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: “СИСТЕМА КООРДИНАЦІЇ ВЗАЄМОДІЇ КОМАНД RED TEAM ТА SOC У МЕЖАХ СЕРВІСНОЇ МОДЕЛІ PURPLE TEAMING”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Ілля РАДЧЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Ілля Радченко
Ім’я, ПРІЗВИЩЕ

Керівник: Дмитро РАБЧУН
к.т.н., професор Ім’я, ПРІЗВИЩЕ

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Радченку Іллі Олександровичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “ Система координації взаємодії команд Red Team та SOC у межах сервісної моделі Purple Teaming ”,
керівник кваліфікаційної роботи Рабчун Дмитро к.т.н., професор,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51

2. Строк подання кваліфікаційної роботи “12” травня 2026р.

3. Вихідні дані до кваліфікаційної роботи*: міжнародні стандарти, MITRE ATT&CK, SOC-CMM, література з SOC, Red Team, Purple Teaming та відкриті джерела з координації команд, бар'єрів та сервісних моделей.*

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати функціональні ролі Red Team та SOC, визначити типові проблеми їх ізольованої роботи
4.2. Дослідити основні бар'єри координації (організаційні, технологічні, метричні) між Red Team та SOC.
4.3. Розробити систему координації на основі сервісної моделі Purple Teaming, включаючи життєвий цикл взаємодії, ролі та узгоджені показники ефективності, надати практичні рекомендації.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “05“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	30.03.2026	
3.	Аналіз особливостей управління інформаційною безпекою підприємства	08.04.2026	
4.	Дослідити основні характеристики сервісної моделі Purple Teaming як теоретичної основи координації Red Team та SOC.	15.04.2026	
5.	Проаналізувати основні проблеми координації Red Team та SOC, включаючи організаційні, технологічні та метричні бар'єри, а також типові розриви взаємодії.	22.04.2026	
6.	Сформулювати висновки за результатами розроблення системи координації Red Team та SOC на основі сервісної моделі Purple Teaming	29.04.2026	
7.	Оформлення роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	10.06.2026	
10.	Захист в ЕК.	12.06.2026	

Здобувач вищої освіти _____ Ілля РАДЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Дмитро Рабчун
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Радченко І.О до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Вплив штучного інтелекту на кібербезпеку: сучасні загрози та захисні технології"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач Радченко Ілля у кваліфікаційній роботі на тему " Система координації взаємодії команд Red Team та SOC у межах сервісної моделі Purple Teaming" дослідив основи Red Team та SOC, проаналізував бар'єри координації та розробив систему на основі Purple Teaming.

Радченко Ілля продемонстрував розуміння актуальності обраної проблематики, уміння опрацьовувати наукові, нормативні та практичні напрями. Під час виконання кваліфікаційної роботи здобувач проявив себе відповідально та організовано, здатен самостійно працювати з матеріалами дослідження і формулювати обґрунтовані висновки.

Все це дозволяє оцінити кваліфікаційну роботу здобувача РАДЧЕНКО Ілля на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Радченко І.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 РАДЧЕНКА Іллі
на тему “Система координації взаємодії команд Red Team та SOC у межах сервісної моделі Purple Teaming
”

Актуальність. Зростання кількості та складності кібератак вимагає ефективної взаємодії між Red Team та SOC. Традиційна ізольована робота цих команд знижує виявлення загроз, тому розроблення системи координації на основі сервісної моделі Purple Teaming є актуальним завданням.

З огляду на зазначене дослідження системи координації взаємодії команд Red Team та SOC у межах сервісної моделі Purple Teaming є актуальним науково-прикладним завданням.

Позитивні сторони.

1. Проаналізовані ролі Red Team та SOC, виявлено бар’єри координації та досліджено Purple Teaming як підхід до їх подолання.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.
3. За результатами дослідження запропоновано практичні рекомендації щодо впровадження системи координації Red Team та SOC, включаючи життєвий цикл взаємодії, розподіл ролей та узгоджену систему метрик.
4. За результатами дослідження запропоновано практичні рекомендації щодо впровадження системи координації, включаючи життєвий цикл взаємодії

Недоліки.

У роботі недостатньо розкрито питання автоматизації процесів Purple Teaming та оцінки витрат на впровадження запропонованої системи для підприємств різного масштабу.

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

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки "відмінно", а здобувач РАДЧЕНКО Ілля заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:

_____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню системи координації взаємодії команд Red Team та SOC у межах сервісної моделі Purple Teaming. Робота складається зі вступу, трьох розділів, що містять 9 рисунків, висновків і списку використаних джерел із 41 найменування. Загальний обсяг роботи становить 67 аркушів, з яких 4 аркуші займають перелік умовних скорочень і список використаних джерел.

Метою роботи є розробка та обґрунтування моделі координації Red Team та SOC на основі сервісного підходу Purple Teaming.

Об'єктом дослідження є процеси виявлення, тестування та реагування на кіберзагрози в системі управління інформаційною безпекою підприємства.

Предмет дослідження – методи, ролі, показники ефективності та технологічні механізми координації команд Red Team і SOC через впровадження моделі Purple Teaming.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, системного аналізу, моделювання бізнес-процесів, експертної оцінки.

Як результат у роботі проаналізовано функціональні ролі Red Team та SOC, визначено основні бар'єри їх координації, досліджено сервісну модель Purple Teaming, розроблено систему узгоджених метрик та життєвий цикл координації, надано практичні рекомендації щодо впровадження.

Галузь застосування. Розроблені підходи можуть бути використані при побудові або вдосконаленні центрів кібербезпеки (SOC), проведенні Purple Team вправ на підприємствах різних галузей, а також у навчальних цілях при підготовці фахівців з кібербезпеки.

Ключові слова: RED TEAM, SOC, PURPLE TEAMING, КООРДИНАЦІЯ

ВЗАЄМОДІЇ, СЕРВІСНА МОДЕЛЬ, КІБЕРБЕЗПЕКА ПІДПРИЄМСТВА, МЕТРИКИ ЕФЕКТИВНОСТІ

ABSTRACT

The qualification work is devoted to the development of a coordination system for Red Team and SOC interaction within the Purple Teaming service model. The work consists of an introduction, three chapters containing 9 figures, conclusions and a list of references containing 41 items. The total volume of the work is 67 pages, of which 4 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to develop and substantiate a model for coordinating Red Team and SOC based on the Purple Teaming service approach.

The object of the study is the processes of detection, testing and response to cyber threats in the enterprise information security management system.

The subject of the study is the methods, roles, performance indicators and technological mechanisms for coordinating Red Team and SOC through the implementation of the Purple Teaming model.

Research methods. To solve the mentioned scientific task, the methods of analysis and synthesis, comparison, classification, system analysis, business process modeling, and expert assessment were used in the work.

As a result, the functional roles of the Red Team and SOC are analyzed, the main barriers to their coordination are identified, the Purple Teaming service model is investigated, a system of coordinated metrics and a coordination life cycle are developed, and practical recommendations for implementation are provided.

Field of application. The developed approaches can be used in the construction or improvement of security operation centers (SOC), conducting Purple Team exercises at enterprises in various industries, as well as for educational purposes in the training of cybersecurity professionals.

Keywords: RED TEAM, SOC, PURPLE TEAMING, COORDINATION, SERVICE MODEL, ENTERPRISE CYBERSECURITY, PERFORMANCE METRICS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

C2	Command and Control (командно-контрольний сервер/фреймворк)
EDR	Endpoint Detection and Response
KPI	Key Performance Indicators
NIST	National Institute of Standards and Technology
Red Team	Команда «червоних» (емуляція реального супротивника, напад)
SIEM	Security Information and Event Management (управління інформацією та подіями безпеки)
SOC	Security Operations Center (центр моніторингу та реагування на інциденти)
TTPs	Tactics, Techniques, and Procedures (тактики, техніки та процедури)

ВСТУП

Актуальність теми. У сучасних умовах зростання кількості та складності кібератак, підприємства інвестують значні ресурси у створення центрів моніторингу та реагування на інциденти (SOC), а також у проведення незалежних тестів на проникнення силами Red Team. Однак на практиці діяльність Red Team та SOC часто здійснюється ізольовано: Red Team зосереджується на пошуку вразливостей і емуляції атак, а SOC – на моніторингу та реагуванні. Такий підхід призводить до низької ефективності виявлення реальних загроз, дублювання функцій та відсутності спільної мови між командами.

Світові стандарти (NIST SP 800-61, MITRE ATT&CK, SOC-CMM) та передова практика пропонують модель Purple Teaming – сервісну модель координації, у межах якої Red Team та SOC працюють разом: Red Team генерує контрольовані атаки, а SOC перевіряє та вдосконалює свої детекти, правила кореляції та процедури реагування. Однак на сьогодні бракує системного підходу до координації взаємодії команд Red Team та SOC у межах саме сервісної (процесно-орієнтованої) моделі Purple Teaming.

З огляду на зазначене дослідження системи координації взаємодії команд Red Team та SOC у межах сервісної моделі Purple Teaming є актуальним науково-прикладним завданням.

Мета роботи полягає у розробці та обґрунтуванні моделі координації Red Team та SOC на основі сервісного підходу Purple Teaming.

Об'єкт дослідження – процеси виявлення, тестування та реагування на кіберзагрози в системі управління інформаційною безпекою підприємства.

Предмет дослідження – методи, ролі, показники ефективності та технологічні механізми координації команд Red Team і SOC через впровадження моделі Purple Teaming.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. Проаналізувати функціональні ролі Red Team та SOC, визначити типові проблеми їх ізольованої роботи.

2. Дослідити основні бар’єри координації (організаційні, технологічні, метричні) між Red Team та SOC.

3. Розробити систему координації на основі сервісної моделі Purple Teaming, включаючи життєвий цикл взаємодії, ролі та узгоджені показники ефективності, надати практичні рекомендації.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, системного аналізу, моделювання бізнес-процесів, експертної оцінки.

Практичне значення одержаних результатів. Застосування розроблених підходів дасть змогу підприємствам підвищити ефективність виявлення кібератак (зменшити час виявлення та реагування), знизити кількість помилкових спрацьовувань, забезпечити системний зворотний зв’язок між тестуванням та реальним моніторингом.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ ФУНКЦІОНУВАННЯ RED TEAM ТА SOC

1.1 Призначення, функції та місце SOC в системі кібербезпеки підприємства

Центр моніторингу та реагування на інциденти кібербезпеки, більш відомий як SOC (Security Operations Center), є важливим елементом сучасної інфраструктури забезпечення інформаційної безпеки будь-якого сучасного підприємства.

В умовах постійного зростання кількості та складності кібератак, а також у зв’язку з посиленням регуляторних вимог до захисту даних, наявність ефективного SOC перестала бути розкішшю, доступною лише найбільшим корпораціям, і перетворилася на критично необхідний компонент для організацій різного масштабу. Розуміння призначення, ключових функцій та місця SOC у загальній системі кібербезпеки підприємства є необхідною передумовою для подальшого аналізу його взаємодії з іншими командами, зокрема з Red Teams, у рамках сервісної моделі Purple Teaming.

Фундаментальне призначення Security Operations Center (SOC) полягає у централізації та систематизації діяльності з кібербезпеки організації. За визначенням, SOC – це централізована команда та технологічне середовище, які цілодобово здійснюють моніторинг, виявлення, розслідування та реагування на кіберзагрози.

Мета SOC – захищати та контролювати системи та мережі організації на постійній основі, а також своєчасно виявляти, аналізувати та реагувати на інциденти кібербезпеки. Місія SOC полягає у захисті компанії від порушень безпеки шляхом виявлення, аналізу та реагування на загрози. Іншими словами, SOC діє як «нервовий центр» всієї діяльності з кібербезпеки, командний пункт, звідки ведеться безперервне спостереження за цифровим периметром організації.

Саме тут сходяться всі потоки подій безпеки з різноманітних джерел – від мережевих екранів та систем виявлення вторгнень до логів серверів і робочих станцій – для подальшої обробки, кореляції та прийняття рішень.

SOC вирішує ширше коло завдань, ніж просто реагування на інциденти, він відповідає за реалізацію функцій, визначених у таких галузевих стандартах, як NIST Cybersecurity Framework, а саме «Виявлення» (Detect), «Реагування» (Respond) та «Відновлення» (Recover). Ці функції тісно пов’язані з безперервним робочим циклом SOC, який включає збір даних з усіх можливих джерел, нормалізацію та збагачення цієї інформації, кореляцію подій для виявлення аномалій, розслідування підозрілої активності та, зрештою, реагування на підтверджені інциденти

Результатом ефективної роботи SOC є обмеження часу доступу зловмисника до цінних систем і даних, а також мінімізація потенційних збитків від реалізованої кібератаки. SOC об’єднує дані з усіх систем безпеки, корелює події, автоматично блокує загрози й надає керівництву повну картину стану кібербезпеки в компанії. Таким чином, SOC виступає не лише як реактивний захисний механізм, але й як стратегічний інструмент, що дозволяє оцінювати ефективність існуючих засобів захисту та визначати напрямки для їх вдосконалення.

Досягнення цієї стратегічної мети стає можливим завдяки реалізації SOC низки ключових функцій, які можна розділити на кілька основних категорій:

1. Безперервний моніторинг та виявлення загроз.

Це основна, найбільш очевидна функція SOC. Аналітики та автоматизовані системи постійно (24x7x365) аналізують потоки подій безпеки з метою виявлення ознак компрометації (IoC) та аномальної поведінки, яка може свідчити про кібератаку. Ефективність цієї функції вимірюється такими показниками, як середній час виявлення інциденту (Mean Time to Detect, MTTD). Чим нижчий MTTD, тим швидше організація дізнається про атаку та може розпочати реагування.

Реагування на інциденти. Це критично важлива функція, що передбачає

координацію дій для стримування, ліквідації наслідків та відновлення порушених сервісів після підтвердження факту атаки. SOC не тільки виявляє інцидент, але й керує процесом його розслідування та усунення. Ключовим показником тут є середній час реагування на інцидент (Mean Time to Respond, MTTR), який вимірює швидкість, з якою команда безпеки переходить від виявлення події до її локалізації або повного вирішення. Оптимальне значення MTTR для більшості типів сповіщень зазвичай становить від двох до чотирьох годин.

2. Проактивний пошук загроз (Threat Hunting). Це більш зріла функція, яка виходить за рамки простого очікування спрацювання сигналізації. Аналітики SOC, здебільшого найвищої кваліфікації, активно «полюють» на приховані загрози, які могли оминути автоматизовані системи виявлення. Це передбачає аналіз великих масивів даних, пошук аномалій та перевірку гіпотез про можливе зловмисне втручання. Threat Hunting дозволяє виявляти складні та цілеспрямовані атаки, які не генерують явних сигнатурних сповіщень.

3. Керування вразливостями та тестування захисту.

Хоча часто це є функцією окремого підрозділу, у багатьох організаціях SOC також відіграє ключову роль у процесі керування вразливостями. Це включає аналіз результатів сканування на вразливості, проведення внутрішніх тестів на проникнення та, особливо важливо в контексті цієї роботи, участь у Purple Teaming вправах для оцінки ефективності власних детектів і процедур реагування.

4. Збір та аналіз розвідданих про загрози (Threat Intelligence).

Ефективний SOC не може існувати у вакуумі. Він постійно споживає та аналізує зовнішні потоки розвідданих про загрози (Threat Intelligence). Це дозволяє команді бути в курсі останніх тактик, технік та процедур (TTPs) зловмисників, адаптувати свої правила виявлення та проактивно шукати в інфраструктурі індикатори, пов’язані з новими загрозами. Фактично, ця функція перетворює SOC з реактивного підрозділу на проактивний.

5. Надання звітності та аналітика**.** SOC є джерелом ключової інформації про стан кібербезпеки для керівництва компанії та вищих посадових осіб, відповідальних за безпеку (CISO). Він готує регулярні звіти про виявлені інциденти, час їх виявлення та реагування, тренди атак, ефективність існуючих засобів захисту та рекомендації щодо їх посилення. Ці дані є основою для прийняття стратегічних рішень щодо інвестування в кібербезпеку.

Для ефективної реалізації цих функцій SOC структурується таким чином, щоб забезпечити як швидкість обробки рутинних сповіщень, так і глибину аналізу складних загроз. У переважній більшості випадків цього досягають за допомогою так званої трирівневої моделі, яка була запозичена з IT-сервісного менеджменту та адаптована для потреб безпеки. Ця модель базується на ескалації завдань між аналітиками різного рівня кваліфікації, і поділяє функції SOC таким чином:

Рівень 1 (Tier 1): Аналітики первинної обробки**.** Це початкова лінія захисту. Співробітники першого рівня виконують функцію «сортувальників» (triage analysts). Вони отримують потік сповіщень від SIEM та інших систем безпеки, проводять їхню первинну перевірку, відсіюють помилкові спрацьовування (false positives) та виконують базове збагачення даних. Якщо сповіщення визнається потенційно серйозним, воно ескалується на рівень 2. Основне завдання Tier 1 – швидко обробити великий обсяг подій і не пропустити критичну загрозу. Оскільки на цьому рівні зосереджено найбільший обсяг роботи, але з найнижчою складністю, тут існує ризик «втоми від сповіщень» (alert fatigue), що може призвести до пропуску реальної атаки.

Рівень 2 (Tier 2): Аналітики розслідування інцидентів**.** Сюди потрапляють сповіщення, які пройшли первинну перевірку і потребують більш глибокого аналізу. Співробітники цього рівня проводять детальне розслідування, вивчають контекст подій, аналізують задіяні системи та дані, та підтверджують або спростовують факт інциденту. Вони використовують розширений набір інструментів для форензики та розслідувань. У разі підтвердження інциденту,

Tier 2 аналітики керують процесом реагування. Вони також часто виконують менторську роль для молодших колег.

Рівень 3 (Tier 3): Старші аналітики та мисливці за загрозами**.** Це найбільш досвідчені та висококваліфіковані фахівці в команді SOC. Вони беруть на себе найскладніші та найкритичніші інциденти, які не змогли вирішити на нижчих рівнях. Їхні функції, окрім вирішення ескальованих інцидентів, включають проактивний пошук прихованих загроз (threat hunting), розробку та вдосконалення правил виявлення, налаштування SIEM-платформ, а також аналіз зовнішніх розвідданих та інтеграцію їх у процеси моніторингу.

Аналітики Tier 3 часто тісно співпрацюють з іншими командами, зокрема з Red Teams, у рамках Purple Teaming вправ. Керівник SOC, за класифікацією Check Point, іноді розглядається як четвертий рівень (Tier 4), оскільки він несе загальну відповідальність за роботу центру та стратегічне узгодження з цілями бізнесу.

Звісно, ефективність SOC значною мірою залежить від обсягу та якості даних, які він отримує. Невипадково SANS Institute в рамках своїх щорічних досліджень неодноразово наголошував на ключових проблемах, з якими стикаються сучасні SOC. Зокрема, згідно з даними щорічного опитування SOC, проведеного SANS Institute у 2025 році, 85% SOC використовують сповіщення з кінцевих точок (endpoint alerts) як основний тригер для запуску процесу реагування на інциденти, що свідчить про переважно реактивну модель роботи.

Крім того, 42% SOC зізнаються, що просто «складають усі вхідні дані у сховища», фактично не отримуючи з них корисної аналітики. Ці дані свідчать про те, що багато організацій все ще перебувають на початкових етапах побудови зрілої практики безпеки, де SOC виконує переважно функцію управління подіями та сповіщеннями. Однак очевидно, що для того, щоб протистояти сучасним загрозам, SOC необхідно рухатися в бік більш проактивної моделі, де ключову роль відіграють функції threat hunting, тісна інтеграція з Threat Intelligence та, власне, взаємодія з Red Teams у форматі Purple Teaming. Стандарт ISO/IEC 27001 та інші міжнародні нормативні

документи також наголошують на необхідності постійного моніторингу та аналізу подій безпеки, що є прямим обґрунтуванням необхідності створення та розвитку SOC.

Оскільки SOC вимагає значних інвестицій в обладнання, програмне забезпечення та, що найважливіше, у висококваліфікований персонал, існує кілька організаційних моделей його впровадження. Вибір конкретної моделі залежить від розміру компанії, її бюджету, рівня зрілості у сфері безпеки та бізнес-вимог. Типові моделі розгортання SOC та їх особливості наведено на рисунку 1.1.

Модель SOC	Опис	Переваги	Недоліки
Власний In-house SOC	Фізичний центр, повністю побудований всередині організації, з власною інфраструктурою та персоналом.	Повний контроль над процесами, даними та технологіями; глибоке розуміння бізнес-контексту; високий рівень кастомізації.	Високі капітальні та операційні витрати; складність найму та утримання персоналу; довгий час побудови (Time-to-Value).
Аутсорсинговий SOC / MSSP	Організація передає функції моніторингу та реагування сторонньому постачальнику (Managed Security Service Provider).	Нижчі початкові витрати; швидкий старт; доступ до досвідчених команд та передових технологій без необхідності купувати.	Менший контроль над даними та процесами; потенційні ризики конфіденційності; залежність від постачальника (vendor lock-in).
Гібридний SOC	Комбінація власного SOC та послуг MSSP. Частина функцій виконується внутрішньою командою, частина – на аутсорсингу (наприклад, цілодобовий моніторинг).	Баланс між контролем та економічністю; гнучкість у розподілі ресурсів; можливість масштабування.	Складність координації між внутрішньою командою та постачальником; потенційне дублювання функцій.

Рис 1.1. Класифікація моделей розгортання SOC

Важливим нюансом, який часто викликає плутанину, є чітке розмежування між SOC (Security Operations Center) та NOC (Network Operations Center). Незважаючи на те, що ці два центри часто співіснують в одній організації, їхні цілі та завдання суттєво відрізняються.

Традиційний NOC зосереджується на забезпеченні доступності та продуктивності мережі та IT-інфраструктури, а також на управлінні конфігурацією мережевих пристроїв. Його основна мета – «тримати мережу в робочому стані». Натомість SOC зосереджується безпосередньо на виявленні,

аналізі та реагуванні на загрози безпеці, що можуть становити загрозу для конфіденційності, цілісності або доступності даних.

Робота NOC базується навколо управління подіями (events), пов'язаними з продуктивністю та доступністю, тоді як SOC працює з інцидентами (incidents) – подіями, які можуть свідчити про порушення політик безпеки. На практиці, звісно, ці два центри тісно співпрацюють: SOC може покладатися на дані від NOC (наприклад, про аномалії в трафіку), а у випадку успішної атаки, яка викликала відмову в обслуговуванні, SOC та NOC працюватимуть спільно для усунення наслідків.

Окремо слід розглянути взаємодію SOC з командою реагування на комп'ютерні інциденти (CSIRT – Computer Security Incident Response Team) або, ширше, з Центром кіберзахисту (CDC – Cyber Defense Center). На практиці ці терміни часто використовуються як синоніми або можуть позначати різні підрозділи в межах однієї організації.

Якщо проводити більш тонке розмежування, то SOC є постійно діючим операційним підрозділом, який забезпечує безперервний моніторинг та є «особою, що приймає перший удар» (front line). CSIRT, у свою чергу, часто розглядається як спеціалізована група (експертний рівень), яка залучається для глибокого технічного розслідування особливо складних або критичних інцидентів, а також для проведення пост-інцидентного аналізу.

Сучасна тенденція полягає в об'єднанні цих функцій в єдиний Центр кіберзахисту (CDC), який під одним дахом об'єднує SOC, CSIRT, Threat Intelligence, Forensic та інші дисципліни. Така конвергенція забезпечує більш ефективну координацію всіх аспектів діяльності з кібербезпеки.

Ключовою ланкою, що забезпечує стратегічне керівництво та зв'язок SOC з бізнесом, є посада директора з інформаційної безпеки (CISO – Chief Information Security Officer). SOC є операційним інструментом реалізації стратегії, розробленої CISO. Хоча CISO відповідає за політики безпеки, відповідність регуляторним вимогам, управління ризиками та стратегічний

бюджет, SOC є тим підрозділом, який виконує щоденну роботу з моніторингу та реагування.

Аналітичні звіти та статистичні дані, що їх генерує SOC, є одним з основних джерел інформації для CISO про реальний стан справ, ефективність існуючих засобів захисту, а також використовуються для обґрунтування необхідності додаткових інвестицій у кібербезпеку.

Нарешті, варто зазначити про тісний взаємозв'язок SOC з процесами управління інцидентами, визначеними в міжнародних стандартах, зокрема ISO/IEC 27001.

Стандарт вимагає від організації визначити процедури для управління інцидентами, пов'язаними з інформаційною безпекою, включаючи відповідальність за їхнє виявлення, звітування та реагування. SOC, незалежно від організаційної моделі, є ключовим механізмом виконання цієї вимоги.

Таким чином, забезпечення постійного моніторингу подій безпеки, що є основною функцією SOC, стає не просто рекомендацією, а обов'язковою умовою для підтримання сертифікації за цим стандартом. Підсумовуючи вищевикладене, SOC є не просто технічним центром, а стратегічним активом, який забезпечує безперервність бізнес-процесів. Розуміння принципів його роботи, функцій та місця в організації є критично важливим для будь-якого подальшого вдосконалення, зокрема для побудови ефективної системи координації з командами Red Team у межах сервісної моделі Purple Teaming.

1.2 Роль Red Team: емуляція загроз, тестування детектів та оцінка захищеності

Центри моніторингу та реагування на інциденти (SOC), розглянуті в попередньому підрозділі, виступають критично важливим, але виключно захисним механізмом сучасної кібербезпеки.

Для всебічного розуміння реальної ефективності цих захисних механізмів, а також для створення умов для їх вдосконалення, необхідний

інший, наступальний, компонент — команда Red Team. Якщо SOC є «щитом» організації, який цілодобово відбиває та реєструє удари, то Red Team виступає в ролі «меча» — професійного інструменту, який завданням якого є імітація дій реального супротивника для перевірки міцності цього щита та виявлення прихованих тріщин у захисті.

У найбільш загальному вигляді Red Team (червона команда) — це група фахівців з кібербезпеки, яка виконує роль нападника. Національний інститут стандартів і технологій США (NIST) у своєму нормативному документі SP 800-53 надає таке визначення: «Вправа з елементами реальних умов, що проводиться як симульована спроба зловмисника скомпрометувати місії та/або бізнес-процеси організації для надання всеосяжної оцінки спроможності системи безпеки захищати інформаційну систему та організацію».

Це визначення містить одразу кілька ключових смислів. По-перше, це не просто аудит чи сканування вразливостей, а активна, наступальна діяльність. По-друге, акцент робиться на досягненні кінцевої мети (скомпрометувати місію або бізнес-процес), а не на формальному пошуку вад. По-третє, метою є не атака заради атаки, а отримання «всеосяжної оцінки» спроможності систем безпеки. Іншими словами, Red Team виконує роль контрольованого супротивника. Його діяльність принципово відрізняється від діяльності команди «синіх» (Blue Team), яку представляє SOC.

Якщо Red Team — це напад (offense), то Blue Team — це захист (defense). Місія Red Team полягає в тому, щоб діяти як реалістичний зловмисник, використовуючи не лише технічні засоби, а й інструменти соціальної інженерії, фізичного проникнення (якщо це дозволено правилами) та інші тактики, техніки та процедури (TTPs) реальних кіберзлочинців. Умовно кажучи, пентестер намагається знайти якомога більше дірок, щоб скласти про них звіт.

А Red Team ставить перед собою одне або декілька завдань: викрасти певний файл, отримати доступ до критичного сервера, зламати обліковий запис керівника, поширити шкідливе ПЗ в мережі. Головна мета — досягти поставленої мети, залишаючись непоміченим якомога довше. Цей підхід

дозволяє отримати відповіді на стратегічні питання безпеки, як-от: «Чи здатний наш SOC виявити складну атаку? Чи спрацюють процедури реагування на інциденти в умовах реального стресу? Як керівництво відреагує на інцидент?».

Роль Red Team не обмежується виключно проведенням одноразових атак. Вона охоплює ширше коло завдань, які можна розділити на три ключові групи: емуляція загроз, тестування детектів та комплексна оцінка захищеності.

Емуляція загроз (adversary emulation) — це серцевина діяльності будь-якої зрілої Red Team. Емуляція загроз — це процес відтворення поведінки реального зловмисника або цілої групи (наприклад, APT-угруповання) в контрольованому середовищі. Замість того, щоб діяти абстрактно, Red Team будує свої атаки на основі розвідданих про загрози (Threat Intelligence), використовуючи саме ті TTPs, які застосовує реальний супротивник. Це дозволяє оцінити не просто наявність вразливостей, а здатність захисту протистояти конкретному, найбільш вірогідному для організації, класу загроз.

Ключовою таксономією для опису та класифікації TTPs є універсальна матриця знань про кіберзагрози — MITRE ATT&CK, яка стала галузевим стандартом. На основі MITRE ATT&CK Red Team може планувати свої дії, охоплюючи всі фази атаки: від розвідки та початкового проникнення до закріплення в системі, латерального переміщення та ексфільтрації даних. Тестування детектів (detection testing) є ключовим завданням для взаємодії з SOC у рамках Purple Teaming. Його суть полягає у перевірці здатності захисних механізмів (SIEM, правил кореляції, систем виявлення вторгнень, EDR-рішень) зафіксувати ту чи іншу дію зловмисника. Проводячи атаку, Red Team генерує специфічні події безпеки.

Аналізуючи, які з цих подій були зафіксовані та спричинили спрацювання сигналізації, а які пройшли непоміченими, SOC отримує точні дані про прогалини в покритті моніторингу. Таким чином, Red Team виконує роль «якісного індикатора» для Blue Team, перетворюючи абстрактні припущення про безпеку на конкретні, вимірювані факти. Саме на цьому базується перехід від ізольованих вправ до повноцінного Purple Teaming.Оцінка захищеності

(resilience validation) — найбільш комплексне завдання Red Team, яке полягає в оцінці всієї системи безпеки організації в її динаміці.

Результатом такої оцінки є не список вразливостей, а звіт, який відповідає на запитання: наскільки організація стійка до цілеспрямованої, складної атаки? Це включає перевірку не лише технологій, але й процесів (наприклад, процедур реагування) та людей (наскільки ефективно співробітники розпізнають фішингові листи, як реагує SOC на тривожні події). За визначенням, Red Team вправи виходять далеко за рамки стандартного пенетраційного тестування, розширюючи його цілі для вивчення можливості організації впроваджувати ефективні кіберзасоби захисту.

Для правильного розуміння ролі Red Team, а також для визначення місця кожної форми оцінки захищеності, необхідно чітко розмежувати Red Teaming та пенетраційне тестування. Хоча ці терміни часто помилково вживаються як синоніми, вони мають фундаментальні відмінності. Пентест відповідає на питання «де у нас дірки?», тоді як Red Team відповідає на більш глибоке питання «що станеться, якщо хтось навмисно спробує нас зламати?». Саме ця друга відповідь стає критично важливою для подальшого розвитку системи кібербезпеки. Основні відмінності між цими підходами систематизовано рисунку 1.2.

Характеристика	Пенетраційне тестування	Red Teaming
Основна мета:	Виявити та підтвердити наявність якомога більшої кількості вразливостей	Оцінити загальну стійкість, здатність виявляти та реагувати на атаку в умовах, наближених до реальних
Підхід:	Технічний, структурований, сфокусований на системах та застосунках	Операційний, цілеспрямований, емулює складного супротивника
Обізнаність захисників:	Як правило, SOC та IT-персонал знають про проведення тесту	(Здебільшого) Захисники не знають про вправу, вважаючи її реальною атакою
Обсяг:	Чітко визначені межі (наприклад, конкретний застосунок або підмережа)	Широкий, невизначений, охоплює всі активи, процеси та людей
Тривалість:	Дні/тижні	Тижні/місяці
Тактики та техніки:	Здебільшого технічні (експлуатація вразливостей, підбір паролів)	Різноманітні: технічні, соціальна інженерія, фізичне проникнення
Результат:	Детальний звіт про вразливості з рекомендаціями щодо їх усунення	Оцінка загальної ефективності захисту, часу виявлення та реагування
Оптимальний контекст:	Організації, які створюють або верифікують базові засоби захисту	Зрілі організації з усталеними програмами безпеки

Рис. 1.2 . Порівняльна характеристика Red Teaming та пенетраційного тестування

Для виконання своїх завдань Red Team використовує складний технологічний стек. Його ключовим компонентом є Command & Control (C2) фреймворки — програмне забезпечення для створення та управління агентурною мережею всередині інфраструктури цілі.

Ці інструменти дозволяють імітувати дії зловмисника на всіх етапах атаки. Основними фреймворками, що використовуються в Red Teaming, є: Cobalt Strike (галузевий стандарт, потужні можливості для латерального переміщення та обходу захисту), Sliver (сучасний відкритий багатоплатформний C2 фреймворк) та MITRE CALDERA (унікальна автоматизована платформа для емуляції супротивника, яка використовує матрицю MITRE ATT&CK).

Вибір конкретного фреймворку залежить від завдань, бюджету та рівня експертизи команди. Діяльність Red Team не є самоціллю. Її кінцева мета — вдосконалення загальної системи кібербезпеки. Найбільш ефективно це досягається через тісну співпрацю з Blue Team (SOC). Ізольована робота

призводить до того, що Red Team знаходить прогалини, але не передає свої знання захисникам, а SOC не має змоги перевірити свою реальну ефективність. Саме для усунення цього недоліку існує методологія Purple Teaming — форма співпраці, де Red Team та Blue Team працюють разом, обмінюючись знаннями та навичками.

У цій моделі Red Team ділиться своїми тактиками, техніками та процедурами, а Blue Team використовує їх для налаштування своїх детектів та вдосконалення процесів. Крім того, Red Teaming є важливою вимогою багатьох нормативних стандартів, зокрема ISO/IEC 27001, та показником найвищого рівня зрілості центру моніторингу згідно з моделлю SOC-CMM. Підсумовуючи, Red Team є набагато більшим, ніж просто «професійні хакери».

Це критично важливий інструмент стратегічного управління кібербезпекою, який дозволяє оцінити реальну ефективність захисту в динаміці. Без нього будь-який SOC ризикує залишитися в ілюзії безпеки, виявляючи лише очевидні загрози та не знаючи про свої справжні сліпі зони. Розуміння сильних сторін та обмежень Red Team, а також його місця в загальній екосистемі безпеки, є фундаментом для створення ефективної системи кіберзахисту. Саме аналіз прогалин, які виникають при ізольованій роботі Red Team та SOC, стане предметом дослідження в наступному розділі цієї кваліфікаційної роботи

.

1.3 Традиційна модель взаємодії Red Team та SOC: обмеження та недоліки

У попередніх підрозділах було детально розглянуто дві ключові складові сучасної системи кібербезпеки підприємства: центр моніторингу та реагування на інциденти (SOC), який виконує захисну функцію, та команду Red Team, що діє як контрольований супротивник.

Логічно припустити, що об'єднання цих двох компонентів має створювати потужний синергетичний ефект, забезпечуючи постійний цикл

вдосконалення захисту: Red Team атакує, SOC виявляє та реагує, після чого засоби захисту налаштовуються краще. Однак на практиці така ідеальна картина зустрічається вкрай рідко.

Здебільшого Red Team та SOC функціонують паралельно, або навіть ізольовано один від одного, що породжує цілу низку серйозних обмежень та недоліків. Цей підрозділ присвячено аналізу саме традиційної, роз'єднаної моделі взаємодії, яка передує появі Purple Teaming, та виявленню фундаментальних проблем, що роблять таку модель неефективною в умовах сучасних кіберзагроз. Традиційна модель взаємодії між Red Team та SOC в більшості організацій може бути охарактеризована як «передавальна» або «звітна». Суть її полягає в наступному: Red Team проводить свою вправу (яка може тривати від кількох тижнів до кількох місяців) в ізоляції від SOC. Команда SOC, у свою чергу, може навіть не знати про факт проведення вправи, особливо якщо мова йде про тест «в сліпу» (blind test), або ж знає про неї, але не має доступу до детальних планів та сценаріїв. Після завершення всіх атак Red Team готує детальний звіт, в якому описує знайдені вразливості, успішні вектори атак, використані TTPs та, можливо, надає рекомендації. Цей звіт передається керівництву або безпосередньо команді SOC. SOC вивчає звіт, вносить певні зміни до своїх правил виявлення або процедур реагування, і на цьому взаємодія вважається завершеною.

На перший погляд, така модель виглядає цілком логічною та працездатною. Проте глибший аналіз розкриває її фундаментальні вади. Захисники отримують інформацію про атаки постфактум, часто через тривалий проміжок часу після їх завершення. Red Team, з іншого боку, не має змоги отримати зворотний зв'язок про те, які саме їхні дії були виявлені, а які ні, і чому. Це призводить до того, що обидві команди продовжують працювати у своїх «бульбашках», не отримуючи реальної користі від потенційної синергії. Для систематизації проблем традиційної моделі їх доцільно розділити на три великі категорії: організаційні бар’єри, технологічні бар’єри та проблеми, пов’язані з метриками та оцінкою ефективності.

Саме ці бар’єри створюють «розриви» (gaps) у взаємодії, які роблять традиційну модель неефективною та штовхають організації до пошуку нових підходів, зокрема Purple Teaming.

Організаційні бар’єри є, мабуть, найбільш значущими, оскільки вони кореняться у структурі, культурі та бізнес-процесах організації. По-перше, це різні, а часто й суперечливі, ключові показники ефективності (KPI). Red Team, як правило, оцінюється за кількістю знайдених критичних вразливостей, успішністю досягнення мети (наприклад, отримання доступу до певного сервера) та часом, протягом якого атака залишалася непоміченою. SOC, навпаки, оцінюється за швидкістю виявлення (MTTD) та реагування (MTTR), а також за кількістю оброблених інцидентів.

Це створює природний конфлікт інтересів: Red Team зацікавлений у тому, щоб атаку не виявили якомога довше, тоді як SOC зацікавлений у негайному виявленні будь-якої аномалії. Крім того, Red Team часто звітує перед вищим керівництвом або незалежним комітетом, тоді як SOC підпорядковується безпосередньо CISO або IT-директору. Це призводить до різних пріоритетів та бюджетних циклів.

Наступним організаційним бар'єром є різний часовий горизонт діяльності. Red Team вправи плануються на тижні або місяці, тоді як SOC працює в режимі реального часу, у хвилинах та годинах. Синхронізувати ці два режими вкрай складно. Технологічні бар’єри пов’язані з тим, що Red Team та SOC використовують різні, часто несумісні, програмно-апаратні комплекси. SOC будує свою роботу навколо SIEM-платформ (Security Information and Event Management), які збирають та корелюють логи з усієї інфраструктури. Red Team, у свою чергу, використовує спеціалізовані C2 фреймворки (Cobalt Strike, Sliver, Caldera), інструменти для пост-експлуатації та обходу захисту.

У традиційній моделі ці два світи майже не перетинаються. Red Team не інтегрує свої логи в SIEM SOC (або робить це постфактум), а SOC не надає Red Team доступу до своїх детектів у реальному часі. Це призводить до ситуації, коли Red Team проводить атаку, яка генерує десятки важливих подій безпеки,

але SOC не бачить їх або бачить лише частково через відсутність належної телеметрії. Як наслідок, після завершення вправи SOC може виявити, що значна частина дій Red Team пройшла непоміченою, але для глибокого аналізу даних вже недостатньо, оскільки первинні логи були перезаписані або втрачені. Проблеми метрик та оцінки ефективності є прямим наслідком організаційних та технологічних бар'єрів.

У традиційній моделі відсутні спільні, узгоджені показники, які б дозволили оцінити якість взаємодії. Red Team звітує про «успішні атаки», SOC – про «виявлені інциденти», але ніхто не вимірює, наприклад, «відсоток атак Red Team, які були виявлені SOC протягом години» або «час від моменту атаки до моменту налаштування нового детекту». Без таких спільних метрик будь-яке вдосконалення має суб'єктивний характер. Крім того, традиційна модель не дозволяє оцінити динаміку: покращується чи погіршується здатність SOC виявляти атаки з часом? Чи стають атаки Red Team складнішими? Відповіді на ці питання неможливі без системного, спільного підходу до збору даних.

Усе це разом призводить до того, що організація має ілюзію безпеки. Керівництво отримує звіт Red Team «ми знайшли 10 критичних вразливостей» та звіт SOC «ми виявили та зупинили 1000 атак за місяць». Однак реальна картина залишається невідомою: скільки з атак Red Team залишилися непоміченими? Чи могла б реальна атака, побудована за тими ж TTPs, довгий час існувати в інфраструктурі? Без тісної координації відповіді на ці питання неможливі.

На рисунку 1.2 схематично зображено основні «розриви», що виникають у традиційній моделі взаємодії Red Team та SOC. Ці розриви ілюструють відсутність зворотного зв'язку в реальному часі, технологічну несумісність та різні системи метрик, які унеможливлюють ефективну співпрацю.

Таким чином, традиційна модель взаємодії Red Team та SOC, заснована на ізольованій роботі та передачі звітів постфактум, має фундаментальні обмеження. Вона не дозволяє реалізувати повний цикл вдосконалення захисту, призводить до конфлікту інтересів, технологічної несумісності та відсутності

спільних метрик. Саме усвідомлення цих вад спонукало світову спільноту до розробки нової парадигми – Purple Teaming, яка буде детально розглянута в наступному підрозділі як сервісна модель координації, що долає описані вище бар'єри.

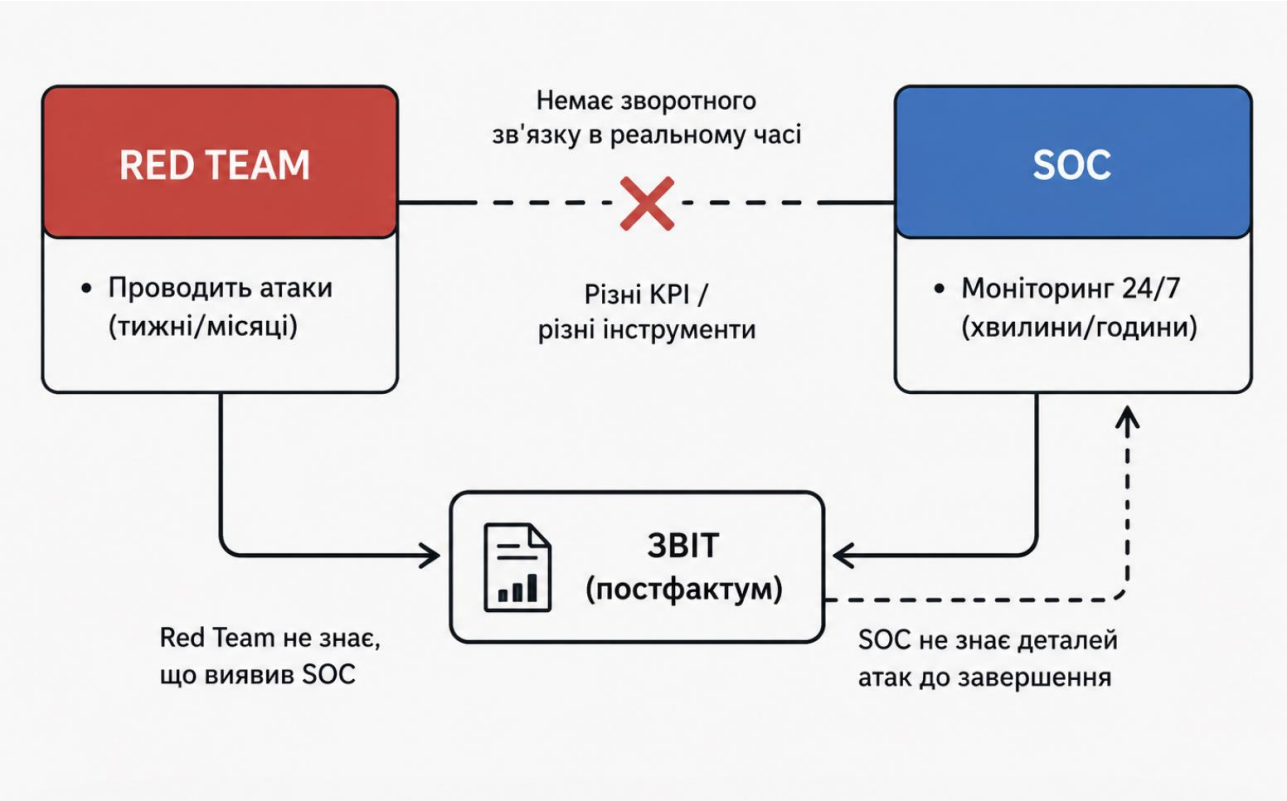

Рис 1.3 . Традиційна модель взаємодії Red Team та Soc

1.4 Purple Teaming як сервісна модель координації: визначення, принципи

Попередній аналіз традиційної моделі взаємодії Red Team та SOC продемонстрував її фундаментальні вади: відсутність зворотного зв’язку в реальному часі, технологічну несумісність, конфлікт ключових показників ефективності та, як наслідок, низьку ефективність вдосконалення захисних механізмів.

Вирішення цих проблем потребує нового підходу, який не просто «поєднує» дві команди, а створює умови для їхньої постійної, системної та взаємовигідної співпраці. Саме таким підходом є Purple Teaming (фіолетова

команда) — сервісна модель координації, яка перетворює протистояння між атакою та захистом на спільний процес підвищення кіберстійкості організації.

Цей підрозділ присвячено визначенню сутності Purple Teaming, його ключовим принципам та обґрунтуванню того, чому саме сервісний підхід є найбільш ефективним для сучасних підприємств. Термін «Purple Teaming» не означає створення окремої, третьої команди в структурі кібербезпеки. Натомість це методологія роботи, спосіб організації взаємодії між існуючими Red Team (напад) та Blue Team (захист, який уособлює SOC).

У літературі зустрічається декілька визначень, але всі вони сходяться на ключовій ідеї: Purple Teaming — це спільна діяльність, під час якої Red Team та Blue Team об'єднують свої знання, інструменти та зусилля для максимізації ефективності обох сторін. Найбільш вдалим, на думку автора, є визначення, запропоноване експертами компанії Red Canary: «Purple Teaming — це не роль і не посада, а практика, за якої Red Team і Blue Team працюють разом протягом усього тесту, обмінюючись інформацією в реальному часі для покращення здатності організації виявляти, реагувати та протистояти атакам».

Іншими словами, Purple Team — це не хтось третій, це стан співпраці, який активується на час проведення вправи або на постійній основі. Важливим аспектом є те, що Purple Teaming не замінює ні Red, ні Blue. Кожна команда зберігає свою основну функцію: Red Team атакує, Blue Team захищається. Але на відміну від традиційної моделі, Purple Teaming передбачає, що ці дії відбуваються не ізольовано, а в тісному циклі зворотного зв'язку. Red Team не просто намагається «перемогти» захист, а допомагає SOC зрозуміти, як саме можна покращити детекти. SOC, у свою чергу, надає Red Team інформацію про те, які атаки є найбільш болючими з точки зору бізнесу, та ділиться своїми спостереженнями про реальні загрози.

Традиційно Purple Teaming сприймався як разові вправи, що проводяться кілька разів на рік. Однак сучасна практика, особливо у великих організаціях з високим рівнем зрілості, еволюціонувала у бік сервісної моделі. Що це означає? Сервісна модель передбачає, що Purple Teaming стає не окремим проектом, а

постійно діючим процесом, інтегрованим у повсякденну діяльність SOC та Red Team. Це аналогічно до того, як хмарні сервіси (IaaS, PaaS) змінили IT: замість того, щоб купувати обладнання раз на рік, організація отримує постійний доступ до ресурсів.

У контексті Purple Teaming сервісна модель означає наступне. Red Team пропонує свої можливості з емуляції загроз як внутрішній сервіс для SOC. SOC, у свою чергу, виступає в ролі «замовника», який може в будь-який момент ініціювати перевірку конкретного детекту, правила кореляції або процедури реагування.

Наприклад, аналітик SOC помітив, що протягом останнього тижня зросла кількість помилкових спрацьовувань за певною сигнатурою. Він може зробити «запит до сервісу Purple Teaming»: відтворити атаку, яка має генерувати саме це сповіщення, та перевірити, чи спрацює воно коректно. Red Team отримує запит, проводить контрольовану атаку, фіксує результат і передає його SOC. Весь цикл може займати не тижні, а години або навіть хвилини. Такий підхід кардинально змінює цінність Purple Teaming для бізнесу. Він дозволяє швидко верифікувати будь-які зміни в засобах захисту, тестувати нові сценарії загроз без очікування планової вправи, а також постійно підтримувати високий рівень готовності SOC.

Для того щоб Purple Teaming був ефективним як сервісна модель, необхідно дотримуватися низки ключових принципів. Ці принципи визначають, як саме має бути організована взаємодія, які ролі задіяні та якими правилами керуються команди. Перший принцип — відсутність «сюрпризів» між командами. У традиційній моделі Red Team часто намагається «перехитрити» SOC. У Purple Teaming, навпаки, всі дії Red Team повинні бути відомі SOC (або принаймні керівництву Purple Teaming) в реальному часі.

Це не означає, що SOC отримує повний план атаки наперед – елемент невизначеності може зберігатися для перевірки оперативності реагування. Але ключова відмінність у тому, що після завершення кожної фази атаки

відбувається негайний розбір: «Ось що ми зробили, ось які події згенерували, ось що ви побачили, а що ні».

Другий принцип — спільне планування та спільні цілі. Перед початком будь-якої Purple Teaming вправи (або в рамках постійного сервісу) команди спільно визначають, які саме сценарії, TTPs або детекти будуть перевірятися. Цілі мають бути спільними та вимірюваними. Наприклад: «Перевірити, чи здатний SOC виявити латеральне переміщення з використанням протоколу SMB протягом 15 хвилин після початку активності». Зауважте, що це ціль, яка стосується обох команд:

Red Team має створити таку активність, а SOC – її зафіксувати. Третій принцип — постійний зворотний зв'язок у реальному часі. Це серце сервісної моделі. Замість того щоб чекати тижнями на фінальний звіт, команди обмінюються інформацією під час проведення атаки. Це можуть бути короткі щоденні стендапи, виділені чати в Slack/Teams або навіть спільна сесія, де Red Team в реальному часі демонструє свої дії, а SOC коментує, які сповіщення вони бачать.

Такий підхід дозволяє миттєво коригувати дії та отримувати максимальну користь від кожної хвилини спільної роботи. Четвертий принцип — автоматизація та інтеграція інструментів. Сервісна модель неможлива без технологічної інтеграції. Red Team та SOC повинні мати спільне середовище для обміну даними. На практиці це означає, що логи C2-фреймворків Red Team мають надсилатися в SIEM SOC в реальному часі (під час вправи). Аналогічно, SOC може надавати Red Team доступ до своїх детектів (або їхніх хешів) для перевірки.

Деякі організації використовують спеціалізовані платформи для Purple Teaming (наприклад, AttackIQ, SafeBreach, Scythe), які дозволяють автоматизувати запуск сценаріїв та збір результатів. П'ятий принцип — спільна система метрик. Як було зазначено в попередньому підрозділі, однією з головних проблем традиційної моделі є різні KPI. У Purple Teaming необхідно створити спільний набір показників, який відображає ефективність координації.

о таких показників можуть належати: час між запуском атаки Red Team та генерацією сповіщення в SOC (час виявлення в контрольованих умовах), відсоток атак Red Team, які призвели до змін у налаштуваннях SOC, кількість нових детектів, створених за результатами вправи, тощо. Ці спільні метрики дозволяють оцінити прогрес і обґрунтувати інвестиції в Purple Teaming.

Порівняно з традиційною моделлю, Purple Teaming демонструє кардинальні відмінності за багатьма параметрами. У традиційній моделі характер взаємодії є ізольованим, «передавальним» — Red Team готує звіт після завершення всіх атак. У Purple Teaming взаємодія стає спільною, інтерактивною та відбувається в реальному часі. Зворотний зв'язок, який у традиційній моделі практично відсутній під час атаки, у Purple Teaming є постійним та двостороннім.

Планування в традиційній моделі здійснюється Red Team самостійно, тоді як у Purple Teaming планування є спільним і базується на потребах SOC. Що стосується метрик, то традиційна модель використовує різні, часто конфліктуючі показники для Red Team та SOC, а Purple Teaming впроваджує спільні, узгоджені метрики, орієнтовані на вдосконалення загальної системи захисту.

Часовий горизонт також суттєво відрізняється: якщо традиційна модель оперує тижнями або місяцями на одну вправу з подальшим формуванням звіту, то Purple Teaming у сервісному виконанні працює в режимі годин або днів, забезпечуючи безперервний процес. Нарешті, кінцева мета традиційної моделі полягає в демонстрації вразливостей, тоді як Purple Teaming спрямований на постійне підвищення стійкості захисту організації.

Таким чином, Purple Teaming як сервісна модель координації є відповіддю на виклики, які не змогла подолати традиційна взаємодія. Вона базується на принципах відкритості, спільного планування, постійного зворотного зв'язку, технологічної інтеграції та спільних метрик.

Саме ці принципи будуть покладені в основу практичної розробки системи координації в третьому розділі даної кваліфікаційної роботи.

Розуміння сутності Purple Teaming дозволяє перейти до аналізу конкретних бар'єрів, які існують на шляху до ефективної координації, що і стане предметом розгляду в наступному розділі.

Висновки до розділу 1

У першому розділі кваліфікаційної роботи було проведено теоретичне дослідження функціональних ролей SOC та Red Team, проаналізовано традиційну модель їхньої взаємодії та розглянуто Purple Teaming як перспективну сервісну модель координації.

Встановлено, що SOC є централізованим підрозділом, який виконує функції безперервного моніторингу, виявлення інцидентів, реагування на загрози, проактивного пошуку загроз та управління вразливостями, причому ефективність його роботи безпосередньо залежить від якості даних та рівня кваліфікації аналітиків, а організаційні моделі розгортання SOC (власний, аутсорсинговий, гібридний) мають свої переваги та недоліки.

Досліджено роль Red Team як контрольованого супротивника, основними завданнями якого є емуляція загроз на основі MITRE ATT&CK, тестування детектів та комплексна оцінка захищеності організації; порівняльний аналіз показав, що Red Teaming, на відміну від пенетраційного тестування, орієнтований не на виявлення якомога більшої кількості вразливостей, а на оцінку загальної стійкості до цілеспрямованої атаки, а ключовим технологічним інструментарієм є C2-фреймворки (Cobalt Strike, Sliver, MITRE CALDERA). Виявлено основні обмеження традиційної моделі взаємодії, заснованої на ізольованій роботі та передачі звітів постфактум, а саме: організаційні бар’єри (різні, часто конфліктуючі KPI, різні часові горизонти планування), технологічні бар’єри (відсутність інтеграції між SIEM SOC та C2-фреймворками Red Team, втрата критичної телеметрії) та метричні бар’єри (відсутність спільних показників ефективності координації), що призводить до ілюзії безпеки та неможливості реально оцінити прогалини в захисті.

Нарешті, обґрунтовано Purple Teaming як сервісну модель координації, яка базується на принципах відсутності «сюрпризів» між командами, спільного планування та спільних цілей, постійного зворотного зв’язку в реальному часі, автоматизації та інтеграції інструментів, а також спільної системи метрик, що дозволяє перетворити протистояння між атакою та захистом на постійний цикл вдосконалення кіберстійкості організації. Таким чином, теоретичні засади, розглянуті в першому розділі, створюють необхідну базу для подальшого аналізу проблем координації (розділ 2) та розроблення практичних рекомендацій щодо впровадження системи Purple Teaming (розділ 3)

Розділ 2 АНАЛІЗ ПРОБЛЕМ КООРДИНАЦІЇ RED TEAM ТА SOC

2.1 Організаційні бар’єри: різні KPI, розділені бюджети, звітність

Після теоретичного аналізу функціонування SOC та Red Team, а також розгляду Purple Teaming як перспективної сервісної моделі координації, необхідно перейти до детального дослідження перешкод, які унеможливлюють ефективну співпрацю між командами в традиційних умовах. Найбільш значущою групою таких перешкод є організаційні бар'єри, оскільки вони кореняться не в технічних обмеженнях, а в структурі управління, системі мотивації, фінансуванні та внутрішніх регламентах підприємства. Ці бар'єри часто виявляються найбільш стійкими до подолання, оскільки пов'язані зі сформованою корпоративною культурою, розподілом повноважень та історично закріпленими практиками звітності.

Першим і найбільш критичним організаційним бар'єром є наявність різних, а часто й прямо суперечливих, ключових показників ефективності (KPI) для Red Team та SOC. Система KPI є основним інструментом управління персоналом, оскільки вона визначає, за що саме звітують команди, як оцінюється їхня робота та, зрештою, як нараховується преміальна частина винагороди. Якщо KPI різних команд конфліктують, між ними виникає антагонізм, а не співпраця. Для SOC, який функціонує в режимі 24/7, основними показниками ефективності є: середній час виявлення інциденту (Mean Time to Detect, MTTD), середній час реагування (Mean Time to Respond, MTTR), кількість оброблених сповіщень за зміну, відсоток помилкових спрацьовувань (false positive rate) та кількість успішно зупинених атак. Ці показники стимулюють SOC до якомога швидшого виявлення будь-якої підозрілої активності та негайного реагування на неї. Для аналітика SOC кожне невиявлене або несвоєчасно виявлене сповіщення є потенційним провалом. Red Team, особливо в моделі «сліпого» тестування (blind test), оцінюється за іншими показниками: кількість успішно реалізованих сценаріїв атак, час,

протягом якого атака залишалася непоміченою, кількість скомпрометованих цільових систем, ступінь досягнення кінцевої мети (наприклад, викрадення певного файлу або отримання прав адміністратора домену). Ці показники стимулюють Red Team до прихованих дій, обходу засобів виявлення та максимально тривалого перебування поза полем зору SOC. Таким чином, KPI SOC нагороджують за швидке виявлення, а KPI Red Team – за непомітність. Це створює фундаментальний конфлікт інтересів. У традиційній моделі, де команди не координуються, цей конфлікт призводить до того, що SOC сприймає Red Team як загрозу, яка намагається обдурити систему, а Red Team сприймає SOC як перешкоду, яку потрібно обійти. Жодна з команд не бачить в іншій партнера для вдосконалення. Наприклад, аналітик SOC, який виявив незвичну активність, може не повідомити про це Red Team, оскільки така інформація дозволить «супротивнику» (навіть якщо це власна Red Team) скоригувати дії та уникнути виявлення, що погіршить показники SOC. З іншого боку, Red Team не ділиться своїми тактиками, техніками та процедурами (TTPs) з SOC, оскільки вдосконалення детектів ускладнить проведення майбутніх атак і знизить їхні власні KPI. Другим суттєвим організаційним бар'єром є розділені бюджети та різні джерела фінансування Red Team та SOC. На більшості підприємств бюджети на кібербезпеку формуються за окремими напрямками або різними центрами фінансової відповідальності. SOC, як правило, фінансується з операційного бюджету IT або департаменту інформаційної безпеки як постійно діючий сервіс. Його бюджет включає витрати на SIEM-платформу, ліцензії на EDR-рішення, заробітну плату аналітикам, оренду приміщень тощо. Red Team, особливо якщо вона не є постійною внутрішньою командою, а залучається час від часу як зовнішній консультант, фінансується з окремого проектного бюджету, часто пов'язаного з оцінкою захищеності, аудитом або вимогами регуляторів. Таке розділення бюджетів призводить до відсутності спільних фінансових стимулів для координації. Керівник SOC не зацікавлений витрачати час аналітиків на спільні вправи з Red Team, оскільки це не закладено в бюджеті та не враховується при оцінці ефективності його

підрозділу. Керівник Red Team не має фінансової мотивації адаптувати свої сценарії під конкретні потреби SOC, оскільки його оплата залежить від виконання проекту (проведення тесту), а не від покращення детектів SOC. У випадку залучення зовнішньої Red Team (MSSP або консалтингова компанія) виникає додатковий бар'єр – захист комерційної інформації, що унеможливлює передавання деталей атак внутрішньому SOC. Третім організаційним бар'єром є різні системи звітності та рівні підпорядкування. SOC звітує перед керівником центру безпеки (CISO) або IT-директором. Його звітність має операційний характер: щоденні звіти про інциденти, щотижневі зведення про стан захисту, щомісячні аналітичні звіти про тренди. Red Team, особливо в рамках комплаєнс-вимог (PCI DSS, ISO 27001), часто звітує безпосередньо перед правлінням, аудиторським комітетом або зовнішнім регулятором. Її звіти мають стратегічний характер, містять узагальнені висновки про рівень захищеності, але рідко включають операційні деталі, корисні для SOC. SOC отримує фінальний звіт Red Team через місяць після завершення вправи, але цей звіт, написаний мовою, зрозумілою керівництву, не містить конкретних технічних індикаторів (IoC, правил кореляції, прикладів мережевих потоків), необхідних аналітикам. Крім того, різні рівні підпорядкування створюють проблеми з пріоритетизацією завдань. Узгодження спільної вправи перетворюється на тривалу бюрократичну процедуру, що за відсутності прямого підпорядкування між командами часто відкладається на користь поточних інцидентів. Нарешті, важливим є культурний бар'єр, тісно пов'язаний з організаційними. У багатьох компаніях історично склалося, що Red Team та SOC сприймають один одного як конкурентів. Результати Red Team вправ часто використовуються для критики SOC («ось скільки атак ви не помітили»), на що SOC відповідає применшенням значущості знахідок («нереалістичні сценарії», «недостатньо ресурсів»). Така культура взаємних звинувачень унеможливлює конструктивну координацію. Подолання цього бар'єру потребує не лише зміни KPI та бюджетних моделей, але й тривалої роботи зі зміни корпоративної культури. Таким чином, організаційні бар'єри (конфліктуючі KPI, розділені бюджети,

різні системи звітності та культурне протистояння) створюють фундаментальні перешкоди для ефективної координації Red Team та SOC. Без їх подолання будь-які технологічні рішення або спроби впровадження Purple Teaming будуть неефективними, оскільки вступають у суперечність із базовими стимулами та структурами управління. Аналіз організаційних бар'єрів є необхідною передумовою для розробки практичних рекомендацій у третьому розділі. Наступним кроком є дослідження технологічних бар'єрів, які, хоча й тісно пов'язані з організаційними, мають власну специфіку.

2.2 Технологічні бар’єри: різні платформи (SIEM, C2), відсутність інтеграції

Навіть за умови зміни системи ключових показників ефективності, об'єднання бюджетів та запровадження спільної звітності, що створює сприятливе організаційне середовище, технологічна несумісність продовжує унеможливлювати ефективну координацію між Red Team та SOC. Організаційні бар'єри пов'язані з управлінням персоналом і фінансуванням, тоді як технологічні бар'єри виникають через відсутність інтеграції між засобами моніторингу (SIEM) та інструментами імітації атак (C2-фреймворки), а також через ненадходження логів Red Team до системи аналітики SOC.

Першим і найбільш суттєвим технологічним бар'єром є застосування різних платформ для збору та аналізу даних. SOC функціонує на базі SIEM-платформи, яка агрегує події безпеки з серверів, мережевого обладнання, застосунків, систем автентифікації, EDR, міжмережевих екранів та проксі-серверів. SIEM виконує кореляцію подій, виявляє закономірності та генерує сповіщення. У свою чергу, Red Team використовує C2-фреймворки (Cobalt Strike, Sliver, Mythic, Covenant), інструменти постексплуатації (Mimikatz, BloodHound, PowerShell Empire), генератори пейлоадів та засоби обходу EDR-рішень. Ці інструменти генерують лог-файли, які зберігаються локально в базі даних C2-фреймворку або на диску оператора Red Team, але не передаються до

SIEM. У традиційній моделі взаємодії SOC отримує лише події від антивірусних систем або систем виявлення вторгнень, не маючи доступу до внутрішніх логів C2, що унеможливлює аналіз причинно-наслідкових зв'язків між діями атакуючого та генерованими подіями. В результаті SOC фіксує лише симптоми (наприклад, підозрілий трафік або аномальний процес), але не бачить першопричини. На момент отримання звіту Red Team (через кілька тижнів після завершення атаки) первинні логи часто виявляються перезаписаними, що унеможливлює подальший аналіз. У зв'язку з цим в рамках Purple Teaming наполягають на інтеграції логів Red Team до SIEM у реальному часі, що дозволяє SOC спостерігати атаку з позиції нападника.

Другим бар'єром є відсутність уніфікованих форматів даних та стандартизованих API для обміну інформацією між інструментами Red Team та SOC. Навіть при прийнятті рішення про інтеграцію логів C2-фреймворку до SIEM виникають технічні труднощі: C2-фреймворки не мають готових конекторів до більшості SIEM-платформ, а формати логів (JSON, XML, syslog, пропрієтарні бінарні формати) відрізняються. Це змушує Red Team розробляти власні скрипти для трансформації та відправлення даних. Крім того, SIEM-платформи мають обмеження за швидкістю прийому подій (events per second, EPS), і активна атака Red Team може генерувати десятки тисяч подій за хвилину, що призводить до перевантаження та втрати даних. Аналогічна проблема існує і в зворотному напрямку: передавання інформації про детекти SOC (хеші сигнатур, правила кореляції) до Red Team для перевірки можливості їх обходу ускладнюється через конфіденційність цих даних, що розкривають внутрішню архітектуру захисту. Відсутність безпечних API унеможливлює такий обмін без ризику витоку.

Третій бар'єр полягає у різному рівні автоматизації та різних часових масштабах обробки даних. SOC високого рівня зрілості автоматизує операції збагачення даних, кореляції, створення тікетів та блокування індикаторів, однак ця автоматизація налаштована на реальні атаки, а не на контрольовані сценарії Red Team. Під час проведення вправи SOC може отримати сотні сповіщень, які

потребують ручного аналізу; через завантаженість аналітиків реальними інцидентами реакція на тестову атаку може бути відсутньою, що спотворює результати. З іншого боку, Red Team часто не має засобів автоматизації для швидкого запуску сценаріїв у відповідь на запити SOC, що призводить до затримок (дні замість хвилин). У сервісній моделі Purple Teaming необхідна висока ступінь автоматизації.

Четвертий бар'єр пов'язаний з безпекою та ізоляцією середовищ. SOC та Red Team, як правило, функціонують у різних мережевих сегментах, і Red Team (особливо зовнішня) працює через VPN, її IP-адреси можуть блокуватися корпоративним міжмережевим екраном. Для інтеграції логів необхідно відкривати доступ, що створює ризик використання цих каналів реальними зловмисниками. Крім того, інструменти Red Team часто застосовують техніки, які є сигнатурами для засобів захисту (створення процесів із підозрілими іменами, зміна реєстру, виклики Windows API). Якщо SOC дозволяє Red Team працювати без блокувань, то в системах захисту формуються «білі списки», що можуть бути використані реальними хакерами. Якщо ж SOC блокує Red Team, проведення Purple Teaming стає неможливим. Вирішення цього протиріччя потребує використання ізольованих середовищ (окремі VLAN, лабораторні сегменти), що не завжди доступне для тестування продуктивних систем.

П'ятим бар'єром є відсутність спеціалізованих платформ для Purple Teaming. Існуючі комерційні рішення (AttackIQ, SafeBreach, Scythe) є дорогими, потребують значної кастомізації та не мають універсального характеру. Більшість організацій змушені розробляти власні інтеграційні скрипти, використовуючи MITRE CALDERA для автоматизації емуляції та TheHive або MISP для обміну інформацією. Це вимагає значних ресурсів на розробку, підтримку та час, що робить такий підхід недоступним для багатьох компаній середнього розміру.

Таким чином, технологічні бар'єри (різнорідність платформ, відсутність інтеграції, неузгодженість автоматизації, проблеми безпеки) створюють серйозні перешкоди для координації Red Team та SOC навіть за умови

організаційної готовності. Вони призводять до втрати критичної телеметрії, спотворення результатів вправ та унеможливлюють автоматизацію спільних процесів. Подолання цих бар'єрів потребує не лише інвестицій в інструменти, але й перегляду архітектури безпеки, впровадження стандартизованих API та створення інтеграційного шару. Подальші шляхи вирішення будуть розглянуті в третьому розділі.

2.3 Проблеми метрик та оцінки ефективності (Red Team vs SOC)

Організаційні та технологічні бар’єри, розглянуті в попередніх підрозділах, безпосередньо впливають на третю, не менш важливу групу перешкод – проблеми, пов’язані з метриками та оцінкою ефективності. Навіть якщо в компанії вдалося змінити систему KPI, об’єднати бюджети та технологічно інтегрувати SIEM з C2-фреймворками, без узгодженої системи вимірювань неможливо відповісти на ключові питання: чи дійсно координація покращила захист? Чи стали детекти SOC кращими після Purple Teaming вправ? Як виміряти успіх спільної роботи?

У традиційній моделі Red Team та SOC використовують різні, часто несумісні метрики, що створює ілюзію ефективності там, де її немає, або, навпаки, приховує реальні прогалини. Цей підрозділ присвячено аналізу проблем метрик, їхнього впливу на координацію та обґрунтуванню необхідності створення спільної системи показників.

Першою і найбільш фундаментальною проблемою є те, що Red Team та SOC використовують різні одиниці вимірювання успіху. SOC традиційно оцінюється за операційними метриками, які відображають його здатність обробляти потік подій та реагувати на інциденти. Найпоширенішими показниками є: середній час виявлення (MTTD – Mean Time to Detect), середній час реагування (MTTR – Mean Time to Respond), кількість оброблених сповіщень за зміну, відсоток помилкових спрацьовувань (false positive rate), час на розслідування одного інциденту.

Всі ці метрики мають одну важливу особливість: вони орієнтовані на процес, а не на результат. Високий MTTD може свідчити про погані детекти, але він також може бути наслідком нестачі персоналу або поганого налаштування SIEM. SOC може мати чудові показники MTTD та MTTR, але при цьому пропускати найскладніші атаки, які не генерують явних сигнатур. Red Team, навпаки, оцінюється за результативними метриками: кількість успішно реалізованих сценаріїв, відсоток досягнутих цілей (наприклад, скомпрометовано 8 з 10 цільових систем), час, протягом якого атака залишалася непоміченою, кількість знайдених критичних вразливостей.

Ці метрики орієнтовані на ефективність атаки, а не на якість захисту. У традиційній моделі, де немає спільних вправ, ці два набори метрик існують паралельно, і ніхто не відповідає на питання: «Чи корелює час виявлення SOC зі складністю атаки Red Team?». Без спільних метрик будь-яке порівняння стає неможливим.

Другою проблемою є різний часовий горизонт вимірювань. SOC працює в режимі реального часу: метрики MTTD та MTTR вимірюються в хвилинах або годинах. Звітність SOC формується щоденно, щотижнево, щомісяця. Red Team, особливо якщо вона проводить складні, багатоетапні атаки, працює в значно довшому часовому масштабі: підготовка може займати тижні, сама атака – дні або тижні, а фінальний звіт готується через кілька тижнів після завершення.

Це призводить до того, що результати Red Team вправи стають доступними для SOC з великим запізненням, коли оперативний контекст вже втрачено. Наприклад, Red Team виявила, що певна техніка латерального переміщення не фіксується SIEM.

Але до моменту отримання звіту (через місяць) SOC міг вже змінити конфігурацію, оновити правила кореляції або навіть замінити SIEM-платформу. Без спільних метрик, що вимірюються в єдиному часовому масштабі (наприклад, «час від запуску атаки до створення нового детекту»), неможливо оцінити динаміку вдосконалення.

Третьою проблемою є відсутність метрик якості детектів. SOC може

звітувати про тисячі виявлених інцидентів, але чи всі вони є реальними загрозами? Скільки з них – помилкові спрацьовування? І навпаки, скільки реальних атак залишилося непоміченими? Без контрольної групи (а саме такою групою виступає Red Team) відповісти на ці питання неможливо. У традиційній моделі SOC не має об'єктивного способу оцінити повноту покриття (coverage) своїх детектів: який відсоток можливих TTPs зловмисників він здатен виявити. Red Team, у свою чергу, не має метрик, які б показували, які саме детекти SOC були «сліпими» для їхніх атак, а які спрацювали. Без цих даних будь-яке вдосконалення є інтуїтивним, а не системним.

Четвертою проблемою є суперечливість метрик, яка створює конфлікт інтересів, описаний раніше. Наприклад, SOC має KPI «зменшити MTTD до 10 хвилин». Red Team має KPI «провести атаку, яка залишатиметься непоміченою не менше 2 годин». Ці дві цілі прямо суперечать одна одній. Якщо SOC досягне свого KPI, Red Team провалить свій. Якщо Red Team досягне свого, SOC покаже поганий MTTD. У такій системі ніхто не зацікавлений у співпраці. Навпаки, кожна команда намагається «переграти» іншу, що є протилежністю Purple Teaming. Без створення спільних, несуперечливих метрик будь-які спроби координації будуть саботуватися на рівні виконавців, оскільки вони суперечать їхнім особистим стимулам.

П’ятою проблемою є відсутність метрик для оцінки самої координації. Навіть якщо організація почала проводити Purple Teaming вправи, як виміряти, чи вони ефективні? Скільки атак Red Team було виявлено SOC? Який відсоток рекомендацій Red Team було впроваджено SOC? Як змінився час створення нового детекту після отримання інформації від Red Team? Без таких метрик координація перетворюється на ритуал, який не приносить вимірних результатів. У підрозділі 3.4 буде запропоновано систему спільних метрик, але для розуміння проблем важливо зазначити, що в більшості організацій такі метрики взагалі відсутні.

Нарешті, шостою проблемою є ігнорування якісних показників. Більшість організацій фокусуються на кількісних метриках, які легко автоматизувати (час,

кількість, відсоток). Але справжня цінність координації часто полягає в якісних змінах: покращення взаєморозуміння між командами, підвищення кваліфікації аналітиків SOC, зменшення «сліпих зон» у знаннях про загрози. Ці аспекти важко виміряти, але вони є критично важливими для довгострокового успіху. Традиційна система метрик повністю ігнорує їх, що призводить до того, що керівництво бачить лише «верхівку айсберга», приймаючи неправильні рішення.

Для кращого розуміння відмінностей між метриками Red Team та SOC, а також їхніх наслідків для координації, нижче наведена порівняльна таблиця. Вона систематизує ключові показники, що використовуються кожною командою, і демонструє, чому ці метрики конфліктують одна з одною.

Категорія метрик	Типові метрики SOC	Типові метрики Red Team
Час виявлення / непомітності	MTTD (Mean Time to Detect), MTTR (Mean Time to Respond)	Час непоміченої присутності, час до початку реагування
Обсяг роботи / успішність	Кількість оброблених сповіщень, відсоток інцидентів, закритих за 1 годину	Відсоток успішно реалізованих сценаріїв, кількість скомпрометованих цілей
Якість виявлення / прихованості	Відсоток помилкових спрацьовувань (false positive rate)	Кількість обійдених детектів, відсутність сповіщень про атаку
Орієнтація	Процесна (як добре ми працюємо)	Результативна (чого ми досягли)
ℹ Ці метрики є конфліктуючими, що унеможливлює спільну оцінку ефективності без додаткової координації.		

Рис 2.1 Порівняльний аналіз метрик Red Team та Soc

Таким чином, проблеми метрик та оцінки ефективності є потрійним викликом: по-перше, Red Team та SOC використовують різні, часто конфліктуючі показники; по-друге, відсутні метрики, які б вимірювали якість координації; по-третє, не враховуються якісні зміни. Без вирішення цих

проблем будь-яка система координації буде неповною. Саме тому в третьому розділі буде запропоновано систему спільних метрик Purple Teaming, яка долає описані вище обмеження. Аналіз організаційних, технологічних та метричних бар’єрів, проведений у цьому розділі, створює необхідне підґрунтя для практичних рекомендацій.

2.4 Аналіз типових розривів на прикладі модельних атак (за MITRE ATT&CK)

У попередніх підрозділах було розглянуто організаційні, технологічні та метричні бар'єри, що перешкоджають координації між Red Team та SOC. Для практичної ілюстрації того, як ці бар'єри призводять до конкретних розривів у взаємодії, доцільно звернутися до модельних атак, побудованих на основі загальновизнаної бази знань MITRE ATT&CK. Ця база даних систематизує тактики (наприклад, «початкове проникнення», «латеральне переміщення») та конкретні техніки, які використовуються зловмисниками. Кожна техніка має унікальний ідентифікатор (T1059, T1021, T1003 тощо). Для аналізу обрано три техніки, які часто застосовуються в реальних атаках і становлять значну складність для виявлення SOC. Розглянемо, які розриви виникають під час виконання цих технік за відсутності належної координації. **Техніка T1059.001 (PowerShell).** Red Team запускає PowerShell-скрипт з використанням команд Invoke-Expression, DownloadString або обфускації (кодування Base64, розбиття команд на фрагменти, динамічне завантаження). Теоретично SOC має отримувати події Windows Event Log, зокрема Event ID 4104, 4103, 400. На практиці детальне логування PowerShell часто вимкнене через побоювання надмірної кількості подій. Навіть за увімкненого логування обфускований код важко піддається автоматичному аналізу, оскільки правила кореляції в SIEM не розраховані на такі варіації. Крім того, отримана подія не дозволяє SOC відрізнити дії Red Team від реального зловмисника або легітимної адміністративної активності. У традиційній моделі звіт Red Team

надходить через три-чотири тижні після атаки, до того часу первинні логи перезаписуються, що унеможливлює аналіз причин неспрацювання правил виявлення. Розрив полягає у втраті контексту та відсутності оперативного зворотного зв'язку. Інтеграція логів C2-фреймворку Red Team до SIEM у реальному часі дозволила б аналітикам отримувати повну картину, однак у традиційній моделі ця інтеграція відсутня.

Техніка T1021.002 (SMB та адміністративні ресурси). Red Team підключається до віддаленої системи через протокол SMB, використовуючи стандартні адміністративні ресурси (C,ADMIN), після чого копіює або віддалено запускає пейлоад. SOC фіксує події входу (4624, 4648), події доступу до файлів (5140, 5142) та аномалії в SMB-трафіку. Однак у великих організаціях кількість таких подій становить десятки тисяч на день, оскільки адміністратори постійно виконують подібні дії. Red Team може свідомо імітувати легітимну активність, обираючи робочий час та використовуючи хости, які часто фігурують у логах адміністраторів. Без додаткового контексту (який міг би бути забезпечений інтеграцією C2-логів) SOC не здатен відрізнити атаку від нормальної активності. У результаті аналітик SOC або ігнорує подію (що призводить до непоміченої атаки), або витрачає значний час на розслідування помилкового спрацьовування. Розрив полягає в неможливості фільтрувати контрольовану атаку серед загального шуму подій. За умови координації Red Team міг би позначати свої підключення спеціальним маркером, однак традиційна модель цього не передбачає.

Техніка T1003 (Credential Dumping). Red Team отримує хеші паролів або самі паролі з пам'яті процесу LSASS, використовуючи Mimikatz або альтернативні методи (rundll32.exe, comsvcs.dll). SOC покладається на спрацювання EDR-сигнатур та події Windows Event ID 4656, 4663. На практиці Red Team часто застосовує методи, відсутні в сигнатурній базі, або ж EDR блокує атаку, але Red Team не отримує повідомлення про блокування. Унаслідок цього Red Team фіксує у звіті «атака успішна», а SOC вважає, що «захист спрацював». Без спільного аналізу неможливо встановити, чи атаку дійсно було зупинено, чи

Red Team просто не помітив блокування. Розрив полягає в неузгодженості оцінок та відсутності зворотного зв'язку між командами.
Аналіз трьох наведених прикладів дозволяє виявити закономірність: розриви виникають не через недостатню кваліфікацію окремих команд, а є наслідком системної проблеми – відсутності спільного планування, інтеграції даних у реальному часі та єдиної системи метрик. Кожна техніка MITRE ATT&CK ілюструє, як організаційні, технологічні та метричні бар'єри перетворюються на реальні прогалини в захисті. Доки Red Team та SOC працюють ізольовано, ці прогалини будуть відтворюватися.
Таким чином, традиційна модель взаємодії є неефективною. Без координації неможливо оцінити реальну ефективність детектів та вибудувати систему постійного вдосконалення. Наступний розділ присвячено практичному впровадженню Purple Teaming – сервісної моделі, що долає описані вище розриви.

Висновки до розділу 2

Отже, ми розібралися з тим, що заважає Red Team та SOC працювати разом. І тут, чесно кажучи, проблем виявилося більше, ніж можна було очікувати. Вони не технічні, не організаційні та навіть не метричні окремо – вони всі разом, переплетені один з одним.

Перше, що впадає в око – це організаційні бар'єри. Уявіть собі: SOC має одні KPI (швидше виявити, швидше відреагувати), а Red Team – зовсім інші (довше залишатися непоміченим, більше цілей скомпрометувати). Вони прямо суперечать одне одному. Хто захоче співпрацювати, якщо успіх одного автоматично означає провал іншого? До цього додаються розділені бюджети – у кожного своя стаття витрат, своє керівництво, своя звітність. І навіть культура в багатьох компаніях формує вороже ставлення: мовляв, Red Team – це ті, хто показує наші слабкі місця. Така атмосфера – не просто перешкода, а справжній глухий кут для будь-якої координації.

Далі – технології. SOC сидить на SIEM, збирає логи з усієї інфраструктури. Red Team користується C2-фреймворками – Cobalt Strike, Sliver, Caldera. Ці два світи майже не перетинаються. Логи атак Red Team не потрапляють в SIEM, а якщо й потрапляють – то постфактум, коли контекст вже втрачено. Немає уніфікованих API, немає стандартних форматів. Інтеграція – це завжди ручна робота або дорогі костилі. До того ж, Red Team використовує ті самі техніки, що й реальні зловмисники. Якщо SOC дозволяє Red Team працювати без блокувань, то створюються «білі списки», якими можуть скористатися хакери. Якщо блокує – Purple Teaming вправа стає неможливою. Технологічне протиріччя, яке неможливо вирішити без спеціальних політик та ізольованих середовищ.

Третя група проблем – метрики. Тут все ще цікавіше. SOC вимірює час виявлення, час реагування, кількість оброблених сповіщень. Red Team – успішність атак, час непоміченості. Це різні одиниці вимірювання, різні часові горизонти, різне розуміння «успіху». А найголовніше – немає жодної метрики, яка б оцінювала саме координацію. Скільки атак Red Team було виявлено SOC? Який відсоток рекомендацій впроваджено? Як швидко після вправи з'явилися нові детекти? На ці питанці ніхто не відповідає. А без вимірювань будь-яке вдосконалення – це пальцем у небо.

Щоб не бути голослівними, ми розглянули три конкретні техніки з MITRE ATT&CK. PowerShell (T1059.001) показав, як обфускація та вимкнене логування роблять атаку невидимою. SMB/Admin Shares (T1021.002) продемонстрував, як важко відрізнити контрольовану атаку від легітимної адміністративної активності. А Credential Dumping (T1003) – як відсутність зворотного зв'язку призводить до взаємно протилежних оцінок однієї й тієї ж події. Кожен приклад – це не абстрактна теорія, а реальна прогалина, яка виникає знову і знову в компаніях, де Red Team та SOC працюють окремо.

Отже, головний висновок розділу такий. Традиційна модель взаємодії себе вичерпала. Вона не просто неефективна – вона створює ілюзію безпеки. Організація витрачає гроші на Red Team та SOC, але не отримує синергії.

Розриви залишаються розривами. І щоб їх подолати, потрібна зовсім інша парадигма – не ізоляція, а координація; не звіти постфактум, а зворотний зв'язок у реальному часі; не конфліктуючі KPI, а спільні метрики. Це підводить нас до наступного розділу, де ми розробимо практичну систему координації на основі сервісної моделі Purple Teaming.

Розділ 3 РОЗРОБЛЕННЯ СИСТЕМИ КООРДИНАЦІЇ RED TEAM ТА SOC НА ОСНОВІ PURPLE TEAMING

3.1 Сервісна модель Purple Teaming: процес від запиту SOC до сценарію Red Team

Для практичної реалізації координації між Red Team та SOC необхідний конкретний механізм, що базується на сервісній моделі Purple Teaming. Основна ідея цієї моделі полягає в трансформації ролі Red Team: вона перестає бути зовнішнім аудитором, який проводить разові перевірки, і стає внутрішнім сервісом для SOC. SOC, у свою чергу, отримує можливість у будь-який час ініціювати перевірку конкретного детекту, правила кореляції або процедури реагування. Процес реалізується через п'ять послідовних кроків.

Крок перший – формування запиту. Ініціатором виступає SOC. Аналітик SOC фіксує аномалію, наприклад, різке зростання кількості помилкових спрацьовувань за певною сигнатурою (SIEM генерує сповіщення «підозрілий запуск PowerShell», яке після розслідування виявляється результатом легітимної адміністративної діяльності). Аналітик висуває гіпотезу щодо необхідності перевірки здатності SOC виявляти певну техніку, наприклад, латеральне переміщення через протокол SMB. У сервісній моделі він ініціює запит до Purple Teaming. Запит має бути конкретним, наприклад: «запустити атаку за технікою T1021.002 на тестовому хості 10.10.0.42 з використанням облікових даних test_user». Деталізація запиту безпосередньо впливає на швидкість отримання результату.

Крок другий – узгодження та планування. Запит попередньо обробляється координатором Purple Teaming – окремою особою (у великих організаціях) або одним із старших аналітиків (як додаткова роль). Координатор перевіряє запит на відповідність політикам безпеки, оцінює потенційний вплив на продуктивність систем та ризики для критичної інфраструктури. Після підтвердження запит передається Red Team. На етапі планування Red Team спільно з SOC (через координатора) уточнюють параметри сценарію: варіант

техніки, необхідність обфускації, доцільність імітації поведінки конкретного APT-угруповання. Планування є спільним: SOC, як власник знань про слабкі місця детектів, бере участь у визначенні сценарію, а Red Team надає експертизу щодо можливих варіантів реалізації техніки, їх переваг та недоліків. Результатом є узгоджений план атаки (цілі, параметри, часові рамки).

Крок третій – запуск контрольованої атаки. Red Team виконує сценарій. На відміну від традиційної моделі, де SOC отримує інформацію про атаку постфактум, у сервісній моделі реалізується технологічна інтеграція: логи C2-фреймворку Red Team у реальному часі надсилаються до SIEM SOC. Аналітики SOC спостерігають за генерацією подій, спрацюванням (або неспрацюванням) правил кореляції. У разі відхилень від плану (наприклад, блокування атаки EDR раніше очікуваного терміну) Red Team може оперативно скоригувати дії, а SOC фіксує цей факт для подальшого аналізу.

Крок четвертий – фіксація результатів та зворотний зв'язок. Після завершення атаки Red Team готує стислий звіт (1-2 сторінки), який містить опис запущеного сценарію, згенеровані події, зафіксовані SOC (або ті, що пройшли непоміченими). SOC додає власні спостереження: отримані сповіщення, витрачений час на аналіз, наявність помилкових спрацьовувань. Звіт є робочим документом, на основі якого приймаються рішення про внесення змін (нове правило кореляції, зміна порогів спрацьовування, оновлення конфігурації EDR, додаткове навчання аналітиків).

Крок п'ятий – вдосконалення та повторення. Ключовою характеристикою сервісної моделі є циклічність: запит – атака – звіт – зміни – новий запит. Purple Teaming не обмежується одноразовими вправами, а є безперервним процесом. З часом у SOC формується бібліотека тестів – набір сценаріїв, що можуть запускатися автоматично (наприклад, регресійне тестування після оновлення SIEM для перевірки працездатності існуючих детектів).

Для ефективного функціонування сервісної моделі необхідне виконання трьох передумов. По-перше, керівництво має змінити систему KPI: оцінювання SOC виключно за швидкістю виявлення є неприйнятним, якщо Red Team навмисно

намагається бути непомітним. Необхідне впровадження спільних метрик (розглянуто в підрозділі 3.4). По-друге, технологічна інтеграція: логи C2-фреймворків мають надсилатися до SIEM у реальному часі, що потребує додаткових налаштувань, придбання спеціальних плагінів або розробки власних скриптів. По-третє, зміна корпоративної культури: SOC не повинен сприймати Red Team як загрозу, а Red Team не має розглядати SOC як перешкоду; обидві команди мають бачити одна в одній інструмент для взаємного вдосконалення.

Приклад функціонування моделі: SOC отримує нове правило виявлення DNS-тунелювання від постачальника SIEM. Для перевірки його працездатності SOC надсилає запит на емуляцію DNS-тунелювання на тестовому сервері. Red Team протягом 15 хвилин готує сценарій (наприклад, з використанням інструментів Iodine або dnscat2) та запускає його. SOC фіксує наявність або відсутність сповіщення. У разі відсутності проводиться аналіз причин (ненадходження логів, завищені пороги, невідповідність правила конкретному середовищу). Весь цикл займає години замість тижнів.

Таким чином, сервісна модель Purple Teaming являє собою чіткий повторюваний процес: запит від SOC → планування → контрольована атака → зворотний зв'язок → вдосконалення. Її впровадження потребує змін на організаційному, технологічному та культурному рівнях. Без цього традиційна модель приречена на збереження розривів, описаних у другому розділі. Наступний підрозділ присвячено вибудовуванню життєвого циклу координації як постійно діючого процесу.

3.2 Життєвий цикл координації (планування, проведення, аналіз, вдосконалення)

Для перетворення Purple Teaming з разової акції на постійно діючий процес необхідне впровадження чіткого життєвого циклу координації, який

включає чотири фази, що повторюються: планування, проведення, аналіз та вдосконалення. Перша фаза – планування – починається з формулювання гіпотези SOC, наприклад: «SIEM-кореляція не фіксує латеральне переміщення через WMI, необхідно перевірити техніку T1047». Red Team оцінює необхідний час, інструменти та потребу в ізольованому середовищі. Спільно визначаються критерії успіху (наприклад, отримання сповіщення SOC протягом визначеного часу, блокування процесу EDR або факт генерації події в SIEM), які мають бути чіткими та не допускати неоднозначного тлумачення. На цій фазі також узгоджується графік проведення атаки (як правило, у нічний час або під час вікон технічних робіт, щоб уникнути впливу на критичні сервіси). Друга фаза – проведення – передбачає безпосередній запуск сценарію Red Team з паралельним спостереженням SOC. Обов'язковими умовами є наявність швидкого каналу зв'язку між командами (для негайного зупинення атаки у разі відхилень), фіксація всіх дій з обох боків (команд Red Team, запитів до C2, сповіщень та розслідувань SOC) для подальшого аналізу, а також обмеження тривалості атаки кількома годинами (оскільки довготривалі сценарії знижують увагу та ефективність команд). Третя фаза – аналіз – проводиться безпосередньо після завершення атаки (бажано того ж дня) за участі представників Red Team, SOC та незалежного модератора. Учасники розбирають хронологію подій, виявляють розриви (наприклад, причини ненадходження події до аналітика: перевантаження SIEM, завищений поріг спрацьовування, людський фактор), а результатом стає короткий перелік дій (5-7 пунктів), таких як додавання нового правила кореляції, збільшення частоти збору логів або проведення тренінгів. Четверта фаза – вдосконалення – передбачає реалізацію складеного переліку дій із закріпленням відповідальних осіб (адміністратор SOC – за зміни в SIEM, інженер безпеки – за оновлення політик EDR, менеджер з навчання – за тренінги) та встановленням термінів виконання. Через два тижні або місяць проводиться повторна перевірка (регресійний тест) шляхом запуску тієї ж атаки; якщо проблему не вирішено, цикл повторюється. Життєвий цикл не обов'язково є лінійним: складні

проблеми можуть виноситися до окремого проекту (беклогу), а прості зміни (наприклад, коригування порогу спрацьовування в SIEM) впроваджуються негайно. Приклад реалізації циклу: SOC фіксує 90% помилкових спрацьовувань правила виявлення SMB-атак (T1021) та висуває гіпотезу про занижений поріг або наявність зайвих подій у кореляції; Red Team запускає три варіації атаки (дві не виявлено, одна виявлена із запізненням 20 хвилин); аналіз виявляє відсутність збору логів з певних контролерів домену; після внесення змін (додавання логів, зміна правила кореляції) повторний тест через місяць демонструє виявлення всіх трьох варіацій за 2 хвилини. Таким чином, життєвий цикл Purple Teaming є системним підходом, у якому планування без проведення є неефективним, проведення без аналізу – безглуздим, а аналіз без вдосконалення – лише фіксацією проблем. Лише за умови комплексної реалізації всіх чотирьох фаз забезпечується постійне підвищення рівня кіберстійкості, що корелює з циклом Демінга (PDCA) – плануй, виконуй, перевіряй, дій.

3.3 Ролі та зони відповідальності в межах Purple Teaming

Для ефективного функціонування Purple Teaming необхідний чіткий розподіл ролей, оскільки відсутність такої структури призводить до розмивання відповідальності та зниження результативності спільних вправ. Purple Teaming не передбачає створення окремого структурного підрозділу («фіолетової команди»); натомість це рольова модель, що реалізується фахівцями Red Team та SOC під час спільних заходів. Визначення наступних ролей є обов'язковим для забезпечення передбачуваності та ефективності координації.

Перша ключова роль – координатор Purple Teaming. В окремих випадках це може бути не окрема штатна одиниця, а особа, що виконує відповідні функції в межах своїх обов'язків. Координатор отримує запит від SOC, перевіряє його коректність, передає Red Team, контролює дотримання графіку, організовує наради та виступає арбітром у разі виникнення суперечок

(наприклад, щодо факту виявлення атаки). Оптимальним є призначення координатора, який має досвід як у наступальних, так і в захисних практиках; за відсутності такого фахівця допускається залучення досвідченого менеджера з кібербезпеки, що не належить ні до Red Team, ні до SOC, що забезпечує його нейтральність. Друга роль – аналітик SOC рівня Tier 2 або Tier 3. Цей фахівець виступає від імені «синіх», формулюючи гіпотезу для перевірки. Саме аналітик, який щоденно працює з детектами, а не його керівник, найкраще розуміє слабкі місця системи виявлення. Його завдання полягає у складанні запиту зрозумілою Red Team мовою, наприклад: «перевірити правило кореляції №471, яке має спрацьовувати на подію 4688 з певними аргументами, але на практиці не спрацьовує». Під час проведення атаки аналітик SOC спостерігає за SIEM, коментує результати, а після завершення бере участь у розборі. Аналітики рівня Tier 1 можуть бути присутні як спостерігачі, але не приймати рішень. Третя роль – оператор Red Team, який безпосередньо реалізує сценарій атаки. Він отримує від координатора сценарій, готує необхідні інструменти та виконує команди. На відміну від традиційного Red Teaming, де пріоритетом є непомітність, у рамках Purple Teaming оператор працює в режимі «прозорості» – він знає, що SOC спостерігає, і може інформувати про свої дії (наприклад, «зараз буде використано техніку T1059.001 з обфускацією»), але не розкриває всіх деталей наперед, щоб не втрачався сенс тестування. Оператор Red Team відповідає за реалістичну імітацію поведінки зловмисника без приховування своїх дій від координатора та аналітиків, а також за негайне зупинення атаки у разі виникнення небезпеки для інфраструктури. Четверта роль – технічний адміністратор (інженер безпеки). Цей фахівець не бере безпосередньої участі в атаці, але забезпечує внесення змін за результатами аналізу. Наприклад, після виявлення проблеми (відсутність логування на певному сервері) саме інженер безпеки налаштовує політики, додає правила кореляції, оновлює конфігурації EDR та забезпечує ізоляцію тестового середовища від продуктивного у разі проведення атак поза бойовими системами. Без його участі будь-які рекомендації залишаються нереалізованими. П'ята роль – керівник (CISO або

керівник SOC/Red Team). Він не втручається в операційну діяльність, але виконує дві ключові функції: затверджує правила проведення вправ (наприклад, можливість атак на продуктивних системах, необхідність ізольованого середовища) та змінює систему KPI та бюджети, якщо Purple Teaming потребує додаткових ресурсів. Підтримка керівництва є критично важливою, оскільки без неї навіть найкращий координатор не матиме достатнього впливу. Зони відповідальності розподіляються наступним чином: координатор відповідає за загальну організацію процесу (передавання запитів, проведення атак, організація розборів, фіксація рішень); аналітик SOC – за якість гіпотези та коректну інтерпретацію результатів; оператор Red Team – за реалізацію сценарію та безпеку атаки; інженер безпеки – за впровадження змін і стан технічної інфраструктури; керівник – за ресурси, політики та усунення організаційних бар'єрів. Відсутність чіткого розподілу ролей призводить до типових проблем: неоформлений запит залишається поза увагою Red Team, відсутність координатора породжує суперечки щодо необхідності перевірки, незалучення інженера безпеки унеможливлює впровадження змін, а незмінені KPI демотивують аналітиків SOC витрачати час на Purple Teaming. Ротація ролей (періодична зміна аналітика SOC, який формулює гіпотези, або тимчасове виконання оператором Red Team ролі спостерігача з боку SOC) сприяє покращенню взаєморозуміння між командами, однак є ознакою високого рівня зрілості організації. Таким чином, Purple Teaming не потребує створення нової команди, але вимагає чіткого призначення відповідальних осіб на всіх зазначених ролях, оскільки без цього навіть найкращі технології та процеси не забезпечать ефективної координації.

3.4 Узгоджена система метрик (спільні KRI/KPI для Red Team та SOC)

Однією з головних проблем традиційної моделі є використання різних, часто суперечливих ключових показників ефективності (KPI) для SOC та Red

Team: SOC орієнтується на час виявлення (MTTD), а Red Team – на час непомітності, що створює фундаментальний конфлікт інтересів, який не усувається навіть за наявності координатора, визначених ролей та технологічної інтеграції. Для подолання цього конфлікту необхідна система спільних метрик, що вимірюють успіх Purple Teaming в цілому, а не окремо кожної команди. Першою такою метрикою є «час верифікації детекту» замість традиційного MTTD: Red Team запускає атаку, SOC фіксує подію, а вимірюється інтервал від моменту атаки до моменту, коли аналітик SOC підтвердив коректне спрацювання детекту. Ця метрика враховує якість виявлення (оскільки сповіщення може бути помилковим або проігнорованим) і покладає спільну відповідальність на обидві команди. Друга метрика – «відсоток атак Red Team, виявлених SOC», який розраховується як відношення кількості підтверджених виявлень (після розслідування аналітиком) до загальної кількості проведених сценаріїв. Цей показник відображає повноту покриття детектами SOC тих тактик, технік та процедур (TTPs), які імітує Red Team; низьке значення свідчить про наявність серйозних прогалин. Третя метрика – «час створення нового детекту після виявлення прогалини» – вимірює повний цикл вдосконалення: від моменту, коли Purple Teaming виявив нездатність SOC виявляти певну техніку, до моменту, коли нове правило кореляції або зміна конфігурації EDR була перевірена повторною атакою. Велике значення цієї метрики вказує на проблеми в процесі впровадження змін. Четверта метрика – «відсоток рекомендацій Red Team, впроваджених SOC» – оцінює, яка частка наданих Red Team рекомендацій реально реалізована та працює (а не лише запланована до впровадження); низький відсоток є індикатором організаційно-культурних проблем, а не технічних. П'ята метрика – «вартість Purple Teaming на один покращений детект», що розраховується як відношення загальних витрат (людино-годин на планування, проведення атаки, аналіз та впровадження змін) до кількості реально покращених детектів або закритих прогалин; висока вартість сигналізує про надмірну бюрократизацію, складність сценаріїв або недостатню автоматизацію. Шоста метрика –

«задоволеність команд», яка визначається шляхом анонімного опитування учасників Purple Teaming (не рідше одного разу на квартал) і дозволяє виявити вигорання, зниження віри в ефективність вправ або інші суб'єктивні фактори, що впливають на якість координації. Всі ці метрики мають використовуватися не для звітності перед керівництвом або покарання команд, а для прийняття рішень: низький відсоток виявлення є підставою для зміни налаштувань, великий час створення детекту – для оптимізації процесу внесення змін, висока вартість – для автоматизації рутинних операцій. Впровадження системи слід починати з двох-трьох найбільш проблемних для організації показників (наприклад, часу верифікації при перевантаженні SOC або відсотка впровадження при ігноруванні рекомендацій), фіксуючи базові значення та відстежуючи динаміку (наприклад, зменшення часу верифікації з 48 до 6 годин за півроку). Важливо не порівнювати власні метрики з галузевими середніми, які не враховують контекст (розмір компанії, складність інфраструктури, кількість аналітиків), а орієнтуватися виключно на власний прогрес. Крім того, слід уникати «підкручування цифр» (наприклад, маркування всіх сповіщень як підтверджених або вибір легких сценаріїв Red Team) – метрики мають бути прозорими, автоматизованими та, головне, не пов'язаними безпосередньо з системою преміювання, а використовуватися як інструмент самодіагностики для спільного виявлення та усунення причин погіршення показників. Таким чином, спільна система метрик перетворює Purple Teaming з цікавої вправи на керований процес вдосконалення; рекомендований мінімальний набір показників для початку включає шість позицій: час верифікації детекту, відсоток виявлених атак, час створення нового детекту, відсоток впроваджених рекомендацій, вартість на один покращений детект та задоволеність команд.

3.5 Практичні рекомендації щодо впровадження системи координації

На основі проведеного аналізу процесів, ролей та метрик сформульовано практичні рекомендації для організацій, які не мають впровадженої системи

Purple Teaming або налагодженої координації між Red Team та SOC. Рекомендується починати з малої пілотної вправи, обравши один найпростіший сценарій (наприклад, перевірку виявлення SOC обфускованого запуску PowerShell) за участю одного аналітика SOC та одного оператора Red Team на тестовому сервері з мінімальним документуванням. Необхідно призначити координатора, бажано з числа осіб, які не належать до жодної з команд, але мають повноваження організовувати спільні заходи та контролювати виконання домовленостей. Слід враховувати людський фактор: перед першою вправою доцільно провести нараду, на якій керівництво підкреслить, що метою є виявлення слабких місць, а не пошук винних, а після вправи – публічно подякувати обом командам. Автоматизацію варто впроваджувати поступово, починаючи з експорту логів C2-фреймворку до SIEM; у разі технічних труднощів допустиме проведення спільних сесій із демонстрацією екрану Red Team та коментарями SOC. Збір спільних метрик (час на планування, кількість проведених та виявлених атак, кількість рекомендацій) слід розпочинати з першого дня, фіксуючи навіть нульові показники як точку відліку. Проведення Purple Teaming на продуктивних системах доцільно розпочинати лише після відпрацювання в тестовому середовищі – окремому сегменті мережі з віртуальними машинами, що імітують типову інфраструктуру. Документування кожної вправи має обмежуватися одним аркушем формату A4, який містить опис виконаних дій, виявлені проблеми, необхідні зміни, відповідальних осіб та терміни. Після кожної вправи обов'язково проводиться короткий розбір (post-mortem) тривалістю до 30 хвилин із почерговим висловленням вражень та пропозицій щодо покращень, фіксуючи реальні зміни, внесені після попередньої вправи. Масштабування слід здійснювати поступово, залучаючи спочатку 2-3 ентузіастів з кожної сторони, які стануть «агентами змін», а після демонстрації результатів інші співробітники приєднаються самостійно. Необхідно отримати підтримку керівництва – достатньо публічного визнання CISO пріоритетності Purple Teaming та закріплення цього у внутрішніх політиках, оскільки без такої підтримки ініціативи знизу виявляються

неефективними. Слід уникати типових помилок: перетворення Purple Teaming на разову акцію (регулярність має бути не менше одного разу на місяць), концентрації виключно на технічних атаках (потребують уваги також соціальна інженерія та внутрішні загрози), ігнорування «легких перемог» (навіть очевидні усунені прогалини є успіхом) та, найголовніше, відсутності зворотного зв'язку між вправами (якщо аналітики SOC не бачать впливу своїх зауважень на налаштування, вони перестають їх висловлювати). У підсумку, успішне впровадження Purple Teaming вимагає початку з малого, регулярності, вимірювання прогресу, терпимості до помилок та формування культури безпеки без звинувачень, що дозволяє перетворити Purple Teaming з разового проекту на постійно діючий процес у зрілій організації.

Висновки до розділу 3

У третьому розділі ми детально розробили практичну систему координації Red Team та SOC на основі сервісної моделі Purple Teaming, і тепер можна підбити підсумки.

По-перше, ми запропонували конкретний механізм роботи – від запиту SOC до сценарію Red Team, який включає п'ять кроків: народження запиту, узгодження та планування, запуск контрольованої атаки, фіксацію результатів із зворотним зв'язком, а також цикл вдосконалення та повторення. Цей механізм перетворює Purple Teaming з абстрактної ідеї на повторюваний процес, де SOC виступає замовником, а Red Team – внутрішнім сервісом емуляції загроз.

По-друге, ми описали життєвий цикл координації, який складається з чотирьох фаз – планування, проведення, аналізу та вдосконалення, – і наголосили, що без регулярного повторення цих фаз будь-яка разова вправа не дасть стійкого ефекту.

По-третє, ми визначили ключові ролі та зони відповідальності: координатор Purple Teaming (нейтральний арбітр), аналітик SOC Tier 2/3

(формулює гіпотези), оператор Red Team (реалізує сценарій), інженер безпеки (впроваджує зміни) та керівник (забезпечує ресурси та знімає організаційні бар'єри). Без чіткого розподілу ролей навіть найкращі технології не запрацюють.

По-четверте, ми запропонували узгоджену систему метрик, яка долає конфлікт традиційних KPI: час верифікації детекту (а не просто MTTD), відсоток атак Red Team, виявлених SOC, час створення нового детекту після виявлення прогалини, відсоток впроваджених рекомендацій, вартість Purple Teaming на один покращений детект та суб'єктивна задоволеність команд. Ці спільні показники дозволяють оцінювати прогрес і керувати процесом вдосконалення.

По-п'яте, ми сформулювали десять практичних рекомендацій для впровадження: починати з малої пілотної вправи, призначити координатора (навіть як роль), враховувати людський фактор і культуру без звинувачень, автоматизувати поступово, збирати метрики з першого дня, використовувати тестове середовище, документувати коротко (один аркуш), проводити швидкі розбори після кожної вправи, масштабувати поступово через ентузіастів і обов'язково отримати підтримку керівництва. Усі ці рекомендації спрямовані на подолання організаційних, технологічних та метричних бар'єрів, які ми виявили в другому розділі. Таким чином, розроблена система координації є цілісною, практично орієнтованою та може бути адаптована для підприємств різного розміру та рівня зрілості. Головний висновок розділу полягає в тому, що Purple Teaming – це не просто технічна вправа, а комплексна зміна в управлінні кібербезпекою, яка вимагає нових процесів, ролей, метрик і, найголовніше, культури співпраці замість суперництва

ВИСНОВКИ

У кваліфікаційній роботі вирішено актуальне науково-прикладне завдання – розроблено систему координації взаємодії команд Red Team та SOC у межах сервісної моделі Purple Teaming.

По-перше, проаналізовано теоретичні засади функціонування SOC та Red Team. Встановлено, що SOC є централізованим підрозділом, який виконує функції безперервного моніторингу, виявлення інцидентів, реагування та проактивного пошуку загроз, тоді як Red Team виступає як контрольований супротивник, що здійснює емуляцію загроз, тестування детектів та комплексну оцінку захищеності. Традиційна модель взаємодії, заснована на ізольованій роботі та передачі звітів постфактум, характеризується розривами в комунікації, технологічній несумісності та конфлікті показників ефективності. Purple Teaming, своєю чергою, є сервісною моделлю координації, яка базується на принципах спільного планування, зворотного зв'язку в реальному часі, технологічній інтеграції та спільних метриках.

По-друге, виявлено та систематизовано основні бар'єри координації. Організаційні бар'єри включають конфліктуючі KPI (SOC зацікавлений у швидкому виявленні, Red Team – у тривалій непомітності), розділені бюджети та різні системи звітності, що створює атмосферу суперництва замість співпраці. Технологічні бар'єри полягають у використанні різних платформ (SIEM для SOC, C2-фреймворки для Red Team), відсутності інтеграції між ними та проблемах безпечного обміну даними, що унеможливлює отримання SOC повної картини атаки в реальному часі. Метричні бар'єри виявляються у відсутності спільних показників оцінки ефективності координації, різних часових горизонтах вимірювань та ігноруванні якісних змін. На прикладі модельних атак за техніками MITRE ATT&CK (T1059.001 PowerShell, T1021.002 SMB, T1003 Credential Dumping) наочно продемонстровано, як ці бар'єри призводять до конкретних розривів: невиявлені атаки, втрата контексту, неузгодженість оцінок та запізнілий зворотний зв'язок.

По-третє, розроблено систему координації на основі сервісної моделі Purple Teaming. Запропоновано механізм роботи від запиту SOC до сценарію Red Team, який включає п'ять кроків: народження запиту, спільне планування, запуск контрольованої атаки з інтеграцією логів у SIEM, фіксацію результатів та цикл вдосконалення. Описано життєвий цикл координації з чотирьох фаз – планування, проведення, аналізу та вдосконалення. Визначено ключові ролі та зони відповідальності: координатор Purple Teaming (нейтральний арбітр), аналітик SOC Tier 2/3 (формулює гіпотези), оператор Red Team (реалізує сценарій), інженер безпеки (впроваджує зміни) та керівник (забезпечує ресурси та знімає організаційні бар'єри). Запропоновано узгоджену систему спільних метрик: час верифікації детекту, відсоток атак Red Team, виявлених SOC, час створення нового детекту після виявлення прогалини, відсоток впроваджених рекомендацій, вартість Purple Teaming на один покращений детект та задоволеність команд.

Надано практичні рекомендації щодо впровадження: починати з пілотної вправи, призначити координатора, враховувати людський фактор, автоматизувати поступово, збирати метрики з першого дня, використовувати тестове середовище, документувати коротко, проводити швидкі розбори, масштабувати через ентузіастів та отримати підтримку керівництва. Практична значущість роботи полягає в тому, що запропонована система координації дозволяє підприємствам підвищити ефективність виявлення кібератак, зменшити час верифікації детектів, усунути «сліпі зони» в моніторингу та створити культуру співпраці замість суперництва між командами нападу та захисту. Розроблені підходи можуть бути використані при побудові або вдосконаленні центрів кібербезпеки (SOC), проведенні Purple Team вправ на підприємствах різних галузей, а також у навчальних цілях при підготовці фахівців з кібербезпеки.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013, IDT). [Чинний від 2016-07-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2016. 28 с.
2. NIST Special Publication 800-61. Computer Security Incident Handling Guide. National Institute of Standards and Technology, 2012. 147 p.
3. NIST Special Publication 800-53. Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology, 2020. 462 p.
4. NIST Special Publication 800-115. Technical Guide to Information Security Testing and Assessment. National Institute of Standards and Technology, 2008. 80 p.
5. MITRE ATT&CK Framework. Enterprise Matrix. Version 15. URL: https://attack.mitre.org (дата звернення: 15.05.2026).
6. SOC-CMM. Security Operations Center Capability Maturity Model. Version 2.0. Amsterdam : Security Operations Center Institute, 2020. 55 p.
7. Red Canary. Purple Team Playbook. 2023. URL: https://redcanary.com/purple-team-playbook (дата звернення: 10.05.2026).
8. SANS Institute. 2025 SOC Survey: Key Findings and Trends. Bethesda : SANS, 2025. 34 p. Bishop Fox. Sliver C2 Framework Documentation. 2024. URL: https://github.com/BishopFox/sliver (дата звернення: 12.05.2026).
9. Cobalt Strike. User Manual. HelpSystems, 2024. 210 p.
10. MITRE CALDERA. Automated Adversary Emulation Platform. GitHub repository. URL: https://github.com/mitre/caldera (дата звернення: 14.05.2026).
11. Crowdstrike. Purple Teaming: A Guide to Improving Detection. 2023. URL: https://www.crowdstrike.com/cybersecurity-101/purple-teaming (дата звернення: 10.05.2026).
12. Mandiant. Red Team vs. Blue Team: What's the Difference? 2022. URL: https://www.mandiant.com/resources/red-team-vs-blue-team (дата звернення: 11.05.2026).

13. Palo Alto Networks. Unit 42: Purple Teaming Best Practices. 2024. URL: https://unit42.paloaltonetworks.com/purple-teaming (дата звернення: 12.05.2026).
14. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. Geneva : ISO, 2022. 92 p.
15. Шевченко О. В. Управління кібербезпекою підприємства: моделі та методи. Київ : КПІ ім. Ігоря Сікорського, 2023. 280 с.
16. Литвиненко В. А. Основи побудови центрів моніторингу кібербезпеки. Харків : ХНУРЕ, 2022. 210 с.
17. Савченко М. І. Інструменти емуляції супротивника в кібербезпеці. Львів : Видавництво Львівської політехніки, 2024. 185 с.
18. NIST Cybersecurity Framework. Version 1.1. National Institute of Standards and Technology, 2018. 58 p.
19. Lockheed Martin. Cyber Kill Chain. URL: https://www.lockheedmartin.com/cyber-kill-chain (дата звернення: 15.05.2026).
20. Tounsi W. Cyber-Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT. London : ISTE Press, 2019. 250 p.
Sanders C., Smith J. Applied Network Security Monitoring. Boston : Syngress, 2014. 470 p.
21. Kovacevic A., Putnik Z. Purple Teaming: A Systematic Approach to Improving Detection Capabilities. Journal of Cybersecurity Research, 2023. Vol. 12, No. 3. P. 45–62.
22. Петренко С. В. Показники ефективності SOC: MTTD та MTTR. Кібербезпека: теорія та практика. 2024. № 2. С. 23–31.
23. Гончар О. І. Роль Red Team в оцінці стійкості інформаційних систем. Захист інформації. 2025. Т. 27, № 1. С. 12–19.
24. Brown J., Williams R. Measuring Purple Team Effectiveness: A Metrics Framework. Proceedings of the 15th International Conference on Cyber Security (ICCS 2024). New York, 2024. P. 88–95.

25. Державний університет інформаційно-комунікаційних технологій. Методичні рекомендації до виконання кваліфікаційних робіт. Київ : ДУІКТ, 2025. 42 с.
26. ENISA. Cybersecurity Maturity Assessment for Enterprises. European Union Agency for Cybersecurity, 2023. 120 p.
27. Check Point. 2025 Security Report. Tel Aviv : Check Point Software Technologies, 2025. 68 p.
28. Kaspersky Lab. Global SOC Survey 2024. Moscow : Kaspersky, 2024. 45 p.
FireEye. Red Teaming vs. Penetration Testing. Milpitas : FireEye, 2021. 20 p.
Kouremetis C. Purple Teaming: Bridging the Gap Between Red and Blue. SANS Institute Reading Room, 2022. 32 p.
29. Ryan J. Mitigating Alert Fatigue in Security Operations Centers. SANS Institute, 2023. 28 p.
30. Applebaum A. A Guide to Threat Hunting. SANS Institute, 2021. 40 p.
31. Морозов В. В. Автоматизація процесів реагування на інциденти в SOC. 32. Безпека інформації в інформаційно-телекомунікаційних системах : матеріали XVI Міжнар. наук.-практ. конф. Київ, 2025. С. 112–115.
33. Калініченко Д. О. Інтеграція Threat Intelligence в роботу SOC. Актуальні питання кібербезпеки : зб. наук. пр. Харків, 2024. С. 78–82.
34. Олійник Т. В. Організаційні моделі SOC: порівняльний аналіз. Управління інформаційною безпекою. 2024. № 4. С. 44–51.
35. MITRE Engage. A Framework for Adversary Engagement. 2022. URL: https://engage.mitre.org (дата звернення: 16.05.2026).
36. TheHive Project. TheHive Documentation. URL: https://thehive-project.org (дата звернення: 14.05.2026).
37. MISP Project. Malware Information Sharing Platform. URL: https://www.misp-project.org (дата звернення: 14.05.2026).
38. Глущенко О. В. Культура кібербезпеки: людський фактор в координації команд. Кіберстійкість підприємства : матеріали Всеукр. наук.-практ. конф. Київ, 2025. С. 34–38.

39. Корнієнко А. М. Метрики ефективності для Purple Teaming. Сучасний стан та перспективи розвитку кібербезпеки : тези доп. II Міжнар. наук.-техн. конф. Львів, 2025. С. 56–58.
40. Черненко Ю. В. Роль CISO в організації взаємодії Red Team та Blue Team. Стратегії кіберстійкості : зб. матеріалів конф. Київ : ДУІКТ, 2026. С. 22–25.
Kovalenko S., Bondarenko O. A Framework for Purple Teaming in Critical Infrastructure. Cybersecurity and Critical Infrastructure Protection, 2025. Vol. 8. P. 15–29.
41. ISO/IEC 27035:2022. Information technology — Information security incident management. Geneva : ISO, 2022. 60 p.