МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ТЕХНОЛОГІЇ ВВЕДЕННЯ В ОМАНУ (DECEPTION TECHNOLOGY) У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА»

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

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

_____ Дмитро ЮНАК

(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61

Керівник: Тетяна МУЖАНОВА, к.держ.упр., доцент

Рецензент:

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека та захист інформації

Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____” _____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Юнаку Дмитру Олеговичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Технології введення в оману (Deception Technology) у забезпеченні кібербезпеки підприємства”,
керівник кваліфікаційної роботи Тетяна МУЖАНОВА, к.держ.упр., доцент
(Ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “30” жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи “11” грудня 2025р.

3. Вихідні дані до кваліфікаційної роботи *технології введення в оману (Deception Technology), технології введення в оману в банківському секторі.*

4. Перелік питань, які мають бути розроблені:
   1. Дослідити теоретичні основи технологій введення в оману в кібербезпеці.
   2. Проаналізувати особливості впровадження технологій введення в оману в банківському секторі.
   3. Розробити модель впровадження DT у SOC банку і запропонувати практичні рекомендації щодо удосконалення процесів реагування SOC із використанням зазначених технологій в банківському середовищі.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10.2025	
3.	Дослідження теоретичних основ технологій введення в оману в кібербезпеці	27.10.2025	
4.	Аналіз особливостей впровадження технологій введення в оману в банківському секторі	10.11.2025	
5.	Розробка моделі впровадження DT у SOC банку і практичних рекомендацій	15.11.2025	
6.	Формулювання висновків за результатами дослідження.	22.11.2025	
7.	Оформлення роботи.	04.12.2025	
8.	Оформлення презентації.	14.12.2025	
9.	Отримання рецензії на роботу.	18.12.2025	
10.	Захист в ЕК.	__.01.2026	

Здобувач вищої освіти _____ Дмитро ЮНАК
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Юнак Д.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Технології введення в оману (Deception Technology) у забезпеченні кібербезпеки підприємства"
Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **ЮНАК Дмитро** у кваліфікаційній роботі дослідив теоретичні основи технологій введення в оману в кібербезпеці; проаналізував особливості впровадження технологій введення в оману в банківському секторі; розробив модель впровадження DT у SOC банку і запропонував відповідні практичні рекомендації.

ЮНАК Дмитро показав високу теоретичну і практичну підготовку, здатність визначати і вирішувати науково-дослідницькі завдання. Кваліфікаційна робота оформлена згідно з вимогами. Виклад матеріалу здійснено послідовно, зроблено практично орієнтовані висновки. Ключові положення роботи представлено у вигляді рисунків і таблиць. Результати дослідження апробовані на конференції "Актуальні проблеми кібербезпеки" 29.10.2025 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача **ЮНАКА Дмитра** на оцінку «відмінно» та рекомендувати присвоєння йому кваліфікацію "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою".

Керівник кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"_____" ____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Юнак Д.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри управління
кібербезпекою та захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ЮНАКА Дмитра Олеговича
на тему «Технології введення в оману (Deception Technology) у забезпеченні кібербезпеки підприємства»

Актуальність. Традиційні засоби моніторингу (IDS/IPS, SIEM, EDR/XDR) не завжди забезпечують своєчасне виявлення атакувальної активності через високу фонову подієвість, значну частку помилкових спрацювань і складність оперативної інтерпретації подій. На цьому тлі технології введення в оману (Deception Technology, DT), які базуються на використанні керованих пасток, псевдоактивів і спеціальних маркерів для нападника, розглядаються як перспективний напрям розвитку активної оборони підприємства.

З огляду на зазначене дослідження технологій введення в оману у забезпеченні кібербезпеки підприємства є актуальним науково-прикладним завданням.

Позитивні сторони.

1. У роботі досліджено теоретичні основи технологій введення в оману в кібербезппеці; проаналізовано особливості впровадження технологій введення в оману в банківському секторі; розроблено модель впровадження Deception Technology (DT) у SOC банку і запропоновано практичні рекомендації щодо удосконалення процесів реагування SOC із використанням зазначених технологій в банківському середовищі.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено послідовно згідно з планом роботи, завдання дослідження виконані. Ключові положення роботи представлено у вигляді рисунків і таблиць. За темою роботи опрацьовано достатня кількість публікацій та електронних джерел.
3. Окремо слід відзначити, що здобувач проаналізував можливі точки інтеграції Deception Technology в інфраструктуру підприємства та виявив сценарії, де дані технології можуть дати найбільший практичний ефект (раннє виявлення розвідки, спроб крадіжки облікових даних, латерального переміщення тощо). Також автор розробив архітектурну модель впровадження DT в інфраструктурі компанії/банку із урахуванням сегментів DMZ, Office та Core, запропонував логічну схему розміщення DT-елементів, їх взаємодії із SIEM, SOAR та EDR/XDR, описав алгоритм обробки інцидентів на основі сигналів від DT-пасток.

Недоліки.

1. Доцільно було б приділити більше уваги вивченню деяких аспектів практичної реалізації запропонованих рішень (наприклад, вартісній оцінці впровадження конкретних DT-платформ, аналізу обмежень ліцензування та ресурсних вимог).

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач ЮНАК Дмитро Олегович заслуговує присвоєння кваліфікації “Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною безпекою”.

Рецензент:

_____
підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 82 с., 7 рис., 10 табл., 62 джерела.

Метою роботи є дослідження технологій введення в оману (Deception Technology, DT) у забезпеченні кібербезпеки підприємства.

Об'єктом дослідження є процеси забезпечення кібербезпеки підприємства/банку.

Предмет дослідження - технології введення в оману в забезпеченні кібербезпеки підприємства/банку.

Методи дослідження. Для вирішення завдань дослідження використано методи системного і порівняльного аналізу, архітектурного моделювання, узагальнення практик SOC та оцінювання ефективності на основі процесних і часових метрик.

Короткий зміст роботи. Як результат у роботі досліджено теоретичні основи технологій введення в оману в кібербезпеці; проаналізував особливості впровадження технологій введення в оману в банківському секторі; розробив модель впровадження DT у SOC банку і запропонував практичні рекомендації.

Галузь застосування. Розроблені підходи можуть бути використані при впроваджені технологій введення в оману у рамках системи моніторингу й реагування на інциденти безпеки SOC підприємства/банку.

КЛЮЧОВІ СЛОВА: ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА/БАНКУ, ЦЕНТР ОПЕРАЦІЙНОЇ БЕЗПЕКИ (SOC), ТЕХНОЛОГІЇ ВВЕДЕННЯ В ОМАНУ (DECEPTION TECHNOLOGY).

ABSTRACT

The text part of the qualification paper for obtaining a master's degree: 82 pages, 7 figures, 10 tables, 62 sources.

The purpose of the work is to study the Deception Technology in the enterprise cybersecurity.

Object of research is the cybersecurity processes of an enterprise/bank.

Subject of research is Deception Technology in cybersecurity of an enterprise/bank.

Research methods. To solve the research tasks, the methods of system and comparative analysis, architectural modeling, generalization of practical SOC and evaluation of efficiency based on process and time metrics were used.

Summary of the work. As a result, the work investigated the theoretical foundations of Deception Technology in cybersecurity; analyzed the features of the Deception Technology implementation in the banking sector; developed a model for implementing Deception Technology in the SOC of the bank and offered practical recommendations.

Field of research. The developed approaches can be used in the implementation of Deception Technology within the framework of the monitoring and response to security incidents of the enterprise/bank SOC.

Keywords: ENTERPRISE/BANK CYBERSECURITY, SECURITY OPERATIONS CENTER (SOC), DECEPTION TECHNOLOGY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

AD	Active Directory
API	Application Programming Interface
APT	Advanced Persistent Threat
DB	Data Base
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DT	Deception Technology
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IR	Incident Response
KPI	Key Performance Indicators
KRI	Key Risk Indicators
MTTD	Mean Time To Detect
MTTR	Mean Time To Repair
PDCA	Plan-Do-Check-Act
SIEM	Security Information and Event Management
SOAR	Security Orchestration Automation and Response
SOC	Security Operations Center
SOP	Standard Operating Procedures
XDR	Extended Detection and Response

ВСТУП

Актуальність теми. Посилення цифровізації бізнесу та зростання складності кібератак формують потребу у розвитку сучасних підходів до раннього виявлення загроз і підвищення ефективності реагування. Ця проблема є особливо критичною для установ банківського сектору через високу цінність даних, значну кількість інтегрованих сервісів і вимоги до безперервності фінансових операцій. Для України актуальність теми посилюється необхідністю зміцнення кіберстійкості фінансових установ і ключових підприємств в умовах підвищених ризиків для критичної інфраструктури та економічної стабільності.

Традиційні засоби захисту (IDS/IPS, SIEM, EDR/XDR) забезпечують базову спроможність моніторингу, однак на практиці SOC стикається з проблемами високого потоку подій, складності швидкої валідації сповіщень і ризику запізнілого виявлення атак у фазах розвідки, компрометації облікових даних і латерального переміщення.

У цих умовах технології введення в оману (Deceptive Technology, DT) розглядаються як додатковий шар активної оборони, що використовує різні приманки (decoys, honeytokens, honey credentials) для формування більш достовірних сигналів і підсилення раннього попередження. Нерозв’язаною частиною загальної проблеми залишається слабка формалізація архітектурних і процесних моделей впровадження DT у банківських установах і обґрунтованих підходів до оцінки її ефективності через показники SOC.

З огляду на зазначене дослідження технологій введення в оману (Deception Technology) у забезпеченні кібербезпеки підприємства є актуальним науковим завданням.

Метою роботи є дослідження технологій введення в оману у забезпеченні кібербезпеки підприємства/банку.

Об’єкт - процеси забезпечення кібербезпеки підприємства/банку.

Предмет дослідження - технології введення в оману у забезпеченні кібербезпеки підприємства/банку.

Для досягнення цієї мети в роботі необхідно виконати наступні *завдання:*

1. Дослідити теоретичні основи технологій введення в оману в кібербезпеці.

2. Проаналізувати особливості впровадження технологій введення в оману в банківському секторі.

3. Розробити модель впровадження DT у SOC банку і запропонувати практичні рекомендації щодо удосконалення процесів реагування SOC із використанням зазначених технологій в банківському середовищі.

Методи дослідження. Для вирішення завдань дослідження використано методи системного і порівняльного аналізу, архітектурного моделювання, узагальнення практик SOC та оцінювання ефективності на основі процесних і часових метрик.

Наукова новизна одержаних результатів полягає в тому, що вперше у межах даного дослідження запропоновано узагальнену сегментну модель впровадження технологій введення в оману у SOC банку, удосконалено процесну логіку взаємодії deception із SIEM/SOAR/EDR у вигляді послідовного алгоритму обробки сигналів, удосконалено методичний підхід до оцінювання ефективності DT через систему KPI/KRI з акцентом на MTTD, MTTR і показники якості сигналів.

Практичне значення отриманих результатів. Практичне значення роботи полягає у можливості використання запропонованих моделей і рекомендацій для побудови або модернізації SOC банків і підприємств із підвищеними вимогами до кіберстійкості. Запропоновані підходи можуть стати основою для розробки use cases, playbooks і внутрішньої системи вимірювання ефективності DT.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу» 28 лютого 2025 року.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ТЕХНОЛОГІЙ ВВЕДЕННЯ В ОМАНУ В КІБЕРБЕЗПЕЦІ

1.1 Актуальний стан та тенденції розвитку кіберзагроз

У сучасних умовах цифрової економіки інформаційні системи для більшості підприємств перестали бути лише допоміжним елементом. Вони фактично перетворилися на основу щоденної діяльності: через них проходять фінансові операції, обіг конфіденційних даних, комунікація з клієнтами та партнерами, внутрішній документообіг, аналітична та управлінська звітність. Будь-який серйозний збій або компрометація таких систем вже давно означає не просто технічну проблему, а повноцінну загрозу для безперервності бізнес-процесів, репутації та фінансової стабільності організації.

У цьому контексті кіберзагрози перестають бути абстрактною категорією. Під кіберзагрозою зазвичай розуміють потенційну або реальну подію, пов’язану з використанням інформаційно-комунікаційних технологій, яка може призвести до порушення конфіденційності, цілісності або доступності інформації, а також до збоїв у роботі критичних сервісів. Іншими словами, мова йде про будь-які дії (як навмисні, так і ненавмисні), що здатні завдати шкоди інформаційним ресурсам підприємства.

Аналітичні звіти з кібербезпеки демонструють стійку тенденцію до зростання кількості кіберінцидентів і ускладнення їхнього характеру. Поступово кіберпростір перетворився на окремий вимір конкуренції, протистояння та навіть війни, де інтереси держав, кримінальних угруповань, хактивістів та окремих зловмисників переплітаються і часто важко піддаються однозначній ідентифікації. На цьому фоні актуальність системного підходу до аналізу кіберзагроз, їхньої класифікації та розуміння тенденцій розвитку є очевидною.

Якщо узагальнити досвід останніх років, можна виокремити кілька ключових тенденцій, які визначають сучасний стан кіберзагроз. Вони не існують ізольовано, а взаємодіють між собою, формуючи складне та динамічне

середовище ризиків.

По-перше, спостерігається стале збільшення інтенсивності та масштабів атак. Кількість інцидентів, про які повідомляють як приватні компанії, так і державні структури, зростає практично щорічно. При цьому частина атак має глобальний характер, коли одна й та сама шкідлива кампанія вражає організації в різних країнах та регіонах.

По-друге, відбувається індустріалізація кіберзлочинності. На зміну одиночним хакерам-одинакам приходять добре організовані групи зі своєю внутрішньою структурою, фінансуванням, розподілом ролей та спеціалізацією. На чорному ринку з'являються пропозиції за моделлю as a service: оренда ботнетів, платформи для запуску атак програм-вимагачів, інструменти для масового фішингу тощо. Це робить кіберзлочинність доступнішою навіть для тих, хто не має глибоких технічних знань.

По-третє, відчутно зростає якість та таргетованість атак. Якщо раніше значну частину інцидентів становили масові кампанії, орієнтовані на широке коло жертв (наприклад, розсилки однотипного шкідливого спаму), то сьогодні все частіше спостерігаються прицільні операції. У їхній основі лежить попередня розвідка інфраструктури, бізнес-процесів, персоналу, що дозволяє будувати атаки під конкретну організацію.

По-четверте, зростає роль штучного інтелекту та автоматизації. ШІ використовується як у захисних механізмах (для виявлення аномалій, кореляції подій, прогнозування ризиків), так і в руках зловмисників: для автоматизованого підбору вразливостей, генерації переконливих фішингових листів, створення deepfake-контенту тощо. У результаті традиційні системи, що спираються лише на сигнатури або прості правила, не завжди встигають адаптуватися до нових патернів атак.

Нарешті, варто згадати фокус на критичних секторах, до яких належать фінанси, енергетика, транспорт, медицина, державне управління. Будь-який вдалий напад на такі об'єкти має ефект, який виходить далеко за межі однієї організації, впливаючи на суспільство та економіку в цілому [1, 2].

Попри постійну еволюцію технічних деталей, більшість кіберзагроз можна згрупувати в кілька узагальнених категорій. Вони різняться як за інструментами реалізації, так і за тим, на яку з ключових властивостей інформації (конфіденційність, цілісність чи доступність) спрямований основний удар.

Найпоширеніші типи кіберзагроз, їх коротка характеристика та цільовий вплив показані в табл. 1.1 [41, 53, 54, 55, 58].

Таблиця 1.1.

Узагальнені типи сучасних кіберзагроз

Тип загрози	Короткий опис	Основна мета (C/I/A)	Приклад для підприємства / банку
Програми-вимагачі (ransomware)	Шкідливе ПЗ, що шифрує файли або системи і вимагає викуп за відновлення	Доступність (Availability)	Шифрування файлових серверів і робочих станцій персоналу
DDoS-атаки	Масове перевантаження сервісу трафіком з метою виведення його з ладу	Доступність	Недоступність інтернет-банкінгу чи платіжного шлюзу
Банківські трояни, інфостілери	Шкідливе ПЗ, яке збирає облікові дані, реквізити карток, сесійні токени	Конфіденційність (Confidentiality)	Викрадення даних інтернет-банкінгу клієнтів
Атаки на бази даних, SQL-ін’єкції	Несанкціонований доступ до БД, модифікація чи видалення записів	Цілісність (Integrity)	Зміна балансів рахунків, даних клієнтів у внутрішніх системах
Фішинг та спір-фішинг	Обман користувачів через підроблені листи/сайти для отримання облікових даних	C → I → A	Отримання логінів працівників для доступу до внутрішніх систем

Продовження табл. 1.1.

Атаки на ланцюги постачання (supply chain)	Компрометація постачальника ПЗ або сервісів для подальшого нападу на клієнтів	Залежно від цілі атаки	Скомпрометований оновлювач ПЗ, що встановлюється на всі сервери банку
Insider-загрози	Дії співробітників чи підрядників, що мають легітимний доступ	Будь-яка з властивостей	Несанкціоноване копіювання БД, спроби шахрайських транзакцій
Wiper-атаки, саботаж	Навмисне знищення або пошкодження даних та систем	Цілісність / Доступність	Видалення журналів, конфігурацій, критичних файлів системи

Як видно з таблиці, загрози можуть по-різному впливати на конфіденційність, цілісність та доступність. Для фінансового сектору особливо небезпечними є атаки, спрямовані на порушення доступності критичних сервісів (онлайн-банкінг, платіжні системи), а також на компрометацію конфіденційних даних клієнтів і фінансової звітності [14, 15].

Сучасні кібератаки, як правило, реалізуються не як одинична дія, а як послідовність взаємопов’язаних етапів. Такий підхід дозволяє зловмиснику планомірно наближатися до своєї мети, мінімізуючи ризик виявлення. У багатьох методичних матеріалах цей процес описується через поняття життєвого циклу кібератаки.

У спрощеному вигляді можна виділити такі типові етапи (Рис. 1.1):

- Розвідка (Reconnaissance). Збирання інформації про ціль: публічні сервіси, доменні імена, відкриті порти, використовувані технології, структуру організації. Часто здійснюється через аналіз відкритих джерел, сканування мережі, соціальну інженерію.
- Початковий доступ (Initial Access). Пошук та використання конкретного вектора проникнення в систему: фішингове повідомлення з шкідливим

вкладенням, експлуатація вразливості у веб-додатку, використання вкрадених облікових даних, підбір пароля до VPN тощо.

- Закріплення (Persistence). Після отримання доступу зловмисник намагається створити умови для тривалої присутності в системі: додає облікові записи, змінює налаштування служб, встановлює бекдори, впроваджує шкідливих агентів.
- Рух усередині мережі (Lateral Movement). Атакувальник досліджує внутрішні сегменти, переміщується між хостами, намагається підвищити рівень привілеїв, шукає сервери з найбільш цінними даними або критичними функціями.
- Досягнення цілі (Impact / Exfiltration). На завершальному етапі досягається основна мета: шифрування даних, їхня крадіжка, модифікація важливих записів, виведення сервісів з ладу, публікація конфіденційної інформації тощо.

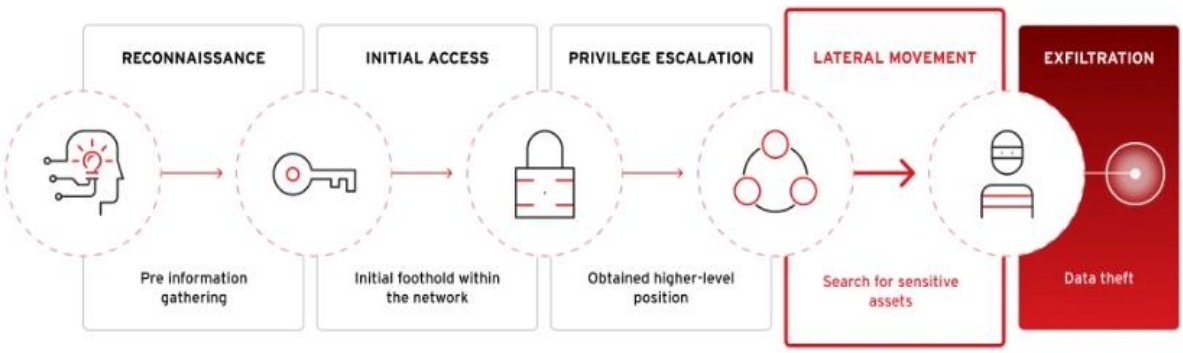

Рис. 1.1. Схема життєвого циклу кібератаки

З точки зору подальшої тематики роботи особливо цікавими є саме проміжні етапи – розвідка та рух усередині мережі. На цих стадіях зловмисник активно зондує інфраструктуру, пробує підключатися до різних ресурсів, тестує гіпотези щодо структури мережі та розміщення критичних активів. Саме тут можна найефективніше застосовувати технології введення в оману: розміщуючи пастки й приманки в логічно «привабливих» для зловмисника місцях, організація отримує можливість виявити його ще до того, як буде завдано реальної шкоди.

Для фінансового сектору кіберзагрози мають особливу вагу. Банки, платіжні компанії, страхові організації оперують великими обсягами коштів та

чутливих персональних даних. Будь-який серйозний інцидент тут може мати не лише прямі фінансові наслідки, а й викликати втрату довіри з боку клієнтів, підвищену увагу регуляторів і медіа.

До характерних загроз для фінансових організацій можна віднести:

- компрометацію акаунтів клієнтів інтернет-банкінгу;
- фішингові кампанії з метою викрадення реквізитів платіжних карток;
- атаки програм-вимагачів на внутрішні інформаційні системи;
- DDoS-атаки на публічні сервіси банку;
- внутрішні шахрайські схеми за участю співробітників або підрядників.

Нижче наведено узагальнюючу таблицю, яка ілюструє приклади загроз саме для фінансових установ [17, 18, 52, 60].

Таблиця 1.2.

Приклади актуальних кіберзагроз для фінансових організацій

Категорія загрози	Приклад сценарію	Потенційні наслідки
Фішинг клієнтів	Підроблений сайт інтернет-банкінгу, розсилка фішингових листів	Викрадення логінів/паролів, несанкціоновані транзакції
Атаки програм-вимагачів	Шифрування серверів документообігу та внутрішніх систем	Зупинка операційної діяльності, простій, фінансові втрати
DDoS-атаки	Масована атака на веб-портал банку та мобільний API	Недоступність сервісів, невдоволення клієнтів
Загрози ланцюжку постачання	Компрометація платіжного провайдера або процесингового центру	Масові інциденти, вплив на кілька банків одночасно
Внутрішні загрози, шахрайство	Несанкціоновані внутрішні перекази, зловживання службовим доступом	Прямі фінансові збитки, юридична відповідальність

В українському контексті ситуація додатково ускладнюється тим, що

кіберпростір є одним із ключових елементів гібридного протистояння. Кібератаки можуть мати не лише кримінальний, а й політичний чи військово-стратегічний характер, бути спрямованими на дестабілізацію роботи державних інституцій, фінансової системи, критичної інфраструктури. Це ще більше підвищує вимоги до побудови стійких, багаторівневих систем захисту.

Проведений аналіз показує, що сучасні кіберзагрози мають низку характерних рис: вони стають масовішими, складнішими, таргетованішими та організаційно більш зрілими. Для фінансових організацій, зокрема банків, це означає роботу в умовах постійно зростаючого тиску з боку зловмисників, коли помилка в сфері кіберзахисту може дорого коштувати не лише в буквальному сенсі, але й у плані довіри та репутації.

Традиційні засоби захисту: периметрові екрани, сигнатурні антивіруси, класичні IDS, – безумовно залишаються важливими елементами захисту, але вже не дають повної впевненості в тому, що атака буде виявлена на ранньому етапі. Часто вони фіксують наслідки вже реалізованих дій, тоді як зловмисник певний час встигав діяти всередині системи.

На цьому тлі логічним кроком є пошук нових підходів, що дозволяють активніше впливати на поведінку зловмисника. Одним із таких підходів є використання технологій введення в оману (Deception Technology, DT), які дозволяють створювати в інфраструктурі контрольовані пастки та приманки, формувати для атакувальника хибну картину середовища та забезпечувати службі безпеки ранні й чіткі сигнали про наявність шкідливої активності.

1.2 Еволюція технологій захисту інформації та поява DT

Еволюція технологій захисту інформації тісно пов’язана зі змінами в архітектурі корпоративних систем і зростанням складності кіберзагроз. Сучасні підходи до кібербезпеки сформувалися не одномоментно, а як результат поступового переходу від простих інструментів блокування загроз до комплексних моделей моніторингу, реагування та активної оборони. Розуміння

цієї еволюції дозволяє логічно пояснити появу «обманних технологій» як закономірного етапу розвитку засобів захисту [4].

Початково корпоративна безпека будувалася за периметровою моделлю, де основним завданням було відокремити внутрішнє середовище від зовнішнього. Такий підхід виглядав практичним у часи, коли інфраструктура була переважно локальною, працівники працювали в офісі, а сервісів із зовнішнім доступом було відносно небагато. Основними інструментами виступали мережеві екрани, базові механізми контролю доступу та антивірусні рішення. Однак розвиток інтернет-технологій і зростання кількості сценаріїв віддаленої роботи поступово виявили обмеженість периметрової логіки: зловмиснику достатньо було знайти один уразливий ланцюг (фішинг, слабкий VPN-доступ, помилка конфігурації), щоб опинитися у «довіреній» внутрішній зоні [24, 25].

Результатом цього стала поява концепції глибинної оборони. Вона передбачає побудову кількох рівнів захисту, щоб компрометація одного з них не означала автоматичного провалу всієї системи. У практичному вимірі це проявилося активним розвитком IDS/IPS, WAF, сегментації мережі, засобів контролю даних, управління вразливостями та посилення політик доступу. На цьому етапі організації поступово переходили від «захисту межі» до «захисту активів усередині».

Коли кількість компонентів безпеки суттєво зросла, з’явилася потреба у централізованому моніторингу. Саме так сформувалася роль SIEM-систем, які дозволяють агрегувати події з різних джерел і здійснювати кореляцію для виявлення складніших сценаріїв атак. Паралельно оформлюється організаційна модель SOC, де процеси аналізу, ескалації та реагування набувають системності. Водночас виникла практична проблема надлишкового потоку подій: багато організацій зіткнулися з alert fatigue, коли критично важливі сигнали можуть губитися серед менш значущих або помилкових спрацювань [21].

Подальший розвиток відбувався у напрямку поведінкового аналізу та більш глибокої телеметрії. З’явилися EDR- і XDR-рішення, які надали можливість бачити деталі активності на кінцевих точках і взаємопов’язувати їх

із мережею, поштою, хмарними середовищами та цифровими ідентичностями. Це стало суттєвим підсиленням можливостей SOC, особливо з точки зору виявлення нетипових дій, безфайловихатак атак і тривалого прихованого перебування зловмисника в мережі [16].

Сучасний етап розвитку захисту інформації все частіше пов’язується з ідеями Zero Trust та активної оборони. Zero Trust формує підхід, де не існує довіреної внутрішньої зони за замовчуванням, а кожна спроба доступу оцінюється динамічно на основі контексту, ризиків і принципу мінімальних привілеїв. У свою чергу активна оборона розширює логіку захисту, організація не лише блокує загрози, а й створює умови, які ускладнюють роботу зловмисника, сповільнюють його і підвищують ймовірність раннього виявлення.

У табл 1.3 показано еволюцію технологій захисту інформації.

Таблиця 1.3.

Узагальнення еволюції технологій захисту інформації

Етап розвитку	Провідна ідея	Типові інструменти	Ключове обмеження
Периметровий	Захистити межу організації	Firewall, ACL, базовий AV	Довіра до внутрішньої мережі
Глибинна оборона	Багатошаровий захист	IDS/IPS, WAF, сегментація, DLP	Висока залежність від правил і конфігурацій
Централізований моніторинг	Бачити загальну картину	SIEM, SOC-процеси	Надлишковий потік подій, “alert fatigue”
Поведінкова аналітика	Виявляти аномалії	EDR/XDR, UEBA, threat hunting	Високі вимоги до даних і експертизи
Активна оборона	Впливати на дії зловмисника	Deception, honeypots, honeytokens	Потреба в грамотному дизайні та інтеграції з SOC

Саме в такому контексті формуються і швидко розвиваються технології введення в оману, які можна трактувати як природне продовження еволюції захисту: від реактивного блокування до проактивного управління поведінкою атакувальника. DT створює в інфраструктурі пастки, приманки та фальшиві активи, взаємодія з якими є сильним сигналом компрометації. Це дозволяє зменшити шум для SOC і сфокусувати увагу аналітиків на подіях з високою вірогідністю реальної загрози [22].

Місце DT у структурі поглибленого захисту показано на рис.1.2.

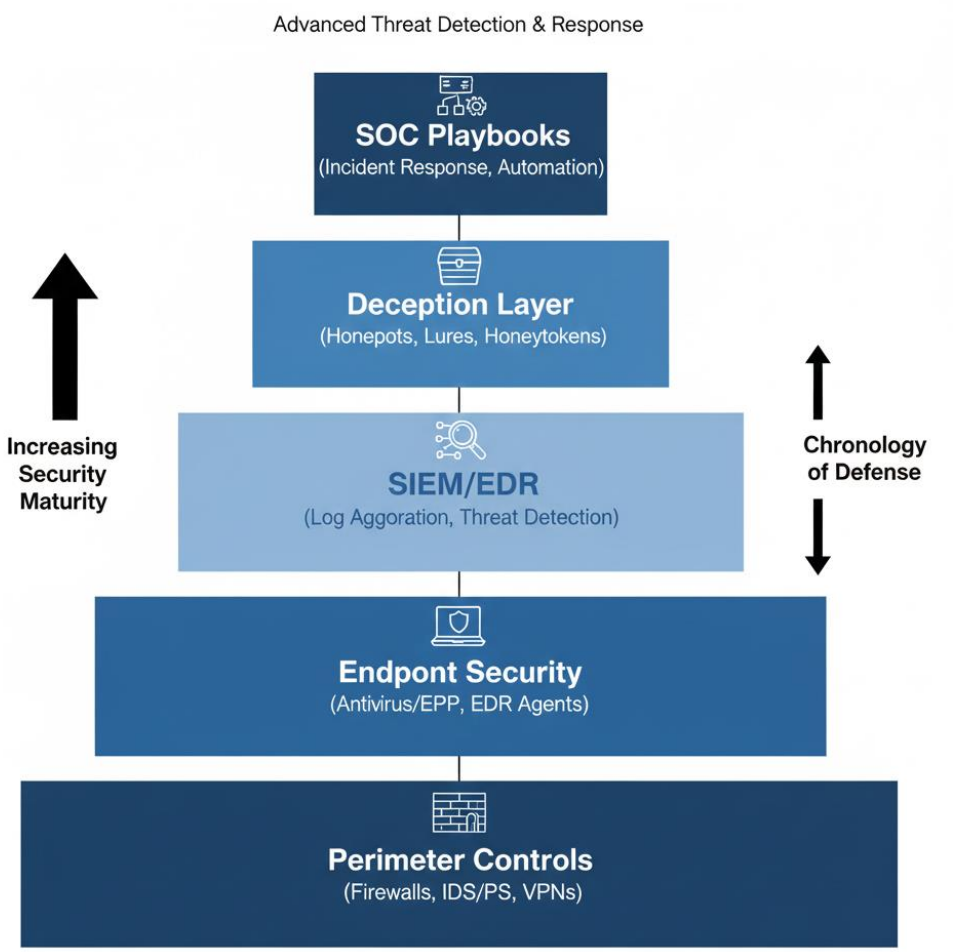

Рис. 1.2. DT у багатошаровій обороні.

1.3 Концептуальні засади Deception Technology

Технології введення в оману в сучасній кібербезпеці розглядаються як один із найпрактичніших інструментів активної оборони. На відміну від

класичних підходів, де основний акцент робиться на блокуванні відомих атак або виявленні аномалій у виробничих системах, концепція DT будує паралельний шар контрольованих об’єктів: приманок, пасток, маршрутизаторів уваги і фальшивих активів, які імітують реальні елементи інфраструктури і провокують зловмисника на взаємодію.

У загальному вигляді DT можна визначити як стратегію кіберзахисту, що створює реалістичні фіктивні активи для відволікання нападника від справжніх ресурсів та одночасного отримання більш точних сигналів про його активність. Важливо, що такі взаємодії вважаються високодостовірними: легітимний користувач зазвичай не має причин звертатися до підставних облікових записів, підроблених серверів або фейкових конфіденційних файлів. Саме тому DT-події часто мають низький рівень помилкових спрацювань порівняно з багатьма іншими засобами моніторингу [3-9].

Ця ідея знаходить підтримку і в контексті стандартів та рекомендацій. Зокрема, у підходах NIST введення в оману розглядається як елемент кіберстійкості та пов’язується з контролем SC-26 Decoys, який відноситься до технік «Misdirection/Deception». Це підкреслює, що впровадження обманних механізмів може бути обґрунтованим не лише технічно, а й з погляду відповідності сучасним практикам безпеки [20].

У фокусі DT знаходиться не просто «зловити хакера на гарячому», а сформувати контрольований простір, де поведінка зловмисника стає більш передбачуваною для SOC. Це особливо актуально в умовах, коли класичні засоби захисту здатні пропустити етапи прихованої розвідки чи латерального переміщення всередині мережі.

У концептуальному плані DT зазвичай вирішують три пов’язані задачі:

1. Раннє виявлення присутності зловмисника. Пастки встановлюються так, щоб атакувальник взаємодіяв із ними ще до безпосереднього доступу до критичних активів.

2. Зміна траєкторії атаки. Декой-ресурси формують для зловмисника хибну картину цінності та логіки мережі, збільшуючи час на розвідку та підвищуючи шанс помилок.

3. Отримання даних для аналітики та threat hunting. Взаємодія з deception-елементами дає додатковий контекст щодо TTPs атакувальника, що може бути корисним для покращення правил у SIEM/EDR і розвитку плейбуків SOC.

Таким чином, DT розглядається як підсилювач класичної оборони, а не як її заміна. У практичних моделях він повинен працювати поруч із SIEM, EDR/XDR, засобами сегментації та управління ідентичностями [5, 8, 43].

У більшості підходів концепція технологій введення в оману розкладається на кілька типових компонентів (Рис. 1.3):

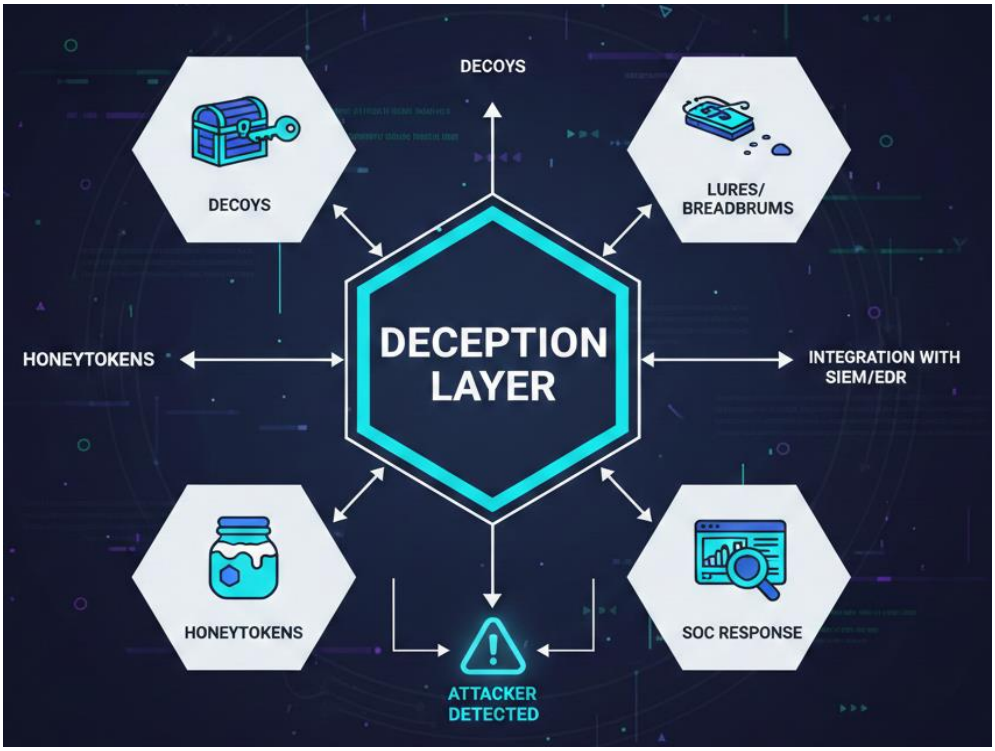

Рис. 1.3. Концептуальна модель DT

- Пастки/приманки (Decoys) - фальшиві системи або їхні частини, що імітують виробничі ресурси: сервери, БД, мережеві сервіси, робочі станції, веб-застосунки.

- Маршрутизатори уваги (Lures/Breadcrumbs) - «сліди», які повинні підказувати зловмиснику напрямок руху: файли з нібито паролями, конфіги, записи реєстру, підказки в каталогах.

- Фальшиві цифрові артефакти (Honeytokens) - підроблені облікові дані, токени доступу, ключі API або документи, використання яких одразу сигналізує про підозрілу активність.

Ці елементи можуть бути реалізовані як у класичній формі honeypots/honeynets, так і в новіших корпоративних платформах DT, які автоматизують розгортання, імітацію сервісів і передачу алертів у SOC.

Класифікація засобів введення в оману потрібна насамперед для того, щоб показати, що цей підхід не зводиться лише до honeypot як окремий сервер у кутку мережі. Насправді сучасні DT-рішення мають багаторівневий характер і можуть відрізнятися за глибиною імітації, місцем у інфраструктурі та типом приманки, на яку має відреагувати зловмисник. Для академічного опису доцільно розглядати кілька паралельних параметрів класифікації, які доповнюють одне одного.

По-перше, DT-засоби можна розрізняти за рівнем взаємодії. Найпростішими є низькорівневі пастки, що імітують лише окремі сервіси або мережеві відбитки. Вони не потребують складного адміністрування, швидко розгортаються і добре працюють як сенсори проти масової розвідки та автоматизованого сканування. Більш реалістичними вважаються середньорівневі приманки, які відтворюють частину логіки ОС чи застосунків і дозволяють отримувати більше даних про дії нападника. Найглибший рівень формують високорівневі пастки, які максимально наближені до справжніх систем; вони дають найцінніший матеріал для аналізу TTPs, однак потребують суворої ізоляції, контролю та продуманого дизайну, щоб не створити додаткових ризиків для продуктивного середовища.

По-друге, DT-засоби доцільно класифікувати за типом об’єктів, які імітуються або створюються як “помилково цінні” для зловмисника. Тут можна виділити декой-системи (фейкові сервери, робочі станції, мережеві сервіси), декой-додатки (імітація веб-інтерфейсів, тестових API, корпоративних сервісів), а також декой-дані (файли, фінансові звіти, договори, бази, які виглядають релевантними для викрадення). Окрему важливу групу формують «солодкі»

приманки (honeytokens): фальшиві цифрові артефакти, зокрема облікові дані, токени, ключі доступу і документи, використання яких є чистим індикатором компрометації.

По-третє, можна говорити про класифікацію за шаром інфраструктури. DT-елементи можуть розміщуватися на мережевому рівні (фейкові сегменти, маршрути, сервіси), на рівні кінцевих точок (декой-станції, пастки в системних каталогах), на серверному рівні (імітації файлових серверів, AD-подібних ресурсів), у площині прикладних систем (декой веб-додатки, внутрішні портали), а також у зоні даних та ідентичностей. У такій логіці DT стає не окремою коробкою, а розподіленим шаром, який можна адаптувати під топологію й пріоритети організації.

Нарешті, важливо підкреслити, що у практичному впровадженні ці класифікації зазвичай комбінуються. Наприклад, у банківській інфраструктурі можуть одночасно використовуватися низькорівневі мережеві приманки для раннього сигналу про сканування, honey-облікові записи для контролю спроб ескалації привілеїв, а також високорівневі сервери у тестових сегментах для збору поведінкових даних під час складних інцидентів. Це дозволяє створити більш живу та переконливу DT-екосистему, яка органічно доповнює SIEM, EDR/XDR та процеси SOC.

Найбільша цінність технологій введення в оману проявляється тоді, коли їх розглядати крізь призму життєвого циклу атаки: на етапі розвідки зловмисник активно вивчає мережу, сканує сервіси, читає структуру домену й шукає “шляхи до цінних активів”, під час первинного доступу і закріплення він намагається підтвердити свої гіпотези щодо корисності отриманого входу, а на стадії латерального переміщення шукає привілейовані облікові записи, файлові пастки, маршрутизатори уваги і фальшиві артефакти сховища, сервери застосунків або сегменти, які можуть вести до платіжних чи клієнтських систем; саме в цей момент добре розміщені здатні перехопити увагу нападника, змусити його взаємодіяти з контрольованим об’єктом і сформувати високодостовірний сигнал для SOC ще до того, як буде завдано прямої шкоди продуктивним активам.

У концептуальному сенсі DT приваблює тим, що дозволяє переносити частину ініціативи на бік захисту, підвищувати ймовірність раннього виявлення, зменшувати шум у моніторингу та отримувати чисті індикатори компрометації, які природно підси SIEM і EDR/XDR, а також дають додатковий контекст для розвідки загроз і розвитку плейбуків SOC.

Водночас цей підхід не є універсальною відповіддю на всі загрози, оскільки ефективність deception залежить від правдоподібності пасток, грамотного розміщення приманок у логічно привабливих для атакувальника зонах, якісної ізоляції високорівневих decoys і правильно налаштованої інтеграції з процесами реагування, інакше існує ризик або викриття deception-середовища досвідченим противником, або зниження практичної цінності сигналів через слабку операційну взаємодію з SOC.

1.4 Порівняння DT з класичними методами виявлення загроз

Порівняння технологій введення в оману з класичними методами виявлення загроз є важливим кроком для розуміння їх реального місця у сучасній архітектурі кібербезпеки. У практиці підприємств, зокрема банківських установ, системи захисту рідко будуються навколо одного інструмента. Найчастіше це комплекс взаємопов’язаних технологій, де кожен компонент закриває свою частину проблеми: периметр, кінцеві точки, мережевий трафік, журнали подій, поведінку користувачів тощо. Саме тому DT потрібно розглядати не як альтернативу всьому «класичному стеку», а як підхід, який змінює логіку виявлення атак на певних етапах і додає SOC точніші сигнали.

Класичні методи виявлення загроз історично формувалися навколо двох базових ідей: виявити відоме (сигнатури, правило, шаблон атаки) і виявити підозріле (аномалія, відхилення від нормальної поведінки).

Саме ці ідеї лежать в основі IDS/IPS, SIEM, багатьох антивірусних і поведінкових механізмів. DT вводить третю вид логіку: виявити зловмисника через його неминучий контакт із контрольованими пастками [3-6].

IDS та IPS як класичні мережеві механізми. Системи IDS/IPS традиційно виконують роль стоирожа мережевих комунікацій. Вони аналізують трафік, порівнюють його з набором сигнатур або правил і намагаються визначити, чи присутні ознаки атаки. У випадку IPS система не лише виявляє загрозу, а й може автоматично блокувати підозрілий трафік.

До сильних сторін IDS/IPS відносять швидкість і відносну ефективність проти масових і типових мережевих атак. Водночас їхні слабкі місця проявляються у складніших сценаріях: добре замасковані або нові техніки можуть залишатися непоміченими, а чутливість системи часто призводить до підвищеного рівня шуму.

DT у цьому контексті діє інакше: вона не аналізує весь трафік світу, а створює цільові точки спостереження, де сама поява мережевої взаємодії вже є підозрілою. Це знижує потребу “вгадувати” шкідливість кожного пакета.

SIEM як інструмент централізованої кореляції. SIEM-система є одним із ключових компонентів сучасного SOC. Вона агрегує події з різних джерел: ОС, мережевих пристроїв, хмарних сервісів, систем захисту, бізнес-додатків. Її основна сила полягає у можливості будувати кореляційні правила, знаходити комплексні сценарії атак і надавати аналітикам широку картину.

Однак практичний виклик SIEM - це баланс між повнотою моніторингу та якістю сповіщень. У реальному середовищі SIEM може генерувати значну кількість тривог, і без зрілої моделі правил і процесів це призводить до перевантаження аналітиків.

DT добре доповнює SIEM тим, що створює події з високою цінністю. Якщо SIEM часто працює як велика система спостереження, то DT додає в неї точкові сигнали, які легше інтерпретувати й швидше обробляти.

Введення в оману як активна модель виявлення. На концептуальному рівні DT базуються на тому, що атакувальник майже неминуче здійснює розвідку, шукає привілейовані ресурси, перевіряє доступи, аналізує структуру мережі. Якщо в цьому середовищі є правдоподібні пастки, приманки та фальшиві артефакти, то контакт із ними стає сильним сигналом присутності зловмисника.

Цінність DT особливо помітна у таких аспектах:

- надання ранніх сигналів на етапах розвідки або латерального руху;
- значне зменшення ймовірності помилкових спрацювань, оскільки легітимні користувачі зазвичай не мають причин звертатися до декой-ресурсів;
- створення додаткового простору для збору даних про техніки нападника, що корисно для пошуку загроз і розвитку правил їх виявлення.

Порівняльна характеристика методів виявлення загроз представлена у табл. 1.4.

Таблиця 1.4.

Порівняння DT з класичними методами виявлення загроз

Критерій	IDS	IPS	SIEM	Deception Technology
Основна роль	Виявлення мережевих атак	Виявлення + блокування	Централізований моніторинг і кореляція	Активне виявлення через пастки і приманки
Тип даних	Мережевий трафік	Мережевий трафік	Логи й події з багатьох джерел	Події взаємодії з приманками і декой-активами
Базова логіка	Сигнатури/ правила, інколи аномалії	Сигнатури/ правила з реакцією	Кореляція, аналітика, правила, контекст	Дотик до пастки - високий ризик
Сильні сторони	Добре проти типових мережевих загроз	Швидке блокування відомих атак	Широка видимість, комплексні сценарії	Високоточні сигнали, раннє виявлення
Типові слабкі місця	Шум, складність налаштування	Ризик блокування легітимного трафіку	Перевантаження тривогами, залежність від зрілості правил	Вимагає правдоподібного дизайну, інтеграції з SOC
Де найбільш ефективно	Периметр, контроль мережевих протоколів	Периметр, критичні канали	Уся організація, централізований SOC	Внутрішня мережа, критичні сегменти, AD/дані
Тип результату для SOC	Сигнал про підозрілий трафік	Сигнал + блокувальна дія	Сповіщення на основі кореляції подій	Чистий індикатор інциденту

Таблиця наочно демонструє, що DT не дублює класичні механізми, а працює в іншій логіці. Якщо IDS/IPS фокусуються на аналізі трафіку, а SIEM на агрегації та кореляції подій, то deception створює контрольні точки, де сама активність є потенційно інцидентною [4, 21-24].

У практичному середовищі найкращий ефект DT досягається не в ізоляції, а у поєднанні з SIEM та EDR/XDR. У такій моделі DT додає високоякісні сповіщення, SIEM забезпечує кореляцію з іншими джерелами, а EDR/XDR допомагає швидко підтвердити пов'язані дії на кінцевих точках і автоматизувати первинні кроки реагування (Рис. 1.4).

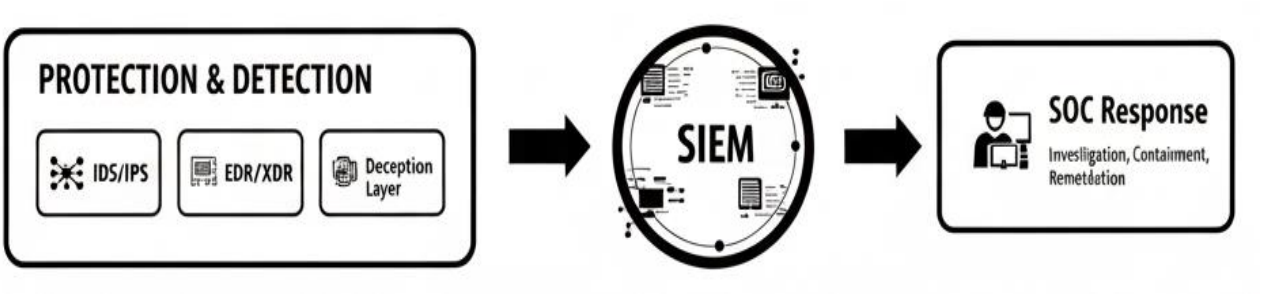

Рис. 1.4. Поєднання DT з SIEM та EDR/XDR

Для банківської сфери це особливо важливо, оскільки саме там стандартні інфраструктури є багаторівневими і відносно стандартизованими: доменні середовища, сервери критичних застосунків, сегменти платіжної інфраструктури, робочі станції операційних підрозділів. DT може бути налаштована так, щоб формувати пастки, які для нападника виглядають як логічні переходи до фінансів або даних клієнтів, а для SOC, як індикатори можливого початку складної, прихованої атаки [26-28].

1.5 Нормативні та стандартні вимоги, пов'язані з DT

DT рідко прямо згадується в законах чи стандартах як обов'язкова технологія, проте її застосування цілком узгоджується з сучасними вимогами до моніторингу, управління ризиками, виявлення інцидентів та забезпечення кіберстійкості. Саме через таке «непряме нормативне підкріплення» DT варто розглядати як технологічний інструмент, що допомагає виконувати вимоги

регуляторів і міжнародних практик, а не як ізольовану інновацію без формального підґрунтя.

На рівні міжнародних підходів одним із найважливіших аргументів є те, що deception концептуально підтримується сучасними контрольними моделями. У NIST SP 800-53 Rev.5 присутній контроль SC-26 (Decoys), у якому закладається сама ідея використання спеціально створених об’єктів як цілей для атак з метою виявлення, відволікання та аналізу дій противника. Це фактично легітимізує deception як елемент сучасної системи кіберзахисту, особливо для організацій, що будують безпеку на базі кращих міжнародних практик [20].

Стандарти сімейства ISO/IEC 27001:2022 та 27002:2022 не описують DT як окрему вимогу, проте вони суттєво посилюють фокус на системному моніторингу, журналюванні та роботі з даними про загрози. У цьому контексті введення в оману може розглядатися як практичний спосіб підвищити якість виконання таких заходів, оскільки події взаємодії з приманками зазвичай мають високий рівень достовірності та добре підходять для аналітики SOC і розвитку внутрішньої розвідки загроз [11-13, 16].

У фінансовій сфері додатковим фактором є вимоги до безпеки платіжних середовищ. Стандарт PCI DSS у версії 4.x стабільно наголошує на необхідності якісного журналювання та моніторингу доступу до критичних компонентів, що в реальних умовах найчастіше реалізується через SIEM та суміжні інструменти. У цій логіці DT не замінює вимог PCI DSS, але може підсилювати їхню практичну реалізацію, надаючи більш чисті тригери для перевірки підозрілих сценаріїв доступу або латерального руху в потенційно чутливих сегментах.

Важливим є і загальноєвропейський тренд на посилення кіберстійкості фінансових організацій. Регуляторна рамка DORA, яка почала застосовуватися з 17 січня 2025 року, підкреслює значення управління IT-ризиками, інцидент-менеджменту, тестування стійкості та контролю постачальників. Навіть якщо українські банки не підпадають під неї прямо, сама логіка такого регуляторного підходу демонструє напрям розвитку галузі: фінансові організації мають не лише захищатися, а й постійно підтверджувати здатність виявляти атаки й утримувати

операційну стійкість. DT добре вкладається в цю парадигму як елемент активної оборони, що дозволяє покращувати раннє виявлення та збирати дані про реальні техніки зловмисників.

У межах України фундаментальним нормативним підґрунтям залишається Закон «Про основні засади забезпечення кібербезпеки України», який закріплює принципи державної політики у сфері кіберзахисту. Практично ж для банківського сектору ключову роль відіграє Положення НБУ щодо організації кіберзахисту в банківській системі України (Постанова №178 від 12.08.2022). Логіка документа полягає у вимозі системності: банк має мати повноцінні процеси управління ризиками, виявлення подій, реагування на інциденти, а також відповідну організаційну та технологічну зрілість. У такому середовищі DT стає не експериментом, а потенційно корисним підсилювачем SOC і джерелом точних сигналів про можливу компрометацію, особливо в критичних сегментах [17, 18, 50, 52, 60].

Додатковий аргумент для банківської сфери України формує наявність галузевих механізмів координації та обміну інформацією про загрози, зокрема практики CSIRT-NBU і MISP-NBU. Це демонструє, що сектор уже має інституційні інструменти для накопичення й поширення релевантних індикаторів. DT у цьому сенсі може виступати одним із джерел високоякісних артефактів і поведінкових даних, які підсилюють як внутрішні процеси SOC, так і загальногалузеву ситуаційну обізнаність.

Отже, нормативне та стандартне поле не вимагає використання технологій введення в оману буквально, проте чітко формує набір завдань, для яких DT є практично доречним рішенням. DT підсилює вимоги моніторингу й логування, сприяє підвищенню точності виявлення інцидентів, збагачує розвідку загроз і підтримує сучасну парадигму активного захисту. Саме тому для банківського SOC DT може розглядатися як обґрунтований компонент архітектури кіберзахисту, що органічно доповнює SIEM та EDR/XDR і підвищує загальну кіберстійкість установи.

Висновки до розділу 1

У розділі 1 описано теоретичні засади застосування технологій введення в оману у кібербезпеці підприємства. Визначено, що зростання складності та таргетованості атак, особливо у фінансовому секторі, вимагає доповнення класичних механізмів виявлення. Показано, що DT є інструментом активної оборони, який підсилює IDS/IPS, SIEM та EDR/XDR завдяки більш точним сигналам і можливості раннього виявлення дій зловмисника. Узгодження цього підходу з сучасними стандартними та регуляторними вимогами обґрунтовує його доцільність у SOC банку й формує основу для подальшого прикладного аналізу.

РОЗДІЛ 2. ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ВВЕДЕННЯ В ОМАНУ В БАНКІВСЬКОМУ СЕКТОРІ

2.1 Система кібербезпеки банківського сектору України

Кібербезпека банківського сектору України сьогодні розвивається як цілісна багаторівнева система, що поєднує державні пріоритети кіберстійкості з галузевими правилами та внутрішньою практикою кожного банку. Це означає, що забезпечення захисту в банківській сфері не обмежується лише технічними засобами або ініціативами окремих установ. Навпаки, воно формується в межах чіткої нормативної та організаційної моделі, де державні засади, регуляторні вимоги та операційні механізми банків мають працювати як взаємодоповнювані елементи.

Національний рівень задає загальну рамку функціонування кібербезпеки як складової стійкості держави. У цьому контексті банки розглядаються не просто як комерційні установи з власними інформаційними системами, а як важлива частина критичної економічної інфраструктури. Такий підхід логічно підвищує вимоги до безперервності фінансових сервісів, захисту клієнтських даних та готовності до масштабних і комплексних кібервпливів. Відповідно, питання кіберзахисту набуває статусу стратегічного й безпосередньо пов’язане з національною безпекою та функціональною стійкістю фінансової системи.

Галузевий рівень у банківській сфері визначається передусім регуляторною позицією Національного банку України. Важливо, що НБУ не обмежується лише формальним встановленням вимог, а розвиває власну інституційну екосистему кіберзахисту фінансового ринку. Такий підхід підсилює практичну керованість і дозволяє створювати загальні стандарти реагування та взаємодії між установами. Фактично формується єдина координаційна модель, яка орієнтована не тільки на контроль, а й на розвиток зрілості сектору.

Центральним нормативним документом у цій системі є положення НБУ, яке регламентує організацію кіберзахисту в банківській системі. Його роль полягає у встановленні вимог до системності захисту, правил інформаційного обміну, підходів до охорони об’єктів критичної інформаційної інфраструктури, а також до незалежного оцінювання стану інформаційної безпеки. Важливою характеристикою такого регуляторного поля є його динамічність: оновлення і коригування вимог свідчать про пристосування нормативної бази до зміни загроз, технологій та практик кібероборони.

Паралельно з нормативною частиною НБУ розбудовує і прикладні механізми галузевого реагування. У межах цієї архітектури функціонує спеціалізований напрям, відповідальний за координацію та підвищення ефективності кіберзахисту як банківського, так і небанківського фінансового сегментів. Помітним елементом цієї системи є галузева команда реагування на комп’ютерні інциденти, яка виконує функції оперативного моніторингу, аналітики загроз, формування рекомендацій, підготовки індикаторів компрометації та підтримки установ у разі масштабних інцидентів. Така модель корисна тим, що забезпечує не лише реакцію на події, а й накопичення секторного досвіду, який може бути швидко трансформований у практичні заходи захисту для всієї банківської екосистеми.

Окрему роль відіграє організований обмін інформацією про загрози. Для банків особливо важливо мати можливість швидко отримувати релевантні дані про актуальні тактики й технічні артефакти атак, спираючись не лише на власний моніторинг, а й на досвід інших гравців ринку. Саме тому розвиток платформ секторної розвідки загроз має стратегічне значення: він дозволяє знизити час на виявлення загроз і підвищити узгодженість дій фінансових установ у ситуаціях підвищеного ризику.

На внутрішньому рівні кожен банк реалізує регуляторні та галузеві вимоги через власну модель кіберзахисту. Вона, як правило, включає управління ризиками, політики й процедури інформаційної безпеки, технічні засоби контролю та безпеки, а також операційну модель моніторингу й реагування.

Ключовою вимогою сучасної практики є не просто наявність окремих інструментів, а їх інтеграція в процеси та забезпечення вимірюваної ефективності. У цьому сенсі розвиток SOC, впровадження SIEM та контроль кінцевих точок через EDR/XDR є базовою необхідністю для банківської сфери, де будь-яка затримка у виявленні інциденту може мати високі операційні й репутаційні наслідки [19, 20, 48-50].

Таблиця 2.1.

Модель кібербезпеки банківського сектору України

Рівень	Змістова роль у системі
Державний	Формує загальні правові та стратегічні засади кібербезпеки як складової національної стійкості.
Галузевий (НБУ)	Встановлює спеціалізовані вимоги до кіберзахисту банків, забезпечує координацію, реагування та правила інформаційного обміну на рівні сектору.
Внутрішньобанківський	Реалізує нормативні вимоги через архітектуру безпеки, процеси SOC, управління інцидентами, ризиками та безперервністю критичних сервісів.

У межах такої системи застосування Deception Technology виглядає методологічно логічним. Банківська модель кіберзахисту орієнтується на підвищення точності виявлення, скорочення часу реагування, розвиток секторного обміну інформацією та захист критичних функцій. Deception може стати технологічним доповненням цієї логіки, оскільки дозволяє формувати високодостовірні сигнали про присутність зловмисника в інфраструктурі та зменшувати навантаження на аналітичні ресурси SOC через більш чисті індикатори компрометації [18, 51].

2.2 Архітектура SOC банку і точки застосування DT

Архітектура SOC у банківській установі формується як поєднання технологічного шару моніторингу та організаційних процесів реагування, які

мають забезпечувати безперервний контроль критичних сервісів і швидке виявлення небезпечної активності. На практиці банк є одним із найбільш складних типів підприємств з точки зору кіберзахисту, оскільки тут одночасно функціонують класичні корпоративні IT-сервіси, спеціалізовані фінансові платформи, платіжні контури, віддалені канали обслуговування, інтеграції з партнерами та регуляторними системами. Внаслідок цього SOC банку не може працювати лише за універсальним сценарієм, він має бути прив’язаний до бізнес-критичних процесів і сегментів інфраструктури, які створюють найбільшу зону ризику.

У типовій моделі SOC центральним елементом виступає середовище збору та аналітики подій, яке агрегує журнали й телеметрію з мережі, серверів, кінцевих точок, систем керування ідентичностями, хмарних сервісів, засобів периметрового захисту та прикладних банківських платформ. Ця шарова модель дозволяє формувати загальну картину подій у середовищі, а також будувати кореляційні сценарії, зокрема щодо компрометації облікових записів, аномальних доступів, нетипових мережевих комунікацій чи використання вразливостей у публічних сервісах. Паралельно важливу роль відіграють рішення класу EDR/XDR, які дають глибший контекст на рівні кінцевих точок і дозволяють швидше підтверджувати або спростовувати підозрілу активність, пов’язану з процесами, скриптами, механізмами закріплення та внутрішнім переміщенням зловмисника.

Однак саме у банківських середовищах традиційна модель моніторингу часто стикається з практичним обмеженням: обсяг подій надто великий, а цінність окремих сигналів може бути нерівномірною. Навіть якісно налаштований стек захисту нерідко генерує широкий спектр алертів, серед яких критично важливі індикатори складних атак можуть маскуватися у загальному потоці. У такій ситуації Deception Technology є DT логічним підсилювачем архітектури SOC, оскільки додає до загального моніторингу окремий шар високодостовірних сигналів, де сама взаємодія з приманкою вже є підставою для підвищеної уваги [4, 21-25, 27].

З погляду архітектури, DT у банку доцільно розглядати як розподілену систему контрольованих об’єктів, яка впроваджується саме у тих точках, де зловмисник найбільш ймовірно проводитиме розвідку або спроби ескалації доступу. Це не означає, що DT має дублювати всі компоненти інфраструктури. Навпаки, її сила полягає у точності і розумному психологічному дизайні. Приманки повинні бути розміщені так, щоб для нападника вони виглядали як природні маршрути руху до цінних активів, а для SOC як маркери небезпечних намірів.

Особливо перспективними для DT у банківській інфраструктурі є доменні та ідентифікаційні контури, сегменти доступу до критичних серверів, зони з підвищеною концентрацією даних, а також проміжні вузли, які можуть бути використані для латерального переміщення. У реальних сценаріях атак саме корпоративні ідентичності, адміністративні групи, файлові ресурси й сегменти управління інфраструктурою часто стають цілями зловмисника не меншою мірою, ніж вузькоспеціалізовані банківські системи. Це пояснюється тим, що компрометація цих універсальних точок відкриває шлях до подальшого контролю над фінансовими сервісами.

На практиці DT добре вписується у логіку SOC як інструмент, що працює на стику трьох важливих задач: раннє виявлення, зниження шуму та збагачення контексту. У першому випадку DT здатна спрацювати на етапах розвідки або первинного проникнення, коли атакувальник здійснює сервісне сканування або шукає пріоритетні облікові дані. У другому випадку події DT зазвичай є рідкісними й більш інформативними, що дозволяє SOC підвищити точність реакції. У третьому випадку приманки працюють як джерело поведінкових даних, які можуть бути використані для розвитку правил SIEM і сценаріїв пошуку загроз [24, 25, 60].

На рис. 2.1 показана узагальнена архітектура SOC банку і точки застосування технологій введення в оману.

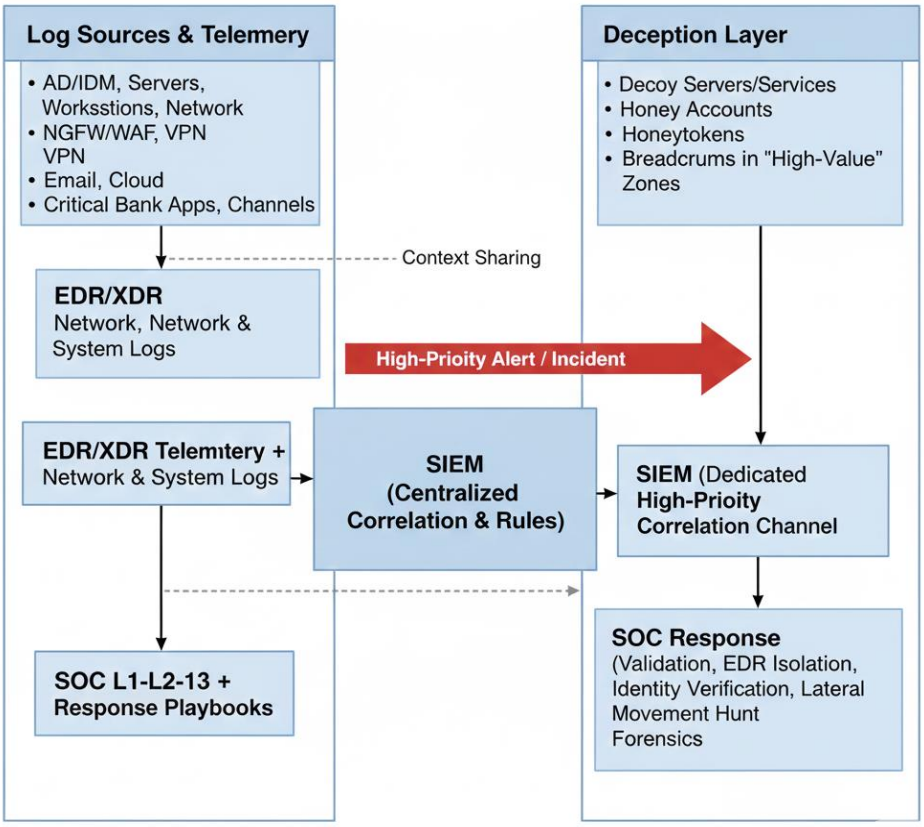

Рис. 2.1 Узагальнена архітектура SOC банку та точки застосування DT

2.3 Інтеграція DT в архітектуру банку

Інтеграція DT в архітектуру банку має сприйматися не як точкове впровадження окремого інструмента, а як формування додаткового рівня активної оборони, що органічно доповнює існуючі механізми моніторингу й реагування. У банківському середовищі особливо важливо уникати ситуацій, коли deception існує автономно у вигляді локального експерименту або ізольованої платформи без чіткої операційної цінності для SOC. Такий підхід не дає системного результату. Натомість справжній потенціал обманних технологій розкривається тоді, коли вона вбудовується у загальну логіку захисту й зміщує акценти від суто реактивного виявлення до контрольованого виявлення через провокування противника на взаємодію з підставними активами [1, 2].

Першим принципом інтеграції є відповідність DT реальній структурі банківської інфраструктури. Банк зазвичай має кілька взаємопов’язаних, але

різних за критичністю контурів: корпоративну мережу, доменну інфраструктуру та системи керування ідентичностями, сегменти адміністрування, канали віддаленого доступу, серверні зони прикладних сервісів, а також компоненти, що підтримують фінансові операції й взаємодію з клієнтами. У такому ландшафті deception доцільно розміщувати не повсюдно, а точково там, де зловмиснику найбільш природно шукати привілеї, ключі доступу або маршрути до даних. Саме точність і правдоподібність у виборі місця часто визначають ефективність цього підходу [5, 8].

Другим важливим принципом є безпечність архітектурного дизайну DT. Банківські системи не мають простору для ризикових експериментів, тому пастки й приманки повинні бути добре ізольованими та передбачуваними у поведінці. Зокрема, високорівневі декой-рішення мають бути розгорнуті так, щоб вони не могли перетворитися на проміжну точку для атак на продуктивне середовище. Мережеве відокремлення, контроль вихідних комунікацій, мінімально необхідні сервіси та чітка модель взаємодії з реальними ресурсами - це базові умови, без яких DT не може розглядатися як зрілий компонент банківської архітектури.

Третім елементом інтеграції є налаштування DT під реалістичні маршрути атак. Для банківського сектору найбільш логічними становляться сценарії, пов’язані з доменними службами, сервісними обліковими записами, псевдосерверами управління, слідами у файлових ресурсах і документах, що імітують фінансово значущу інформацію. Такі приманки працюють не лише як технічні сенсори, а як інструменти керування увагою противника: вони формують для атакувальника правдоподібну картину цінності середовища й водночас створюють для SOC події з підвищеною достовірністю.

Четвертий аспект - технологічна інтеграція технологій введення в оману з екосистемою SOC. Найбільш результативною є модель, у якій DT-події не залишаються в межах окремої панелі продукту, а потрапляють у SIEM як висопріоритетне джерело даних і корелюються з журналами доменних служб, мережевих компонентів, серверів і телеметрією EDR/XDR. У цьому випадку

SOC отримує не просто сигнал підозрілої взаємодії, а розширений контекст: який обліковий запис був залучений, звідки відбулася активність, чи зафіксовані ознаки ескалації привілеїв або латерального руху, які процеси запускалися на кінцевій точці. Така зв'язка підвищує швидкість і якість валідації інциденту та зменшує ризик як пропуску атаки, так і надмірної реакції.

П'ятий аспект - включення DT у процесну модель реагування. У зрілих банківських SOC події, пов'язані з decoys і honeytokens, мають запускати зрозумілий алгоритм перевірки: швидку валідацію через суміжні джерела, перевірку активності пов'язаних облікових записів, оцінку потенційного розповсюдження та ініціацію локалізаційних дій за потреби. Якщо в банку застосовується автоматизація реагування, DT може виступати безпечним тригером для керованих і обмежених дій, наприклад, збору додаткової телеметрії чи запуску пошукових запитів у SIEM/EDR. У фінансовій установі це особливо важливо, адже будь-які автоматичні рішення мають бути збалансованими з вимогами безперервності операцій.

Враховуючи високі вимоги банків до безперервності сервісів та контрольованості змін, впровадження DT доцільно здійснювати поступово. Поетапна модель дозволяє спочатку відпрацювати точні сценарії для ідентичностей і доменного середовища, а далі масштабувати приманки на серверні сегменти, дані та прикладні сервіси, не створюючи додаткових архітектурних ризиків. Такий підхід забезпечує одночасно передбачуваність для IT-підрозділів і практичну користь для SOC, що відображено в таблиці 2.2.

Таблиця 2.2.

Поетапна модель впровадження Deception Technology у банку

Етап	Зміст робіт	Основні цілі	Очікуваний результат для SOC
Пілотний	Обмежене розгортання фіктивних акаунтів і файлів у контрольованих зонах; базова інтеграція з SIEM	Перевірка правдоподібності приманок і коректність сповіщень	Перші "чисті" алерти, простий сценарій валідації

Продовження табл. 2.2.

Розширений	Додавання decoy-серверів у ключові сегменти; налаштування кореляції з доменними й мережевими логами	Виявлення розвідки та латерального переміщення	Підвищення точності інцидентів і зменшення шуму
Операційно зрілий	Інтеграція з EDR/XDR; стандартизація плейбуків; регулярні перевірки ефективності	Перетворення DT на частину повсякденних процесів SOC	Швидша валідація інцидентів і скорочення часу реагування
Масштабований	Розгортання у прикладних сервісах, даних і віддаленому доступі; контроль охоплення сценаріїв	Підсилення критичних банківських контурів	Раннє виявлення комплексних атак у пріоритетних зонах

2.4 Огляд рішень на ринку засобів введення в оману

Сучасний ринок технологій введення в оману сформувався як комбінація повноцінних комерційних платформ і гнучких рішень з відкритим кодом. Такий спектр підходів дозволяє використовувати DT як у масштабних корпоративних моделях захисту, так і в більш локальних сценаріях, орієнтованих на швидке та раннє виявлення підозрілої активності. Для банківського сектору визначальною є не стільки привабливість пасток чи складність їх імітації, скільки практична корисність для SOC: можливість органічного включення у процеси моніторингу і реагування, висока надійність сигналів і здатність фіксувати дії нападника ще на етапах розвідки, пошуку облікових даних або спроб внутрішнього переміщення.

Серед комерційних рішень варто відзначити Labyrinth Deception Platform, яка позиціонується як інструмент для раннього виявлення внутрішньої мережевої активності на основі високорівневих приманок та автоматизованого розгортання пасток у корпоративному середовищі. У характеристиках платформи робиться акцент на зменшенні кількості помилкових спрацьовувань

і на здатності інтегруватися з уже наявними системами моніторингу і реагування [38].

Acalvio представляє DT-підхід корпоративного рівня, де технологія розглядається як масштабований, розподілений шар активної оборони для складних гібридних інфраструктур. Платформа ShadowPlex орієнтована на ранню фіксацію дій противника під час розвідки та спроб руху мережею, а також позиціонується як рішення, придатне для сценаріїв IT, хмарних середовищ і, за необхідності, сегментів OT [8, 36].

Cymmetria належить до перших комерційних гравців у цій сфері та асоціюється насамперед із рішенням MazeRunner. Концептуально платформа будувалася на ідеї керованих “маршрутів” для зловмисника, де приманки спрямовують зловмисника до пасток, формуючи контрольоване середовище для спостереження і збору даних про його поведінку. З часом цей підхід доповнювався механізмами автоматизації та інтеграційними можливостями через API [39].

TrapX тривалий час розглядався як потужна корпоративна DT-платформа, орієнтована на масштабне розміщення пасток і швидке створення імітаційного шару, що генерує високодостовірні сповіщення. Важливою подією для ринкового контексту стало придбання TrapX компанією Commvault у 2022 році, що потенційно розширило інтерпретацію продукту у напрямі кіберстійкості та захисту критичних даних у межах портфеля великого вендора. Для банків цей вектор може бути цікавим у сценаріях, де DT розглядається не лише як інструмент виявлення, але й елемент ширшої моделі стійкості та відновлення після інцидентів [40].

Illusive Networks поступово змістив акцент від класичного DT до більш спеціалізованої площини Identity Threat Detection and Response. Після приєднання до Proofpoint наприкінці 2022 року рішення позиціонується як платформа для захисту ідентичностей із використанням обманних механізмів для виявлення латерального переміщення і блокування атак до моменту доступу до реальних активів. Для банківських SOC це має практичну цінність з огляду на

критичність AD, технічних і привілейованих облікових записів у типових сценаріях компрометації [29, 30].

Attivo Networks також протягом тривалого часу залишався одним із найвідоміших брендів DT-напряму, розвиваючи портфель ThreatDefend із виразною орієнтацією на ризики ідентичностей і доменних середовищ. Після придбання SentinelOne у 2022 році можливості Attivo були інтегровані у ширший контур захисту ідентичностей та XDR-екосистеми, що посилило потенціал виявлення крадіжок облікових даних, ескалації привілеїв і внутрішнього руху зловмисника [37].

Поряд із комерційними платформами суттєве місце в практиці SOC зберігають open-source підходи. Найвідомішими прикладами є OpenCanary, Cowrie та T-Pot. OpenCanary можна розглядати як легкий багатопротокольний honeypot із гнучкими механізмами сповіщення, включно з передаванням подій через syslog, що спрощує інтеграцію в SIEM. Cowrie більш спеціалізований на SSH/Telnet і дає змогу фіксувати активність типу brute force і досліджувати взаємодію порушника з псевдосесіями. T-Pot, розроблений командою Deutsche Telekom, поєднує набір різних honeypot-компонентів із можливостями візуалізації на базі Elastic Stack, що робить його корисним для лабораторних і напівпромислових сценаріїв аналізу атак.

З точки зору банківської установи open-source DT є зручним стартовим або дослідницьким інструментом: він дозволяє швидко перевірити релевантність концепції, сформувати початкові use cases і навчити команду SOC працювати з новим типом сигналів. Однак для продуктивних контурів банку зазвичай потрібні більш керовані корпоративні рішення з прогнозованою підтримкою, формалізованими інтеграціями та зрілою моделлю ізоляції, що забезпечує баланс між інноваційністю та вимогами до стабільності критичних фінансових сервісів [31-33].

У табл. 2.3 представлено порівняння DT-рішень для використання в SOC банку.

Таблиця 2.3.

Порівняльний аналіз DT-рішень для використання в SOC банку

Вендор	Продукт	Основні цілі	Сильні сторони для банку
Labyrinth	Labyrinth Deception Platform	Раннє виявлення, високорівневі приманки, автоматизація розгортання	Орієнтація на високодостовірні сигнали, зниження шуму, інтеграційність
Acalvio	ShadowPlex	Масштабована корпоративна DT для IT/Cloud/OT	Підходить для великих гібридних банківських середовищ, сильний акцент на ранньому виявленні руху в мережі
Cymmetria	MazeRunner	Breadcrumbs + decoys як керовані сценарії	Корисно для дослідницьких і розвідувальних сценаріїв SOC
TrapX	DeceptionGrid (нині в екосистемі Commvault)	Масштабна імітація інфраструктури	Цікавий варіант для банків, що пов’язують DT із ширшими задачами кіберстійкості та захисту даних
Illusive Networks	Proofpoint Identity Threat Defense	ITDR + DT, захист AD та ідентичностей	Дуже релевантне рішення для банків через доменну критичність і ризики крадіжок ідентичності й ескалації привлеїв
Attivo Networks	ThreatDefend / Singularity Hologram у контексті SentinelOne	ITDR + DT у XDR-логіці	Сильні сценарії захисту ідентичностей, видимість латерального руху

2.5 Практичні кейси та результати застосування DT у банках

Практична значущість технологій введення в оману для банківської інфраструктури найкраще проявляється у прикладних сценаріях, де важлива не теоретична привабливість концепції, а її реальний ефект для SOC: скорочення часу до першого сигналу, підвищення точності виявлення і можливість отримати поведінкові артефакти противника без прямого ризику для продуктивних систем.

Банки працюють із різноманітними середовищами від стандартних корпоративних контурів до платформ, пов'язаних із фінансовими операціями, дистанційними каналами обслуговування та критичними системами управління ідентичностями. Такий ландшафт створює ситуацію, коли навіть зрілі IDS/IPS, SIEM чи EDR-інструменти можуть або продукувати надмірний потік сигналів, або вимагати значного часу на доведення реальності загрози. У цьому контексті DT виконує роль додаткового тихого сенсорного шару, де взаємодія з приманкою майже завжди має підозрілу природу.

Для банківської сфери характерні кілька напрямів застосування DT, які найчастіше дають вимірюваний ефект:

- контроль доступу до висококритичних платіжних компонентів і пов'язаних процесів, що традиційно належать до зони підвищеного інтересу кіберзлочинних і APT-груп;
- сценарії захисту Active Directory та сервісних/привілейованих облікових записів, адже саме вони відкривають противнику шлях до масштабного контролю над внутрішніми ресурсами;
- виявлення латерального переміщення у мережі, яке часто є невидимою фазою атаки: зловмисник діє обережно, використовує легітимні інструменти, а його активність маскується під звичні адміністративні дії [26-30].

Реальні та наближені до реальних приклади використання DT. У відкритих матеріалах зустрічаються кейси, де DT застосовується як захисний бар'єр навколо найбільш цінних для банку активів. Один із таких прикладів

описує використання імітаційних об’єктів, пов’язаних із профілем SWIFT, у глобальній банківській організації. У цьому випадку DT слугувала як контрольований контур раннього контакту для виявлення нетипового інтересу до платіжного середовища. Важливим мотивом стала потреба підсилити видимість бічного руху, який залишався складним для впевненого виявлення лише традиційними засобами моніторингу. Результатом стали зафіксовані спроби взаємодії з DT-елементами, що дало змогу оперативно підтвердити ризики і зупинити потенційні маршрути проникнення до продуктивних елементів.

Інший тип практичної аргументації демонструють приклади, пов’язані з контрольованими вправами Red Team у банківських середовищах. У таких сценаріях DT забезпечує ранні тригери, коли тестова атакувальна активність намагається використати підставні облікові дані або контактує з “привабливими” сервісами, що імітують критичні ресурси. Для SOC це має прикладну цінність, оскільки дозволяє підтвердити працездатність ланцюжка реагування без необхідності чекати виявлення реальної шкоди або технічно очевидних слідів компрометації у виробничих системах.

У сучасних банківських практиках також відчутно посилюється фокус на напрямі ITDR, де DT використовується як інструмент, тісно пов’язаний із захистом ідентичностей. Такий підхід логічний для фінансових організацій: атаки на облікові записи, доменні служби та механізми управління доступом часто є коротким шляхом до масштабної компрометації внутрішнього середовища. Звідси випливає і практичний висновок: DT-артефакти у площині ідентичностей можуть бути одним із найбільш результативних елементів загальної банківської моделі раннього виявлення.

DT як інструмент виявлення внутрішнього переміщення зловмисника. Для банківських SOC контроль латерального переміщення є одним із ключових критеріїв зрілості детекції. Саме на цій фазі противник зазвичай переходить від первинного доступу до активного пошуку цінних ресурсів, тестування привілеїв і підготовки до дій із високими фінансовими наслідками. У таких умовах DT дає важливу перевагу, побудовану на простій

операційній логіці: легітимному користувачу майже немає причин взаємодіяти з серверами-приманками, пастками або підставними обліковими записами. Отже, подібні сигнали формують для SOC високопріоритетний, малошумний канал, який дозволяє швидше відокремити реальну загрозу від припущення.

Приклад із SWIFT-орієнтованими DT-сценаріями добре ілюструє цю думку: метою було не просто створення пасток заради пасток, а точкове підсвічування аномального інтересу до критичної платіжної площини і виявлення нетипових маршрутів руху всередині мережі.

Оцінка ефективності за даними відкритих джерел і тестових середовищ. Окрім описів банківських практик, суттєву доказову цінність формують лабораторні та дослідницькі моделі DT. Високовзаємодійні Windows- або AD-орієнтовані середовища, розгорнуті у публічному або напівпублічному форматі, демонструють стійкий інтерес порушників до корпоративних сервісів автентифікації, віддаленого доступу і типових механізмів адміністрування. Для банків таке спостереження має прикладний зміст, оскільки саме шар Windows/AD є одним із найбільш перспективних напрямів розміщення DT-елементів, якщо метою є раннє виявлення пошуку облікових даних, спроб ескалації або прихованого переміщення.

З методологічної точки зору важливим є також те, що DT у сучасних інтерпретаціях розглядається ширше, ніж класичні honeypots. Це вже комплексна стратегія активної оборони, що може проявлятися на рівні даних, сервісів, ідентичностей і мережевих маршрутів. Такий підхід підкріплює обґрунтування для банківського сектору, що DT не є екзотичним додатком, а логічним розширенням можливостей SOC у частині раннього виявлення і побудови доказової бази.

Узагальнення типових банківських сценаріїв DT. Нижче наведено узагальнену таблицю, яка відображає, як технології введення в оману можуть бути застосовані в типових для банків інцидентних ситуаціях.

Таблиця 2.4.

Класифікація загроз та протидії рішення DT

Тип загрози	Мотивація і цілі атакувальника	Які DT - елементи доречні	Що отримує SOC
Атаки на платіжні контури та критичні транзакційні компоненти	Доступ до інфраструктури операцій, компрометація процесів проведення платежів	Декой-сервіси/сегменти, підставні портали, токени в документах і технічних описах	Раннє виявлення інтересу до критичних активів і нетипових маршрутів руху
Компрометація AD і привілейованих облікових записів	Ескалація, захоплення доменного рівня, розширення контролю над інфраструктурою	Фіктивні облікові записи, підставні адміністративні ресурси, приманки	Високодостовірні сигнали про спроби отримання привілеїв
Тривалі APT-кампанії	Повільна розвідка, закріплення, накопичення доступів	Розподілена мережа різноманітних приманок у критичних сегментах	Зменшення часу до першого надійного індикатора, збирання поведінкових TTP
Фінансово мотивовані атаки з використанням легітимних інструментів	Швидкий рух до даних і систем, монетизація доступу	Реалістичні файлові приманки, honeytokens у цінних директоріях	Зручні для кореляції в SIEM/EDR чисті тригери для швидкої валідації

Висновки до розділу 2

Проаналізовано специфіку впровадження технологій введення в оману в банківському секторі України з урахуванням регуляторного поля, архітектури SOC та особливостей критичних банківських контурів. Показано, що

застосування DT є найбільш доцільним у якості додаткового шару активної оборони, який підсилює SIEM і EDR/XDR, формуючи високодостовірні сигнали та покращуючи раннє виявлення розвідки загроз і внутрішнє переміщення зловмисника. Розглянуто ринкові рішення провідних вендорів і open-source підходи, а також узагальнено практичні кейси, які підтверджують ефективність обманних технологій у сценаріях атак на ідентичність, AD і платіжно-транзакційні зони.

РОЗДІЛ 3 РОЗРОБКА МОДЕЛІ ВПРОВАДЖЕННЯ DT У SOC БАНКУ

3.1 Архітектурна модель DT-платформи для банку

Архітектурна модель технологій введення в оману для банківської установи має формуватися як окремий, керований шар активної оборони, який гармонійно доповнює функції SOC і зменшує ризики пропуску складних атак. На відміну від класичних механізмів виявлення, що переважно працюють із подіями продуктивного середовища, DT створює контрольовані об’єкти-цілі, контакт із якими майже не має легітимних пояснень. У банківських умовах це особливо важливо, оскільки будь-яка технологія, що підвищує достовірність сигналів і зменшує аналітичний шум, напряму впливає на якість реагування та стійкість критичних сервісів.

В основі банківської DT-платформи доцільно закласти три взаємодоповнювані групи об’єктів:

- honeypots як імітовані сервіси або вузли інфраструктури, що створюють правдоподібні точки інтересу для зловмисника;
- honeytokens, тобто цифрові артефакти і дані-приманки, які розміщуються в середовищі без необхідності розгортання повноцінного хоста;
- підробні облікові записи, що імітують облікові дані різного рівня доступу та використовуються для фіксації небезпечних спроб автентифікації або руху до привілейованих ресурсів.

Слід відзначити, що в банківській практиці ці три класи не конкурують між собою, а формують єдину логіку: honeypots дають “сцену” для взаємодії, honeytokens підсилюють контроль за даними та файловими маршрутами, а honey credentials закривають критично важливу площину ідентичностей.

Важливо, щоб розміщення DT-об’єктів у банку не відбувалося за принципом механічного копіювання інфраструктури. Модель має бути

сценарною і відображати найбільш імовірні маршрути нападника, починаючи з первинного доступу і завершуючи спробами ескалації привілеїв або пошуку чутливих даних. Саме тому стратегія розгортання DT має опиратися на сегментацію мережі та розуміння того, які типи активності характерні для кожного контуру [2-5, 43, 44].

У DMZ доцільно фокусуватися на таких елементах DT, які орієнтовані на зовнішньо доступні сценарії. Тут логічно застосовувати імітації веб і сервісних компонентів, а також API DT, що дозволяє фіксувати ранні спроби сканування, автоматизовані запити, пошук вразливостей і тестування типових помилок конфігурації. Для банку це створює додатковий рівень видимості на периметрі, який не замінює WAF чи IDS/IPS, але дає інший тип сигналу більш поведінковий і менш залежний від відомих сигнатур.

Ключовий сегмент (Core) банку потребує найбільш виваженого архітектурного підходу. Саме тут зосереджуються системи найвищої критичності, тому DT має бути не лише правдоподібною, а й максимально безпечною з точки зору ізоляції. У межах цього контуру найвищу практичну цінність мають AD-орієнтовані приманки та підробні облікові записи, адже доменні сервіси і привілейовані облікові записи є одним із найкоротших шляхів до масштабної компрометації середовища. Тому архітектурно виправданим є створення таких приманок, які виглядають як логічні “проміжні цілі” на шляху до критичних ресурсів. У цьому випадку будь-яка взаємодія з ними працює як індикатор наміру, а не випадкової активності.

Окрему увагу в ключовому сегменті варто приділити DB-honeypots і data honeytokens. Банківська інфраструктура історично має високу концентрацію даних, і багато атак з часом трансформуються у пошук економічно значущих інформаційних масивів. Саме тому імітації баз даних або стилізовані файли-приманки можуть бути корисними для виявлення несанкціонованих спроб доступу до цінних сховищ. У правильно налаштованій моделі ці елементи мають виглядати природною частиною корпоративного середовища не надто очевидною пасткою, але і не настільки “глибоко захованою”, щоб зловмисник до

них не дійшов у логіці свого руху.

Офісний сегмент (Office) у цій моделі виконує іншу роль. Саме робоче середовище часто є точкою старту більшості атак через фішинг, компрометацію кінцевих точок або зловживання легітимними обліковими записами. Тому DT у цьому контурі має бути легшою, більш чисельною, але не критичною з погляду інфраструктурного ризику. Найбільш доречними є файлові honeytokens, приманки в робочих каталогах, а також обмежені за правами honey credentials, які дають SOC ранні сигнали про підозрілий інтерес до внутрішніх ресурсів і спроби прокласти маршрут до основної зони.

Архітектурна безпека DT у банку має бути закладена як принцип, а не як додаткова опція. Приманки не повинні створювати нових векторів атаки або перетворюватися на міст до продуктивних систем. Це означає необхідність строгого мережевого відокремлення, контрольованих протоколів, обмеження вихідних комунікацій і чіткої регламентації, які саме типи взаємодії дозволені. У банківському середовищі така дисципліна є критичною умовою прийнятності технології, адже будь-який новий компонент безпеки повинен підсилювати стійкість, а не ускладнювати ризиковий профіль [36-38].

У підсумку архітектурну модель DT-platform для банку доцільно визначити як сегментований, сценарно орієнтований шар активної оборони, що складається з honeypots, honeytokens та honey credentials і розміщується відповідно до логіки атакувальних маршрутів у DMZ, Office і Core. Такий підхід дозволяє створити в SOC окремий канал високодостовірних подій, які особливо цінні при виявленні розвідки, спроб компрометації ідентичностей, доступу до даних і латерального переміщення. Водночас саме ця модель формує операційну основу для наступного етапу дослідження розробки алгоритму взаємодії DT-платформи з SIEM та EDR у рамках процесів реагування SOC банку (Рис. 3.1).

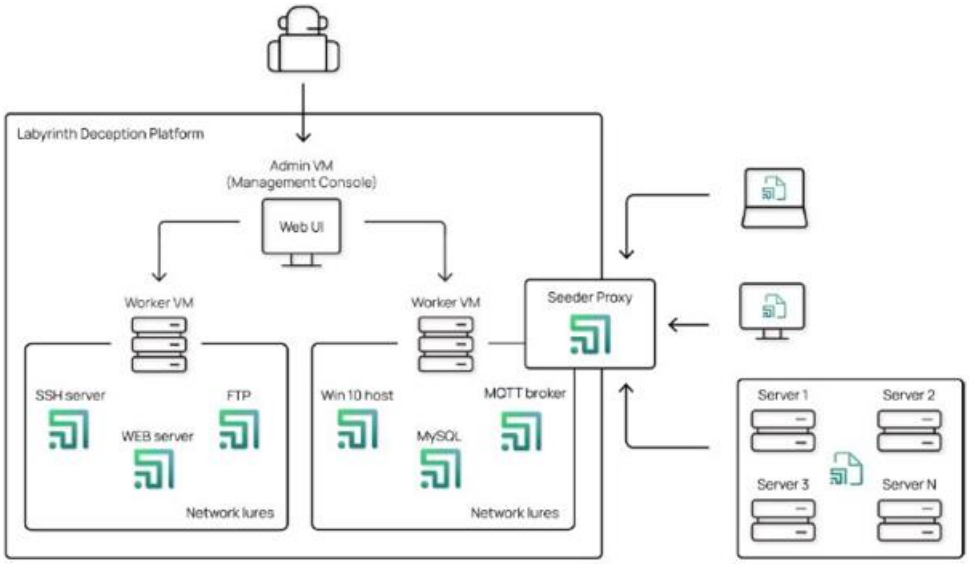

Рис. 3.1. Приклад архітектурної модель DT-платформи на базі Labyrinth

3.2 Процес взаємодії DT-системи з інструментами SOC

У банківському середовищі DT дає максимум користі лише тоді, коли вона не є ізольованою платформою з власною окремою панеллю, а працює як частина повноцінного циклу SOC. Власне, сама по собі наявність honeypots чи honeytokens ще не створює системного ефекту. Системний ефект з'являється тоді, коли DT-події стають керованим джерелом телеметрії для SIEM, запускають процесні сценарії у SOAR і підтверджуються або локалізуються на рівні EDR/XDR. Така зв'язка дозволяє скоротити шлях від сумнівного сигналу до операційно підтвердженого інциденту і зменшує витрати часу на ручну валідацію. Загальні підходи до впровадження SIEM/SOAR як інструментів прискорення виявлення та реагування на інциденти описуються і в практичних рекомендаціях для організацій.

У такому випадку процес взаємодії DT з інструментами SOC розглядається як наскрізна прикладна модель, де кожний компонент додає новий рівень доказовості перед тим, як SOC переходить до активних дій. Це особливо важливо для банку, де автоматизація має бути швидкою, але керованою, і зберігати баланс між безпекою та безперервністю критичних сервісів [16].

Інтеграція з SIEM. SIEM у цій моделі виступає “точкою перетворення” DT-сигналу на зрозумілий інцидентний контекст. Для SOC важливо не просто отримати факт взаємодії з приманкою, а зрозуміти, хто, звідки, з яким наміром і в якій фазі можливого сценарію атаки здійснив таку дію.

Технології введення в оману доцільно інтегрувати в SIEM, оскільки це дозволяє зробити DT частиною єдиної картини подій. DT дає чистий тригер, а SIEM накладає на нього доменний, мережевий і endpoint-контекст. Крім цього, банківська аналітика отримує високодостовірне джерело сигналів. Взаємодія з honeytoken або спроба використання підробних облікових записів за своєю природою є нетиповою для законної діяльності. Саме тому DT-події мають сенс як високопріоритетні вхідні дані для кореляції. Сама концепція введення в оману як технології, що не замінює інші засоби, а інтегрується з ними і може впроваджуватись на будь-якому етапі розвитку програми безпеки, добре описується у профільних оглядах.

На технічному рівні більшість DT-рішень, включно з open-source, підтримують стандартне журналювання і передачу алертів у загальноприйнятих форматах. Наприклад, OpenCanary може відправляти сповіщення у різні сховища логів, зокрема через Syslog, що робить його зручним джерелом для SIEM-інтеграції.

Для сучасних SIEM існують уже підготовлені інтеграційні пакети. Зокрема, в екосистемі Elastic доступна інтеграція OpenCanary, яку можна підключити через стандартний каталог Integrations у Kibana, після чого журнали починають індексуватися та використовуватися в аналітиці. Аналогічно, у Google Security Operations (Chronicle) описані типові парсери, які нормалізують OpenCanary SYSLOG/JSON-логи у єдину модель даних.

У банківському SOC після підключення DT як джерела даних є сенс налаштовувати окрему логіку пріоритезації. Наприклад, подія використання підробних облікових записів має автоматично отримувати вищий рівень критичності, ніж звичайна аномалія входу без підтверджувальних ознак. Далі SIEM може збагачувати інцидент шляхом підтягування інформації про тип

акаунта, його контекст у системі управління ідентичностями, історію нетипових логінів, а також корелювати подію з мережевими ознаками розвідки або спроб руху до сусідніх ресурсів.

Так формується ключовий практичний ефект, за якого DT-подія перестає бути цікавою технічною знахідкою і перетворюється на чіткий сигнал із бізнес-зрозумілою вагою для SOC.

Передача подій у SOAR і автоматизація.

SOAR рівень потрібен, щоб реакція на DT була стандартизованою, повторюваною і контрольованою. У сучасних SOC-підходах SOAR використовується для запуску плейбуків на основі правил або стану інциденту, що дає змогу зменшувати ручну роботу та прискорювати рішення. У Microsoft Sentinel, наприклад, плейбуки реалізуються через Azure Logic Apps, а їх можна прив’язувати до аналітичних правил чи правил автоматизації.

Система DT може генерувати сигнали різної глибини ризику. Honeytoken у файловій зоні офісного сегмента і спроба використання адміністративних фейкових акаунтів у Core - це різні типи ситуацій. SOAR дозволяє фіксувати цю різницю процесно, не однаковою реакцією на все, а різними сценаріями для різних профілів подій.

У банку органічно виглядає підхід м’якої автоматизації. Він передбачає, що для частини сповіщень DT SOC запускає автоматизований збір контексту, але не робить агресивних дій без додаткового підтвердження.

У такому плейбуку SOAR може:

- автоматично створити інцидент і визначити відповідний рівень (L1/L2);
- витягнути пов’язані SIEM-події за короткий часовий проміжок;
- виконати перевірку, чи є паралельні ознаки внутрішніх рухів;
- додати інциденту технічні та бізнесові теги;
- сформувати структурований підсумок для швидкої валідації аналітиком.

Цей формат дозволяє отримати практичний результат без ризику зайвої автоматичної жорсткості.

Зв’язка з EDR/XDR, підтвердження та автоматична реакція. EDR/XDR

рівень у цій моделі потрібен як технічний доказовий шар. DT повідомляє, що хтось торкнувся приманки, але саме EDR дає відповідь на головне практичне запитання SOC, чи є на конкретній кінцевій точці ознаки реальної атаки.

По-перше, це потрібно для прискорення рішення. Якщо SIEM уже показує сумнівний контекст, EDR може підтвердити запуск підозрілих процесів, появу інструментів віддаленого адміністрування або поведінкові ознаки підготовки до закріплення. По-друге, для безпечної локалізації. Ізоляція хоста або блокування доступу в банківській установі мають застосовуватися обережно, але виявлення підтвердженої активності після DT-тригера - це якраз той випадок, де контрольована автоматична реакція може бути виправданою.

На практиці SOAR може викликати EDR-дії через API. Наприклад, Microsoft Defender for Endpoint має API для ізоляції пристрою. Документація підкреслює, що в режимі ізоляції дозволені лише обмежені з'єднання, а у випадку повного VPN-тунелю можливі проблеми з доступом до хмарних сервісів захисту. У такому випадку рекомендується split-тунелювання для відповідного трафіку. Такі нюанси важливі саме для банку, оскільки вони показують, чи є автоматична реакція технічно сумісною з архітектурою віддаленого доступу.

Таким чином, у правильній моделі EDR є не просто командою ізолювати на кожен DT-тригер, а скоріше умовним механізмом, який активується при виконанні кількох критеріїв підтвердження.

Практичний наскрізний сценарій для SOC банку. Опишемо ситуацію, в якій DT є стартом процесу розслідування й реагування на інцидент. В офісному сегменті зафіксовано спробу використання honey credentials. DT-система формує сповіщення і передає його в SIEM. Далі SIEM автоматично збагачує подію шляхом перевірки, чи фіксувалися нетипові входи з цього хоста, чи є підозрілі запити до доменних ресурсів, чи не відбувалося підключення до серверних зон, які не характерні для ролі користувача.

Після цього інцидент через SOAR переходить у плейбук. Система збирає додатковий контекст, будує коротку часову лінію і робить первинну оцінку траєкторії. Якщо плейбук бачить ознаки, що подія може бути частиною

внутрішнього переміщення, він ініціює перевірку на рівні EDR.

На боці EDR запускається збір активних процесів і аналіз нетипових командних ланцюжків. Якщо EDR підтверджує підозрілу активність, SOC отримує достатню доказову базу для локалізації інциденту. У разі дозволеного політиками сценарію SOAR може ініціювати ізоляцію хоста через EDR API, дотримуючись вимог мережевої сумісності.

У підсумку реалізація такої моделі дає банку низку суттєвих переваг:

- зниження частки слабких неперевірених тривог у ручній роботі L1, оскільки DT-події мають вищу природну достовірність;
- швидшу валідацію інцидентів за рахунок того, що SIEM одразу збагачує DT-тригери доменними, мережевими та endpoint-даними;
- стандартизовану реакцію через SOAR, де дії не залежать від суб'єктивності чергової зміни, а працюють за єдиним сценарним шаблоном;
- можливість контрольованої автоматичної локалізації загроз у тих випадках, коли ризик підтверджується EDR/XDR.

У більш широкому контексті це означає, що DT починає виконувати роль інструмента підсилення зрілості SOC, а не просто додаткової технічної опції. Саме таку сумісність технологій введення в оману із SIEM/SOAR-ландшафтом і клієнтськими процесами безпеки описують і профільні огляди підходів до впровадження DT.

3.3 Алгоритм обробки інцидентів на основі DT-пасток

У межах створення рівня введення в оману для банківського SOC принципове значення має не лише технічна наявність приманок, пасток чи фіктивних акаунтів, а й процесна регламентація їх використання в управлінні інцидентами. Саме формалізований алгоритм реагування переводить DT із технологічного доповнення у практичний інструмент щоденної роботи. У банках, де критичні сервіси вимагають стабільності, а аналітичні потоки подій

часто перевантажені, DT-інциденти мають бути вписані у стандартний цикл SOC із заздалегідь визначеними тригерами, зрозумілими умовами автоматизації та чіткою траєкторією ескалації між рівнями аналітиків.

У прикладному вимірі це означає, що подія взаємодії з обманним активом не повинна залишатися локальною подією в системі вендора. Вона має запускати регулярний процес, зрозумілий усім учасникам SOC, підкріплений правилом пріоритезації, набором перевірок і структурованими рішеннями щодо подальших дій. Такий підхід дає банку можливість не лише швидше реагувати, а й накопичувати аналітичний досвід для корекції пасток, поліпшення кореляційних правил і розвитку плейбуків у наступних ітераціях [23-25, 47].

DT плейбуки в логіці банківського SOC. Плейбуки є операційним сценарієм, де ключовою стартовою подією виступає контакт із контрольованим DT-об’єктом. У класичних інцидентних процесах SOC часто змушений працювати із неочевидними ознаками та значним рівнем фонових активностей, тоді як DT-сигнал за своєю природою вже містить підвищений рівень підозрілості. Тобто в плейбук логічно закладати тезу, що взаємодія з пасткою або токеном є скоріше індикатором наміру, ніж випадковою технічною помилкою.

Практична користь плейбуків проявляється в тому, що він задає стабільну структуру дій від перевірки контексту активу і сегмента до зіставлення з даними SIEM/EDR, визначення ступеня впливу й ухвалення рішення щодо стримування. У банківському варіанті плейбук має бути гнучким, але водночас достатньо регламентованим, щоб забезпечувати однакову якість роботи незалежно від зміни, досвіду або навантаження аналітика.

Окремо варто підкреслити необхідність модульності, оскільки один загальний плейбук однаково ефективно не покриє DMZ-пастки, AD-орієнтовані сценарії і токени на рівні даних. Тому доцільно передбачити розгалуження логіки залежно від типу тригера і ризику для конкретної банківської зони [3, 5, 26, 27, 29, 30].

Тригери інцидентів у DT-середовищі. Тригери в архітектурі введення в оману - це чітко визначені умови, за яких сигнал із пастки трансформується в

інцидент або принаймні в пріоритетний кейс для перевірки. Для банків логічно класифікувати такі тригери за ризиковою суттю, а не лише за технічним типом DT-об’єкта.

Перший клас тригерів доцільно пов’язувати зі сценаріями розвідки та первинного проникнення. Це можуть бути спроби доступу до периметрових заманювальних сервісів, нетипові звернення до імітованих API або активність, яка виглядає як підготовка до початкової компрометації. Цінність таких сигналів полягає у часовій перевазі: вони можуть з’являтися ще до того, як нападник сформує стійкий доступ.

Другий клас є найбільш значущим для банківського середовища і охоплює тригери, пов’язані з ідентичностями. Спроба використання фіктивних акаунтів або взаємодія з обманними елементами AD часто сигналізує про підготовку до ескалації привілеїв чи внутрішнього пересування. У цьому випадку навіть одиничний факт взаємодії має достатньо підстав для підвищеної пріоритезації.

Третій клас - тригери, орієнтовані на дані. У банках це можуть бути контрольні “цінні” файли або токенізовані артефакти, які імітують фінансово значущі документи чи записи. Їхня функція полягає не лише у фіксації спроб доступу, а й у створенні контрольованої ознаки того, що противник переходить від розвідки до пошуку об’єктів із потенційною бізнес цінністю.

Автоматичні дії SOC у відповідь на DT-сигнали. Практична сила DT у SOC суттєво зростає, коли система реагування не обмежується ручною перевіркою, а має передбачуваний набір автоматизованих кроків. Для банків особливо важливо зберігати обережність і забезпечити. щоб автоматизація була корисною, але не надмірно агресивною.

На базовому рівні автоматичні дії повинні фокусуватися на збагаченні контексту. Після спрацювання пастки інцидент автоматично доповнюється інформацією про сегмент, критичність активу, відповідальну за сервіс особу та пов’язані події з мережевих і доменних джерел. Така автоматизація не створює операційного ризику, але різко прискорює рішення L1.

На середньому рівні доцільно застосовувати умовні превентивні обмеження, якщо профіль ризику події достатньо виразний. Наприклад, у випадках тригерів ідентичності система може запускати пріоритетний пошуковий запит по суміжних логах або ініціювати тимчасову перевірку доступів до чутливих ресурсів.

Розширений рівень автоматизації передбачає використання EDR-реакцій або мережевих заходів стримування, але лише за умов додаткової кореляції. Тобто DT-сигнал виступає початковим аргументом, а остаточне рішення про активне стримування спирається на підтверджувальні дані поведінки хоста і мережевого контексту.

Логіка ескалації подій/інцидентів. Через високу інформативність DT-сигналів банківський SOC має закласти формалізовані правила ескалації (підвищення рівня пріоритетності подій і, відповідно, передача завдання на вищий рівень управління безпекою). Тут важливий контекстний підхід, який передбачає, що пріоритет визначається не лише типом пастки, а комбінацією факторів: сегментом, роллю облікового запису, критичністю вузла, а також наявністю паралельних ознак у SIEM/EDR.

Події в офісному середовищі можуть залишатися на рівні L1 за умови швидкої технічної валідації. Натомість тригери, що стосуються доменного рівня або ключового сегмента, повинні автоматично піднімати інцидент на L2, а за наявності ознак реальної спроби компрометації AD чи критичних сервісів залучати L3 або IR-команду банку.

Такий процес ескалації дозволяє перетворити DT на керований механізм пріоритетизації, а не просто на додаткову категорію сповіщень.

Таблиця 3.1.

Класифікація загроз та протидії рішення DT

Тип тригера	Приклад сигналу	Базова реакція SOC	Логіка ескалації
Периметрові/ DMZ	Доступ до декой-сервісу або імітованого API	Швидке збагачення контексту, перевірка джерела, контроль суміжних подій	L1, перехід на L2 за підтвердженням кореляцією
Рівень ідентичності	Спроба використання підробним акаунтів	Пріоритетна кореляція з AD/EDR, запуск прискореної перевірки	L2 як базовий рівень
Дані/файли	Відкриття honeytoken-файлу	Аналіз поведінки хоста, перевірка доступів і маршрутів	L1 → L2 за наявності супутньої активності
Core-сегмент	Звернення до декой-AD/DB	Розширений аналіз привілеїв, оцінка потенційного масштабу	L2 → L3/IR

3.4 Оцінка ефективності впровадження DT у SOC банку

Оцінювання ефективності впровадження технологій введення в оману в банківському середовищі є принципово важливим етапом, який перетворює інноваційний технологічний підхід на керований компонент програми кібербезпеки. На практиці в SOC часто виникає ситуація, коли новий інструмент технічно інтегровано, але його реальний внесок у покращення виявлення і реагування залишається неочевидним для керівництва або суміжних підрозділів. У фінансовому секторі, де інвестиції у безпеку мають бути обґрунтованими з точки зору бізнес-ефекту та зниження ризику, така “невидимість” результату є

небажаною. Саме тому доцільно розглядати DT не лише як шар виявлення, а як елемент, який має формувати вимірювані зміни на рівні ефективності SOC і ризикового профілю банку.

У загальній світовій практиці оцінювання роботи SOC найбільш уживаними залишаються метрики часу виявлення та реагування, а також показники якості сигналів і процесної дисципліни. У багатьох оглядах SOC-метрик акцентується, що такі показники, як MTTD і MTTR, є базовими для вимірювання спроможності команд швидко ідентифікувати загрози та локалізувати їх наслідки. У документах і коментарях щодо вимірювання відповідно до сучасних фреймворків з кібербезпеки також часто згадуються MTTD і MTTR як приклади ключових індикаторів результативності заходів. З урахуванням цього у дипломній роботі використано саме ці показники як основу оцінювання ефективності DT у банківському SOC.

Разом із тим, для повноцінної оцінки важливо розділити два рівні показників. KPI розглядаються як метрики операційної результативності SOC після інтеграції DT у щоденний цикл моніторингу й реагування. Під KRI розуміють показники ризикового виміру, які демонструють, як змінюється фон загроз у найбільш чутливих для банку площинах: ідентичності, AD, спроби латерального переміщення, ранньої розвідки периметра, інтересу до зон даних. Такий поділ дозволяє показати не лише швидкість і зручність роботи аналітиків, а й стратегічний зміст впровадження, тобто його цінність для управління кіберризиком банку [23, 24, 47, 60].

Щоб оцінка ефективності виглядала переконливо в академічному та практичному сенсі, вона має спиратися на поняття базової лінії. У банківському SOC цю базову лінію доцільно сформувати на основі інцидентів певного періоду до впровадження DT або до етапу її повної інтеграції в SIEM/SOAR/EDR. Надалі порівнюється, як змінюються часові та якісні показники для тієї ж категорії інцидентів після введення DT-тригерів у регулярну кореляцію і плейбуки реагування.

Важливо підкреслити, що DT за своєю концепцією найчастіше дає ефект не як масивний генератор подій, а як високодостовірний сенсор. У відкритих джерелах цей підхід пояснюється тим, що легітимний користувач зазвичай не має причин взаємодіяти з активами-приманками. Тому DT здатна формувати сигнали з дуже низьким рівнем хибних спрацювань і тим самим зменшувати операційний шум. Для банків це означає, що зміни варто шукати не стільки у загальній кількості інцидентів, скільки у скороченні часу їх первинної валідації і у збільшенні частки інцидентів із чітко підтвердженим наміром порушника.

В окремих випадках під час оцінювання може бути корисним розподіл результатів за сегментами (DMZ/Office/Core), оскільки очікуваний ефект у цих середовищах відрізняється. Для периметра основним результатом буде швидше виявлення ранньої розвідки та спроб тестування сервісів; для офісного середовища - зростання якості сигналів у сценаріях початкового проникнення та раннього руху до внутрішніх ресурсів, а для ключового сегменту - підвищення ймовірності раннього перехоплення сценаріїв ідентичності та внутрішнього переміщення зловмисника. Саме в такому варіанті DT органічно подається як технологія, яка підсвічує дії противника ще до отримання доступу до реальних критичних активів.

У практиці сучасних SOC ключовими показниками залишаються Mean Time to Detect (MTTD) та Mean Time to Respond (MTTR). MTTD традиційно трактують як середній час, потрібний команді, щоб виявити інцидент від моменту початку небезпечної активності, а MTTR - як середній час від виявлення/підтвердження до локалізації, усунення або стабілізації ситуації. У навчальних і практичних матеріалах щодо SOC-метрик підкреслюється, що зниження цих показників зазвичай свідчить про підвищення зрілості засобів виявлення, кращу інтеграцію телеметрії та оптимізацію процесів SOC.

У контексті DT особливо важливо розглядати MTTD і MTTR не загалом по SOC, а в розрізі DT-інцидентів. Такий аналітичний фокус дозволяє показати точковий ефект технології й обґрунтувати її внесок у загальну систему моніторингу.

На практиці це можна описати як дві паралельні точки вимірювання.

1. MTTD для інцидентів, де DT стала первинним тригером. Їхній MTTD потенційно буде нижчим, оскільки пастки й токени створюють штучні контрольовані контакти й змушують нападника проявити себе раніше, ніж він досягне реального активу. У відкритих описах DT саме цей ефект раннього перехоплення часто називають одним із її ключових практичних результатів.

2. MTTR для інцидентів, де DT істотно пришвидшила валідацію. Тут акцент не в тому, що SOC реагує на кожне DT-сповіщення агресивно, а в тому, що високодостовірна природа таких сигналів дозволяє швидше перейти від гіпотези до процесно підтвердженого рішення. У багатьох описах SOAR підходів та плейбук-автоматизації прямо зазначається, що автоматизація типових кроків аналізу та реагування може суттєво скорочувати MTTR. DT у цій логіці підсилює ефект SOAR: якісний тригер дає підстави запускати плейбуки без зайвих затримок і з меншим ризиком марної автоматизації.

Доречно зазначити, що MTTD і MTTR - це не просто технічні KPI, а фактичне відображення того, наскільки довго порушник може діяти непоміченим і наскільки швидко банк здатний зменшити масштаби потенційних наслідків. Тому їхня динаміка має прямий зв’язок з управлінням ризиками і обгрунтуванням інвестицій у безпеку.

Окрім часу, для банківського SOC критичним фактором є точність і практична чистота сповіщень. У відкритих джерелах DT неодноразово описується як технологія з високою точністю сигналів і потенційно дуже низьким рівнем хиибнопозитивних результатів, оскільки взаємодія з decoy-активом є нетиповою для законної діяльності. Для фінансових організацій це надзвичайно привабливий аспект, оскільки навіть помірне зменшення шуму здатне суттєво вплинути на якість роботи L1 і загальну стабільність процесу управління інцидентами.

Підвищення точності виявлення можна виправдано описувати через кілька взаємопов’язаних KPI:

1. Частка підтверджених інцидентів серед DT-тривог. Якщо після впровадження технології зростає відсоток випадків, коли DT-тригер приводить до інциденту з реальними ознаками атаки або небезпечної активності, це свідчить про правильне сценарне проєктування пасток і коректний вибір місць їх розміщення.

2. Скорочення часу первинної валідації L1. Зменшення часу, який L1-аналітик витрачає на прийняття рішення щодо істинності сигналу, є практичним маркером того, що DT справді полегшує операційну роботу SOC.

3. Зменшення частки інцидентів із нечітким висновком. Цей показник можна сформулювати у вигляді внутрішньої метрики якості аналізу. Якщо після впровадження DT SOC частіше приходить до однозначних висновків про сценарій і намір противника, це свідчить, що технологія підсилює доказову базу інцидентів.

Усе це дозволяє переформатувати оцінку DT із “технологія є/немає” у чітке вимірювання її внеску у якість сигналів.

Якщо KPI відповідають на питання, як працює SOC, то KRI покликані з’ясувати, як змінюється ризикова картина. У сучасних підходах до вимірювання безпеки KRIs часто розглядаються як індикатори, що допомагають керівництву відстежувати тренди загроз і ризиків між аудитами й квартальними оглядами програми кіберзахисту.

Для банків у межах DT доцільно запропонувати такі індикатори ризиків:

- Частота спроб використання honey credentials. Зростання цього показника може свідчити про підвищення тиску на ідентичності й доменні механізми, що є одним із найнебезпечніших типів загроз для фінансових установ.
- Рівень DT-активності у ключовому (Core) сегменті. Оскільки core-інфраструктура є найбільш критичною, будь-яка тенденція до збільшення таких подій має розглядатися як важливий сигнал для управління ризиком.

- Динаміка звернень до data honeytokens. Це може бути непрямим показником зміни пріоритетів зловмисника у бік пошуку даних або підготовки до ексфільтрації.

Перевага KRI в архітектурі введення в оману полягає в тому, що вони дозволяють відстежувати не лише “результат інциденту”, а й передінцидентні сигнали, тобто розуміти, як змінюється поведінковий профіль загроз для банків [41, 53-55].

Таблиця 3.2.

Узагальнений набір KPI та KRI для оцінки DT у SOC банку

Категорія	Показник	Що вимірює на практиці	Очікуваний ефект від DT
KPI	MTTD для DT-тригерів	Час до виявлення активності нападника, що потрапила у пастку	Скорочення за рахунок раннього контакту з decoy/honeytoken/honey credential
KPI	MTTR для DT-інцидентів	Швидкість локалізації після підтвердження	Зниження через запуск стандартизованих playbooks і менший обсяг ручної валідації
KPI	Рівень підтверджених подій серед DT-тривог	Якість сигналу, близькість до істинно позитивного	Зростання завдяки високоточній природі DT-сенсорів
KPI	Час первинної валідації L1	Операційне навантаження першої лінії	Скорочення за рахунок більш однозначних тригерів

Обґрунтування ефективності DT у банку. Встановлено, що правильне розміщення пасток у DMZ/Office/Core створює умови для раннього контакту.

Це положення спирається на практичну природу DT: пастки й токени мають бути розташовані так, щоб вони відображали реальні маршрути, якими зловмисник зазвичай рухається від первинного доступу до внутрішніх ресурсів. Периметрові приамнки і API DT у DMZ дозволяють фіксувати розвідку та пробні дії ще на ранніх етапах, у той час як office-артефакти дають ранні індикатори "пошуку шляху" всередині корпоративного середовища. Core-орієнтовані AD/DB приманки, натомість, сигналізують про те, що нападник уже наближається до критичних активів. У відкритих описах DT саме сегментне й сценарне розміщення розглядається як передумова отримання раннього та високодостовірного сигналу.

Інтеграція із SIEM/SOAR/EDR перетворює контакт на процес. Ранній контакт сам по собі ще не гарантує зниження ризику, якщо він не потрапляє в операційний цикл SOC. Передача DT-подій у SIEM дозволяє корелювати їх із доменними, мережевими та endpoint-джерелами. Далі SOAR переводить ці сигнали в повторювані плейбуки, а EDR/XDR додає технічне підтвердження на рівні кінцевих точок і забезпечує можливість контрольованої локалізації. Саме такий підхід до підсилення SOC через плейбуки і автоматизацію часто описується як фактор зменшення ручної роботи і скорочення часу відповіді.

Процес дає вимірювані покращення часу і якості виявлення. Коли deception-події стають частиною SIEM-кореляцій і SOAR-плейбуків, SOC перестає витрачати надмірний час на інтерпретацію слабких або сумнівних тригерів. DT-сигнали мають природно вищу достовірність, що скорочує час первинної валідації й дає підстави швидше переходити до розширеного аналізу. Це прямо відображається в покращенні MTTD і в прискоренні ухвалення рішення щодо інциденту, а також у зростанні частки підтверджених подій серед DT-тривог. Тезу про те, що DT може забезпечувати дуже низькі хибнопозивтині і більш чисті сигнали порівняно з багатьма класичними каналами, підтверджують оглядові матеріали вендорів і аналітичні пояснення застосувань технології.

Покращення часу і якості приводить до зниження операційних і ризикових показників. Це фінальний і найважливіший рівень результатів для банку. Зниження MTTD зменшує час присутності зловмисника в середовищі без контролю; зниження MTTR скорочує масштаби потенційних наслідків; підвищення якості сигналів розвантажує L1, мінімізує ризик пропуску реальної атаки на фоні шуму і дає більше часу на проактивні задачі пошуку загроз. У сукупності це може проявлятися і на рівні KRI, наприклад, у зниженні негативних тенденцій щодо напрямів ідентичності та ключового сегменту банку за рахунок більш раннього і точкового перехоплення маршрутів нападника. У загальних рекомендаціях щодо SOC-метрик підкреслюється, що саме часові показники і якість виявлення є основою для демонстрації реального внеску безпеки у зниження ризику [3-5, 26].

3.5 Рекомендації щодо удосконалення процесів DT-реагування SOC

Впровадження DT у банківському SOC має сенс лише тоді, коли технологія не обмежується створенням окремого набору пасток, а прямо впливає на якість процесу управління інцидентами. Розглянемо DT у ролі інструмента організаційного й операційного посилення SOC, який змінює логіку триажу, робить ескалацію більш обґрунтованою, підвищує повторюваність реакцій і дозволяє розширити автоматизацію без надмірних ризиків для критичних сервісів.

На практиці основна проблема багатьох SOC полягає в тому, що сигнали про небезпечну активність часто є слабкими, і вони можуть бути результатом як наступальної поведінки, так і легітимної технічної роботи системи. У банківському середовищі, де технічні ландшафти складні, а активність користувачів і сервісів інтенсивна, цей фактор породжує високе навантаження на L1, збільшує час первинної валідації та створює ризик пропуску найважливіших інцидентів на фоні шуму. DT змінює цю ситуацію принципово, дозволяючи SOC опиратися на події, які самі по собі є сильним контекстом наміру. Тобто взаємодія з пасткою чи honeytoken частіше свідчить про

підозрілий інтерес, ніж про випадкову аномалію. На цій властивості й будується рекомендована модель удосконалення реагування [21-24].

Вбудовування DT у стандартний цикл SOC. Першим кроком до реального процесного ефекту є включення DT-подій у регулярний SOC-потік на рівні регламентів і відповідальності. Для банка важливо зафіксувати, що DT - це не експеримент безпеки, а повноцінне джерело сигналів про інциденти з підвищеною достовірністю. Це має бути відображено у внутрішній документації SOC, зокрема в матриці джерел виявлення, правилах пріоритетизації, списках стандартних кейсів для L1 і профілях ескалації для L2/L3.

Практично такий підхід означає, що будь-яка DT-подія повинна автоматично формувати кейс або мінімум триажний запис у системі управління інцидентами. Аналітик не повинен витрачати час на пошук цієї події в окремій вендорській консолі. Все має починатися у звичних для SOC системах через SIEM/Incident Queue. Окремо варто відзначити, що DT-сповіщення не призначені для масового виявлення всього можлимивого. Їхня цінність у підсвічуванні коротких, специфічних фрагментів атакувальної діяльності, що робить їх ідеальним джерелом для процесів точкової ескалації [3, 5, 8-10].

Оптимізація триажу. Однією з найвідчутніших практичних переваг DT у банку є можливість зменшити час первинної оцінки інциденту на L1. У класичних сценаріях аналітик часто витрачає значну частину часу на перевірку того, чи є тривога реальною, чи це випадкова аномалія, чи помилка конфігурації. Для DT-подій підхід може бути іншим, а саме триаж має стартувати не із сумніву, а з припущення, що подія є потенційно значущою.

Саме тому рекомендовано запровадити у SOC окремий швидкий триажний профіль для DT-сповіщень. Його логіка полягає у тому, що L1 перевіряє не чи це атака, а яка ймовірна фаза сценарію і яких доказів не вистачає. Це тонка, але дуже важлива зміна мислення, яка робить реакцію більш операційно ефективною. У банківській традиції реагування такий підхід зазвичай сприймається позитивно, тому що він зменшує витрати часу на рутинні перевірки і дає більше простору для аналітичної частини роботи.

Розробка багаторівневої моделі реагування. Найкращою практикою для банків є побудова ланцюгів плейбуків з декількома рівнями активності, що дозволяє уникнути ситуації, коли SOC або занадто агресивно реагує на кожен DT-тригер, або навпаки надто довго утримує інцидент у підвішеному стані.

У рамках такої моделі варто сформувати:

- базовий плейбук розвідки для DMZ/периметра, який має обмежуватися швидким збагаченням контексту, визначенням джерела активності, перевіркою суміжних мережевих сигналів. У цьому сценарії важливо не припиняти половину доступів, а виявити чи повторюється поведінка, чи є системність, і чи є ознаки переходу до наступної фази атакувального циклу;
- плейбук ідентичностей для фіктивних облікових записів і AD-орієнтованих пасток, який є одним із найважливіших сценаріїв для банку. Саме тут доцільна прискорена ескалація на L2 при першому ж сильному підтвердженні (наприклад, поєднання DT-події з аномальною автентифікацією або нетиповими спробами доступу до доменних ресурсів). Практична мета цього плейбуку зупинити сценарій до того, як нападник отримає стабільні привілеї в домені.

плейбук даних для honeytokens у файлових сховищах або тестових базах даних (BD). У банківських умовах це може бути інструмент раннього попередження про інтерес до чутливих масивів. У відповідь плейбук повинен підхоплювати дані з DLP/EDR/мережевих джерел і формувати обґрунтоване припущення: чи дійсно зловмисник збирає дані, чи це локальна підозріла активність без розвитку.

Така багаторівнева структура робить реагування більш живим і ближчим до реальних сценаріїв банківської інфраструктури.

Розвиток автоматизації. Щоб DT не залишилася декоративною технологією, SOC має розширювати автоматизацію поступово. Рекомендованою є тактика рухатися від безпечних дій до більш активних у міру того, як команда накопичує впевненість у якості сигналів і стабільності процесів.

На першому етапі автоматизація має охоплювати збагачення та документацію. Це автотегування інциденту, підтягування інформації про актив, формування короткої часової лінії подій, запуск швидких пошукових запитів у SIEM. Ефект цього рівня не завжди видно ззовні, але він відчутний для SOC вже на повсякденному рівні роботи змін.

На другому етапі доцільно додати пріоритезацію пошуку загроз (priority-hunting), коли DT-подія автоматично запускає короткі сценарії перевірки пов’язаних ознак у сусідніх сегментах. У банківській сфері це особливо корисно для сценаріїв руху маршрутом офіс – сервірні зони або DMZ - внутрішні шлюзи.

На третьому етапі можливі умовні стримувальні дії. Важливо наголошувати саме на умовності, а самі автоматичні обмеження мають спрацьовувати лише при збігу кількох факторів. Наприклад, хибні акаунти використано з нетипового хоста, EDR фіксує підозрілу поведінку, і є ознаки мережевої розвідки. У такому випадку реакція стає алгоритмічно виправданою.

Ця модель добре підходить для банків, оскільки дозволяє зберігати стабільність критичних процесів і водночас поступово збільшувати швидкість реальних дій при підтверджених інцидентах.

Удосконалення процесів ексалації. Ще однією важливою рекомендацією є відхід від плоскої моделі ескалації, де рішення залежить лише від типу сповіщення, для DT у банку краще працює контекстна ескалація. У таких випадках SOC має заздалегідь визначити:

- як саме змінюється пріоритет DT-події в залежності від сегмента;
- як підвищується рівень інциденту, якщо пастка пов’язана з AD або сервісними акаунтами;
- які пороги підтвердження потрібні для переведення інциденту на рівень L2 або L3/IR.

Такі правила корисні, оскільки вони стандартизують комунікацію між SOC і власниками бізнес-систем. Коли ескалація оформлена зрозуміло, її простіше захистити на рівні менеджменту, нормативної відповідності чи внутрішнього

контролю.

Навчання та культура роботи з DT-сигналами. DT - це технологія, яка вимагає не тільки налаштувань, а й певного стилю мислення SOC. У банку доцільно включити у програму навчання аналітиків короткі практичні модулі:

- як відрізняється DT-подія від класичних аномалій;
- чому “одиночний сильний тригер” може бути важливішим за багато слабких подій;
- як правильно формувати висновок про намір нападника на основі мінімального набору ознак.

Таким чином створюється культуру, у якій DT використовують як повсякденний сенсор, що підсилює видимість поведінки противника.

Процес безперервного вдосконалення. Окремо слід відзначити важливість постійного оновлення DT-ландшафту. Практична помилка багатьох організацій полягає у тому, що пастки розгортаються разово і живуть без змін. У реальному банківському середовищі це неефективно, оскільки інфраструктура змінюється, а атакувальні маршрути адаптуються під нові технології й бізнес-архітектуру.

У цьому контексті рекомендовано запровадити цикл:

1. періодичний перегляд “гарячих зон” атакувальних сценаріїв;
2. точкове перенесення пасток ближче до нових активів або сервісів;
3. додавання нових honeytokens під актуальні бізнес-процеси;
4. регулярний аналіз того, які пастки працюють добре, а які не дають корисних сигналів.

У таблиці 3.1 представлена Дорожня карта удосконалення реагування SOC із використанням технологій введення в оману.

Таблиця 3.3.

Дорожня карта удосконалення реагування SOC із DT

Етап	Фокус	Які зміни в процесах SOC	Практичний результат
Пілот	Перевірка концепції	Введення DT як джерела в SIEM, ручна валідація L1	Формування первинних випадків застосування і критеріїв пріоритезації
Контрольована експлуатація	Стандартизація	Окремі плейбуки для DMZ/Office/Identity, базове охоплення	Скорочення часу первинного триажу, стабільна екскалація подій і реагування
Масштабування	Глибша інтеграція	Автоматичні пошукові сценарії, пріоритезація пошуку загроз, розширене збагачення даними EDR	Підвищення якості виявлення, зниження операційного навантаження
Керована автоматизація	Умовне стримування	Реакції на рівні EDR/мережі за умов підтвердження кількох індикаторів	Скорочення MTTR у реальних інцидентах без зайвого ризику для бізнесу

Висновки до розділу 3

У розділі проведено всебічний аналіз поточного стану системи Центру оперативного управління безпекою (SOC) банку, оцінено ключові показники ефективності SOC та надано рекомендації для покращення його ефективності.

Аналіз поточного стану показав, що існуюча система SOC має ряд сильних сторін, таких як наявність сучасного обладнання і кваліфікованого персоналу. Проте, виявлено й певні недоліки, зокрема недостатня автоматизація деяких процесів і неефективне управління інцидентами, що може призводити до затримок у реагуванні на загрози.

Оцінка ключових показників ефективності DT SOC, зокрема середнього часу реагування на інциденти (MTTR), кількості помилкових спрацювань (false positives) і рівня задоволеності користувачів, вказала на необхідність вдосконалення певних аспектів діяльності SOC. Особлива увага приділена показникам, що впливають на швидкість і точність виявлення та реагування на інциденти.

Для покращення ефективності системи SOC було запропоновано ряд рекомендацій щодо удосконалення реагування SOC із DT, серед яких підвищення рівня автоматизації за рахунок впровадження сучасних інструментів ШІ та МН, проведення регулярного навчання персоналу й оптимізація процесів обробки DT-подій. Також рекомендується вдосконалення процедур моніторингу та звітності для забезпечення більш прозорого та оперативного управління безпекою.

Впровадження запропонованих рекомендацій дозволить підвищити загальну ефективність DT SOC, що, в свою чергу, сприятиме кращому захисту інформаційних ресурсів організації від сучасних кіберзагроз.

ВИСНОВКИ

У кваліфікаційній роботі комплексно розкрито роль і потенціал технологій введення в оману (Deception Technology) у забезпеченні кібербезпеки підприємства на прикладі банківського сектору. Загальна логіка дослідження будувалася на поєднанні теоретичних засад, аналізу галузевої специфіки та розробки практичної моделі впровадження DT у процеси SOC. Такий підхід дозволив показати, що DT не є “альтернативою” класичним засобам виявлення загроз, а виступає додатковим високодостовірним шаром захисту, який підсилює здатність організації фіксувати ранні ознаки атак, зокрема розвідку, спроби компрометації облікових даних та латеральне переміщення.

У розділі 1 було сформовано теоретичний фундамент теми: розглянуто сучасну динаміку кіберзагроз, етапи еволюції засобів захисту та концептуальні засади DT. Визначено, що ключова цінність цього підходу полягає у створенні контрольованих пасток і маркерів, які генерують сигнали з високою ймовірністю безпекової значущості. Також обґрунтовано порівняльну роль DT відносно традиційного інструментарію (IDS/IPS/SIEM/EDR) і показано, чому для складних корпоративних середовищ, зокрема банків, важливим є саме інтеграційний формат впровадження цієї технології.

Розділ 2 присвячений прикладному аналізу використання DT у банківському секторі. Охарактеризовано специфіку системи кібербезпеки банків України і типову архітектуру SOC, визначено точки, де DT здатна забезпечити максимальний ефект відповідно до сегментації інфраструктури й пріоритетів захисту ідентичностей та критичних сервісів. Зроблено огляд ринку рішень, включно з комерційними та open-source платформами, узагальнено практичні сценарії застосування, які демонструють релевантність DT у вирішенні завдань раннього виявлення внутрішньомережевої підозрілої активності. У результаті зроблено висновок, що найбільш перспективним для банків є поєднання стратегічних корпоративних рішень із можливістю пілотування, навчання і тестових сценаріїв на базі відкритих інструментів.

У розділі 3 запропоновано практично орієнтовану модель впровадження DT у SOC банку. Розроблено архітектурну логіку розміщення приманок, пасток і хибних облікових записів у DMZ, офісному та основному сегментах банку, а також описано процес взаємодії DT із SIEM, SOAR і EDR/XDR. Окремо сформовано алгоритм обробки інцидентів на основі DT-тригерів із контекстною ескалацією і поетапним підходом до автоматизації. Показано, що ефективність такого впровадження доцільно оцінювати через поєднання KPI та KRI з акцентом на зниження MTTD і MTTR, підвищення точності виявлення та зменшення операційного навантаження на першу лінію SOC. Запропоновані рекомендації щодо удосконалення реагування уточнюють шлях від пілотного впровадження до зрілої моделі, де DT стає повноцінним засобом підсилення процесів виявлення і стримування загроз на рівні банківської інфраструктури.

Таким чином, у роботі доведено, що DT є перспективним напрямом розвитку банківського SOC, здатним підвищити якість моніторингу і прискорити реагування в умовах високої складності сучасних атак. Практичне значення отриманих результатів полягає у створенні структурованої моделі впровадження DT, яка може бути адаптована під реальні контури банку та використана як основа для подальшого розвитку варіантів застосування, плейбуків і метрик ефективності. У перспективі подальших досліджень доцільним є розширення тестування запропонованої моделі на конкретних інфраструктурних сценаріях банку, деталізація економічного обґрунтування витрат і вигод, а також поглиблення інтеграції DT із напрямами ITDR, XDR та DLP для формування комплексної стратегії активної оборони.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cybersecurity Trends: Resilience through Transformation. *Gartner*. URL: https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends

2. Global Cybersecurity Outlook 2025. *World Economic Forum*. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/digest/

3. Information Security and Computer Systems (KPI). URL: https://its.iszzi.kpi.ua/article/view/249897

4. Deception Technology: architecture and classification. *Information Security and Computer Systems (KPI)*. URL: https://its.iszzi.kpi.ua/article/view/249897

5. Demystifying Deception Technology: A Survey. *arXiv*. URL: https://arxiv.org/abs/1804.06196

6. A comprehensive survey on cyber deception techniques to improve honeypot performance. Computers & Security. URL: https://www.sciencedirect.com/science/article/pii/S0167404824000932

7. Advancing Cybersecurity with Honeypots and Deception Strategies. *MDPI*. URL: https://www.mdpi.com/2227-9709/12/1/14

8. Deception Technology: Enhancing Cybersecurity with the Power of Deception. *Medium (InfosecMatrix)*. URL: https://medium.com/infosecmatrix/deception-technology-enhancing-cybersecurity-with-the-power-of-deception-karthikeyan-nagaraj-4de2728ccf99

9. Honeypots and Deception Technology - Turning Offense into Defense. *Medium*. URL: https://medium.com/%40attvikas.chauhan/new-read-honeypots-and-deception-technology-turning-offense-into-defense-3c8dc887cb21

10. From Honeypots to AI-Driven Defense: The Evolution of Cyber Deception. *Acalvio*. URL: https://www.acalvio.com/blog/active-defense/from-honeypots-to-ai-driven-defense-the-evolution-of-cyber-deception/

11. Технологія обману. Що таке Deception і як обманюють хакерів. *10Guards*. URL: https://10guards.com/ua/blog/2022/09/21/deception-technology-and-how-it-can-trap-cyberattackers/

12. Активні мережеві приманки (Deception). *AMind*. URL: https://www.amind.ua/ua-services/active-network-decoys-deception

13. MITRE Engage™. An Adversary Engagement Framework. *MITRE*. URL: https://engage.mitre.org/

14. MITRE Engage: A Framework and Community for Cyber Deception. *MITRE*. URL: https://www.mitre.org/news-insights/impact-story/mitre-engage-framework-and-community-cyber-deception

15. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems – Requirements. *ISO*. URL: https://www.iso.org/standard/27001

16. ISO/IEC 27035-1:2023 Information technology - Information security incident management. Part 1: Principles and process. *ISO*. URL: https://www.iso.org/standard/78973.html

17. ДСТУ ISO/IEC 27035-1:2018 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. *Budstandart*. URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=80309

18. ENISA Threat Landscape 2024. *ENISA*. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

19. Threat Landscape – Cyber Threats. *ENISA*. URL: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape

20. NIST SP 800-61 Rev. 3: Computer Security Incident Handling Guide. *NIST*. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

21. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради*, 2017, № 45, ст.403. URL: https://zakon.rada.gov.ua/go/2163-19

22. Regulatory and legal framework of cybersecurity. *CSIRT-UA*. URL: https://csirt.csi.cip.gov.ua/en/pages/regulatory-and-legal-framework

23. Computer Security Incident Response Team in the banking system of Ukraine (CSIRT-NBU). *NBU*. URL: https://cyber.bank.gov.ua/rfc2350.pdf

24. Cyber Security Center of the National Bank of Ukraine. *NBU*. URL: https://cyber.bank.gov.ua/en

25. What Is a Security Operations Center (SOC)? *IBM*. URL: https://www.ibm.com/think/topics/security-operations-center

26. What is a Security Operations Center (SOC)? *CrowdStrike*. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/security-operations-center-soc/

27. 10 Security Operations Center Best Practices. *VMRay*. URL: https://www.vmray.com/soc-best-practices/

28. Security Operations Center (SOC) – для чого він, і що може дати організації? *ISSP*. URL: https://www.issp.training/post/security-operations-center-soc-dlya-choho-vin-i-shcho-mozhe-daty-orhanizatsiyi

29. 11 стратегій SOC від MITRE. Роадмап для вдумливої роботи українських CISO. *Octava Defence*. URL: https://octava.ua/11-strategij-soc-vid-mitre-roadmap-dlya-vdumlyvoyi-roboty-ukrayinskyh-ciso/

30. How Can Banks Use Deception Technology to Their Advantage? *BizTech Magazine*. URL: https://biztechmagazine.com/article/2019/06/how-can-banks-use-deception-technology-their-advantage

31. How Deception Technology Creates Digital Traps for Banking Attackers. *Fidelis Security*. URL: https://fidelissecurity.com/threatgeek/deception/deception-technology-in-banking-cybersecurity-defense/

32. Deception Technology for Financial Institutions in India. *Treacle Technologies*. URL: https://treacletech.com/deception-technology-for-financial-institutions-in-india/

33. Three Use Cases for Deception Technology in Financial Services. Illusive Networks. *BankInfoSecurity*. URL: https://www.bankinfosecurity.com/whitepapers/three-use-cases-for-deception-technology-in-financial-services-w-5235

34. Illusive Uses Deception to Reduce Cyber Risks for Financial Services. EMA Impact Brief. URL: https://cdn2.hubspot.net/hubfs/725085/EMA%20Impact%20Brief%20-%20Deception%20to%20Reduce%20Cyber%20Risks%20for%20Financial%20Services.pdf

35. OpenCanary. Open-source Canary Services. OpenCanary Documentation. *OpenCanary*. URL: https://opencanary.readthedocs.io/

36. OpenCanary by Thinkst Canary. Modular and Decentralised Honeypot. *GitHub*. URL: https://github.com/thinkst/opencanary

37. Open Canary – приманка для хакера. *Habr*. URL: https://habr.com/ru/companies/otus/articles/800047/

38. Cowrie. Medium to High Interaction SSH and Telnet Honeypot. *Cowrie*. URL: https://docs.cowrie.org/en/latest/README.html

39. T-Pot. The All in One Multi Honeypot Platform. *Github*. URL: https://github.com/telekom-security/tpotce

40. ShadowPlex Preemptive Cybersecurity Platform. *Acalvio*. URL: https://www.acalvio.com/shadowplex-platform/

41. ThreatDefend Platform. Overview. *Attivo Networks*. URL: https://www.asia-net.com.hk/wp-content/uploads/2021/11/Attivo_Networks-ThreatDefend_Overview.pdf

42. Labyrinth Deception Platform. IITD. *Labyrinth Security Solutions*. URL: https://labyrinth.tech/platform

43. Cymmetria. MazeRunner Cyber Deception Solution. *Cybersecurity Excellence Awards*. URL: https://cybersecurity-excellence-awards.com/candidates/cymmetria/

44. Trap the Hackers: Building and Analyzing a T-Pot Honeypot (Part 1). *Medium*. URL: https://medium.com/%40jiumael/trap-the-hackers-building-and-analyzing-a-t-pot-honeypot-b15f3b6c5ea2

45. Trends of fraud operations on the banking market and ensuring economic security of banks. Economy and State. URL: https://www.economy.nayka.com.ua/pdf/5_2020/13.pdf

46. Honeypot and cyber deception as a tool for detecting cyber attacks in IoT networks. *CEUR Workshop Proceedings*. URL: https://ceur-ws.org/Vol-3374/paper06.pdf

47. Vaishali Shirsath. A Survey on Current States of Honeypots and Deception Techniques for Attack Capture. *IJERT*. 2021. Volume 9, Issue 3. URL: https://www.ijert.org/research/a-survey-on-current-states-of-honeypots-and-deception-techniques-for-attack-capture-IJERTCONV9IS03092.pdf

48. Matthew Bringer, Christopher Chelmecki. A Survey: Recent Advances and Future Trends in Honeypot Research. *International Journal of Computer Network and Information Security*. 2012. URL: https://www.researchgate.net/publication/265974200_A_Survey_Recent_Advances_and_Future_Trends_in_Honeypot_Research

49. An Analysis of Honeypots and their Impact as a Cyber Deception Tool for Intelligence Gathering. *arXiv*. URL: https://arxiv.org/abs/2301.00045

50. An Analysis of Honeypots and their Impact as a Cyber Deception Tool for Intelligence Gathering. *arXiv*. URL: https://arxiv.org/abs/2301.00045

51. Команда реагування на кіберінциденти в банківській системі України. CSIRT-NBU. *Національний банк України*. URL: https://cyber.bank.gov.ua/

52. Сервіси CSIRT-NBU для банків України. *Національний банк України*. URL: https://cyber.bank.gov.ua/bankam

53. Положення про організацію кіберзахисту в банківській системі України. *Національний банк України*. URL: https://bank.gov.ua/admin_uploads/article/proekt_2021-11-04.pdf?v=7

54. Документи міжнародних організацій та країн-партнерів у сфері кіберзахисту. Державний центр кіберзахисту. ДССЗЗІ України. URL: https://cip.gov.ua/ua/news/perelik-dokumentiv-mizhnarodnikh-organizacii-ta-krayin-partneriv-u-sferi-kiberzakhistu

55. Україна впроваджує норми NIST Cybersecurity Framework 2.0.| *ДССЗЗІ України*. URL: https://cip.gov.ua/ua/news/ukrayina-vprovadzhuye-naikrashi-svitovi-praktiki-u-sferi-kiberbezpeki-ta-vprovadzhuye-normi-nist-cybersecurity-framework-2-0

56. Cyber-banking fraud risk mitigation: conceptual model. Banks and Bank Systems. *Business Perspectives*. URL: https://www.businessperspectives.org/images/pdf/applications/publishing/templates/article/assets/6695/BBS_en_2015_02_Dzomira.pdf

57. Digital Fraud in Banking: Supervisory and Financial Stability Implications. *Basel Committee on Banking Supervision (BIS)*. URL: https://www.bis.org/fsi/fsisummaries/exsum_23902.pdf

58. Digital Fraud in Banking. *Association of Supervisors of Banks of the Americas (ASBA)*. URL: https://asbasupervision.org/wp-content/uploads/2025/06/ASBA_ Digital_Fraud_in_Banking_April2025_ENG.pdf

59. Caprian I.The Application of Artificial Intelligence for Detection and Prevention of Banking Fraud. *Problems of Economy*. 2023. № 2 (56). URL: https://www.problecon.com/export_pdf/problems-of-economy-2023-2_0-pages-204_212.pdf

60. Akanbi Caleb. Fraud Detection in Banking Systems. 2025. ResearchGate | URL: https://www.researchgate.net/publication/388565206_Fraud_Detection_in_Banking_Systems

61. Dwiyana Nurul Fajar, Indira Januarti. Fraud Detection in Banking Sector: A Bibliometric Analysis. *International Journal of Economics, Finance and Management (IJEFM)*. 2025. Volume 08. Issue 08. URL: https://ijefm.co.in/v8i8/Doc/27.pdf

62. Survey on Honeypot: Detection, Countermeasures and Challenges. *AIP Conference Proceedings*. URL: https://pubs.aip.org/aip/acp/article/3244/1/030063/3322828/Survey-on-honeypot-Detection-countermeasures-and