International Science Journal of Engineering & Agriculture
2025; 4(6): 1-14
https://isg-journal.com/isjea
doi: 10.46299/j.isjea.20250406.01
ISSN: 2720-6319

INTERNATIONAL
SCIENCE GROUP

Технології обману в кібербезпеці: інтеграція cowrie та ELK Stack для виявлення атак на мережевий трафік

Ігор Андрущак
Луцький національний технічний університет, Луцьк, Україна
ORCID 0000-0002-8751-4420

Віктор Кошелюк
Луцький національний технічний університет, Луцьк, Україна
ORCID 0000-0002-4136-5087

Ілля Веремій
Луцький національний технічний університет, Луцьк, Україна
ORCID 0009-0003-1381-9920

Анотація: У статті досліджуються технології обману (Deception Technologies) у сфері кібербезпеки з метою підвищення ефективності виявлення атак на мережевий трафік. Основна мета роботи полягає у практичному дослідженні інтеграції системи Cowrie, що забезпечує емуляцію серверів протоколів Secure Shell та Telnet, із платформою Elastic Stack (Elasticsearch, Logstash, Kibana) для збору, обробки та візуалізації даних про підозрілу активність. Дослідження спрямоване на розробку методики налаштування honeypot-системи та її інтеграції в централізовану аналітичну систему з метою своєчасного реагування на потенційні загрози. Методи дослідження включають аналіз сучасних технологій обману та їх порівняння, конфігурацію та оптимізацію cowrie для збору логів про мережеві атаки, а також інтеграцію отриманих даних у Elastic Stack. Для оцінки ефективності системи використовувався експериментальний підхід із фіксацією типів атак, джерел вторгнень та поведінки зловмисників у мережі. Візуалізація даних у Kibana дозволила здійснювати детальний аналіз активності та формувати оперативні звіти про інциденти безпеки. Результати дослідження показали, що інтегрована система cowrie та Elastic Stack ефективно фіксує та класифікує спроби несанкціонованого доступу, атаки на паролі та інші типові мережеві загрози. Було встановлено, що комбінування емуляції пасток із централізованим аналізом даних дозволяє підвищити швидкість виявлення атак та покращити розуміння поведінки зловмисників. Налаштування логування та кореляції даних забезпечує гнучкий підхід до моніторингу та аналітики безпеки. Наукова новизна дослідження полягає у розробці інтегрованого підходу до застосування технологій обману в кібербезпеці з використанням honeypot cowrie та платформи аналізу даних Elastic Stack для виявлення, моніторингу та аналізу атак на мережевий трафік. Запропоновано методику автоматизованого збору та кореляції даних про несанкціоновані дії, що дозволяє підвищити точність детекції та швидкість реагування на загрози. Дослідження демонструє ефективність інтеграції емульованих пасток із системою візуалізації та аналітики, забезпечуючи більш глибоке розуміння поведінки атакуючих та можливість прогнозування потенційних сценаріїв вторгнень у мережеву інфраструктуру. У висновках підкреслюється, що технології обману є ефективним інструментом протидії кіберзагрозам, а їх інтеграція з платформами аналітики, такими як Elastic Stack, значно підвищує спроможність організацій реагувати на інциденти. Рекомендації включають впровадження подібних систем у корпоративних та хмарних середовищах, регулярне оновлення конфігурацій honeypot та вдосконалення методів візуалізації й аналізу даних. Майбутні напрями розвитку передбачають автоматизацію реагування на інциденти на основі зібраних даних, інтеграцію з системами управління інформацією та подіями безпеки, а також використання машинного навчання для прогнозування та попередження нових типів атак.

Ключові слова: cowrie, deception technologies, honeypot, ELK Stack, кіберзагрози.

1. Вступ

Незважаючи на багаторічні дослідження та розвиток технологій у сфері комп'ютерної безпеки, вона залишається складною і вразливою галуззю, у якій традиційні підходи часто не забезпечують повного захисту від сучасних загроз. Хронічні проблеми безпеки інформаційних систем підкреслюють необхідність пошуку інноваційних методів, здатних доповнювати класичні механізми контролю та захисту. Одним із перспективних напрямів є застосування стратегій обману (deception technologies) як активного інструменту кіберзахисту. У повсякденному житті обман використовується для створення ілюзії безпеки, наприклад, увімкнене світло в будинку може дати зловмиснику хибне уявлення про присутність мешканців. В IT-системах обман застосовується значно рідше і часто має прихований характер, проте його потенціал для зміни поведінки нападника є суттєвим [1, 2].

На відміну від традиційних методів безпеки, які здебільшого спрямовані на виявлення або блокування атак, обман діє через моделювання середовища та маніпулювання сприйняттям зловмисника, змушуючи його здійснювати дії, вигідні захиснику. Такий підхід дозволяє компенсувати слабкі сторони класичних механізмів і створює додатковий рівень стійкості системи. Інтеграція обману із традиційними засобами безпеки може суттєво підвищити ефективність захисту, роблячи інформаційні системи більш адаптивними та важкодоступними для кібератак.

У сфері кібербезпеки використання обману залишається недостатньо розвиненим, хоча він може стати критично важливим інструментом захисту [3]. Дослідження військових стратегій обману демонструють, що ефективне введення супротивника в оману є складною професійною навичкою, яка потребує глибокого розуміння принципів, методів та психології дезінформації. У контексті інформаційних систем обман може застосовуватися для створення кібер-пасток, таких як honeypot-системи, які впливають на процеси прийняття рішень зловмисниками, відволікають їхні дії або збирають інформацію про атаки. Такі технології обману забезпечують додатковий рівень захисту, підвищують ефективність превентивних заходів і заповнюють прогалини традиційних методів кібероборони, стаючи ключовим елементом сучасної стратегії інформаційної безпеки.

Термін «IT-безпека» охоплює широкий спектр технічних, організаційних та процедурних заходів, спрямованих на захист визначеного набору інформаційних активів від різноманітних загроз. Ці активи зазвичай класифікують відповідно до ключових цілей безпеки, відомих як CIAA: конфіденційність, цілісність, автентифікація та доступність. Конфіденційність гарантує, що інформація доступна лише уповноваженим користувачам; цілісність забезпечує недоторканість даних і запобігає їх несанкціонованим змінам; автентифікація підтверджує особу користувачів і джерел даних; доступність гарантує безперервність доступу до інформаційних ресурсів. Класична IT-безпека здебільшого зосереджується на досягненні цих цілей у традиційних IT-системах і на мінімізації ризику несанкціонованих дій [4, 5].

Deception Technologies (DT) – сучасний підхід, що не завжди безпосередньо відображає класичні цілі CIAA, але орієнтований на більш абстрактні та проактивні завдання, такі як виявлення вторгнень, моніторинг підозрілої активності та аналіз поведінки потенційних зловмисників. DT особливо ефективні в хмарних середовищах, де масштабованість та динамічність ресурсів дозволяють створювати пастки та фальшиві системи, які імітують реальні сервіси. Однією з ключових особливостей DT є використання концепції Security by Obscurity (SbO) – навмисного ускладнення або приховування деталей системи, що ускладнює зловмиснику розуміння її структури. Хоча SbO не рекомендується як основний метод у традиційній безпеці, у DT він слугує ефективним інструментом уповільнення атакуючих і відволікання від реальних цілей. Особливо це важливо у хмарних інфраструктурах, де невідомість наявності пастки значно підвищує шанси на своєчасне виявлення зловмисної активності та мінімізацію ризиків для критично важливих сервісів.

Початкові рішення у сфері DT спиралися на використання honeypot-систем. Концепція honeypot – це спеціально підготовлений цифровий об'єкт, призначений для приваблення й виявлення шкідливої мережевої активності [6]. По суті honeypot виступає як приманка: це може бути фізична машина, віртуальна машина або виділені мережеві сервіси, що навмисно виглядають «звичними» або вразливими, щоб зацікавити зловмисників. Коли атака відбувається, програмне забезпечення honeypot-а фіксує всі дії, збирає сліди компрометації та детальну телеметрію – від мережевих пакетів і команд до використовуваних експлойтів і поведінкових патернів. Зібрані дані не стільки слугують для відновлення втрачених ресурсів, скільки виконують роль інструмента спостереження: вони допомагають аналізувати тактики й методи атак, формувати сигнали раннього попередження та покращувати захисні механізми.

Honeypot також є важливим засобом для інцидент-резолюшну та навчання аналітиків – на підставі логів можна відтворити атаки і розробити контрзаходи. Конфігурація honeypot-а зазвичай передбачає навмисне створення слабких місць (наприклад, відкрите портів, застаріле ПЗ чи очевидні облікові записи), щоб підвищити ймовірність залучення зловмисника. Водночас такі системи повинні бути ізольовані від продуктивної інфраструктури, щоб запобігти ескалації ризиків [7, 8]. У сукупності honeypot – це активна стратегія кіберзахисту, що поєднує детектування, розвідку та навчання для підвищення стійкості мереж і систем.

Водночас внесок honeypots у безпеку має радше реактивний характер. Якщо система просто імітує реальні об'єкти та обмежується лише реєстрацією дій, вона здатна виявляти переважно некваліфікованих порушників. Прості honeypots відтворюють поведінку реальних систем, але навіть поверхневий аналіз їхніх параметрів, наприклад відкритих портів чи доступних служб віддаленого управління, може видати зловмиснику, що перед ним не справжній ресурс, а приманка [9]. Таким чином, honeypots є цінним інструментом для збору розвідувальної інформації про атаки, навчання команд безпеки та дослідження методів кіберзлочинців. Вони не замінюють стандартні технології захисту, але ефективно доповнюють їх, дозволяючи компаніям отримувати унікальні дані про потенційні загрози та підвищувати рівень своєї кібербезпеки.

Наступним етапом розвитку технологій honeypot стало створення більш реалістичних систем, здатних імітувати поведінку справжніх комп'ютерних систем на основі шаблонів реакції реальних сервісів та програм. Такі рішення дозволяють не лише приваблювати потенційних зловмисників, а й детально аналізувати їхні дії для підвищення рівня безпеки. З поширенням Honeypot у корпоративних та хмарних мережах зловмисники почали активно розробляти спеціальні інструменти для їх виявлення та обходу. Ефективність технологій Honeypot, як і систем «обманки» загалом, значною мірою ґрунтується на психології атакуючих та передбачуваних схемах їхньої поведінки. В сучасних умовах захисту це передбачає розвиток динамічних та масштабованих конфігурацій, які можуть розгортатися у хмарних кластерах, легко адаптуватися до нових загроз і створювати більш непередбачувані середовища. Використання відкритих інструментів та модулів дозволяє швидко модернізувати honeypot-системи та підвищувати їхню стійкість до спроб виявлення зловмисниками [10, 11].

Технології обману в галузі кібербезпеки представляють собою системний підхід до захисту інформаційних систем шляхом створення умов для дезінформації потенційних зловмисників. Суть підходу полягає у розгортанні по всій IT-інфраструктурі спеціалізованих пасток та приманок, які імітують справжні активи та сервіси, тим самим створюючи ілюзію реальної цільової системи. Взаємодія з такими приманками дозволяє безпечно фіксувати та аналізувати методи, техніки та вектори атак, що забезпечує детальне розуміння поведінки атакуючих і підвищує ефективність превентивних заходів [12]. Концепція технологій обману бере початок від класичних honeypots, де основна мета полягала у створенні пасток для залучення хакерів. Сучасні платформи Deception Detection Platforms (DDP) розвинули цю ідею, значно розширивши функціонал і підвищивши ефективність захисту.

Deception-платформи інтегрують комплекс технологічних компонентів, включаючи пастки (Decoys, Traps), приманки (Lures), спеціалізовані додатки, інформаційні ресурси, бази

даних та об’єкти Active Directory. Сучасні DDP надають розширені функціональні можливості для раннього виявлення загроз, детального аналізу атак та автоматизованого реагування на кіберінциденти. Технологія Deception передбачає створення високореалістичних емуляцій IT-інфраструктури організації, що дозволяє маніпулювати поведінкою потенційних зловмисників і стимулювати їх до взаємодії з контрольованими об’єктами. Це забезпечує не лише попередження або локалізацію атак на ранніх стадіях, а й збирання цінних даних про методи та стратегії атакуючих, підвищуючи ефективність аналітики безпеки. У порівнянні з традиційними ханіпотами, які мають обмежений функціонал і потребують високого рівня кваліфікації персоналу, сучасні Deception-платформи забезпечують значний рівень автоматизації процесів, що сприяє оптимізації управління інцидентами та підвищенню загального рівня кіберзахисту організації.

2. Об’єкт і предмет дослідження

Об’єктом дослідження є процес виявлення та аналізу кіберзагроз у мережевому середовищі через призму технологій обману (deception technologies). Дослідження зосереджується на взаємодії між honeypot-системою cowrie, яка емулює вразливі SSH/Telnet сервіси для приманювання зловмисників, та аналітичною платформою ELK Stack, що забезпечує збір, обробку, зберігання та візуалізацію даних про атаки. Конкретними складовими об’єкта є: мережевий трафік, що надходить до honeypot-системи; журнали подій про спроби несанкціонованого доступу; методи та інструменти зловмисників (експлойти, brute-force атаки, malware); патерни поведінки атакуючих; а також інтеграційні механізми між компонентами системи виявлення загроз. Об’єкт охоплює технічну інфраструктуру раннього попередження про кіберінциденти, що дозволяє організаціям проактивно виявляти нові вектори атак, аналізувати тактики, техніки та процедури (TTPs) зловмисників, і формувати ефективні стратегії кібербезпеки на основі реальних даних про загрози.

Предметом дослідження є застосування технологій обману у кібербезпеці через інтеграцію cowrie та ELK Stack для виявлення атак на мережевий трафік. Cowrie виступає як honeypot, який імітує вразливі сервіси та фіксує спроби несанкціонованого доступу, тоді як ELK Stack забезпечує централізоване збирання, аналіз і візуалізацію цих даних. Дослідження фокусується на методах виявлення та класифікації атак, оцінці ефективності обманних технологій у виявленні SSH-атак, brute-force та сканування портів, а також на оптимізації обробки логів. Окрему увагу приділено архітектурі інтеграції cowrie та ELK Stack у корпоративних і хмарних мережах, підвищенню точності моніторингу та швидкості реагування на інциденти кібербезпеки, а також аналізу обмежень і ризиків застосування таких технологій у реальних умовах.

3. Мета та задачі дослідження

Метою цього дослідження є вивчення та практичне застосування технологій обману у кібербезпеці через інтеграцію системи cowrie та платформи ELK Stack для виявлення атак на мережевий трафік. Дослідження спрямоване на оцінку ефективності емуляції пасток (honeypot) для фіксації несанкціонованих спроб доступу, атак на паролі та використання відомих вразливостей. Основним завданням є створення системи, яка дозволяє збирати, обробляти та візуалізувати дані про підозрілу активність мережі, забезпечуючи своєчасне реагування на інциденти безпеки. Особлива увага приділяється налаштуванню cowrie для максимального збору інформації про дії зловмисників та інтеграції цих даних у централізовану аналітичну систему ELK Stack. Результати дослідження мають на меті підвищення захищеності мережевих інфраструктур та демонстрацію практичного використання технологій обману як ефективного інструменту протидії кіберзагрозам.

Для досягнення поставленої мети дослідження передбачалося виконання таких завдань:

✓ огляд сучасних технологій обману у кібербезпеці. Було проведено аналіз існуючих підходів до використання honeypot-систем та інших Deception Technologies для виявлення та запобігання кібератакам, визначено переваги та обмеження різних рішень, а також проведено порівняння популярних систем на ринку;

✓ вибір і обґрунтування використання cowrie та ELK Stack. На основі аналізу було обрано honeypot cowrie як ефективний інструмент емуляції SSH- та Telnet-серверів для збору даних про атаки, а ELK Stack – для централізованого збору, обробки та візуалізації інформації про мережевий трафік. Було розглянуто можливості інтеграції цих систем для отримання максимальної аналітичної цінності;

✓ налаштування та оптимізація cowrie. Виконано конфігурацію cowrie з урахуванням збору детальної інформації про атаки, логування дій зловмисників та збереження даних у структурованому вигляді для подальшої обробки. Здійснено тестування системи на виявлення типових атак і несанкціонованих спроб доступу;

✓ інтеграція cowrie з ELK Stack. Було розроблено та реалізовано механізм передачі логів cowrie у Logstash, їх обробку та індексацію в elasticsearch, а також налаштовано візуалізацію та моніторинг за допомогою Kibana для оперативного відстеження підозрілої активності;

✓ аналіз та інтерпретація результатів. Проведено оцінку ефективності інтегрованої системи у виявленні атак, визначено типи атак, що найбільш часто фіксуються, та сформовано рекомендації щодо поліпшення налаштувань системи;

✓ розробка методичних рекомендацій. На основі отриманих даних створено практичні рекомендації щодо використання cowrie та ELK Stack у корпоративних і хмарних мережах для підвищення рівня кібербезпеки за допомогою технологій обману.

Ці завдання дозволяють системно підійти до дослідження, забезпечити збір та аналіз реальних даних про кібератаки та продемонструвати ефективність інтеграції технологій обману для захисту мережевих інфраструктур.

4. Аналіз літератури

Технології обману в кібербезпеці стали предметом активних наукових досліджень протягом останніх років, демонструючи значний потенціал для виявлення та аналізу кіберзагроз. Сучасні кіберзагрози стають дедалі складнішими, що вимагає проактивних заходів для захисту цифрових активів [13]. У цьому контексті honeypot-системи виступають критичними інструментами для виявлення загроз, їх аналізу та попередження.

Cowrie є середньоінтерактивним honeypot-системою для протоколів SSH та Telnet, призначеною для реєстрації атак грубої сили та взаємодії зловмисників з командною оболонкою. Дослідження 2024 року продемонструвало ефективність Cowrie у виявленні різноманітних типів атак. При розгортанні Cowrie на Raspberry Pi протягом тридцяти днів було зібрано детальні дані про поведінку зловмисників, що виявило переважання атак через SSH над Telnet, часте використання слабких паролів та географічну концентрацію атак з Китаю, Індії та Австралії. Подальший аналіз підтвердив, що Cowrie зареєстрував приблизно сто п'ятдесят тисяч атак з майже тисячі унікальних IP-адрес лише за тиждень роботи [14].

Однак стандартне розгортання Cowrie має суттєві обмеження. Поточною проблемою стандартної конфігурації Cowrie є те, що вона легко виявляється зловмисниками за допомогою автоматизованих скриптів та інструментів [15]. Дослідження виявило, що сімдесят два відсотки honeypot-систем розгорнуті зі стандартними налаштуваннями, що робить їх легко ідентифікованими за допомогою інструментів на кшталт NMAP та Shodan [16]. Це підкреслює необхідність індивідуальної конфігурації для підвищення рівня обману.

Для ефективного аналізу великих обсягів журналів, що генеруються honeypot-системами, дослідники звертаються до платформ управління логами. ELK Stack є популярною платформою аналізу та управління логами з відкритим кодом, яка виконує збір, обробку,

нормалізацію та зберігання даних журналів з різних джерел. Хоча ELK Stack забезпечує потужні можливості централізованого логування, у базовій формі він не є повноцінною системою SIEM, а радше інструментом для тих, хто має персонал, навички та терпіння створити власне рішення [17].

Інтеграція Cowrie з ELK Stack демонструє значний потенціал для автоматизованого аналізу загроз. Інтеграція honeypot та ELK Stack може стати рішенням системи безпеки для виявлення атак з одночасним забезпеченням візуалізації для адміністраторів, при цьому Cowrie забезпечує кращу продуктивність системи виявлення в реальному часі з середньою затримкою три цілих сімдесят п'ять сотих секунди. Elastic SIEM поєднує функції виявлення загроз, механізм автоматичного виявлення якого дозволяє швидко розслідувати загрози та реагувати на них, а також захист кінцевих точок в єдине рішення [18].

Сучасні дослідження також акцентують увагу на використанні штучного інтелекту для підвищення ефективності аналізу. Автоматизований підхід з використанням агентів штучного інтелекту для обробки журналів Cowrie продемонстрував ефективність системи у перетворенні великих обсягів низькорівневих даних журналів у структуровані звіти та зрозумілі візуалізації [19]. Дослідження підкреслює безперебійне включення honeypot-систем у поточні протоколи безпеки, включаючи міжмережеві екрани та стратегії реагування на інциденти, надаючи комплексне розуміння тактик, технік та процедур зловмисників.

Комплексний підхід до технологій обману демонструє перспективні напрямки розвитку. Технології honeypot стають дедалі популярнішими в кібербезпеці, оскільки вони надають цінні дані про поведінку противника з низьким рівнем помилкових спрацьовувань [20]. Подальший розвиток включає впровадження машинного навчання для адаптивного виявлення та створення хмарних honeypot-систем [13], що відкриває нові можливості для захисту мережевої інфраструктури від еволюціонуючих кіберзагроз.

5. Методи досліджень

Методологічна основа даного дослідження ґрунтується на комплексному практичному експерименті, спрямованому на створення інтегрованої системи ідентифікації, збору та систематичного аналізу шкідливої мережевої активності. У роботі застосовано експериментальний підхід із залученням гібридної методології, яка органічно поєднує елементи кількісного та якісного дослідження для забезпечення всебічного аналізу отриманих результатів.

Реалізація експерименту здійснюється поетапно: спочатку в ізольованому контрольованому середовищі з можливістю детального спостереження за процесами, а згодом передбачається масштабування розробленого рішення на автентичне мережеве оточення з реальними загрозами. Ключовою метою обраної методології є практична демонстрація ефективності інтеграції спеціалізованого середовища-пастки (honeypot) з потужною платформою централізованого збирання логів та інтерактивної візуалізації даних безпеки [5]. Така інтеграція дозволяє суттєво підвищити оперативність моніторингу інформаційної безпеки, забезпечити глибший аналіз векторів кібератак, виявити закономірності в діях зловмисників та сформувати проактивну стратегію захисту мережевої інфраструктури від сучасних кіберзагроз.

У сучасному динамічному ландшафті інформаційної безпеки honeypot-системи стали незамінним інструментом для проактивного виявлення, моніторингу та глибокого аналізу кіберзагроз. Cowrie посідає особливе місце серед SSH та Telnet honeypot-рішень завдяки своїй здатності реалістично емулювати вразливі системи, що дозволяє приваблювати кіберзловмисників та детально досліджувати їхні методи роботи [6]. Поєднання Cowrie з потужним ELK Stack формує комплексну аналітичну платформу, здатну збирати величезні обсяги інформації про атаки, ефективно обробляти їх та візуалізувати у зручному форматі в режимі реального часу.

Cowrie функціонує як honeypot середнього рівня взаємодії, майстерно імітуючи поведінку справжніх SSH та Telnet сервісів. Система ретельно фіксує всі спроби несанкціонованого доступу, використані облікові дані, виконані команди в емульованому оточенні, завантажені шкідливі файли та повний ланцюжок дій атакувальників [9]. Така детальна документація надає фахівцям з кібербезпеки унікальну можливість досліджувати тактики, техніки та процедури (TTP) хакерів у контрольованому безпечному середовищі, повністю уникаючи ризиків для критичної продуктивної інфраструктури.

ELK Stack представляє собою інтегрований набір open-source інструментів для централізованого управління логами. Elasticsearch забезпечує масштабоване зберігання та швидкий пошук по структурованих даних, Logstash виконує збір, трансформацію та нормалізацію логів з різних джерел, тоді як Kibana пропонує потужний веб-інтерфейс для створення інтерактивних дашбордів, візуалізації складних даних та проведення детального аналітичного дослідження.

Ключова відмінність технології DT від традиційних honeypot-систем (HP) полягає в принципово іншій архітектурній організації. Якщо класичні honeypot'и функціонували як ізольовані окремі вузли-пастки, то DT представляє собою інтегровану централізовану платформу для керування цілою мережею фіктивних об'єктів. Кожен такий об'єкт-пастка (decoy) залишається автономним honeypot'ом, проте всі вони підключені до єдиного центру управління, що координує їхню роботу та збирає телеметрію [10].

Функціональні можливості систем класу DT значно розширені порівняно з попередниками. Зокрема, такі платформи забезпечують автоматизоване розгортання пасток у мережевому середовищі, централізований збір і консолідацію даних з усіх робочих вузлів, динамічну адаптацію до мережевої топології.

Втім, технологія не позбавлена недоліків. Головною проблемою залишається висока складність і трудомісткість початкового налаштування системи. Для мінімізації цього недоліку можна застосувати кілька контрмір: інтеграцію DT-сервісу з існуючими системами моніторингу та аналізу мережевого трафіку з наступною автоматичною генерацією пасток на основі виявлених закономірностей; проведення активного сканування мережевої інфраструктури для виявлення потенційних точок розміщення decoy-об'єктів; пасивне прослуховування трафіку (за наявності технічної можливості) для виявлення атак. Звичайно, зберігається можливість ручного конфігурування, однак це суттєво знижує ефективність та оперативність розгортання системи.

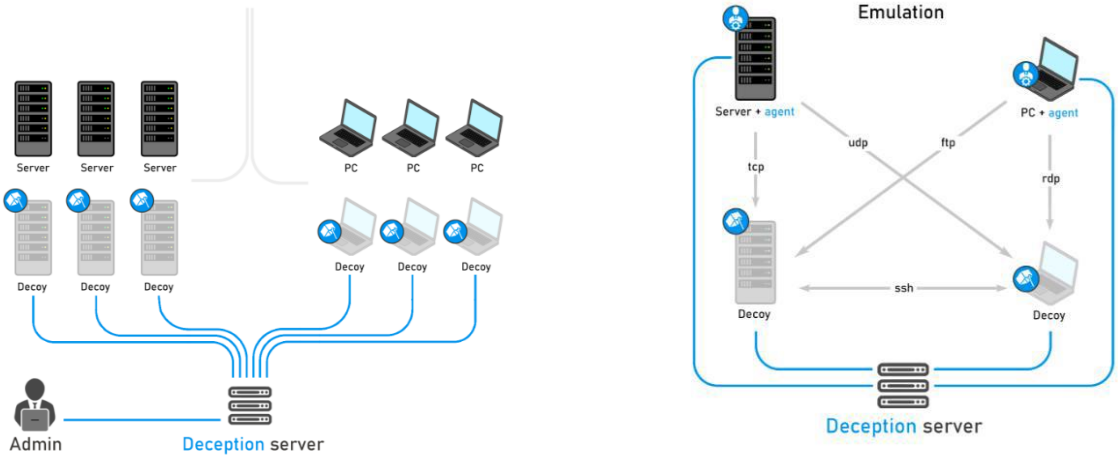


Рис 1. Honeypot-емуляція в архітектурі Deception [4].

Принципова відмінність між традиційними honeypot-системами та десептивними технологіями полягає в їхньому підході до виявлення загроз. Класичні honeypot функціонують як ізольовані елементи інфраструктури, що пасивно очікують на потенційне втручання,

залишаючись відокремленими від решти мережевих компонентів і не генеруючи помітної мережевої активності. Натомість, десептивні технології спроектовані з діаметрально протилежною метою – активно провокувати та залучати зловмисників через створення переконливого мережевого сліду.

Ключовим аспектом ефективності десептивних технологій є стратегічне направлення атакуючого до підготовленої пастки. Це досягається шляхом створення ілюзії справжнього, функціонуючого сервісу в мережевому просторі. Зловмисник повинен отримати непрямі підказки про місцезнаходження цілі, вважаючи її легітимним компонентом інфраструктури. Наприклад, десептивний вузол може бути навмисно сконфігурований як вразливий до методів активного сканування мережі, демонструючи характеристики «живої» системи в загальному трафіку.

Особливо вагомою перевагою десептивних технологій над традиційними honeypot є здатність до динамічної емуляції реалістичної мережевої взаємодії. Така взаємодія може відбуватися між різноманітними вузлами інфраструктури: між десептивними системами та приманками, між моніторинговими агентами та пастками [7]. Конкретна реалізація визначається обраним технологічним рішенням і може варіюватися від простого обміну базовими TCP/UDP пакетами до складної передачі даних із використанням специфічних протоколів прикладного рівня мережевого стеку.

Специфіка імплементації безпосередньо залежить від призначення конкретної пастки. Наприклад, моніторинговий агент можна запрограмувати на періодичне підключення до десептивного SSH-сервера, де він проходитиме повноцінну процедуру автентифікації та навіть виконуватиме типові системні команди, створюючи максимально автентичну картину функціонування реального сервісу.

Критично важливим аспектом функціонування пастки є її здатність реєструвати та відстежувати всі без винятку спроби встановлення з’єднання. Кожна така спроба, незалежно від її природи – справжньої чи симульованої – негайно фіксується системою та передається у вигляді сповіщення на центральний сервер моніторингу. Це означає, що навіть штучно згенеровані підключення тестового характеру викликають відповідну реакцію системи безпеки.

Процес впровадження honeypot-системи cowrie з інтегрованим ELK Stack передбачає послідовне виконання декількох ключових кроків. На початковому етапі здійснюється встановлення програмного забезпечення Cowrie на окремий сервер або віртуальну машину, що спеціально виділена для цієї мети. Критично важливим є використання повністю ізольованого мережевого середовища, оскільки це дозволяє суттєво знизити потенційні загрози для основної корпоративної інфраструктури та запобігти можливому поширенню шкідливого програмного забезпечення. Після завершення первинного конфігурування система cowrie автоматично генерує детальні логи у зручному JSON-форматі, що значно полегшує їх подальшу інтеграцію з компонентом logstash для централізованої обробки даних.

На аналітичному етапі дослідження системи ключову роль відіграє платформа Kibana, яка забезпечує комплексні можливості для створення інтерактивних візуалізацій та інформаційних панелей моніторингу. Кількісний аналіз охоплює декілька важливих напрямків: визначення частотності атакуючих активностей, аналіз їх географічного походження та розподілу, дослідження найпоширеніших паролів, а також систематизацію типів команд, що виконуються зловмисниками. Якісна складова аналізу фокусується на ретельному вивченні поведінкових моделей атакуючих, розрізненні між автоматизованими ботнет-мережами та цілеспрямованими атаками, детальній класифікації виявленого шкідливого програмного забезпечення за типами та характеристиками.

Кінцевим результатом реалізації запропонованої методології стає створення повнофункціональної аналітичної системи, здатної в режимі реального часу здійснювати збір, систематизацію та глибокий аналіз інформації про кіберінциденти та атаки. Така комплексна система забезпечує можливість оперативного виявлення спроб несанкціонованого доступу та

компрометації захищених систем, детального вивчення тактик, технік і процедур зловмисників, а також слугує надійною експериментальною платформою для проведення подальших науково-практичних досліджень у галузі інформаційної безпеки. Таким чином, застосована дослідницька методологія органічно поєднує експериментальне моделювання загроз, систематичне спостереження, збір і обробку статистичних показників, логічний аналіз отриманих даних та їх наочну візуалізацію. Здобуті результати мають значну цінність як для практичного застосування в реальних системах захисту, так і для навчально-дослідницької діяльності, демонструючи високу ефективність технологій обману у комплексних системах кібербезпеки.

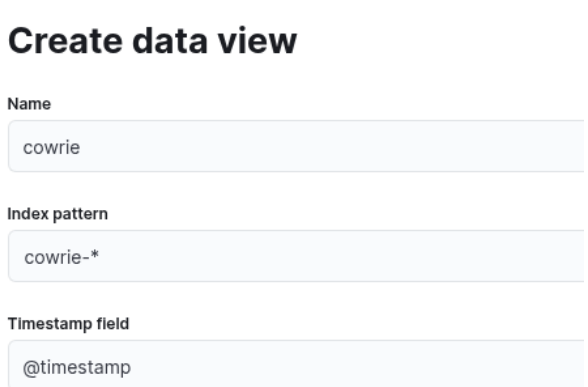
6. Результати досліджень

Для практичної реалізації дослідження було обрано поєднання системи honeypot cowrie та стеку для централізованого аналізу логів ELK. Використання cowrie забезпечує можливість емулювати SSH та Telnet-сесії з метою збору даних про несанкціоновані спроби доступу, команди атакуючих та потенційно шкідливі файли. ELK Stack реалізує багаторівневий підхід до обробки та аналізу інформації: elasticsearch слугує системою індексації та зберігання даних; logstash виконує попередню обробку логів cowrie, забезпечуючи структурування та фільтрацію даних; kibana надає графічний інтерфейс для побудови аналітичних дашбордів та візуалізації тенденцій атак.

На підготовчому етапі здійснюється розгортання лабораторного середовища. Використовується віртуалізована інфраструктура на базі VMware з трьома віртуальними машинами: сервер cowrie (Ubuntu Server 24.04), сервер ELK Stack (мінімум 8GB RAM) та контрольна станція для моніторингу. Встановлення cowrie проводилось на Ubuntu Server 24.04. Виконання процесу включало створення ізольованого віртуального середовища python та інсталяцію необхідних бібліотек.

Cowrie встановлюється у віртуальному середовищі python, конфігурується для емуляції SSH на стандартному порту 22 та Telnet на порту 23. Налаштовується логування у форматі JSON для спрощення подальшої обробки. ELK Stack розгортається відповідно до офіційної документації Elastic. Elasticsearch конфігурується з оптимальними параметрами JVM heap, створюються індекси з відповідним mapping для полів cowrie. Logstash налаштовується з input плагіном для читання логів cowrie, filter секцією для парсингу JSON та збагачення даних через GeoIP плагін, та output для відправки в elasticsearch.

Інтеграція з ELK Stack передбачала елементи налаштуванння для elasticsearch (встановлення та запуск індексуючого сервісу для зберігання структурованих логів); logstash (створення конфігураційного файлу cowrie.conf, який реалізує зчитування та обробку JSON-логів cowrie); kibana (підключення до Elasticsearch та створення індексу cowrie-logs-* з метою побудови аналітичних дашбордів). На рисунку 2 продемонстровано основні елементи налаштуванння складових ELK Stack.




```
# /etc/logstash/conf.d/cowrie.conf
input {
  file {
    path => "/var/log/cowrie/cowrie.json"
    start_position => "beginning"
    sincedb_path => "/dev/null"
    codec => json
  }
}

output {
  elasticsearch {
    hosts => ["http://localhost:9200"]
    index => "cowrie-%{+YYYY.MM.dd}"
  }
  stdout { codec => rubydebug }
}
```

Рис 2. Конфігурація налаштувань збору логів cowrie (авторська розробка).

Експериментальна фаза дослідження охоплює систематичний збір емпіричних даних упродовж періоду в 5-ти днів. Протягом цього часу honeypot-система піддається автентичним кібератакам з глобальної мережі Інтернет, з детальною реєстрацією всіх спроб встановлення з'єднання, застосованих автентифікаційних даних, виконаних зловмисниками команд та завантажених шкідливих файлів. Одночасно здійснюється керований тестувальний процес із застосуванням попередньо визначених сценаріїв атак для валідації точності методів збору та аналітичної обробки інформації. В рамках експериментального дослідження акумулюються метрики щодо загальної кількості спроб несанкціонованого доступу, періодичності повторних атакувальних дій, найпоширеніших комбінацій логінів та паролів, семантичної структури виконуваних команд, а також відсоткового співвідношення автоматизованої бот-активності відносно цілеспрямованих людських атак.

Після збору первинних даних настав етап їх детального аналітичного опрацювання. Застосовуючи потужний інструментарій платформи Kibana, було проведено багатовимірне дослідження зафіксованих кібератак. Аналіз охоплював вивчення динаміки атак у часовому вимірі, що дозволило виявити періоди найвищої активності зловмисників. Окрема увага приділялася географічному картуванню джерел атак для визначення регіональних особливостей кіберзагроз. Досліджувалися повторювані шаблони поведінки атакувальників, типологія використовуваних команд, а також природа й призначення завантажуваних шкідливих файлів. На рисунках 3 та 4 відображено виявлення аномального трафіку за допомогою інтеграції cowrie та ELK Stack.

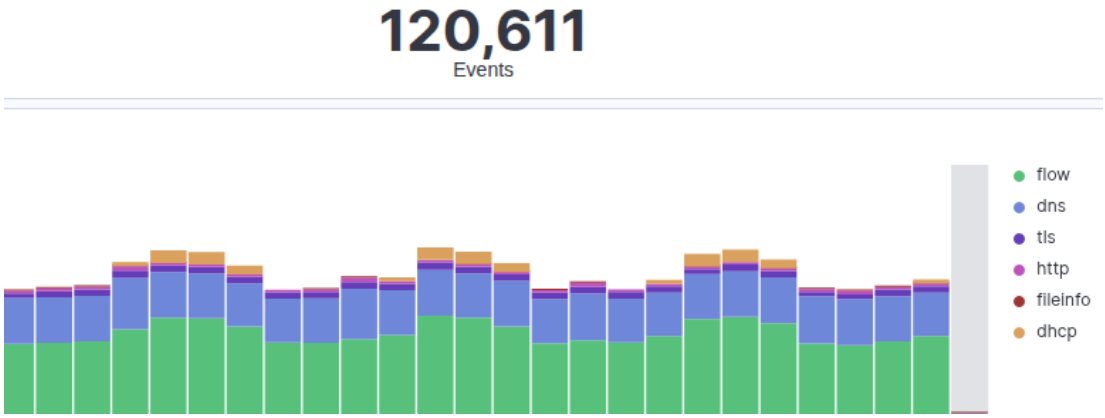


Рис 3. Результат Kibana з виявлення аномального трафіку (авторська розробка).

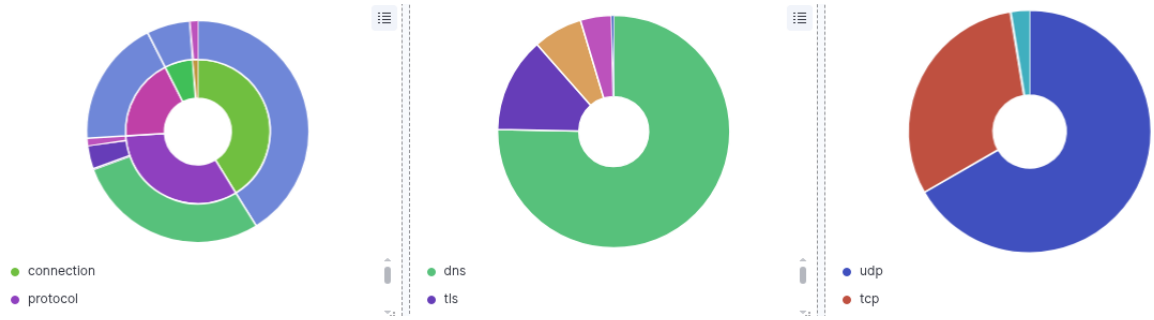


Рис 4. Журнал транспортних та мережевих протоколів (авторська розробка).

Фінальна фаза методології зосереджується на комплексній оцінці ефективності створеної інтеграції. Здійснюється порівняльний аналіз показників детектування інцидентів безпеки до впровадження ELK Stack та після нього. Оцінюються критичні параметри: оперативність реагування фахівців з безпеки, якість і наочність візуального представлення даних, можливості горизонтального масштабування архітектури системи. На основі отриманих результатів формулюється аргументований висновок щодо практичної доцільності та

перспектив використання зв'язки cowrie + ELK як повноцінного компонента корпоративної системи кіберзахисту або як спеціалізованого навчального середовища для підготовки аналітиків інформаційної безпеки. Такий комплексний підхід до аналізу дав змогу сформулювати обґрунтовані висновки стосовно найпоширеніших сценаріїв кібератак, виокремити характерні поведінкові патерни зловмисників та об'єктивно оцінити результативність інтегрованої системи honeypot із засобами моніторингу.

7. Висновки

У ході проведеного дослідження було розглянуто інтеграцію системи honeypot Cowrie із ELK Stack (Elasticsearch, Logstash, Kibana) для забезпечення ефективного моніторингу та аналізу мережевого трафіку з метою виявлення потенційних кібератак. Практична реалізація даного підходу підтвердила, що поєднання спеціалізованого honeypot із потужними інструментами збору, обробки та візуалізації даних дозволяє підвищити рівень розпізнавання атак та скоротити час реагування на інциденти.

Ключовою перевагою реалізованої інтеграції є можливість автоматизованого збору, структурування та візуалізації великих обсягів даних про спроби несанкціонованого доступу. Cowrie, функціонуючи як high-interaction honeypot, забезпечує реалістичне середовище для імітації вразливих SSH та Telnet сервісів, що дозволяє залучати атакувальників та фіксувати їхні дії з високою деталізацією. Кожна спроба аутентифікації, виконана команда, завантажений файл або встановлене з'єднання ретельно документуються у форматі JSON, що оптимізує подальшу обробку. Cowrie, як програмний SSH і Telnet honeypot, забезпечує можливість детального збору інформації про дії зловмисників, включаючи команди, використані для спроб проникнення, а також логіни та паролі, що застосовуються під час атак. Завдяки своїй здатності емулювати реальні серверні сервіси, Cowrie дозволяє створювати «пасивну пастку», яка не лише фіксує спроби компрометації, а й генерує багаті дані для подальшого аналізу.

ELK Stack у цьому контексті виступає як інструмент централізованого збору та обробки логів, що забезпечує можливість їх структурованого зберігання, пошуку та візуалізації. Використання logstash для інтеграції логів cowrie, elasticsearch для їх індексації та kibana для побудови графіків та панелей моніторингу дозволяє фахівцям із безпеки швидко ідентифікувати аномалії в трафіку, оцінювати частоту та типи атак, а також відстежувати поведінку потенційних зловмисників у реальному часі.

Практичне впровадження інтегрованої системи продемонструвало низку ключових переваг. По-перше, система забезпечує гнучкий підхід до аналізу загроз: можна налаштовувати фільтри, оповіщення та дашборди під специфічні сценарії атак. По-друге, отримані дані дозволяють формувати аналітичні звіти для стратегічного планування безпеки та виявлення повторюваних схем атак. По-третє, інтеграція cowrie та ELK Stack знижує навантаження на традиційні системи захисту, оскільки частина роботи з раннього виявлення загроз переноситься на автономний honeypot.

У процесі дослідження також було відзначено деякі обмеження та виклики. Зокрема, велика кількість генерованих логів потребує належної оптимізації зберігання та обробки даних, а також правильної конфігурації системи сповіщень, щоб уникнути «шуму» та хибнопозитивних сповіщень. Крім того, важливо забезпечити ізоляцію honeypot від реальної мережі для запобігання потенційному використанню його як плацдарму для подальших атак.

Отже, інтеграція cowrie та ELK Stack є ефективним інструментом для покращення кіберзахисту мережевої інфраструктури. Вона дозволяє не лише виявляти спроби несанкціонованого доступу та аналізувати тактики зловмисників, а й формувати структуровану базу знань для подальшого вдосконалення захисних механізмів. Результати дослідження підтверджують доцільність використання такої інтеграції як складової комплексної стратегії інформаційної безпеки та відкривають перспективи для подальших

досліджень у сфері автоматизованого моніторингу мережевого трафіку та протидії кіберзагрозам.

Список літератури:

1) Sverstyuk A.S., Andrushchak I.Ye. (2025). Features of modern use and application of aspects of Blockchain technology / Scientific publication «Expert opinion» Issue: 1. 2025. pp. 97-102. ISBN – 979-8-89965-344-5. / URL: https://www.expert-opinion.pp.ua

2) Tymoshchuk, D. & Yatskiv, V. (2024). Interactive cybersecurity training system based on simulation environments. Measuring and computing devices in technological processes, (4), 215–220. https://doi.org/10.31891/2219-9365-2024-80-26

3) Андрущак, І., Кошелюк, В., & Ясашний, Д. (2025). Підвищення безпеки контейнерів за допомогою розгортання honeypot. International Science Journal of Engineering & Agriculture, 4(3), 15–26. https://doi.org/10.46299/j.isjea.20250403.02

4) Бабич С.В. (2022). Визначення технології обману. Формування моделі Deception. Збірник матеріалів проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно-інтегровані технології» (АКІТ - 2022), Тернопіль, 2022. – с. 115-117

5) Kosheliuk, V., & Tulashvili, Y. (2024). Implementing honeypots for detecting cyber threats with AWS using the ELK. International Journal of Computing, 23(4), 618-624. https://doi.org/10.47839/ijc.23.4.3761

6) Cabral, W.Z., Valli, C., Sikos, L.F., Wakeling, S.G. (2021). Advanced Cowrie Configuration to Increase Honeypot Deceptiveness. In: Jøsang, A., Futcher, L., Hagen, J. (eds) ICT Systems Security and Privacy Protection. SEC 2021. IFIP Advances in Information and Communication Technology, vol 625. Springer, Cham. https://doi.org/10.1007/978-3-030-78120-0_21

7) Andrushchak I. (2024). Aspects of blockchain technology as a component of information security. Technical, agricultural and physical sciences as the main sciences of human development: collective monograph / International Science Group. – Boston : Primedia eLaunch, 2024. 172-182 p. https://doi.org/10.46299/ ISG.2024.MONO.TECH.1

8) P. Krajčík, M. Mikuláš, P. Helebrandt and I. Kotuliak. (2025). Improvement of Cowrie honeypot interaction and deception capabilities. Communication and Information Technologies (KIT), Vysoke Tatry, Slovakia, 2025, pp. 1-9, https://doi.org/10.1109/KIT67756.2025.11205433

9) M. N. Azzahri et al. (2024). The Application of Cowrie Honeypot to Analyze Attacks on SSH and Telnet Protocols. IEEE 2nd International Conference on Electrical Engineering, Computer and Information Technology (ICEECIT), Jember, Indonesia, 2024, pp. 290-295, https://doi.org/10.1109/ICEECIT63698.2024.10859786.

10) Morić, Z., Dakić, V., & Regvart, D. (2025). Advancing Cybersecurity with Honeypots and Deception Strategies. Informatics, 12(1), 14. https://doi.org/10.3390/informatics12010014

11) Mukti, Fransiska Sisilia & Sukmawan, R. (2021). Integration of Low Interaction Honeypot and ELK Stack as Attack Detection Systems on Servers. Jurnal Penelitian Pos dan Informatika. 11. https://doi.org/10.17933/jppi.v11i1.336.

12) Visalom, R.-M., Mihăilescu, M.-E., Rughiniș, R., & Țurcanu, D. (2025). Intercepting and Monitoring Potentially Malicious Payloads with Web Honeypots. Future Internet, 17(9), 422. https://doi.org/10.3390/fi17090422

13) Morić, Z., Dakić, V., & Regvart, D. (2025). Advancing Cybersecurity with Honeypots and Deception Strategies. Informatics, 12(1), 14. https://doi.org/10.3390/informatics12010014

14) Azzahri, Muhammad & Selian, Restu & Muchallil, Sayed & Nurdin, Yudha & Afidh, Razief & Umam, Khairul & Dawood, Rahmad. (2024). The Application of Cowrie Honeypot to Analyze Attacks on SSH and Telnet Protocols. 290-295. 10.1109/ICEECIT63698.2024.10859786.

15) W. Cabral, C. Valli, L. Sikos and S. Wakeling, "Review and Analysis of Cowrie Artefacts and Their Potential to be Used Deceptively," 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2019, pp. 166-171, doi: 10.1109/CSCI49370.2019.00035.

16) Cabral, W.Z., Valli, C., Sikos, L.F., Wakeling, S.G. (2021). Advanced Cowrie Configuration to Increase Honeypot Deceptiveness. In: Jøsang, A., Futcher, L., Hagen, J. (eds) ICT Systems Security and Privacy Protection. SEC 2021. IFIP Advances in Information and Communication Technology, vol 625. Springer, Cham. https://doi.org/10.1007/978-3-030-78120-0_21

17) Elliot Anderson. (2023). Is the ELK Stack a SIEM? URL: https://www.lumificyber.com/blog/is-the-elk-stack-a-siem/

18) Hassen Hannachi. (2024). Elastic — Elastic SIEM Fundamentals. URL: https://hassen-hannachi.medium.com/elastic-elastic-siem-fundamentals-3337d580fafe

19) Karaarslan, E., Güler, E., Yüce, E.E., & Coban, C. (2025). Towards Log Analysis with AI Agents: Cowrie Case Study. ArXiv, abs/2509.05306.

20) Amir Javadpour, Forough Ja'fari, Tarik Taleb, Mohammad Shojafar, Chafika Benzaïd. (2024) A comprehensive survey on cyber deception techniques to improve honeypot performance. Computers & Security, Volume 140, 2024, 103792, https://doi.org/10.1016/j.cose.2024.103792.

Cybersecurity deception technologies: integrating cowrie and ELK Stack to detect network attacks

Igor Andrushchak
Department of Software Engineering, Lutsk National Technical University, Lutsk, Ukraine
ORCID 0000-0002-8751-4420

Viktor Kosheliuk
Department of Computer Science, Lutsk National Technical University, Lutsk, Ukraine
ORCID 0000-0002-4136-5087

Ilya Veremiy
Department of Computer Science, Lutsk National Technical University, Lutsk, Ukraine
ORCID 0009-0003-1381-9920

Abstract: The article examines deception technologies in the field of cybersecurity to enhance the effectiveness of detecting attacks on network traffic. The primary objective of this work is to conduct a practical study on integrating the cowrie system, which emulates SSH and Telnet servers, with the ELK Stack platform (Elasticsearch, Logstash, Kibana) for collecting, processing, and visualizing data related to suspicious activity. The research aims to develop a method for configuring a honeypot system and integrating it into a centralized analytical system, enabling a timely response to potential threats.The research methods include the analysis of modern deception technologies and their comparison, the configuration and optimization of cowrie for collecting logs about network attacks, as well as the integration of the obtained data into the ELK Stack. To assess the effectiveness of the system, an experimental approach was employed, focusing on the types of attacks, sources of intrusions, and the behavior of attackers within the network. Data visualization in Kibana allowed for a detailed analysis of activity and the generation of operational reports on security incidents. The study's results showed that the integrated system of cowrie and ELK Stack effectively captures and classifies unauthorized access attempts, password attacks, and other typical network threats. It was found that combining trap emulation with centralized data analysis enables an increase in the speed

of attack detection and enhances the understanding of attacker behavior. Configuring logging and data correlation provides a flexible approach to monitoring and security analytics.The scientific novelty of the study lies in the development of an integrated approach to applying deception technologies in cybersecurity, utilizing the honeypot cowrie and the ELK Stack data analysis platform for the detection, monitoring, and analysis of attacks on network traffic. A method for the automated collection and correlation of data on unauthorized actions is proposed, which enables an increase in the accuracy of detection and the speed of response to threats. The study demonstrates the effectiveness of integrating emulated traps with a visualization and analytics system, providing a deeper understanding of attacker behavior and the ability to predict potential scenarios of intrusions into the network infrastructure.The findings highlight that deception technologies are an effective tool for counteracting cyber threats, and their integration with analytics platforms, such as ELK Stack, significantly enhances organizations' ability to respond to incidents. Recommendations include implementing such systems in corporate and cloud environments, regularly updating honeypot configurations, and improving data visualization and analysis methods. Future directions involve automating incident response based on collected data, integrating with SIEM systems, and using machine learning to predict and prevent new types of attacks.

Keywords: cowrie, deception technologies, honeypot, ELK Stack, cyber threats.