки, які використовують зловмисники для атак на корпоративну інфраструктуру; інтеграція з системами виявлення атак (IDS/IPS) та SIEM-системами для передачі інформації про атаки в режимі реального часу. Таке комплексне рішення дозволяє оперативно реагувати на загрози та блокувати їх у справжній, а не фальшивій корпоративній мережі.

Використання Honeynet дозволяє не лише виявляти та ідентифікувати зловмисників у мережі, але й отримувати цінну інформацію про їхні методи і техніки, що сприяє покращенню загальної системи безпеки організації.

У корпоративному середовищі Honeynet допомагає побудувати захист, спрямований на попередження атак, створюючи пастки для зловмисників та аналізуючи їхню активність у контрольованих умовах. Honeynet дозволяє отримати доступ до інформації про інструменти та техніки, які використовують зловмисники для проникнення в мережу. Це може включати нові експлойти, методи соціальної інженерії та шкідливі програми. Завдяки Honeynet, зловмисники можуть бути спрямовані на фальшиві сервери, що зменшує ризик несанкціонованого доступу до реальних корпоративних ресурсів. Інформація, зібрана Honeynet, дозволяє фахівцям з безпеки краще розуміти загрози та розробляти нові методи захисту. Зокрема, Honeynet допомагає аналізувати вразливості мережі та оптимізувати захисні механізми. Honeynet є ефективним інструментом для навчання персоналу. Фахівці мають можливість практично відстежувати дії зловмисників, що дозволяє краще готуватися до реальних загроз.

В той же час при використанні Honeynet в корпоративному інформаційному середовищі слід враховувати, що дані, зібрані в Honeynet, можуть містити конфіденційну інформацію, яка теж повинна бути захищена.

УДК 004:37:001:62

Збірник наукових праць за матеріалами XVI Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2024». Хмельницький. 2024. 582с.

У збірнику наукових праць подані перспективні практичні розробки аспірантів, студентів та здобувачів в області сучасних інформаційних технологій. Розглянуто актуальні проблеми комп'ютерних наук, комп'ютерної інженерії, прикладної математики й інженерії програмного забезпечення, приведено ряд робіт по впровадженню інформаційних технологій у виробництво та управління. Висвітлено перспективні розробки сучасних систем пошуку, обробки й захисту інформації, медійних та комунікаційних системи.

УДК 004:37:001:62

Матеріали конференції відтворені з авторських оригіналів, друкуються в авторській редакції та наведені в алфавітному порядку прізвищ авторів. При макетуванні можливі незначні зміни компоновки контенту авторських оригіналів. Відповідальність за якість та зміст публікацій несе автор.

Участь у конференції та складові всіх її етапів (розгляд праць, перевірка на плагіат, макетування, публікація збірника наукових праць та видача сертифікатів) є безкоштовними для всіх учасників. Оргкомітет конференції висловлює подяку учасникам конференції та сподівається на подальшу співпрацю.

З питань проведення конференції та подальшого обміну інформацією звертатись на e-mail конференції: *apkt.khnu@gmail.com*

УДК 004.056.5

Захаров В.В., Рижий Я.О., Філюк Є.В, Чешун В.М.

Хмельницький національний університет

РОЛЬОВА ДЕКОМПОЗИЦІЯ ТЕХНОЛОГІЇ АТРИБУТИВНОГО ЦИФРОВОГО ПІДПИСУ

Визначені і деталізовані основні етапи реалізації технології атрибутивного цифрового підпису в системах електронного документообігу, описані схеми застосування технології, представлено рольову декомпозицію взаємодії суб'єктів технології в процесі накладання сигнатури підпису на документ та її верифікації одержувачем завіреного підписом файлу документа, а також рольову декомпозицію взаємодії суб'єктів технології в процесі формування і накладання підпису на вимогу постачальника послуг.

The main stages of the implementation of the attribute digital signature technology in electronic document management systems are defined and detailed, the technology application schemes are described, the role decomposition of the interaction of the subjects of the technology in the process of superimposing a signature signature on a document and its verification by the recipient of the document file certified by the signature is presented, as well as the role decomposition of the interaction of sub objects of technology in the process of forming and applying a signature at the request of the service provider.

Електронний цифровий підпис (ЕЦП) є важливим елементом сучасних технологій автоматизованого документообігу. Він забезпечує безпечність, юридичну чинність електронних документів, ефективність їх обробки, дозволяє ідентифікувати автора, гарантує цілісність вмісту та має у цифровому середовищі таку ж юридичну силу, як традиційний підпис на папері.

Відповідно до Закону України [1], «електронний підпис – це електронні дані, додані підписувачем до інших електронних даних або логічно з ними пов'язані, що використовуються ним як підпис».

Традиційна технологія формування ЕЦП на основі асиметричної криптографії застосовує пару ключів (приватний та публічний) та алгоритми обчислення хеш-функцій електронного документа [2]. Такий підхід гарантує високий рівень безпеки та можливість перевірки цілісності документа, що робить криптографічний ЕЦП важливим інструментом для забезпечення конфіденційності та автентифікації в електронному документообігу.

Однак, використання криптографічного ЕЦП має певні недоліки, такі як знеособлення підписанта, обмежене спеціалізоване застосування, а також потреба у сертифікованих довірених сервісах для підписання кожного документа [3].

В попередній роботі [4] авторами здійснено ідентифікацію та класифікацію атрибутів для реалізації технології атрибутивного цифрового підпису в системах

електронного документообігу, запропоновано спосіб формалізованого представлення різних класів атрибутів в математичній моделі та презентовано схему синтезу сигнатури підпису на основі формалізованого представлення особових атрибутів підписанта.

Технологія синтезу підпису базується на принципах гнучкості, адаптивності та мультиатрибутності ЕЦП.

В технології передбачено реалізацію двох схем підпису: аутентифікації та підпису. В схемі аутентифікації атрибути можуть бути вибірково розкриті користувачем-підписантом під час аутентифікації певному постачальнику послуг. В схемі підпису підписант може вибірково розкривати та додавати атрибути до ЕЦП на основі атрибутів. Таким чином, підтвердження вибіркового розкриття використовується або для аутентифікації, або для створення підпису (з хешем повідомлення).

Технологія цифрового підпису із застосуванням особових атрибутів підписанта в системах електронного документообігу складається з чотирьох етапів: генерація ключа, видача атрибутів, генерація підпису та перевірка підпису.

Генерація ключа відбувається при ініціалізації сервісу користувача-підписанта, коли він встановлюється на комп'ютер або мобільний телефон та вперше запускається користувачем. У цей момент генерується секретний ключ у вигляді випадкового 256-розрядного двійкового числа, який безпечно зберігається сервісом. Цей секретний ключ використовується для видачі атрибутів, аутентифікації при запиті атрибутів і підписання цифрового вмісту.

Процес видачі атрибутів передбачає, що користувач може отримати атрибути від авторизованих емітентів. Емітент підписує облікові дані, що містять запитувані атрибути, своїм закритим ключем. Під час перевірки підпису відкритий ключ емітента використовується верифікаторами. Такий підхід забезпечує відправника атрибутів довіреною підписаною інформацією, яку можна перевірити та використовувати в майбутньому.

На рисунку 1 представлена рольова декомпозиція взаємодії суб'єктів технології в процесі накладання сигнатури ЕЦП на документ та верифікації сигнатури ЕЦП одержувачем завіреного підписом файлу документа.

На рисунку 2 представлена рольова декомпозиція взаємодії суб'єктів технології в процесі формування і накладання підпису на вимогу постачальника послуг (надання атрибутів постачальнику послуг).

Фактично, в обох сценаріях створення підпису здійснюється сервісом користувача-підписанта (мобільним додатком або програмним застосунком на ПК) під контролем та керівництвом підписанта, а також під контролем менеджера технології (серверного застосунку). Сервіс користувача-підписанта надає необхідні атрибути, мітку часу та вибірковий доказ розкриття інформації, щоб переконатися, що саме користувач сервісу підписав повідомлення та має відповідні атрибути, що були видані емітентом.

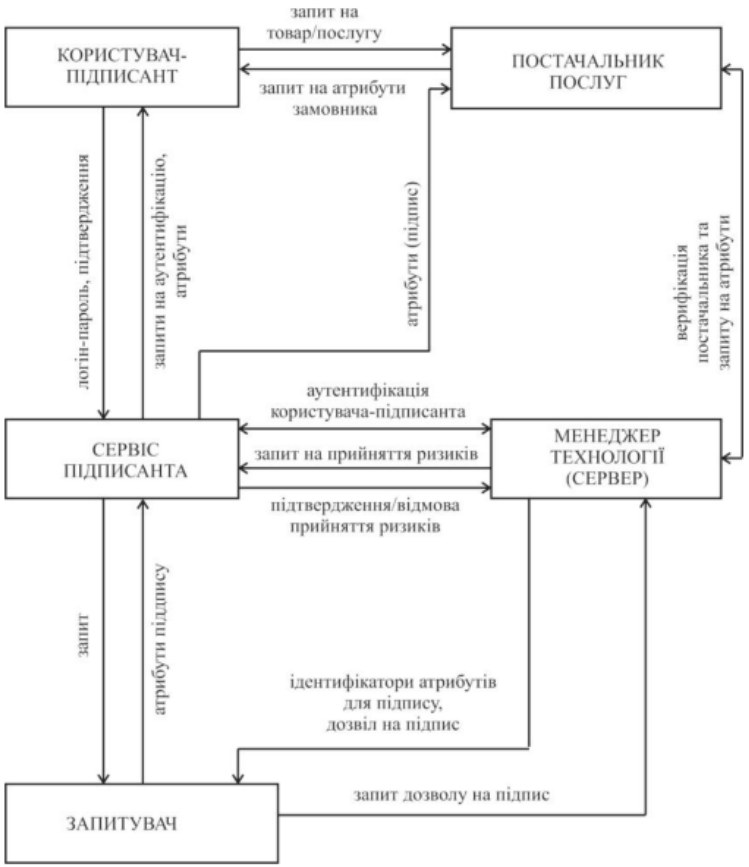

Рисунок 2 – Рольова декомпозиція взаємодії суб'єктів при формуванні-накладанні підпису на вимогу постачальника послуг

Технологія використовує підтвердження з нульовим знанням для того, щоб оберігати як секретний ключ технології, так і підпис від верифікатора. Це забезпечує додатковий рівень конфіденційності, оскільки верифікатор не отримує доступу до важливих облікових даних технології цифрового підпису. Секретний ключ і підпис у технології зберігаються прихованими, щоб забезпечити відсутність зв'язку між ними та забезпечити безпеку облікових даних підписанта. Першим атрибутом кожного отриманого облікового запису завжди є секретний ключ

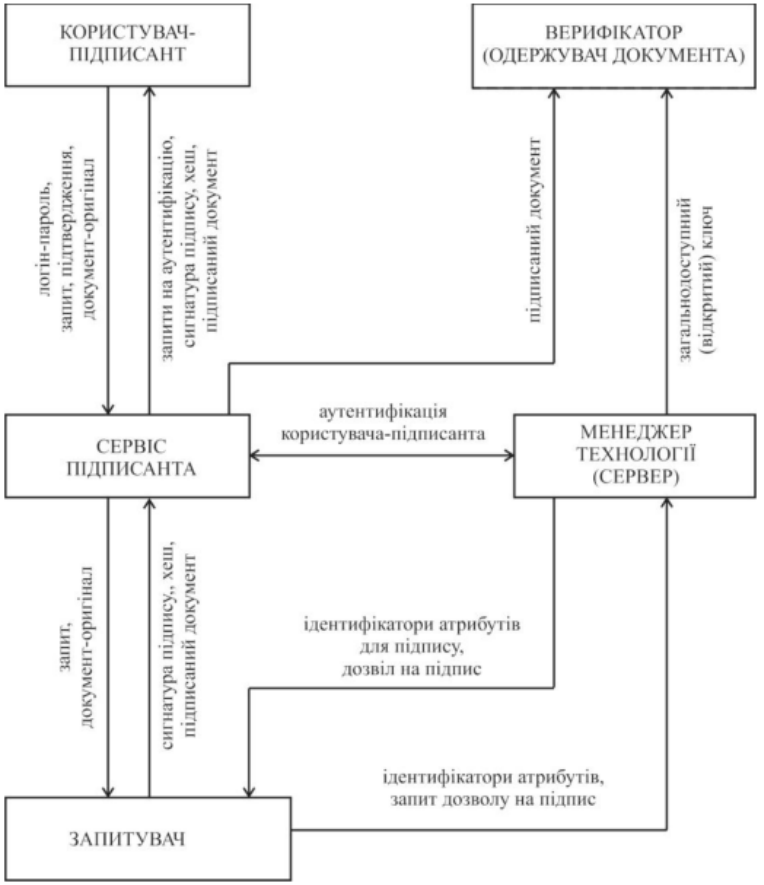

Рисунок 1 – Рольова декомпозиція взаємодії суб'єктів при накладанні сигнатури ЕЦП на документ та її верифікації

Перевірка підпису реалізується за допомогою алгоритму верифікації сигнатури ЕЦП. Верифікатори, які бажають підтвердити підпис на основі атрибутів, повинні мати відкритий ключ відповідного емітента, який надав пов'язані атрибути мобільному додатку. Відкритий ключ емітента використовується для перевірки підпису. Верифікатор перевіряє дійсність мітки часу та переконується, що повідомлення (в межах підпису) було підписано користувачем-підписантом, який має відповідні атрибути, видані емітентом.

УДК 004.056.5

Захаров В.В., *студент 2 курсу спеціальності «Кібербезпека та захист інформації» ОПП «Кібербезпека та захист інформації»*[1]
Чешун Д.В., *викладач*[2]
студент групи ІПЗ-23-1
Чешун В.М., *канд. техн. наук, доцент кафедри кібербезпеки*[1]

ВИЯВЛЕННЯ ЗАГРОЗ ADVANCED PERSISTENT THREATS З ДОПОМОГОЮ HONEYNET-ПРИМАНКИ СЕРЕДНЬОГО РІВНЯ ВЗАЄМОДІЇ OPENCANARY

Хмельницький національний університет, Україна[1]
Хмельницький фаховий економіко-технологічний коледж УЕП[2]

Постановка проблеми

Серед ключових проблем сучасного цифрового суспільства постає безпека інтернет-ресурсів. Постійне зростання кількості кібератак, вдосконалення шкідливих програм та розвиток технік соціальної інженерії ставлять під загрозу як приватні дані користувачів, так і критичну інфраструктуру [1].

Одним із напрямків протидії кіберзлочинам є технології використання мережевих приманок (Deception technology) – це стратегія відволікання кіберзлочинців від справжніх активів підприємства та перенаправлення їх у приманку чи пастку. Приманка імітує законні сервери, програми та дані, щоб зловмисник був обманом змушений повірити, що він проник і отримав доступ до найважливіших активів підприємства, хоча насправді це не так [2]. Стратегія використовується для мінімізації збитків і захисту справжніх активів організації [3].

Метою будь-якої позиції безпеки є захист від будь-якого несанкціонованого доступу, і технологія обману може бути корисною технікою, яку можна використовувати, коли виникла підозра про порушення [1]. Перенаправлення кіберзлочинців на підроблені дані та облікові дані може бути ключовим фактором захисту реальних активів підприємства.

Щоб функціонувати належним чином, технологія приманок має бути ефективною і не повинна бути очевидною як для зловмисників, так і для співробітників підприємства, підрядників або клієнтів.

Аналіз останніх досліджень та публікацій

Сьогодні технологіям мережевих приманок приділяється надзвичайно велика увага, адже виграш від їх застосування як для бізнес структур, так і для структур протидії розвідці з відкритих джерел набагато перевищує витрати на впровадження подібних технологій [3,4].

Автори робіт [2,3], за результатами аналізу переваг та недоліків використання приманок як засобу забезпечення інформаційної безпеки приходять до однозначного висновку, що технології Deception, Honeypot, Honeynet, Honeytoken є невід'ємною частиною сучасного захисту інформації від атак і мають великі перспективи застосування та розвитку.

В статті [5] на основі технології приманок визначають стратегію гри з нульовою сумою між захисником мережі та зловмисником і пропонують масштабований алгоритм для ефективного розподілу приманок на графі атак.

В [4] пропонується двоетапний підхід обману, заснований на розподілі приманки Honeypot. На першому етапі розробляється політика проективного оманливого розподілу приманок, а на другому етапі пропонується підхід реактивного обману, який динамічно розподіляє приманки відповідно до оновлень IDS.

У документі [6] презентується багатохмарна система безпеки як розвиток механізмів безпеки, щоб забезпечити відволікання зловмисника. Мета полягає в тому, щоб отримати

підписанта. Користувач доводить емітенту, що він знає перший атрибут (секретний ключ), використовуючи доказ нульового знання. Таким чином, емітент розпізнає свого користувача як правильного, не розкриваючи секретний ключ користувача емітенту. Надалі емітент може безпечно підписати атрибути.

Перелік посилань

1. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 01.12.2022р. URL:https://zakon.rada.gov.ua/laws/show/2155-19/ed20231231#Text (дата звернення: 29.10.2024).
2. Метьолкін А.О., Кардашук В.С. Дослідження методів підвищення криптографічної стійкості. Вісник східноукраїнського національного університету імені Володимира Даля. 2018. № 6 (247). С. 90-95.
3. Ke Gu, Keming Wang, Lulu Yang. Traceable attribute-based signature. Journal of Information Security and Applications. Volume 49. 2019. Article ID 102400.
4. Рижий Я.О., Мельник М.М., Чешун О.В., Орленко В.С. Класифікація атрибутів особи і формування цифрового підпису на їх основі. Збірник наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2023». Хмельницький. 2023. С.252-256.

Для моніторингу та виявлення загроз APT створюється спеціальний обліковий запис користувача OpenCanary, дані якого розповсюджуються на всі клієнтські машини мережі. У домені Windows це можна зробити за допомогою команди: runas /user:<Domain>\<User>. Ця команда надсилає хеш-комбінацію «ім'я користувача»+NTLM у пам'ять, не підключаючись до контролера домену.

Відстеження використання облікового запису OpenCanary потребує налаштування аудиту подій входу в систему через політику домену. Це включає увімкнення аудиту подій входу та фільтрацію помилок у подіях входу (подія #533).

Журнали подій контролера домену передаються на центральний сервер для централізованого моніторингу. Синтаксичний аналізатор файлу журналу збирає події аудиту, пов'язані з помилками, і передає їх через протокол Hpfeeds. Відповідний канал Hpfeeds має бути підписаний центральним сервером керування.

Якщо зловмисник застосовує інструменти для отримання хешів, наприклад, Mimikatz, облікові дані користувача OpenCanary можуть бути зчитані та використані для атаки. У випадку їх використання для автентифікації, центральний інтерфейс повинен:

– відображати IP-адресу або ім'я хоста скомпрометованої машини;
– показувати IP-адресу, до якої відбувається рух бокового доступу;
– візуалізувати використаний NTLM-хеш і відповідне ім'я користувача.

Інформація, зібрана системою Honeynet, передається оператору. Він аналізує дані для визначення джерела компрометації та сценаріїв руху APT у мережі. Отримані дані використовуються для ініціювання роботи групи реагування на інциденти (CERT), яка досліджує, яким чином зловмисник проникнув у мережу, та запобігає подальшому поширенню загрози.

Висновки

В роботі наведено рекомендації щодо практичної реалізації одного із можливих варіантів застосування Honeynet-приманки середнього рівня взаємодії OpenCanary для виявлення загроз атаки Advanced Persistent Threats. Honeynet реалізується у мережі, побудованій на основі Active Directory, яка включає щонайменше один контролер домену. Запропонований підхід забезпечує точкове виявлення загроз, виявлення слабких місць у системі безпеки та допомагає запобігти ескалації APT-атак.

Перелік джерел посилання

1. Чубаєвський В. І. Корпоративна інформаційна безпека: монографія. Київ: Держ. торг.-екон. ун-т, 2022. 272 с.

2. Опірський І. Р. Василишин С.І., Піскозуб А.З. Аналіз використання програмних приманок як засобу забезпечення інформаційної безпеки. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2020. №2(10). С. 88-97. doi: 10.28925/2663-4023.2020.10.8897.

3. Гапоненко О. І., Марченко В.В., Гайдур Г.І. Переваги та недоліки Honeypot–приманки для хакерів. *Сучасний захист інформації*. 2020. № 2(42). С. 59-63.

4. Honeypot allocation for cyber deception under uncertainty / A.H. Anwar, C.A. Kamhoua, N.O. Leslie, C. Kiekintveld. *IEEE Trans. Netw. Serv. Manag*. 2022. 19 (3). P. 3438-3452.

5. Honeypot allocation over attack graphs in cyber deception games/ A.H. Anwar, C. Kamhoua, N. Leslie. *2020 International Conference on Computing, Networking and Communications (ICNC). IEEE*. 2020. P. 502-506.

6. Multi-cloud integration security framework using honeypots / T. Alyas, K. Alissa, M. Alqahtani, T. Faiz, S.A. Alsaif, N. Tabassum, H.H. Naqvi. Mob. Inf. Syst. 2022. P. 1-13.

7. Advanced Persistent Threats: Attack Stages, Examples, and Mitigation. *HackerOne Attack Resistance Platform.* URL:https://www.hackerone.com/knowledge-center/advanced-persistent-threats-attack-stages-examples-and-mitigation (дата звернення: 3.11.2024).

8. What are the different types of cyber threat actors? Sophos 2024 Threat Report. URL:https://www.sophos.com/en-us/cybersecurity-explained/threat-actors (дата звернення: 3.11.2024).

більше часу для аналізу атаки та пом'якшення вторгнення без компромісів. Механізм розроблено з використанням технології Honeypot.

Поряд з значними напрацюваннями щодо методів застосування технологій приманок та принципів їх розгортання, практичним аспектам вибору і застосування існуючих рішень Honeypot і Honeynet для протидії певному класу атак на сьогодні уваги приділяється мало.

Постановка задачі

Advanced Persistent Threats (APT), або розвинені постійні загрози, є одними з найскладніших викликів у сфері кібербезпеки [7]. Це цілеспрямовані та довготривалі атаки, які здійснюються досвідченими групами зловмисників, часто за підтримки державних структур або великих організацій. Їхня мета – непомітне проникнення у систему, тривале перебування в ній і здобуття критично важливої інформації або завдання шкоди.

Про потужність APT-атак свідчать приклади з історії [8]: складний комп'ютерний хробак Stuxnet, який успішно вразив ядерні об'єкти Ірану наприкінці 2000-х років і вважається результатом спільної операції США та Ізраїлю; злам Sony Pictures у 2014 році : північнокорейською хакерською групою Lazarus Group, що призвело до витоку конфіденційних даних компанії та внутрішніх комунікацій; атаки на Національний комітет Демократичної партії США у 2016 році російської хакерської групи APT29 (Cozy Bear), можливими наслідками якої вважають спотворення результатів виборів в США.

Потенційна можливість протидії таким атакам вбачається в застосуванні мережевих приманок.

Основною задачею дослідження є визначення принципів і надання рекомендацій щодо використання існуючих технологій мережевих приманок для протидії атакам типу Advanced Persistent Threats.

Виклад основного матеріалу

Ймовірно, APT сьогодні є однією з найсерйозніших загроз для компаній і їхніх критично важливих активів. APT не лише тривалий час залишаються непоміченими в мережі, але й активно збирають інформацію про її структуру та топологію, готуючись до подальшого бокового переміщення. APT можуть залишатися у системі протягом значного часу, перш ніж досягнуть своєї мети – викрадення цінних даних або порушення роботи мережі.

Виявлення таких дій є критично важливим для запобігання подальшому поширенню загрози та мінімізації шкоди, завданої мережею APT. Оскільки APT в мережі надзвичайно небезпечні, то дуже важливо виявити їх присутність якомога швидше.

Пропонований сценарій виявлення зосереджений на моменті, коли APT починають рухатися мережею, переміщуючи облікові дані користувачів між клієнтськими машинами. Ці облікові дані не співвідносяться з реальними обліковими записами у домені, що є ключовою ознакою компрометації. На клієнтських машинах з операційною системою Windows зловмисники часто зчитують збережені облікові дані з процесу LSASS (Local Security Authority Subsystem Service) і використовують їх для автентифікації. Цей метод, відомий як «передача хешу» (Pass-the-Hash), є одним із найбільш поширених способів бокового руху в скомпрометованих мережах. У цьому сценарії передбачається, що зловмисник вже проникнув в одну з машин і встановив бекдор для збереження доступу.

Серед інших механізмів безпеки, як інструмент для виявлення APT-атак в мережі розглядається Honeynet-приманка середнього рівня взаємодії OpenCanary. OpenCanary має достатні потужності для виявлення фази вторгнення та експлуатації APT, виявлення аномального руху в мережевому просторі.

Розглянемо сценарій використання Honeynet користувача OpenCanary.

Для виявлення APT пропонується використовувати мережу, побудовану на основі Active Directory, яка включає щонайменше один контролер домену. Контролер домену виконує автентифікацію користувачів у домені, використовуючи орієнтований на клієнт-серверну архітектуру мережевий протокол Kerberos. Клієнтські машини в мережі мають можливість підключатися до контролера домену, отримуючи доступ до спільних ресурсів, таких як файли та сервери.

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Захарова Володимира Володимировича
ПІБ здобувача вищої освіти

Студента ФІТ, 2 курсу, групи КБЗІм-23-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений та надаю свою згоду на обробку й збереження університетом моєї роботи в інституційному репозитарії Хмельницького національного університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-обчислювального комплексу StrikePlagiarism та/або програмнотехнічного засобу Anti-Plagiarism і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення текстових збігів в роботах.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

12.12.2024
дата

підпис

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 11%**

	Документ		Сумарний збіг по Базі Даних	
ID: 158617 Назва: Метод організації системи захисту корпоративної інформації на основі технології Honeynet Додано в БД: 2024-12-13 Автора: Захаров Володимир Керівники: Чешун В.М. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	125475	1811	2517 (2%)	30 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Володимир Захаров

Співавтор:

Назва: Метод організації системи захисту корпоративної інформації на основі технології Honeynet

Науковий керівник: Віктор Чешун

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:1.4%

Коефіцієнт подібності 2:0.3%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2024-12-13 13:08:13.0

Після аналізу Звіту подібності констатую наступне:

☐ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

Дата 13.12.2024 експерт 

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Метод організації системи захисту корпоративної інформації на основі технології Honeynet

Автор: Захаров Володимир Володимирович

Спеціальність: 125 – Кібербезпека та захист інформації

Освітня програма:Кібербезпека та захист інформації

Науковий керівник:Віктор ЧЕШУН, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 99%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism складає 98,6%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 24.09.2024, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100%, визначається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ Віктор ЧЕШУН

Гарант ОП _____ Віра ТІТОВА

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Студент Захаров Володимир Володимирович

Тема Метод організації системи захисту корпоративної інформації на основі технології Honeynet

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Обсяг кваліфікаційної роботи освітнього ступеня «магістр»:

кількість листів креслень - ; кількість сторінок записки 99

1. Короткий зміст роботи та прийнятих рішень Кваліфікаційна робота присвячена визначенню базових теоретичних положень, способів і засобів реалізації методу організації системи захисту корпоративної інформації на основі технології Honeynet, орієнтованого на вдосконалення і розширення можливостей системи захисту корпоративної інформації за рахунок комплексного застосування можливостей зазначеної технології

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота відповідає поставленому завданню як в теоретичній, так і в практичній частині.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, чітко визначено об'єкт, предмет та методи дослідження, сформульована актуальність; визначені задачі, які необхідно вирішити для досягнення поставленої мети, практична цінність отриманих результатів, їхня новизна та наведені відомості про публікації. У першому розділі проведене дослідження вразливостей та способів захисту корпоративної інформації і технологій реалізації мережевих пасток в системах захисту. В другому розділі обгрунтовано, що найбільш оптимальним вибором для комплексного захисту є Honeynet, оскільки вона забезпечує високий рівень інтерактивності, дозволяє детально аналізувати дії зловмисників і надає широкі можливості для дослідження методів атак. В третьому розділі роботи визначено концепцію організації системи захисту корпоративної інформації на основі технології Honeynet і запропоновані рішення щодо організації системи захисту корпоративної інформації на основі технології Honeynet для комплексного захисту ресурсів корпоративної комп'ютерної мережі, вебзастосунків і систем моніторингу та управління. В четвертому розділі обґрунтовано вибір платформи Modern Honey Network для практичної реалізації системи захисту корпоративної інформації на основі технології Honeynet та розроблено політики безпеки використання системи захисту корпоративної інформації на основі технології Honeynet для захисту ресурсів корпоративної комп'ютерної мережі, вебзастосунків і систем моніторингу та управління.

4. Позитивні сторони роботи Кваліфікаційна робота має комплексну наукову і практичну цінність. Наукова цінність полягає у визначенні принципів організації системи захисту корпоративної інформації на основі технології Honeynet для комплексного захисту різних категорій ресурсів корпоративної інфосистеми. Практична цінність полягає наданні рекомендацій щодо вибору платформи для комплексного розгортання Honeynet та визначенні положень політик безпеки використання методу.

5. Негативні сторони роботи В роботі відсутня інформація про апробацію запропонованого методу моделюванням або в реальних умовах.

6. Оцінка графічного оформлення та пояснювальної записки роботи Оформлення всіх матеріалів кваліфікаційної роботи є якісним, здійснене з дотриманням актуальних стандартів та інституційних положень ХНУ. Пояснювальна записка відповідає нормам щодо її оформлення як за структурою, так і за представленням і форматуванням матеріалу.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та наскрізно пов'язаний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Презентаційний та ілюстративний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Мартинюк Валерій Володимировович
завідувач кафедри АКІТР, доктор технічних наук, професор

« 13 » 12 2024. (підпис)