**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**
**КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ**

# КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Система ситуативної обізнаності: аналіз логів і виявлення аномалій мережі на базі хмарної платформи Google Cloud»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерна інженерія
*(код, найменування спеціальності)*
Освітньо-професійної програми Комп'ютерна інженерія
*(назва)*

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

*(підпис)* Денис РЕКУН
*Ім'я ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КІД-41
Денис РЕКУН
Ім'я ПРІЗВИЩЕ

Керівник: Борис КОНДРАТЮК,
*науковий ступінь, вчене звання* Ім'я ПРІЗВИЩЕ

Рецензент: _____
*науковий ступінь, вчене звання* Ім'я ПРІЗВИЩЕ

**Київ 2024**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**Навчально-науковий інститут Інформаційних технологій**

Кафедра 123 Комп'ютерної інженерії
Ступінь вищої освіти бакалавр
Спеціальність 123 Комп'ютерна інженерія
Освітньо-професійна програма Комп'ютерна інженерія

**ЗАТВЕРДЖУЮ**
Завідувач кафедрою Наталія ЛАЩЕВСЬКА
Ім'я ПРІЗВИЩЕ
«_____» _____ 2024р.

# ЗАВДАННЯ
# НА КВАЛІФІКАЦІЙНУ РОБОТУ

Рекун Денис Сергійович
*(прізвище ім'я по батькові здобувача)*

1. Тема кваліфікаційної роботи: Система ситуативної обізнаності: аналіз логів і виявлення аномалій мережі на базі хмарної платформи Google Cloud

керівник кваліфікаційної роботи Борис КОНДРАТЮК,
*(Ім'я ПРІЗВИЩЕ, науковий ступінь, вчене звання)*

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 20 ___ р. № _____

2. Строк подання кваліфікаційної роботи «_____» _____ 20 24 р.

3. Вихідні дані до кваліфікаційної роботи: _____

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Основи ситуативної обізнаності
2. Ситуативна обізнаність в мережевому середовищі
3. Google Cloud

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання «_____» _____ 20 ___ р.

# КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Збір даних | 26.02-22.03.2024 | Виконано |
| 2 | Обробка матеріалу | 23.03-05.04.2024 | Виконано |
| 3 | Розробка теоретичної частини | 06.04-10.04.2024 | Виконано |
| 4 | Аналітична робота | 11.04-30.04.2024 | Виконано |
| 5 | Конструктивні пропозиції | 01.05-03.05.2024 | Виконано |
| 6 | Висновки за результатами аналізу | 04.05-08.05.2024 | Виконано |
| 7 | Розробка презентації | 09.05-12.05.2024 | Виконано |
| 8 | Передзахист | 13.05-17.05.2024 | |
| 9 | Здача в деканат | 27.05-03.06.2024 | |

Здобувач вищої освіти _____ Денис РЕКУН
*(підпис)* *(Ім'я ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Борис КОНДРАТЮК
*(підпис)* *(Ім'я ПРІЗВИЩЕ)*

# РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 50 сторінок, 15 рисунків, 3 таблиць, 23 джерел.

*Мета роботи* — дослідження позитивного впливу інтегрування систем ситуаційної обізнаності в мережеву аналітику, кібербезпеку. Розгляд доступності технологій ситуативної обізнаності для застосування під час експлуатації мережевої інфраструктури.

*Об'єкт дослідження* — адаптація загальних принципів ситуативної обізнаності до мережевого аналізу.

*Предмет дослідження* — ідентифікація та інформування про аномальну поведінку мережі на хмарній платформі Google Cloud.

*Короткий зміст роботи:* У цій публікації досліджується концепція ситуаційної обізнаності (СО) в контексті мережевої безпеки та виявлення аномалій на хмарній платформі Google (GCP). Адаптуючи існуючі моделі ситуаційної обізнаності, досліджується, як мережеві аналітики можуть використовувати хмарну інфраструктуру для покращення розуміння кіберзагроз та визначення пріоритетів реагування на них. Розглядаються складнощі ландшафту кіберзагроз, підкреслюється важливість збору даних, аналізу та етичних міркувань при моніторингу мереж.

У документі підкреслюється, що інтеграція людського досвіду з автоматизованими інструментами, особливо в інтерпретації мережевих потоків і виявленні аномалій, має вирішальне значення для ефективної СО. За допомогою практичних демонстрацій на GCP показано можливості хмарних віртуальних машин і механізмів ведення журналів для створення та виявлення аномальної поведінки. Ці приклади підкреслюють потенціал хмарних платформ у підтримці ініціатив з мережевої безпеки. На завершення пропонуються майбутні напрямки досліджень, включаючи вивчення передових методів виявлення аномалій,

алгоритмів машинного навчання і розробку комплексних фреймворків СО для конкретних мережевих середовищ. Це дослідження має на меті надати мережевим аналітикам інструменти та знання для проактивної протидії кіберзагрозам і забезпечення безпеки та стійкості цифрової інфраструктури.

КЛЮЧОВІ СЛОВА: СИСТЕМА СИТУАТИВНОЇ ОБІЗНАНОСТІ, МЕРЕЖЕВИЙ МОНІТОРИНГ, АНАЛІЗ ЛОГІВ, GOOGLE CLOUD, GCP

## ABSTRACT

The text part of the qualification work for the bachelor's degree include: _50_ pages, _15_ figures, _3_ tables, _23_ sources.

*The purpose of the work* is to study the positive impact of integrating situational awareness systems into network analytics and cybersecurity. Research of the availability of situational awareness technologies for use in the network infrastructure.

*The object of the study* is the adoption of general principles of situational awareness to network analysis.

*The subject of the study* Network security on Google Cloud Platform, including network traffic analysis and anomaly detection.

This paper explores the concept of situational awareness (SA) in the context of network security and anomaly detection on the Google Cloud Platform (GCP). By adapting existing models of situational awareness, it explores how network analysts can leverage cloud infrastructure to improve their understanding of cyber threats and prioritize their response. It discusses the complexities of the cyber threat landscape and emphasizes the importance of data collection, analysis, and ethical considerations when monitoring networks.

The paper emphasizes that the integration of human expertise with automated tools, especially in interpreting network flows and detecting anomalies, is critical to effective SA. Through hands-on demonstrations at GCP, the capabilities of cloud virtual machines and logging engines to generate and detect anomalous behavior are shown. These examples highlight the potential of cloud platforms to support network security initiatives. Finally, future research directions are proposed, including the study of advanced anomaly detection techniques, machine learning algorithms, and the development of comprehensive CO frameworks for specific network environments. This research aims to provide network analysts with the tools and knowledge to

proactively counter cyber threats and ensure the security and resilience of digital infrastructure.

KEYWORDS: SITUATIONAL AWARENESS SYSTEM, NETWORK MONITORING, LOG ANALYSIS, GOOGLE CLOUD, GCP

**ЗМІСТ**

# ВСТУП

За останні роки обізнаність громадськості про проблеми мережевої безпеки значно зросла. Незважаючи на найнадійніші захисні заходи, вразливість, притаманна мережевим системам, призводить до того, що відхилення від типової поведінки мережі є прикрою неминучістю. Як наслідок, фокус кібербезпеки змістився від суто реактивного захисту і тепер організації надають пріоритет розробці проактивних та інтелектуальних стратегій захисту, які дозволяють виявляти загрози на ранніх стадіях. Така еволюція в підходах має важливе значення для мінімізації потенційних втрат і захисту чутливих активів у цифрову епоху. Стрімке зростання Інтернету речей та хмарних технологій призводить до проривних інновацій, але також створює нові проблеми безпеки. Управління великою кількістю підключених пристроїв та сучасні методи атак, висувають все більші вимоги до фахівців, відповідальних за їхню захищеність. Підтримка безпеки в умовах такої комплексності вимагає не лише технічних навичок, але й глибокого розуміння людських обмежень адже вони повинні синтезувати величезні обсяги даних, щоб приймати обґрунтовані рішення під тиском обставин.

З точки зору дескриптивного прийняття рішень, достатня поінформованість щодо стану системи має першочергове значення для роботи інженера, що обслуговує її. Важливе усвідомлення потенціалу людської помилки (через такі індивідуальні фактори, як розсіяність уваги, втома або перенавантаження), а також факторів зовнішнього впливу. Перечислені фактори можуть перешкоджати якнайкращій ефективності виконання поставлених завдань та інтерпретації тривожних сигналів. Когнітивні обмеження в цих сферах безпосередньо впливають на здатність спеціаліста сприймати і формувати точне уявлення про робоче середовище. У відповідь на ці виклики, системи ситуаційної обізнаності стали важливими інструментами для підвищення ефективності роботи людини та зменшення стресу. Ці системи автоматизують і беруть на себе частину робочого навантаження, оптимізуючи процес прийняття рішень і роблячи об'єкт

спостереження більш прозорим. Полегшуючи когнітивне навантаження на людей, системи ситуаційної обізнаності дають їм змогу робити обґрунтований вибір і підтримувати чітке розуміння оперативної обстановки, що в кінцевому підсумку сприяє підвищенню безпеки системи і її загальної ефективності.

Система ситуаційної обізнаності в контексті мережевої безпеки поглинає широкий спектр вхідних даних для побудови комплексної картини мережевого середовища в реальному часі. Необроблений мережевий трафік, а також попередньо оброблені потоки та журнали з таких джерел, як “VPC Flow Logs” (у хмарному середовищі Google Cloud) є основним джерелом цієї інформації. Ці дані показують схеми зв'язку, адреси джерела і призначення, протоколи, що використовуються, і потенційні аномалії.

Сила системи ситуаційної обізнаності полягає в її здатності перетворювати необроблені вхідні дані у форму, зручну для сприйняття аналітиками. Обробляючи мережевий трафік, потоки, журнали та інші джерела даних, система виокремлює значущі закономірності і виділяє найважливіші ідеї. Цей фільтр складної інформації є фундаментальним для процесу візуалізації. Вони надають інтуїтивно зрозуміле, легко засвоюване уявлення про стан мережі, що дозволяє інженеру швидко визначати області, які потребують уваги. Ефективні графічні інтерпретації діють як когнітивні допоміжні засоби, зменшуючи розумове навантаження, пов'язане з інтерпретацією та кореляцією величезних обсягів даних. Це вивільняє когнітивні ресурси інженера для прийняття рішень і вирішення проблем на більш високому рівні.

Хоча складність вилучення цінної інформації з мережевих даних зазвичай обмежувала коло користувачів систем ситуаційної обізнаності лише добре забезпеченими організаціями, ця парадигма змінюється. Хмарні технології, особливо ті, що використовуються в рамках хмарної платформи Google, спрощують процес збору, аналізу і візуалізації даних. Ці доступні інструменти пом'якшують традиційні бар'єри, пов'язані з витратами і технічними знаннями. Тепер приватні особи і невеликі організації мають можливість забезпечити надійну ситуаційну

обізнаність, що дає їм змогу займати проактивну позицію в питаннях безпеки, яка раніше була притаманна лише великим підприємствам.

Враховуючи цей зсув у бік більшої доступності, я маю намір дослідити потенціал побудови системи ситуативної обізнаності про мережеву безпеку, спеціально адаптованої до моїх потреб, використовуючи можливості хмарної інфраструктури Google. Моя мета — використання таких інструментів, Kubernetes, Cloud Logging, Python Flask щоб отримати кращу видимість мережевої активності. Такий проактивний підхід дозволить мені більш ефективно виявляти та вирішувати потенційні проблеми безпеки, захищаючи свої мережеві активи та забезпечуючи оптимальний захист даних.

# 1 ОСНОВИ СИТУАТИВНОЇ ОБІЗНАНОСТІ

## 1.2 Концепція

Концепція ситуаційної обізнаності була визначена під час Першої світової війни Освальдом Бельке, який усвідомив «важливість отримання інформації про ворога до того, як ворог отримає подібну інформацію і розробить методи для досягнення своєї мети». [1] Ця ідея розмежування між розумінням людиною-оператором стану системи і фактичним станом системи лежить в основі визначення ситуаційної обізнаності. До кінця 1980-х років ця ідея не привертала особливої уваги в технічній і науковій літературі, але відтоді вона актуалізувалась. Одне з пояснень значної затримки в часі між початковою ідентифікацією явища та зрілістю концепції — це ступінь усвідомлення реальної проблеми. Початковий поштовх до досліджень і розробок був здійснений в авіаційній галузі, де існує значний тиск на пілотів і авіадиспетчерів здобувати кращу ситуаційну обізнаність. [2] Цей виклик виник у зв'язку з усвідомленням того, що дизайн систем більше не є оптимізованим для експлуатації людиною, а за певних умов «перевищує людські можливості відстеження». Мабуть, не дивно, що становлення досліджень ситуаційної обізнаності тісно пов'язане з підвищенням ступеня автоматизації управління польотами. Дійсно, багато дослідників називають скляну кабіну (тобто заміну традиційної кабіни, що складалася з безлічі циферблатів, доступ до яких здійснювався паралельно, невеликою кількістю ЕПТ-дисплеїв, що надавали пілотам послідовний доступ до інформації) причиною психологічного дистанціювання пілотів від складних процесів свого літака і постійних змін ситуації. [3][4]

Вудс [5] зазначає, що для того, щоб люди підтримували адекватну обізнаність про стан системи, їм необхідно відстежувати розвиток подій (переривчасті лінії, рис. 1.2), оскільки вони поступово розгортаються (чорна лінія, рис 1.1). Він стверджує, що інциденти розвиваються шляхом поширення збоїв у часі. Ці

проблеми загострюються, якщо обслуговуючий персонал не може адаптуватися до нових подій що з’являються. Це може призвести до розриву зв'язку між станом системи і розумінням людиною-оператором стану системи (права частина рис. 1.1, де пунктирна лінія (розуміння людиною ситуації) відходить від чорної лінії (фактичний стан системи)). В результаті керуючі дії на основі помилкової ситуаційної обізнаності можуть потенційно зробити неприємний інцидент ще гіршим, як, наприклад, події, що заклали підґрунтя вибуху на Чорнобильській АЕС. [6]

Рисунок 1.1 — Відстеження ситуації

Хоча концепція ситуаційної обізнаності (англ. Situational Awareness) виникла в авіації, вона має велике значення для мережевого аналізу і безпеки:

— *паралельні цілі*: Мережеві аналітики повинні балансувати між кількома пріоритетами, включаючи моніторинг трафіку, виявлення аномалій і забезпечення цілісності системи;

— *прийняття рішень в умовах обмеженого часу*: Час реагування має вирішальне значення для зниження загроз, а затримка або неправильні дії можуть мати серйозні наслідки для мережевої безпеки.

— *об’єм інформації*: Широкий спектр потоків даних і потенційних інцидентів конкурують за увагу аналітика, що вимагає ефективного визначення пріоритетів.

Враховуючи потенційну важливість і застосовність цієї концепції для безпеки, особливо з огляду на те, що навіть невеликі прогалини в ситуаційній

обізнаності можуть мати серйозні наслідки важливо проаналізувати сучасний стан і розглянути, як її можна адаптувати до мережевої сфери. [7]

## 1.2 Визначення

Вдале узагальнення ситуативної обізнаності в одному реченні, хоча це поняття є набагато складнішим за своєю суттю: «Допомагати людям осмислити оточуючий світ, зрозуміти, що відбувається, і як приймати кращі рішення». Йдеться не лише про те, що ви бачите, але й про те, як зрозуміти те, що ви бачите. Зокрема стверджується, що бажана теорія усвідомлення ситуації повинна пояснювати динамічний вибір цілей, увагу до відповідних критичних сигналів, очікування щодо майбутніх станів ситуації та зв'язок між усвідомленням ситуації і типовими діями. [8]

Домінує три основних визначення поняття:

— ситуативна обізнаність — це сприйняття елементів навколишнього середовища в межах певного обсягу часу і простору, розуміння їхнього значення і прогнозування їхнього стану в найближчому майбутньому; [7]

— ситуативна обізнаність — це свідоме динамічне відображення ситуації індивідом. Вона забезпечує динамічну орієнтацію в ситуації, можливість відображення не тільки минулого, теперішнього і майбутнього, але й потенційних можливостей ситуації. Динамічна рефлексія містить логіко-понятійні, образні, свідомі та несвідомі компоненти, що дає змогу людині створювати ментальні моделі зовнішніх подій; [9]

— ситуаційна обізнаність — це інваріант у системі агент-середовище, який генерує миттєві знання та поведінку, необхідні для досягнення цілей, визначених арбітром продуктивності в середовищі. [10]

Хоча наведені визначення ситуаційної обізнаності пропонують унікальні перспективи, їхні основні елементи можна об'єднати в рамках структури, що

складається з таких ключових компонентів: Особа або система, що володіє когнітивними здібностями, включаючи робочу пам'ять, ментальні моделі, сформовані на основі знань і досвіду, а також здатність до рефлексії та прогнозування. Складний і динамічний контекст, що оточує агента, котрий охоплює різні підсистеми.

Розглядаючи три визначення ситуаційної обізнаності, запропоновані раніше, кожне з них можна пояснити з огляду на ці основні елементи. Ендслі [7] наголошує на сприйнятті агентом навколишнього середовища, а також на здатності прогнозувати майбутні стани. На противагу цьому, Сміт та Хенкок [10] зосереджуються на динамічній взаємодії між агентом і середовищем як основній детермінанті ситуаційної обізнаності, таким чином, вона зосереджується на тому, як два основні елементи системи працюють разом. Бенді та Мейстер [9] висвітлюють рефлексивні процеси агента, зокрема взаємозв'язок з ментальними моделями та уявлення поточного стану системи. Основні відмінності між цими визначеннями полягають у відносному акценті, який робиться на:

— оперативній пам'яті агента проти довготривалих знань;

— характеристикам взаємодії агента з середовищем у формуванні ситуаційної обізнаності.

Таке інтегроване розуміння ситуаційної обізнаності має прямий вплив на безпеку мережі та аналіз журналів. Журнали мережі являють собою величезні записи про елементи навколишнього середовища. Ефективні системи ситуаційної обізнаності здатні їх ефективно використовувати.

## 1.3 Моделі

Хоча усвідомлення важливості ситуаційної обізнаності в кібербезпеці зростає, багатьом організаціям бракує чіткого усвідомлення її практичної реалізації. Щоб вирішити цю проблему, докладаються зусилля для перетворення

існуючих моделей в більш зрозумілі рамки. Такі моделі, як модель сприйняття-розуміння-проекція Ендслі та петля СОРД (анг «OODA»), забезпечують теоретичну основу. Однак проблема полягає в тому, щоб перевести ці концепції в практичні кроки, характерні для сфери кібербезпеки.

Трирівнева модель ситуаційної обізнаності [7] (зображена на рис. 1.2.): спочатку була розроблена для виконання авіаційних завдань (наприклад, пілотування літаків і управління повітряним рухом, де люди повинні бути в курсі подій, що динамічно змінюються), але стверджується, що вона може бути поширена і на інші сфери, такі як виробництво електроенергії, нафтохімічна, ядерна промисловість, командування і управління, медицина, мережевий аналіз. По суті, будь-яке завдання, що вимагає від людей відстежувати події, є потенційним кандидатом для дослідження і застосування ситуаційної оцінки.

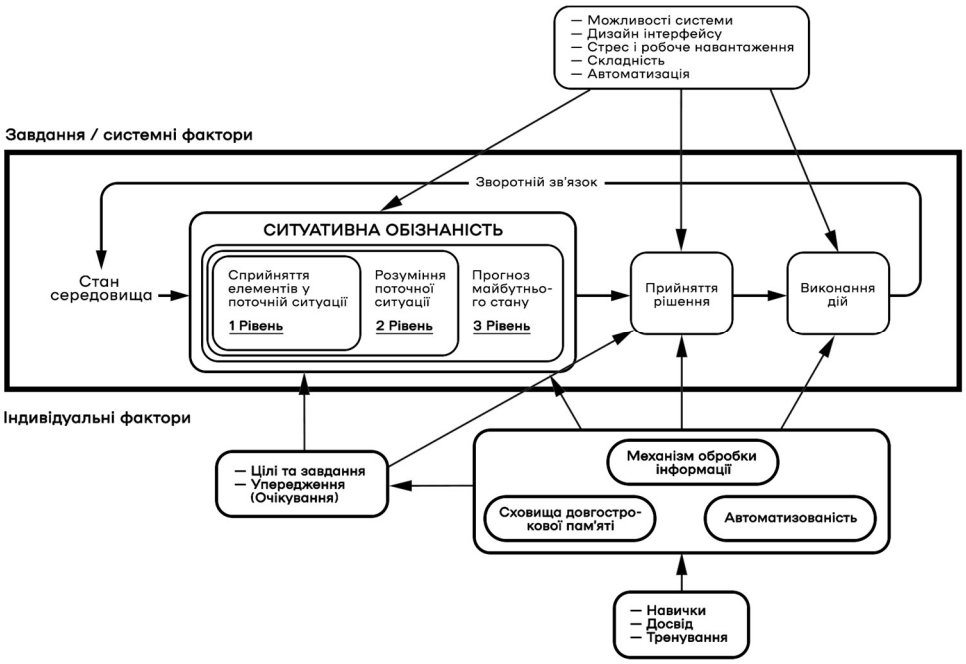



Рисунок 1.2 — Модель ситуаційної обізнаності в динамічному прийнятті рішень.

Модель Ендслі складається з трьох ієрархічних рівнів ситуаційної оцінки, кожен з яких є необхідною (але не обов'язково достатньою) передумовою для переходу на наступний, вищий рівень. Ця модель слідує ланцюжку обробки інформації, від сприйняття, через інтерпретацію, до прогнозування. Від

найнижчого до найвищого, рівні ситуаційної обізнаності виглядають наступним чином:

— *Рівень 1:* Сприйняття елементів навколишнього середовища. Це найнижчий рівень ситуаційної обізнаності, який пов'язаний зі сприйняттям пілотом інформації від приладів літака, поведінки літака, інших людей у кабіні, інших літаків у небі, рельєфу місцевості, управління повітряним рухом. На цьому етапі не виконується інтерпретація даних, все, що мається на меті — це первинне отримання інформації в необробленому вигляді. Якщо на цьому етапі вдасться отримати дані, оператор зможе підтвердити стан певної змінної (наприклад, швидкість польоту, висота, оберти двигуна, рівень палива, місцезнаходження, курс і т.д.), але не зможе інтегрувати дані;

— *Рівень 2*: Розуміння поточної ситуації. Може слідувати за сприйняттям елементів (хоча і не обов'язково), якщо дані інтегровані і синтезовані для отримання ідеї їх відповідності завданням пілота. Стверджується, що розуміння необхідне для того, щоб усвідомити значення вхідних елементів і отримати картину того, що відбувається (наприклад, час і відстань з наявним паливом, тактичний статус загроз, статус місії і т.д.). Таким чином, пілот може зробити висновки про те, чи його дії призведуть до запланованих результатів. Ендслі стверджує, що досягнутий рівень розуміння є показником досвіду пілота. Менш досвідчені особи можуть досягти нижчого рівня 2 ситуативної обізнаності, незважаючи на те, що вони досягли такого ж рівня 1 ситуативної обізнаності, як і їхні більш досвідчені колеги;

— *Рівень 3*: Прогнозування майбутнього стану. Це найвищий рівень ситуаційної обізнаності, який пов'язаний зі здатністю прогнозувати майбутнє елементів навколишнього середовища (наприклад, прогнозування потенційних конфліктів повітряних суден). Точність прогнозу значною мірою залежить від точності СО 1-го та 2-го рівнів. Передбачення прогнозованої майбутньої ситуації надає пілоту (і диспетчеру повітряного руху) час для вирішення конфліктів і планування курсу дій для досягнення своїх цілей. Аналогічно, інший персонал, який виконує критичні за часом дії, значною мірою покладається на прогнозування, щоб передбачити проблеми і вчасно їх вирішити.

Як видно з рисунка 1.2. ситуаційна обізнаність вбудована в когнітивну модель людської діяльності в динамічній системі. Ендслі показала, як на ситуативну обізнаність впливають завдання та індивідуальні фактори. Це пояснює, чому дві людини, які стикаються з різними завданнями, можуть прийти до різних висновків, так само як і люди з різними здібностями, досвідом і підготовкою.

Трирівнева модель, запропонована Ендслі [7], показує, що ступінь усвідомлення зростає в міру того, як інформація обробляється на вищих рівнях. Вона вказує на те, що розуміння передбачає інтеграцію зовнішніх даних зі знаннями та цілями, що, в свою чергу, формує прогнозований стан світу. Модель видається абстрактною оскільки базується на загальних когнітивних процесах, пропонуючи широку теоретичну конструкцію з багатьма сферами застосування. У сфері динамічних систем Ендслі пропонує обговорювати ситуативну обізнаність у термінах специфічних для системи підкатегорій, таких як обізнаність щодо способу дії, просторова обізнаність і часова обізнаність.

Цикл СОРД (Рисунок 1.3.): є нелінійним процесом з постійним зворотним зв'язком і каналами прямого і неявного керівництва та контролю. Для Бойда це був "еволюційний, відкритий, далекий від рівноваги процес самоорганізації, становлення та природного відбору" [11].

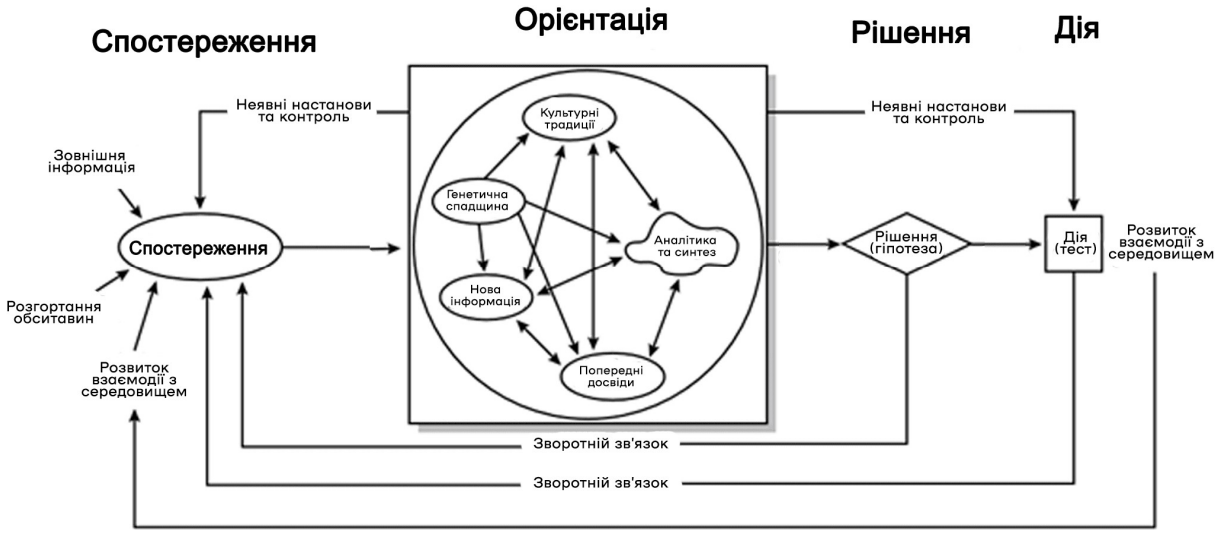



Рисунок 1.3 — Цикл СОРД (Спостереження Орієнтація Рішення Дія) [13]

Петлі СОРД пояснюють дії та реакції, а також те, як діють інші — супроти-

вники, союзники та сторонні спостерігачі. Розуміння інших орієнтацій та обставин є критично важливим для успішної конкуренції з супротивниками. Петля СОРД є не лише аналітичним інструментом, а й моделлю [12]. Вона не залежить від дисципліни, забезпечує контекст, підкреслює часовий вимір і дає уявлення про обчислення рішень. Як теорія, це спроба описати, пояснити і зреагувати у швидкоплинному перебігу подій. Модель складається з таких чотирьох основних процесів:

— Спостереження: починається з безперервного збору необроблених даних з різних джерел у мережевому середовищі. Це включає моніторинг мережевого трафіку (потоків пакетів, протоколів, адрес джерела і призначення), збір журналів подій з серверів, брандмауерів та інших пристроїв, а також використання зовнішніх каналів розвідки загроз, щоб отримати уявлення про відомі вразливості і схеми атак.

— Орієнтування: На цьому етапі аналітики контекстуалізують зібрані дані, щоб зрозуміти їхній вплив на безпеку та роботу мережі. Це передбачає кореляцію подій для виявлення потенційних моделей атак шляхом виявлення зв'язків між, здавалося б, ізольованими точками даних. Крім того, аналітики оцінюють моделі трафіку, використання ресурсів і аномалії в часі, щоб встановити базові лінії для нормальної поведінки і виявити відхилення, які можуть свідчити про загрозу. Ризики визначаються за пріоритетністю на основі критичності активів, серйозності потенційних вразливостей і ймовірності їх використання.

— Рішення: На основі аналізу і визначення пріоритетності загроз, проведеного на етапі "Орієнтування", аналітики визначають найбільш ефективний план дій. Це можуть бути стратегії стримування, такі як ізоляція заражених систем, блокування шкідливого трафіку або розгортання патчів. Крім того, планування реагування на інциденти може передбачати створення детальних процедур для потенційних сценаріїв загроз. Для посилення захисту можуть знадобитися коригування політики, зокрема оновлення правил брандмауера, контролю доступу або конфігурацій безпеки.

— Дія: На цьому етапі рішення виконуються з точністю і дотриманням заздалегідь визначених планів реагування або адаптацію цих планів у режимі реального часу відповідно до умов, що змінюються. Усунення вразливостей, таких як виправлення систем, реконфігурація пристроїв або виведення з експлуатації скомпрометованих активів, є важливим аспектом етапу "Дії". Ефективна комунікація та співпраця мають важливе значення, включаючи обмін інформацією з відповідними командами, зацікавленими сторонами та зовнішніми організаціями, за необхідності.

# 2 СИТУАТИВНА ОБІЗНАНІСТЬ В МЕРЕЖЕВОМУ СЕРЕДОВИЩІ

## 2.1 Ландшафт кібернетичних загроз

У сфері мережевих послуг важливим початком є обґрунтування доцільності накопичення, обробки та аналізу великих обсягів мережевих даних та візуалізація цих інтенсивних обчислювальних операцій. Раціональність такої практики це створення основи надійних стратегій кібербезпеки. Тому при розробці та впровадженні інструментів моніторингу міркування безпеки грають вирішальну роль. Нинішні рівні ризиків значно перевищують ті, що були в минулому, втім занепокоєння щодо вразливості комп'ютерних систем й без того існувало серед користувачів протягом тривалого періоду часу.

Поширеною помилковою думкою є те, що кіберзлочинність це новітнє явище кількох останніх десятиліть. Однак вразливості в комп'ютерних системах існують значно довше, так само як і зловмисники, які намагаються ними скористатися. На рисунку 2.1 зображено спробу візуалізувати історичну еволюцію кіберзлочинності, починаючи з її витоків у 1940-х — роках створення перших цифрових машин.

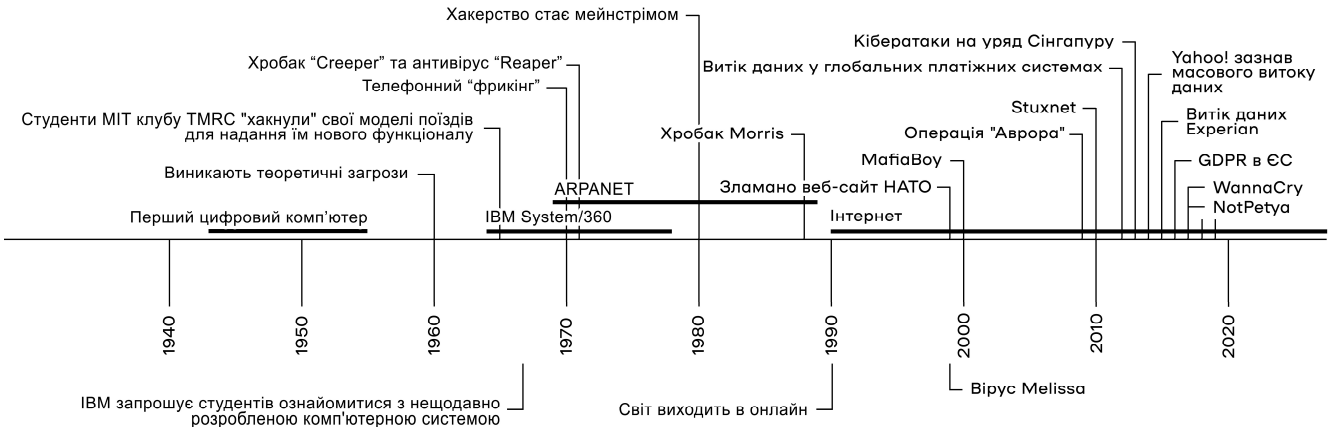



Рисунок 2.1. — Хронологія зростаючих кіберзагроз

У перші два десятиліття після розробки цифрових комп'ютерів (1940-50 рр.)

потенціал для широкомасштабних кібератак був незначним. Доступ до цих перших мейнфреймів був дуже обмежений, їх обслуговував спеціалізований персонал і їм не вистачало широкої взаємопов'язаності, яка згодом сприяла поширенню атак. Піонер комп'ютерних технологій Джон фон Нейман заклав теоретичне підґрунтя для самовідтворення комп'ютерних програм у своїй роботі "Теорія самовідтворювальних автоматів" [14]. Хоча це фундаментальне дослідження не містило явних зловмисних намірів, згодом воно стало основою для розуміння і розробки комп'ютерних вірусів. Значущість ситуативної обізнаності в цей час мінімальна, доступ був дуже обмежений, а мереж не існувало. Основна увага приділялася фізичній безпеці самих систем. Корисні інструменти: базове ведення системного журналу (для аудиту доступу та апаратних проблем).

Шосте десятиліття стало свідком еволюції терміну "хакерство". З модифікації моделей поїздів в Массачусетському технологічному інституті, воно згодом перейшло до комп'ютерних систем. Хоча несанкціонований доступ мав місце, ці ранні інциденти були в основному мотивовані цікавістю і викликом обійти захист, а не політичною чи фінансовою вигодою. Інновації в техніці злому продовжувалися. Примітною подією 1967 року стало те, що компанія «IBM» запросила студентів дослідити нову комп'ютерну систему, що призвело до виявлення в ній вразливостей. Це підкреслило необхідність проактивних заходів безпеки в системах, що, можливо, стало першим прикладом етичного хакінгу — нині формалізованої дисципліни з кібербезпеки. Важливість ситуаційної обізнаності в цей період обмежена але зростає, інциденти вказують на необхідність розуміння мотивації та методів зловмисників. Засоби контролю: системні журнали та журнали доступу для відстеження проникнень

1970 роки ознаменували період усвідомлення кібербезпеки як необхідності. Ключовою подією стало створення мережі передових досліджень (англ. Advanced Research Project Agency Network, далі ARPANET)[15], попередника сучасного Інтернету. У цьому контексті з'явився один з перших задокументованих комп'ютерних хробаків. Боб Томас, розробник ARPANET, створив програму «Creeper», яка демонструвала поведінку самовідтворення на комп'ютерах,

об'єднаних у мережу. «Creeper» не був зловмисним, натомість вказував на потенційні вразливості в цих взаємопов'язаних системах. На цей виклик відреагувала галузь кібербезпеки, що тільки но формувалася. Рей Томлінсон, який розробив систему електронної пошти для ARPANET, створив програму «Reaper», щоб знайти і знешкодити хробака «Creeper». Цей ранній приклад підкреслює вирішальну роль виявлення та нейтралізації загроз. Важливість ситуативної обізнаності стає значною, знайомий перший випадок розповсюдження коду, що самовідтворюється в мережі, що вказує на вразливості з більш широким потенціалом впливу. Інструменти:

— моніторинг мережевого трафіку для виявлення аномальних патернів;

— моніторинг системної активності для виявлення дій хробака;

— цетралізація записів журналів для кореляції подій у різних системах.

1980 рр. стали свідками ескалації гучних кібератак, зокрема, зломів у Національному центрі телекомунікацій, «AT&T» та Лос-Аламоській національній лабораторії. У фільмі 1983 року «Військові ігри» відображено загрозу автоматизованих атак з потенційно катастрофічними наслідками, що підкреслює зростаючий інтерес та занепокоєння громадськості стосовно даної теми. У цьому десятилітті також з'явилися терміни "троянський кінь" і "комп'ютерний вірус", що згодом стали повсюдно вживаними. Геополітична напруженість, спричинена холодною війною, збільшила поширеність і витонченість кібершпигунства. 1980 рр. остаточно стали рубіконом у розвитку кіберзлочинності, важливість ситуативної обізнаністі висока і стає зрозумілим потенціал широкомасштабних порушень автоматизованих систем з економічними та політичними наслідками. Інструменти:

— системи виявлення вторгнень (англ. Intrusion Detection System — далі IDS) для мережевого трафіку і системних аномалій;

— платформи для обміну розвідданими про загрози для попередження про шаблони атак, що використовуються різними групами;

— централізоване управління інформацією та подіями безпеки (англ. Security Information and Even Management — далі SIEM).

1990 рр. характеризує вибухове зростання Інтернету, що трансформувало можливості зв'язку та відкрило нову еру цифрової взаємодії. Однак це розширення також сприяло безпрецедентному поширенню кіберзлочинності. Індустрія кібербезпеки розвивалася паралельно, прагнучи протистояти масиву все більш витонченого шкідливого програмного забезпечення. Важливість ситуативної обізнаності стає критичною. Широкі можливості підключення та різноманітне шкідливе програмне забезпечення вимагають всебічного моніторингу для ефективного захисту. Інструменти:

— розширені IDS та системи запобігання вторгненням (англ. Intrusion Prevention System — далі IPS) для виявлення складних атак;

— виявлення на основі поведінки та евристик нових типів шкідливих програм.

Сучасність представлена усіма видами атак, які можна собі уявити, вони описані в таблиці 2.1.

Таблиця 2.1 — Характеристика та приклади класів комп'ютерних атак [16]

| *Назва атаки* | *Характеристики* | *Приклади* |
|---|---|---|
| Вірус | 1. Програма, що самовідтворюється і заражає систему без відома або дозволу користувача. 2. Збільшує рівень зараження мережевої файлової системи, якщо доступ до неї здійснюється з іншого комп'ютера. | Trivial.88.D, Polyboot.B, Tuareg |
| Хробак | 1. Програма, що самовідтворюється і поширюється через мережеві сервіси на комп'ютерних системах без втручання користувача. 2. Може завдати значної шкоди мережі, споживаючи її пропускну здатність. | SQL Slammer, Mydoom, CodeRed Nimda |
| Троян | 1. Шкідлива програма, яка не може реплікувати себе, але може спричинити серйозні проблеми з безпекою в комп'ютерній системі. 2. Виглядає як корисна програма, але | Mail Bomb, фішингова атака |

Продовження таблиці 2.1 — Характеристика та приклади класів комп'ютерних атак

| *Назва атаки* | *Характеристики* | *Приклади* |
|---|---|---|
| Троян | насправді має секретний код, який може створити чорний хід до системи, що дозволяє їй легко робити все, що завгодно в ній, і може бути викликана, коли хакер отримує контроль над системою без дозволу користувача. | Mail Bomb, фішингова атака |
| Відмова в обслуговуванні (DoS) | 1. Намагається заблокувати доступ до системних або мережевих ресурсів. 2. Втрата сервісу — це нездатність певної мережі або хост-сервісу, наприклад, електронної пошти, функціонувати. 3. Здійснюється шляхом примусового перезавантаження комп'ютера (комп'ютерів), на який спрямована атака, або шляхом споживання ресурсів. 4. Користувачі більше не можуть адекватно спілкуватися через недоступність сервісу або через перешкоди в роботі засобів зв'язку. | Переповнення буфера, ping of death(PoD), TCP SYN, smurf, teardrop |
| Мережева атака | 1. Будь-який процес, що використовується для зловмисних спроб порушити безпеку мережі, починаючи з канального рівня і закінчуючи прикладним рівнем, за допомогою різних засобів, таких як маніпуляції з мережевими протоколами. 2. Незаконне використання облікових записів і привілеїв користувачів, виконання дій з видалення мережевих ресурсів і пропускної здатності, дій, що перешкоджають доступу законних авторизованих користувачів до мережевих сервісів і ресурсів. | Пакетна ін'єкція, SYN-флуд |
| Фізична атака | Спроба пошкодити фізичні компоненти мереж або комп'ютерів. | Холодний запуск, зла покоївка |
| Атака за паролем | Спрямована на підбір пароля за короткий проміжок часу і зазвичай проявляється серією невдалих спроб входу в систему. | Словникова атака, атака SQL ін'єкцій |
| Атака збору інформації | Збирає інформацію або знаходить відомі вразливості, скануючи комп'ютери чи мережі. | SYS/FIN/ XMAS-скан. |

Продовження таблиці 2.1 — Характеристика та приклади класів комп'ютерних атак

| *Назва атаки* | *Характеристики* | *Приклади* |
|---|---|---|
| Атака User to Root (U2R) | 1. Нападник може скористатися вразливостями, щоб отримати привілеї суперкористувача системи, хоча запускається як звичайний... користувач системи. 2. Вразливості включають підбір паролів, атаку по словнику або соціальну інженерію. | Rootkit, loadmodule, perl |
| Атака Remote to Local (R2L) | 1. Можливість надсилати пакети до віддаленої системи через мережу, не маючи жодного облікового запису в цій системі, отримувати доступ до системи як користувач або як root і виконувати шкідливі операції. 2. Здійснює атаку на загальнодоступні сервіси (такі як HTTP і FTP) або під час з'єднання захищених сервісів (таких як POP і IMAP). | Warezclient, warezmaster, imap, ftp write, multihop, phf, spy |
| Зондування | Сканує мережі для виявлення дійсних IP-адрес та збору інформації про хост (наприклад, які послуги він пропонує, яка операційна система використовується). (ii) Надає зловмиснику інформацію зі списком потенційних вразливостей, які згодом можуть бути використані для запуску атаки на обрані системи та сервіси | Перевірка IP-адрес, перевірка портів |

Визначення базового рівня мінімально необхідної безпеки (далі МНБ) є вирішальним кроком у створенні оптимального захисту для будь-якої системи. Цей рівень повинен відповідати і спиратися на інформацію з різних фреймворків і стандартів безпеки. Мета полягає в тому, щоб надати керівні вказівки, які виходять за рамки простих рекомендацій щодо продуктів. Чітко визначена МНБ має впливати на вибір додаткових рішень для забезпечення безпеки, сприяючи створенню багаторівневої та ефективної системи кібербезпеки. Ключовий виклик для аналітиків полягає в тому, щоб підтримувати актуальне розуміння мінливого ландшафту загроз, в якому постійно з'являються нові вразливості та методології

атак. Недостатнє усвідомлення розбіжностей між очікуваним («має бути») і фактичним («є») станом може створити прогалини, які можна використати, навіть якщо ці розбіжності не були проблематичними в попередніх оцінках. Кілька поширених типів перешкод на шляху до надійної ситуаційної обізнаності в операціях з кібербезпеки це некомплексний моніторинг, проблеми з використанням даних, невідповідність пріоритетів. Ці проблеми підкреслюють важливість забезпечення належної комунікації та узгодження між командами безпеки.

## 2.2 Пріоритизація

Онією з важливих сфер, якої завжди бракувало в концепції ситуаційної обізнаності з кібербезпеки [17], незалежно від того, чи мова йде лише про мережу, чи про більш загальні питання, є те, про що саме отримується ситуаційна обізнаність? Тобто, які активи складають сферу або зону відповідальності, як сказали б військові, які бізнес-послуги підтримуються, які політичні та правові аспекти, а також аспекти управління необхідно розуміти, щоб бути в змозі осмислити те, що відбувається?

У сучасному середовищі поширених і постійних кіберзагроз, особливо для великих підприємств і навіть менших організацій, стає зрозумілою важливість ширшого контексту. Ця точка зору, як наслідок вимагає всебічного розуміння екосистеми, в якій працює обрана мережа. Сюди входять програми, дані та всі елементи, що є ключовими у функціонуванні організації. Такий цілісний погляд дозволяє підприємствам виявляти аномалії — важливий крок, який виходить за рамки простого запобігання атакам чи загрозам, фактично це і є визначення того, чого очікують від фахівців з ситуаційної обізнаності. Відповідні дії дозволяють визначати пріоритети та ефективно нівелювати загрози, які становлять найбільший ризик для організації.

У сучасній кібербезпеці пріоритетність загроз є однією з ключових категорій

віхідних даних. Організації повинні визначити найбільш критичні загрози, які потребують негайного реагування [18]. Визначення пріоритетів значною мірою залежить від оперативного контексту. Наприклад, служба швидкого реагування стикається з принципово іншим ландшафтом загроз, ніж великий ритейлер. Збої в роботі мережі, такі як атаки типу "відмова в обслуговуванні" (англ. «Denial of Service — далі DoS) або програми-вимагачі (англ. «ransomware»), створюють безпосередні ризики для екстреного зв'язку, тоді як для ритейлера пріоритетом може бути захист фінансових даних і запобігання шахрайству. Ці приклади підкреслюють необхідність адаптації стратегій контролю наслідків до унікальних загроз і вразливостей з якими стикається організація в її конкретному контексті (таб. 2.2).

Таблиця 2.2 — Вплив контексту на пріоритетність загроз.

| *Загроза* | *Операційний контекст* | | |
|---|---|---|---|
| | *Служба невідкладної допомоги* | *Великий роздрібний продавець* | *Приватна мережа* |
| Програма-вимагач | Порушення критично важливого зв'язку та потенційний збій у роботі систем життєзабезпечення.<br><br>Мінімізація наслідків: надавати пріоритет надійним резервним копіям та процесам відновлення в автономному режимі. В екстремальних ситуаціях, пов'язаних із загрозою життю, розглянути можливість виплати викупу. | Крадіжка фінансових даних клієнтів та потенційна шкода репутації бренду.<br><br>Мінімізація наслідків: зосередження на шифруванні даних, суворому контролі доступу та регулярному усуненні вразливостей. Впровадження системи виявлення. | Порушення внутрішніх операцій, потенційний витік конфіденційних даних (ком. таємниці, інтелект. власності).<br><br>Мінімізація наслідків: сегментація мережі, впровадження принципів нульової довіри, зосередження на надійному шифруванні та контролі доступу |

Продовження таблиці 2.2 — Вплив контексту на пріоритетність загроз.

| *Загроза* | *Операційний контекст* | | |
|---|---|---|---|
| | *Служба невідкладної допомоги* | *Великий роздрібний продавець* | *Служба невідкладної допомоги* |
| Витік даних | Витік конфіденційної інформації про реагування на інциденти.<br><br>Мінімізація наслідків: зосередьтеся на розділенні даних, використанні захищених каналів зв'язку та впровадженні суворих політик доступу за принципом «тільки для службового користування». | Розкриття даних клієнтів (адреси, інформація про кредитні картки, історія покупок), що може призвести до подальшого шахрайства.<br><br>Мінімізація налідків: надійне шифрування даних, та впровадження планів реагування на інциденти , дотримання вимог до звітності. | Розкриття внутрішніх даних, але основна увага приділяється операційному впливу, а не проблемам конфіденційності.<br><br>Мінімізація наслідків: суворий контроль доступу, ведення журналів, виявлення аномалій для незвичайних моделей доступу до даних. |
| Атака на відмову в обслуговуванні (DoS) | Порушення екстреного зв'язку, що збільшує час реагування та потенційно впливає на надання допомоги пацієнтам.<br><br>Мінімізація наслідків: впровадження послуг захисту від DDoS-атак, резервних систем та пріоритетна фільтрація трафіку під час атаки. | Простої платформ електронної комерції, що призводять до втрати доходів та незадоволення клієнтів.<br><br>Мінімізація наслідків: використання хмарних засобів захисту від DoS, CDN та надійне балансування навантаження. | Порушення внутрішньої комунікації та інструментів співпраці, що призводить до зниження продуктивності<br><br>Мінімізація наслідків: сегментація мережі та забезпечення резервування критично важливих сервісів. |

Використання методологій оцінки ризиків надає рейтинговий спосіб оцінити та ранжувати потенційні загрози, виявлені у мережевому середовищі. Головні

елементи розрахунків ризиків це ступінь шкоди або збитків, які загроза може завдати активам (серйозність), ймовірність того, що певна загроза використає вразливість і спричинить інцидент та йотенційні наслідки успішної атаки (вплив). Серйозність часто класифікується як низька, середня, висока або критична. Ймовірність можна оцінити на основі історичних даних, розвідки загроз і сканування вразливостей. В той час як вплив вимірюється з точки зору фінансових втрат, шкоди репутації, перебоїв у наданні послуг або серйозності витоку даних.

Методології оцінювання ризиків включають якісну, напівкількісну та кількісну оцінку ризиків. Якісна методологія передбачає присвоєння суб'єктивних оцінок (наприклад, низький, середній, високий) кожному з компонентів (серйозності, ймовірності та впливу). Потім ці оцінки об'єднуються для отримання загального рейтингу ризику. Попри простоту, цьому методу бракує точності. Напівкількісна поєднує якісні позначення з числовими значеннями для створення більш деталізованої оцінки ризику. Наприклад, серйозність може бути оцінена за шкалою від 1 до 5, ймовірність за шкалою від 1 до 3, а вплив за шкалою від 1 до 10. Метод що ґрунтується на числових даних для обчислення оцінки ризику часто включає складні формули, які враховують такі фактори, як вартість активів, потенційні фінансові втрати та ймовірність їх виникнення. Кількісна оцінка може бути більш точною, але вимагає більше даних і досвіду.

Для ефективного визначення пріоритетності загроз необхідний багатосторонній, системний підхід. Це виходить за рамки ролі традиційного аналітика, який зосереджується виключно на специфічних подіях. Замість цього фахівці з ситуаційної обізнаності повинні розглядати ситуацію на загальносистемному рівні. Це передбачає всебічне розуміння архітектури. Ключовими факторами є розгортання пристроїв, механізми контролю доступу, місцезнаходження розробників і протоколи доступу. Візуалізація цих елементів у вигляді окремих шарів продемонстрована на Рис. 2.2.

Наприклад, базовий рівень включає в себе пристрої та підключення до інфраструктури. На нього накладається рівень безпеки, що охоплює захисні та моніторингові пристрої. Нарешті, операційний рівень включає в себе процеси та

аналіз, що проводяться персоналом служби безпеки.

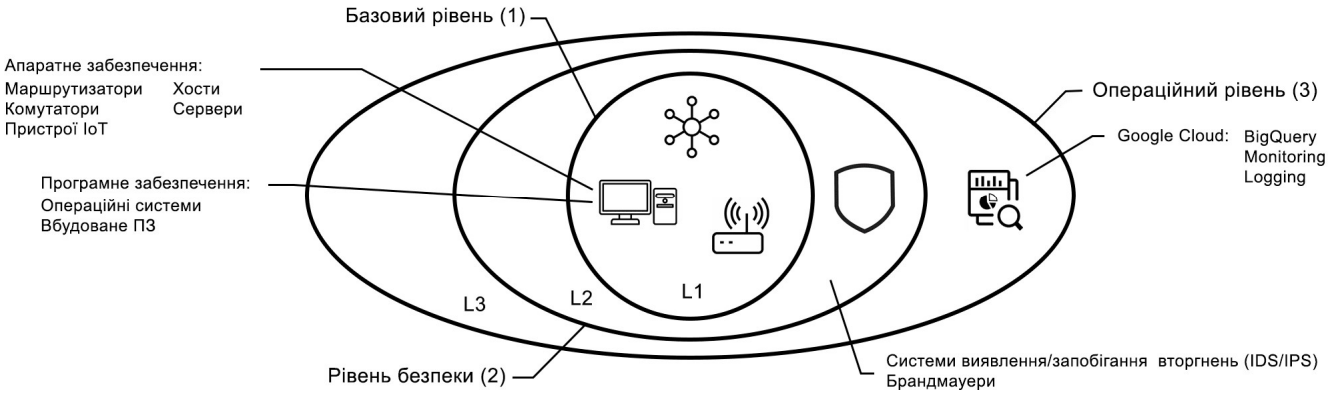



Рисунок 2.1 — Візуалізація рівнів системної архітектури

Щоб досягти комплексного бачення загроз, необхідно застосовувати інструменти і методології, які виходять за рамки традиційної ізоляції. Це узгоджується з концепцією "ниток місії" або робочих процесів, які забезпечують наскрізну перспективу. Без чіткого розуміння основних місій та операційних процесів вашої організації неможливо точно оцінити стан її безпеки. Після того, як цей фундамент створено, ви можете заглибитися в особливості системи, щоб виявити відповідні дані та визначити відповідні дії для зменшення ризиків.

Зростаюча міграція клієнтів до хмарної інфраструктури створила динамічне середовище в програмно-визначених мережах. Щоб забезпечити надійну безпеку в цьому контексті, необхідно мати глибоке розуміння як вимог безпеки, так і базової фізичної мережевої інфраструктури. Ці знання необхідні для ефективного визначення джерел даних і сприяння процесам прийняття правильних рішень. Ці фактори підкреслюють постійний розвиток галузі ситуативної обізнаності та потребу в адаптивних методах надання безпеки.

Емпіричні спостереження показують, що одним з найбільш фундаментальних, але часто недооцінених аспектів надійної мережевої безпеки є розробка комплексних каталогів активів. Ефективне управління активами виходить за рамки простої інвентаризації апаратного та програмного забезпечення. Воно вимагає глибокого розуміння призначення кожного ресурсу та його взаємозалежності в рамках загальної системної архітектури. Просте перерахування

компонентів має обмежену цінність без контекстуалізації їхніх ролей і взаємозв'язків у ширшій мережі.

## 2.3 Адаптація трирівневої моделі

Не зважаючи на те що СОРД пропонує цінну основу для швидкого прийняття рішень в динамічних середовищах [12], аналіз мережевої безпеки вимагає більш структурованого підходу. З цією метою трирівнева модель (сприйняття, осмислення, прогнозування) забезпечує більш комплексний і методичний підхід до аналізу загроз мережевій безпеці. Нижче наведено основні переваги трирівневої моделі для мережевих інженерів:

Акцент на ситуаційній обізнаності:

— Трирівнева модель чітко фокусується на розвитку ситуаційної обізнаності, розділяючи процес на окремі абстрактні етапи: сприйняття, осмислення і проектування. Такий фокус забезпечує систематичне розуміння мережевого середовища, потенційних загроз і майбутніх ризиків.

— Модель СОРД, визнаючи важливість спостереження, не робить явного акценту на створенні комплексної ментальної картини мережі.

Глибший аналіз та ідентифікація загроз:

— Етап № 2 «осмислення» тришарової моделі сприяє глибшому аналізу зібраних даних. Мережеві інженери можуть співвідносити події, аналізувати тенденції та виявляти тонкі аномалії, які можуть бути пропущені в більш швидкому циклі СОРД. Це дозволяє виявляти складні загрози, які можуть бути не одразу помітними.

— Модель СОРД наголошує на визначенні пріоритетності загроз на основі початкового аналізу, що може призвести до ігнорування менш очевидних, але потенційно серйозних ризиків.

Проактивне врегулювання загроз:

— Етап № 3 "прогнозування" тришарової моделі заохочує мережевих інженерів прогнозувати майбутні стани мережі. Такий проактивний підхід дозволяє виявити потенційні вразливості та вжити превентивних заходів до того, як відбудеться атака.

— Модель СОРД в першу чергу фокусується на реагуванні на події, які спостерігаються, що потенційно робить мережу вразливою до непередбачуваних загроз.

У той час як модель СОРД забезпечує цінну основу для швидкого прийняття рішень у критичних ситуаціях, трирівнева модель пропонує гнучкий системний підхід до аналізу мережевої безпеки. Акцент трирівневої моделі на ситуаційній обізнаності, більш глибокому аналізі, проактивному менеджменту наслідків і безперешкодній інтеграції з інструментами мережевого аналізу робить її найкращим вибором для мережевих інженерів, які прагнуть підтримувати оптимальний рівень безпеки. Адаптована під мережеві потреби модель Ендслі зображена на рис. 2.3.


Рисунок 2.3 — Адаптована трирівнева модель

Рівень 1: Аналітики збирають інформацію з мережевого трафіку, системних журналів, сповіщень брандмауера, інвентаризації активів і сканування вразливостей. Вони спостерігають за окремими точками даних, такими як використання пропускної здатності, IP-адреси, відкриті порти, рівні виправлень і версії програмного забезпечення.

Рівень 2: Аналітики інтегрують і синтезують дані, щоб зрозуміти їх значення для роботи мережі. Вони розуміють взаємозв'язок між моделями трафіку і потенційними проблемними місцями, кореляцію подій для виявлення загроз або вплив вразливостей на критичні активи, чи функціонує мережа належним чином і де знаходяться потенційні аномалії.

Рівень 3: Аналітики використовують своє розуміння поточних умов (рівень 2) для прогнозування потенційних векторів атак, неминучих перевантажень ресурсів або наслідків змін конфігурації. Передбачуване моделювання загроз дозволяє проактивно вгамовувати їх наслідки і розробляти обґрунтовані плани реагування для підтримки оптимального стану мережі та її безпеки.

На відміну від фізичного середовища, де ми безпосередньо відчуваємо загрози через наші органи чуття, кіберпростір залишається значною мірою неосяжним. Атаки розгортаються як послідовності пакетів даних, позбавлені відчутних сигналів, які ми легко сприймаємо у фізичному світі. Брак інтуїтивного сприйняття приховує справжню природу і масштаб кіберзагроз, перешкоджаючи нашій здатності розуміти ситуацію в міру її розгортання. Щоб подолати це обмеження сприйняття, ми повинні застосовувати структуровані фреймворки, такі як система ситуаційної обізнаності (далі — ССО) зображена на рис. 2.4, до аналізу мережевих потоків.

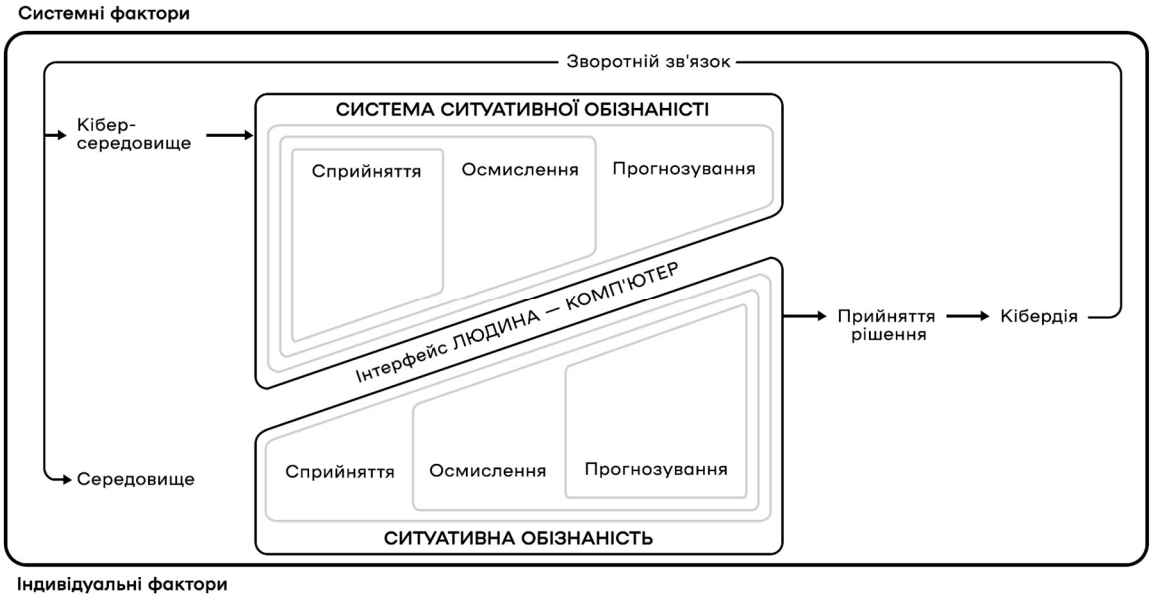



Рисунок 2.4 — Система ситуативної обізнаності

Умовний інтерфейс між людиною та даними є ССО, ось що вона пропонує:

— Візуалізація: Інструменти аналізу потоку для перетворення необроблених даних на змістовні візуалізації. Графіки, діаграми та карти можуть допомогти виявити закономірності, аномалії та потенційні траєкторії атак, на які не звернули б увагу серед необроблених даних.

— Контекстуалізація: Співставлення даних мережевого потоку з журналами хостів, розвідданими про загрози та інформацією про вразливості збагачує розуміння. Сплеск вихідного трафіку набуває значення, якщо він пов'язаний з відомою активністю шкідливого програмного забезпечення або скомпрометованою системою.

— Розпізнавання патернів: Ситуаційна обізнаність наголошує на вивченні минулих подій і встановленні базових показників. Комп’ютерні системи можуть автоматично виявити відхилення від нормального потоку і сигналізувати про потенційні загрози, навіть якщо вони не були безпосередньо задокументовані раніше.

Існує досить обширний список інструментів інтегрованих в умовну ССО, серед них для аналізу мережевого трафіку використовуються:

— Zeek (раніше Bro): потужний засіб для моніторингу мережевої безпеки з відкритим вихідним кодом для глибокої перевірки пакетів, поведінкового аналізу та виявлення аномалій;

— Suricata: високопродуктивний мережевий IDS/IPS з чудовими можливостями виявлення на основі цифрових слідів і встановлених правил;

— ntopng: забезпечує візуалізацію, аналіз і усунення несправностей мережевого трафіку в режимі реального часу.

Управління інформацією та подіями безпеки (SIEM):

— Splunk: провідна на ринку система SIEM з потужними можливостями агрегації, індексування, пошуку та візуалізації логів.

— Elastic Stack (ELK): стек з відкритим вихідним кодом, що поєднує Elasticsearch (пошук та аналітику), Logstash (обробка логів) та Kibana (візуалізація).

Платформи розвідки загроз (TIP):

— ThreatConnect: платформа для агрегування, аналізу та обміну даними про загрози з можливістю інтеграції з різними інструментами безпеки.

— Anomali: пропонує управління розвідданими про загрози, пошук загроз і можливості реагування на інциденти.

Сканери вразливостей:

— Nessus: широко використовуваний сканер вразливостей для виявлення слабких місць в системах і додатках.

— OpenVAS: сканер вразливостей з відкритим вихідним кодом, що пропонує комплексну оцінку вразливостей мережі.

Додаткові інструменти:

— Бібліотеки машинного навчання: TensorFlow, PyTorch або scikit-learn для розробки власної моделі виявлення аномалій.

## 2.4 Мережеві потоки

Виникнення сучасного кіберсередовища нерозривно пов'язане з мережевим підключенням. Ізольовані комп'ютери пропонують обмежені можливості для кіберзагроз; саме мережа сприяє взаємодії та потенційним вразливостям у великих масштабах.

Модель взаємодії відкритих систем ISO 7498 (англ. Open Systems Interconnection, OSI), зображена на рис. 2.5., яку часто критикують за її сувору багатошаровість у сучасних мережах, надає цінну інформацію про фундаментальні принципи комунікації. Акцент на відкритих системах є особливо актуальним у сфері кібербезпеки. У моделі OSI мережеві потоки в основному знаходяться на мережевому (3-й рівень) і транспортному (4-й рівень) рівнях. З огляду на мережецентричну природу кіберзагроз, розуміння цих потоків має важливе значення для розуміння ситуації. Аналіз мережевих потоків забезпечує стандартизований спосіб вилучення ключової інформації про схеми зв'язку,

незалежний від протоколів вищого рівня. Це означає ідентифікацію таких елементів, як IP-адреси джерела і призначення, протоколи (TCP, UDP) та інші метрики, які виявляють потенційні проблеми з безпекою або аномальну поведінку.

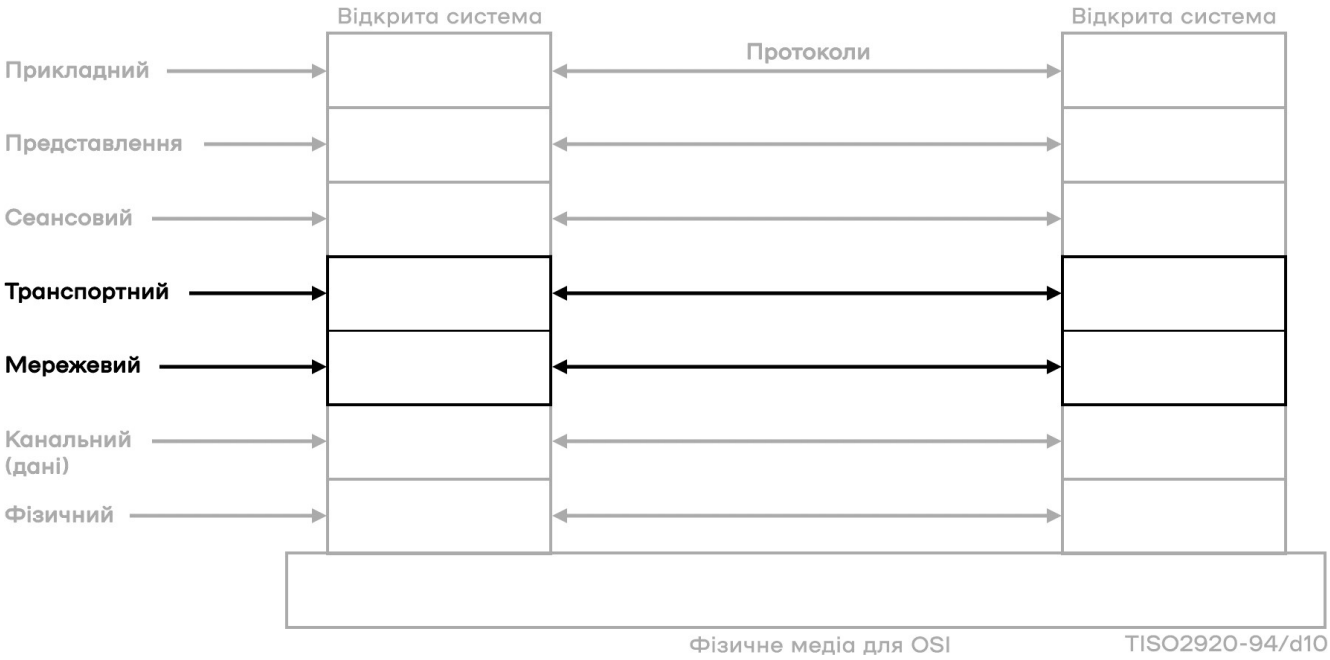



Рисунок 2.5 — Семирівнева еталонна модель та однорангові протоколи [19]

Сирі дані про мережеві потоки у своїй найпростішій формі дають обмежене безпосереднє розуміння складних мережевих взаємодій. Розглянемо наступний приклад на рис. 2.6. Цей ізольований запис потоку показує дві IP-адреси: 192.168.1.105 та 192.151.100.6, порт призначення 80 — ймовірно, веб-трафік. Існує протокол 6, який говорить, що це TCP, кілька пакетів, пара прапорів. Звучить нудно, чи не так?

```
          sIP|          dIP|sPort|dPort|pro|packets|flags|initF|  type|
192.168.1.105| 198.51.100.6|49152|   80|  6|      4| SRPA| S   |outweb|
 198.51.100.6|192.168.1.105|   80|49152|  6|      3| S PA| S  A| inweb|
```

Рис. 2.6 — Знімок мережевого трафіку

Хоча ці елементи є основоположними, їм бракує контексту і високорівневої інтерпретації, необхідної для мережевих аналітиків, щоб отримати дієві висновки і

підтримувати обізнаність про ситуацію. Первинні дані про потоки за своєю суттю є дрібними. Цей низькорівневий фокус може затьмарити закономірності вищого рівня, які є більш важливими для прийняття рішень. Ситуаційна обізнаність залежить від перетворення необроблених даних про потік у значущі візуалізації. Це може включати аналіз протоколів, історичні порівняння та кореляцію між різними джерелами даних. Мережеві аналітики відіграють вирішальну роль у застосуванні галузевих знань та інструментів для перетворення необроблених даних на розуміння більш високого рівня.

Незважаючи на те, що необроблені дані є основною вхідною інформацією для моделей ситуаційної обізнаності, методи візуалізації значно підвищують щільність інформації та полегшують аналіз. Розглянемо графік часового ряду обсягів мережевого трафіку в байтах (рис. 2.7). Ця проста візуалізація пропонує більше розуміння порівняно з необробленими мережевими потоками, допомагаючи аналітику перейти від базового сприйняття (рівень 1) до більш глибокого розуміння (рівень 2) поведінки мережі.

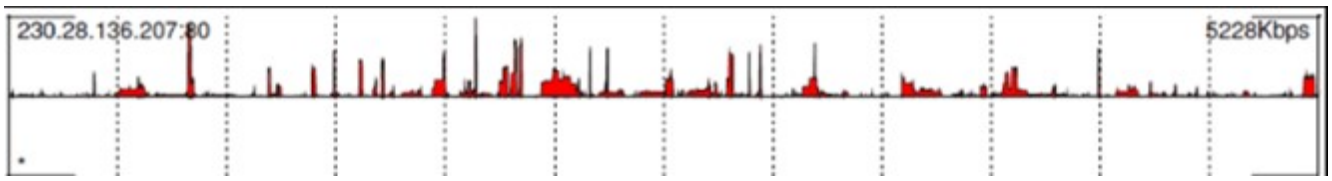



Рисунок 2.7 — Часовий графік обсягу (байт) трафіку.

Хоча в цьому прикладі не вистачає розширеного аналізу трендів або порівняльних поглядів, він ілюструє потенціал машинних перетворень для покращення людського розуміння. Завдяки включенню ліній трендів, історичних порівнянь (наприклад, «минулого тижня» і «цього тижня») або виявлення аномалій, візуалізації можуть ще більше підвищити рівень розуміння, що призведе до більш обґрунтованих висновків. Аналітична система для прогнозування мережевих загроз з використанням даних мережевого потоку (з 3-4 рівнів моделі OSI) поєднуватиме перехоплення трафіку в реальному часі, глибоке дослідження пакетів і розширену аналітику. Система складатиметься з датчиків, стратегічно розміщених для

перехоплення трафіку з ключових сегментів мережі. Потім ці необроблені дані надходили б до високопродуктивного процесора, де відбувався б комплексний аналіз на основі алгоритмів машинного навчання і виявлення аномалій для ідентифікації шаблонів, аномалій і слідів, що вказують на відомі загрози або потенційні вразливості. Система буде постійно співвідносити цей аналіз в режимі реального часу з каналами розвідки загроз, політиками безпеки та історичними даними, щоб забезпечити надання проактивних рекомендацій з захисту системи.

## 2.5 Інтерфейс людина-система

Сирі дані в необробленому вигляді створюють проблеми для інтерпретації та прийняття рішень. Ефективні системи ситуаційної обізнаності вирішують цю проблему шляхом надання аналітичних інструментів, які витягують значущу інформацію. Однак не менш важливим є розробка інтерфейсу, через який ця інформація подається людині-аналітику.

Інтерфейси між системами ситуаційної обізнаності і людьми-операторами відрізняються за складністю і функціональністю, часто поділяючись на дві великі категорії:

Низькорівневі інтерфейси: Ці інтерфейси, такі як інтерфейси командного рядка (англ. Command Line Interface — далі CLI) або сеанси захищеної оболонки (англ. Secure Shell — далі SSH), забезпечують прямий доступ до необроблених даних. Хоча вони цінні для досвідчених аналітиків, вони вимагають значних когнітивних зусиль для інтерпретації та контекстуалізації інформації. Ці інтерфейси в першу чергу задовольняють індивідуальні потреби аналітиків, вимагаючи від них самостійного отримання більш високого рівня знань і прогнозів. Приклади:

Інтерфейси командного рядка (CLI):

— tcpdump (збирає і показує необроблені пакети мережевого трафіку);

— tshark (подібна до tcpdump, але з розширеними можливостями фільтрації);

— netstat (показує мережеві з'єднання, таблиці маршрутизації та статистику інтерфейсів);

— dig (інструмент пошуку DNS для запитів до DNS-сервера);

— traceroute (визначає маршрут, яким пакет досягає місця призначення).

Інтерфейси прикладного програмування (API):

— REST (використовуються для програмного доступу до даних і функціональності в різних інструментах і платформах безпеки);

— Syslog (стандартний протокол для надсилання лог-повідомлень від мережевих пристроїв і програм);

Необроблені логи:

— Логи веб-сервера — містять детальні записи активності веб-сервера. Журнали брандмауера: Записують трафік, який був дозволений або заблокований брандмауером.

— Логи IDS/IPS: Записують сповіщення, що надходять від систем виявлення та запобігання вторгненням.

— Логи операційної системи: Містять системні події та інформацію, пов'язану з безпекою.

Інтерфейси високого рівня: Ці інтерфейси використовують більш просунуті графічні методи та агрегації даних, щоб представити складну інформацію в доступнішому та інтуїтивно зрозумілому форматі. Виокремлюючи основні ідеї та закономірності, вони сприяють швидкому розумінню та прийняттю рішень. Ці інтерфейси часто призначені для підтримки співпраці та обміну знаннями між командами аналітиків. Приклади інтерфейсів високого рівня налічують:

Візуалізації та дашборди:

— Grafana: Платформа з відкритим вихідним кодом для створення гнучких та інтерактивних дашбордів, ідеально підходить для візуалізації даних часових рядів з різних джерел.

— Graylog: Платформа з відкритим вихідним кодом для управління журналами з потужними можливостями візуалізації для виявлення закономірностей і аномалій в даних журналів.

Доповнена реальність (AR) і віртуальна реальність (VR):

— Накладення доповненої реальності на карти: Відображення мережевого трафіку, сповіщень про загрози або інформації про безпеку в режимі реального часу на географічних картах для полегшення реагування на інциденти.

— VR-середовища: Візуалізація топології мережі та подій безпеки з ефектом занурення для покращення розуміння ситуації та спільного аналізу.

Мобільні інтерфейси:

— Мобільні додатки для оповіщень SIEM: Push-сповіщення та спрощені інформаційні панелі для доступу до критично важливої інформації про безпеку в дорозі.

— Платформи обміну повідомленнями (наприклад, Slack, Microsoft Teams): Інтеграція сповіщень про загрози безпеці та звітів про інциденти в командні канали зв'язку для швидкого реагування.

Інтерфейси управління та контролю (англ. Command & Control, C2):

— Платформи ОБАР (англ. Security Orchestration, Automation and Response): Надають централізовані інтерфейси для координації та автоматизації робочих процесів реагування на інциденти безпеки.

Інтерфейси природної мови:

— Чат-боти та віртуальні асистенти: Дозволяють користувачам запитувати дані про безпеку та отримувати інформацію за допомогою природної мови.

## 2.6 Накопичення та зихист даних

Збереження мережевих журналів (подій брандмауера, IDS-сповіщень, потоків трафіку тощо) забезпечує хронологію мережевої активності. Це дозволяє

відстежити походження інцидентів з порушеннм безпеки, виявити закономірності та зрозуміти еволюцію загроз. Мережеві аномалії (незвичний трафік, неочікувані спроби доступу) часто є першими ознаками кібератаки. Щоб їх виявити, потрібен еталон «нормальної» активності, з яким можна звіритись. Дані збережені в довготривалому сховищі надають можливість сформувати такий еталон. Коли трапляються злочинні дії, докладні збережені журнали допомагають відстежити кроки зловмисника, оцінити збитки та зібрати докази для потенційного судового позову. Без цих даних ефективне реагування стає неймовірно складним. Більше того багато галузей та регуляторних органів (наприклад, Євпропейська комісія) вимагають певних періодів зберігання журналів для цілей аудиту та дотримання законодавчих норм. [20]

Традиційно дані з кібербезпеки в організаціях зберігаються в окремих сховищах, потенційно на різних платформах і в різних інструментах управління (наприклад, Splunk, ArcSight). Така фрагментація призводить до значної витрати ресурсів та перешкоджає ефективності реагування. Отже, організації потребують уніфікованого, методологічно інтегрованого підходу до збереження даних. Консолідація має потенціал для значного покращення економічної доцільності збереження даних поверх безпекових преференцій.

Зусилля, спрямовані на покращення ситуаційної обізнаності, зосереджені на розробці інструментів для полегшення консолідації даних включають використання озер даних або таких технологій, як Elastic Stack (укр. «гнучкий стос»), що дозволяють зберігати різні типи даних у централізованому сховищі. Озера даних це великі сховища, які можуть зберігати як структуровані (наприклад журнали), так і неструктуровані дані (наприклад електронні листи або документи) в їхньому вихідному форматі. Озера даних забезпечують гнучкість для майбутнього аналізу і дозволяють об'єднувати дані з різних джерел. Elastic Stack з відкритим вихідним кодом (приклади: Elasticsearch, Logstash, Kibana) пропонує потужні можливості агрегації, індексування, пошуку та візуалізації логів. Він має високу масштабованість і гнучкість. API або програмні інтерфейси забезпечують доступність.

Важливо зазначити, що не всі доступні дані є важливими для ефективної загальної операційної картини. Визначення пріоритетів на основі місії організації та ландшафту загроз має вирішальне значення для визначення конкретних елементів даних, що доцільно зберігати. Також необхідно визначити, як довго зберігати різні типи логів, виходячи з вимог організації і типів аналізу, який виконується. Важливо враховувати масштабованість сховища, щоб впоратися зі зростаючим обсягом даних, що генеруються в міру розширення мережі.

## 2.7 Аналіз

Аналітичні процеси і практики, мають бути інтегровані з процесами і практиками інших спеціальних інженерних дисциплін, включаючи кібербезпеку, системну інженерію, мережеву інженерію і забезпечення місії організації.

У контексті мережевої інженерії аналіз має на меті визначити, чи є властивості та поведінка системи, що нас цікавить, достатніми для того, щоб організація, яка використовує цю систему, могла задовольнити свої вимоги щодо забезпечення кіберстійкості в умовах загроз, які включають в себе атаки перечислені в таблиці 2.1 на ст. 27. Залежно від стадії життєвого циклу системи, програмних міркувань та інших факторів аналіз може рекомендувати зміни архітектури, інтеграцію нових продуктів або технологій в систему, зміни у використанні існуючих продуктів або технологій, а також зміни в операційних процедурах, що відповідають стратегії управління ризиками організації. [ст. 53]

Первинні мережеві дані, такі як захоплення пакетів або логи трафіку, часто містять велику кількість інформації, що виходить за рамки базової статистики, такої як використання пропускної здатності або кількість пакетів. Аналізуючи ці необроблені дані з достатньою швидкістю, ми можемо виявити приховані закономірності, аномалії та тенденції, які показують, як взаємодіють різні компоненти мережі, які додатки використовуються і як трафік проходить через ін-

фраструктуру. Після чого вжити дій для запобігання більшої шкоди від атаки.

Для того щоб виявити потенційні проблеми до того, як вони переростуть у серйозні проблеми, необхідно так би мовити потрапити у вікно для вибірки (рис. 2.7) і встигнути змоделювати наступні кроки.

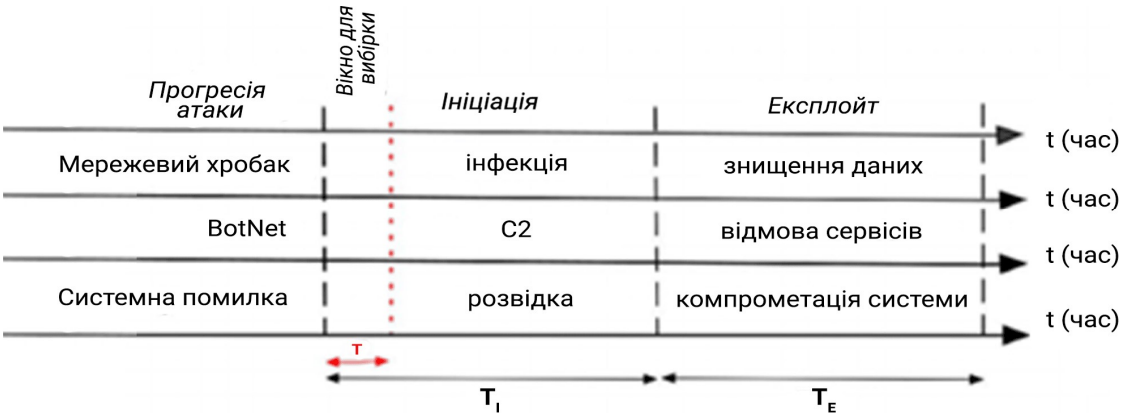



Рисунок 2.7 — Моделювання розвитку кібератаки в мережі

Розуміючи нюанси мережевої активності за допомогою більш широких метрик, можливо точно визначити тип мережевої атаки, яка здійснюється проти конкретної системи. Ось приклад (таблиця 2.2) опису типової аномальної поведінки мережевого трафіку на основі кіберзагроз, перелічених у таблиці 2.1.

Таблиця 2.2 — Індикатори мережевого трафіку про здійснення атаки [16]

| *Назва атаки* | *Динаміка мережевого трафіку* | *Видимість* |
|---|---|---|
| Вірус | Незвичайні сплески мережевого трафіку, низька продуктивність мережі, несподівані передачі файлів | Часто легко виявити в журналах мережевого трафіку |
| Хробак | Великий обсяг мережевого трафіку, низька продуктивність мережі, несподівані з'єднання з невідомими IP-адресами | Подібно до вірусів, зазвичай помітні в мережевому трафіку |
| Троян | Прихований у звичайному, на перший погляд, трафіку, можуть встановлювати приховані канали зв'язку | Важко виявити без спеціалізованих інстру-ментів глибокої пере-вірка пакетів |

Продовження таблиці 2.2 — Індикатори мережевого трафіку про здійснення атаки

| *Назва атаки* | *Динаміка мережевого трафіку* | *Видимість* |
|---|---|---|
| Відмова в обслуговуванні (DoS) | Аномально високий обсяг трафіку з декількох джерел, незвичні типи пакетів (наприклад, SYN-флуд, ping-флуд) | Іноді легальний трафік може мімікрувати під DoS-атаки, що ускладнює їх розрізнення. |
| Мережева атака | Незвичайні маршрути трафіку, спроби несанкціонованого доступу, маніпуляції з мережевими протоколами | Деякі мережеві атаки мають чіткі ознаки, в той час як інші можуть бути розумно замасковані |
| Фізична атака | — | — |
| Атака за паролем | Повторні невдалі спроби входу, незвичні способи входу з несподіваних місць | Видно в журналах автентифікації та може викликати сповіщення в системах безпеки |
| Атака збору інформації | Сканування або «прослуховування» трафіку на декількох портах, підозрілі DNS-запити | Малопомітна та відбувається по-вільно, щоб уникнути виявлення. |
| Атака User to Root (U2R) | Спроби несанкціонованого доступу до привілейованих ресурсів, незвичайний службовий трафік | Використовує вразливості. Мінімальна. |
| Атака Remote to Local (R2L) | Спроби несанкціонованого доступу із зовнішніх джерел | Замасковані під легальний трафік |
| Зондування | Сканування або сканування трафіку на декількох портах, підозрілі DNS-запити | Подібно до атак зі збору інформації, часто відбувається малопомітно і поволі |

Аналітика мережевого потоку охоплює широкий спектр методологій, кожна з яких призначена для отримання конкретної інформації з даних мережевого трафіку. Цю аналітику можна умовно розділити на три окремі площини: площина даних, площина управління та площина кінцевих точок.

Аналітика площини даних фокусується на фактичних даних, що передаються через мережевий потік. Ця аналітика характеризується своєю легкістю і високою

оперативністю, оскільки вона повинна йти в ногу зі швидкістю передачі даних. Аналітика площини даних добре підходить для таких завдань, як підрахунок, швидкі вимірювання та базові метричні обчислення. Потокова аналітика часто використовується в цій галузі, щоб отримати повне розуміння площини даних та інформації, якою обмінюються кінцеві точки.

І навпаки, аналітика площини управління зосереджується на конфігурації мережевого зв'язку, зокрема на механізмах, за допомогою яких кінцеві точки встановлюють з'єднання і визначають місцезнаходження одна одної. До цієї категорії належать аналітика DNS і маршрутизації, які покладаються на складні моделі, що вимагають значних обчислювальних витрат. Однак конфігурація площини керування є відносно стабільною порівняно з динамічним потоком даних, що робить аналітику площини керування добре придатною для глибокого аналізу і нечастих оновлень.

Аналітика кінцевих точок займає проміжне місце між аналітикою площини даних і площини управління, зосереджуючись на вивченні кінцевих точок комунікації. Ця сфера охоплює аналіз репутації, інвентаризацію систем та інші аналізи, які використовують інформацію, отриману як з площини даних, так і з площини контролю. Аналітика кінцевих точок стає все більш затребуваною, і її можна ефективно проводити, використовуючи багаті потокові дані.

Аналітика мережевих потоків може бути використана для вимірювання різних ключових показників, в тому числі:

— Постійність: Вимірює тривалість і частоту відвідування користувачами веб-сайту, надаючи цінну інформацію про поведінку та залученість користувачів.

— Популярність: Кількісно вимірює використання та попит на певну послугу або продукт, дозволяючи організаціям оцінити його успіх та адаптуватися до мінливих тенденцій.

— Відповідність: Оцінює ступінь відповідності шаблонів мережевого трафіку встановленим нормам, допомагаючи виявити аномалії та потенційні загрози безпеці.

Ці показники, разом з іншими, отриманими з даних про мережевий потік,

надають багато інформації, яку можна використовувати для оптимізації продуктивності мережі, підвищення безпеки і поліпшення загального користувацького досвіду.

## 2.8 Етичні міркування щодо моніторингу мережі та виявлення аномалій

Використання методів моніторингу мереж і виявлення аномалій викликає значні етичні питання, які потребують ретельного вивчення. Хоча ці інструменти необхідні для гарантування безпеки, вони також можуть порушувати недоторканність приватного життя та індивідуальні свободи звичайних користувачів. Моніторинг мережі за своєю суттю передбачає збір та аналіз даних мережевого трафіку, які можуть містити особисту інформацію або розкривати чутливі деталі поведінки користувачів. Це викликає занепокоєння щодо конфіденційності даних і потенціальних впливів зловживань або несанкціонованого доступу. [21][22] Системи виявлення аномалій можуть використовуватися для виявлення незвичних або підозрілих форм поведінки, що може призвести до посиленої уваги до окремих осіб або груп. Це викликає занепокоєння щодо ймовірності дискримінаційного профілювання або переслідування на основі сприйнятих аномалій. Алгоритми виявлення можуть ненавмисно зберегти упередження, присутні в навчальних даних, що призводить до дискримінаційних результатів. Важливо переконатися, що алгоритми розроблені та впроваджені таким чином, щоб зменшити вплив упередженості та підвищити об'єктивність. Системи виявлення аномалій можуть генерувати помилкові позитивні сигнали, позначаючи законну діяльність як підозрілу. Це може призвести до марних розслідувань або санкцій, завдаючи шкоди окремим особам і організаціям.

Дуже важливо інформувати користувачів і співробітників про види моніторингу мережі та виявлення аномалій, які проводяться, про мету цих заходів і

про те, як будуть використовуватися зібрані дані. Отримання інформованої згоди від людей перед збором або аналізом їхніх мережевих даних є фундаментальним етичним принципом. Однак у деяких випадках отримання прямої згоди може бути недоцільним або неможливим. У таких ситуаціях слід розглянути альтернативні механізми забезпечення прозорості та підзвітності. Необхідно розробити чіткі політики та процедури, вони повинні стосуватися збереження даних, контролю доступу та протоколів реагування на інциденти. Повинні бути створені незалежні механізми нагляду для забезпечення відповідального та етичного використання цих інструментів. Це може включати регулярні аудити, зовнішні перевірки або створення комітетів з етики.

Діяльність з моніторингу мережі та виявлення аномалій повинна відповідати законам про захист даних, таким як Загальний регламент про захист даних (GDPR). У певних галузях, таких як охорона здоров'я або фінанси, можуть існувати додаткові правила для захисту конфіденційних даних. Техніки анонімізації та маскування даних:

— Псевдонімізація заміна ідентифікаційної інформації (наприклад, IP-адреси) псевдонімами або токенами. Це дозволяє відстежувати активність, не розкриваючи справжню особу.

— Зведення даних на вищому рівні, наприклад, за сегментами мережі або періодами часу. Це приховує індивідуальні дії.

— Внесення випадкового шуму або варіацій у даних, що ускладнює ідентифікацію осіб.

— Заміна конкретних значень ширшими категоріями (наприклад, заміна конкретної IP-адреси на підмережу).

— k-анонімність: маючи структуровані дані, що стосуються конкретних осіб, випускати дані з науковими гарантіями того, що особи, які є суб'єктами цих даних, не можуть бути повторно ідентифіковані, тоді як дані все ще залишатимуться практично корисними. [23]

Методи маскування даних:

— Заміна конфіденційних даних реалістичними, але підробленими дани-

ми (наприклад, заміна реальних імен користувачів випадково згенерованими).

— Випадкова перестановка елементів даних

— Шифрування конфіденційних даних таким чином, щоб їх було неможливо прочитати без ключа. Однак одного лише шифрування може бути недостатньо, оскільки шаблони трафіку все одно можна проаналізувати.

# 3 GOOGLE CLOUD

## 3.1 Хмарні обчислення

Термін, запроваджений Національним інститутом стандартів і технологій США [24], хмарні обчислення — стали повсюдною технологією з глобальними наслідками. Вона характеризується п'ятьма ключовими особливостями: самообслуговуванням на вимогу, широким доступом до мережі, об'єднанням ресурсів, швидкою еластичністю та вимірюваним сервісом. Користувачі можуть обирати обчислювальні ресурси, такі як обчислювальна потужність, сховище та мережева пропускна здатність, через веб-інтерфейс без втручання людини. Ці ресурси доступні через Інтернет і беруться з великого пулу, який обслуговується хмарним провайдером, що дозволяє досягти економії за рахунок масштабу. Еластична природа хмари дозволяє користувачам швидко збільшувати або зменшувати ресурси за потреби, сплачуючи лише за те, що вони використовують.

Еволюцію хмарних обчислень можна простежити за трьома окремими хвилями. Перша хвиля характеризується колокацією і пропонувала користувачам фінансові вигоди від оренди фізичного простору в центрах обробки даних. Друга хвиля — віртуалізовані центри обробки даних, що замінила фізичну інфраструктуру віртуальними аналогами, зберігши за користувачами контроль конфігурації систем. Третя хвиля, започаткована Google, перейшла до контейнерної архітектури — повністю автоматизованої та еластичної хмари, що поєднує автоматизовані сервіси та масштабовані дані. Ця модель автоматично забезпечує і конфігурує інфраструктуру, необхідну для роботи додатків.

Google Cloud Platform, на якій втілюється ця хмарна модель третьої хвилі, доступна для бізнесу і приватних користувачів. Google стверджує, що в майбутньому компанії все більше диференціюватимуть себе завдяки програмному забезпеченню, яке в основі своїй базуватиметься на високоякісних даних, це означає, що всі компанії є або неминуче стануть дата-орієнтованими на.

## 3.2 Взаємодія з Google Cloud

Google Cloud пропонує чотири основні способи доступу до своїх сервісів та взаємодії з ними:

— Веб-графічний інтерфейс користувача (хмарна консоль), що дозволяє користувачам розгортати, керувати, відстежувати та усувати несправності ресурсів. Цей інтерфейс забезпечує централізовану платформу для управління ресурсами, перевірки працездатності, контролю бюджету, пошуку та доступу до віртуальних машин по SSH.

— Cloud SDK і Cloud Shell: Cloud SDK надає набір інструментів командного рядка для управління ресурсами і додатками Google Cloud, включаючи Google Cloud CLI для загальної взаємодії і bq для BigQuery. Cloud Shell пропонує доступ до хмарних ресурсів за допомогою браузера на основі командного рядка з попередньо налаштованою віртуальною машиною Debian з постійною директорією і легкодоступними, автентифікованими інструментами Cloud SDK.

— Хмарні сервіси Google надають інтерфейси API для забезпечення програмного керування за допомогою спеціального коду. Бібліотеки Cloud Client і Google API Client доступні на багатьох мовах програмування (Java, Python, PHP, C#, Go, Node.js, Ruby, C++), що спрощує інтеграцію API.

— Мобільний додаток, що дозволяє користувачам керувати екземплярами Compute Engine і Cloud SQL, контролювати додатки App Engine, отримувати доступ до платіжних відомостей та сповіщень, візуалізувати ключові метрики та отримувати сповіщення про інциденти.

## 3.3 Створення віртуальної машини

Для початку роботи необхідно активувати Cloud Shell у верхній частині консолі Google Cloud. Після з’єднання, користувач вже автентифікований, а проєкт

має унікальний ідентифікатор Project_ID.

gcloud — це інструмент командного рядка він постачається інтегрованим в Cloud Shell. Для створення віртуальної машини необхідно скористатись наступною командою:

«gcloud compute instances create instance1
--project=Project_ID
--zone=us-east1-c
--machine-type=e2-medium
{…}
type=IPV4_ONLY,subnet=default
{…}
--tags=http-server
--create-disk=auto-delete=yes,boot=yes,device
name=instance1,image=projects/debian-cloud/global/images/debian-12-bookworm-v20240415, {…}»

«gcloud compute instances create instance» — це основна команда для створення нового екземпляра віртуальної машини Google Compute Engine. Значення параметрів: «--project=Project_ID» вказує проект Google Cloud, у якому буде створено віртуальну машину, «--zone=us-east1-c» зона розташування віртуальної машини, «--machine-type=e2-medium» виділяє ресурси процесора та пам'яті, «type=IPV4_ONLY,subnet=default» конфігурація мережі, «...instance,image =projects/debian-cloud/global/images/debian-12...» операційна система.

## 3.4 Огляд хмарних логів

Google Cloud Logging (GCL) слугує централізованим сервісом керування

журналами в екосистемі Google Cloud Platform (GCP). Він відіграє ключову роль у забезпеченні ситуаційної обізнаності мережі, агрегуючи, зберігаючи та дозволяючи аналізувати дані журналів, що надходять з різних ресурсів GCP, додатків і навіть користувацьких екземплярів віртуальних машин. Короткий опис функіональності кожного блоку на сторінці Cloud Logging (рис. 3.1):

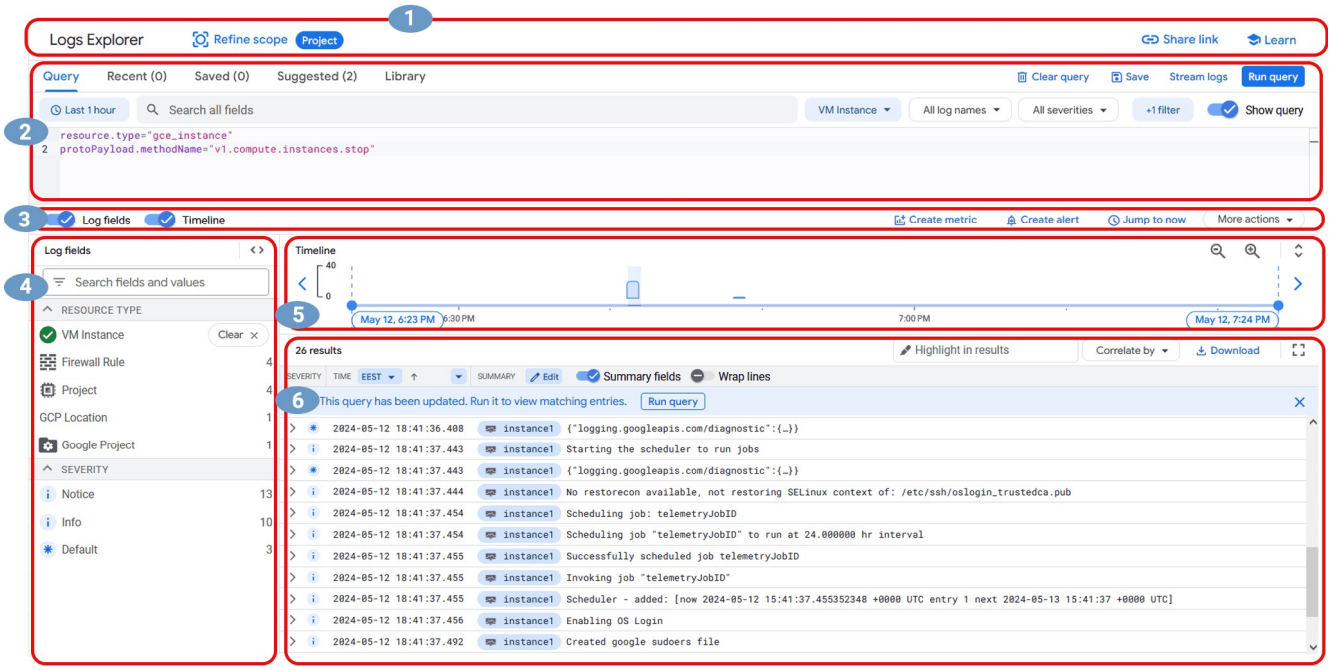



Рисунок 3.1 — Графічний інтерфейс інструменту Cloud Logging

— Панель операцій (1). Використовується для маніпуляцій над записами журналу: створення, збереження та завантаження запитів; фільтрування; потокового відтворення у реальному часі; експорту у різні формати.

— Панель запитів (2) використовується для пошуку, фільтрації та агрегування даних журналу на основі певних критеріїв.

— Панель (3) надає інструменти для керування відображеними результатами запиту: налаштування часового діапазону, посторінковий перегляд, групування та сортування, завантаження результатів у форматі CSV або JSON

— Панель спеціалізації логів (4) надає інформацію про тип і формат даних.

— Часовий графік (5) надає візуальне представлення розподілу записів у

журналі в часі чим допомагає виявити тенденції та закономірності.

— Панель (6) показує результати виконаного запиту. Записи журналу відображаються у табличному форматі з відповідними полями. Їх можна розгорнути, щоб переглянути повну інформацію, включно з необробленим повідомленням логу.

Метрики на основі журналів, отримані з кластерів Google Kubernetes Engine (GKE), є незамінними для комплексного моніторингу системи. GKE полегшує централізовану агрегацію журналів завдяки інтеграції з операційним інструментарієм Google Cloud, уможливлюючи аналіз і сповіщення в режимі реального часу. Такий спрощений доступ до журналів прискорює процеси виявлення несправностей і їх усунення, а отримані метрики дають уявлення про продуктивність додатків і використання інфраструктури, сприяючи оптимізації системи. Крім того, метрики на основі журналів полегшують аудит безпеки, відстежуючи такі події, як спроби автентифікації та підозрілу активність. Для розгортання стандартного кластера GKE необхідно виконати наступну команду в cloud shell:

«gcloud container clusters create gmp-cluster --num-nodes=1 --zone us-east1-c»

Для роботи з метриками необхідно створити робочий простір імен за допомогою:

«kubectl create ns gmp-test»

Тепер, щоб розгорнути просту програму, яка відправлятиме метрики в кінцеву точку виконується:

«kubectl -n gmp-test apply -f

https://storage.googleapis.com/spls/gsp091/gmp_flask_deployment.yaml»

Де частина запиту після «-f» вказує на розташування YAML-файлу, який визначає розгортання — це ресурс, який керує набором реплік-подів (у цьому випадку запущених екземплярів програми Flask, популярного веб-фреймворку Python) і забезпечує їхню належну роботу.

«kubectl -n gmp-test apply -f

https://storage.googleapis.com/spls/gsp091/gmp_flask_service.yaml»

Ця команда дуже схожа на першу але керує службою і вказує на розташування YAML-файлу, який визначає сервіс який надаватиме стабільну кінцеву точку мережі (наприклад, IP-адресу та порт) для доступу до реплік-подів програми. Переконатися, що додаток Python Flask подає метрики можна за допомогою наступної команди (сервіси в просторі імен "gmp-test" виставляються через балансувальник навантаження і мають кінцеву точку /metrics):

«curl $(kubectl get services -n gmp-test -o jsonpath='{.items[*].status.loadBalancer.ingress[0].ip}')/metrics»

У ній використовується інструмент командного рядка «kubectl» для взаємодії з кластером Kubernetes. «get services» отримує інформацію про всі сервіси у вказаному просторі імен («-n gmp-test»). «-o jsonpath='{.items[*].status. loadBalancer.ingress[0].ip}'» фільтрує вивід, щоб витягти лише IP-адресу балансувальника навантаження (точки входу для зовнішнього трафіку), пов'язану з кожним сервісом. Потім використовується команда «curl» для отримання кінцевої точки /metrics від сервісу, що працює за знайденою IP-адресою. Ця кінцева точка зазвичай надається програмами, оснащеними Prometheus, популярним інструментарієм для моніторингу та сповіщення.

Щоб створити метрику за якою потім здійснюватиметься оповіщення необхідно повернутись в Cloud Explorer та у панелі № 3 (зображена на рис. 3.1) перейти в меню створення показника (рис. 3.2)

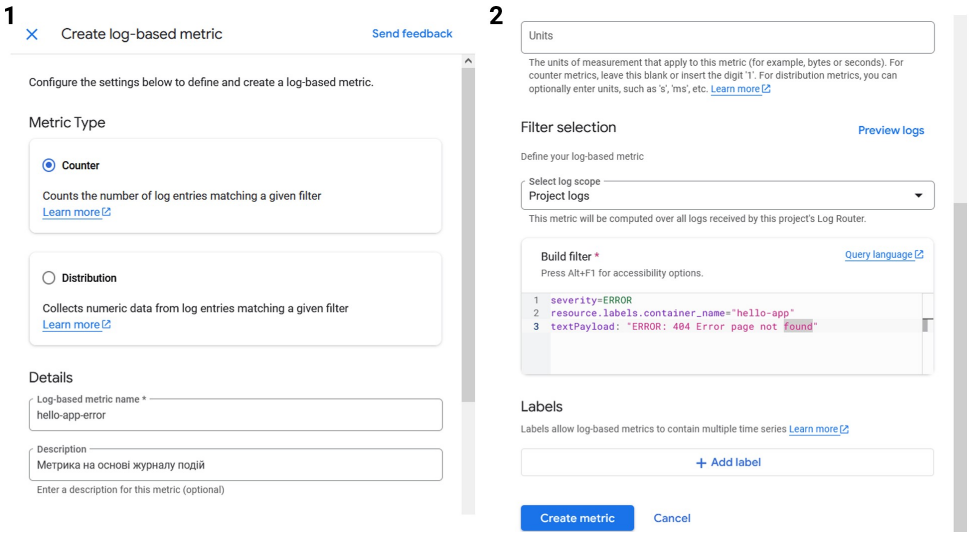



Рисунок 3.2 — Вікно створення показника на базі записів журналу

Для створення оповіщень за створеними метриками у лівій частині вікна «Logging» необхідно обрати «Log-based metrics». Потім у визначених користувачем показниках натиснути 3 вертикальні крапки і обрати «Create alert from metric». Залишити налаштування стандартними, перейшовши у вкладку «Нотифікації та назва» де потрібно налаштувати канал зв'язку (електронна пошта на яку відправлятиметься повідомлення). В меню «Канали сповіщення» додати пошту.

### 3.5 Створення аномальної поведінки (людська помилка)

Для того, щоб спровокувати систему оповіщення налаштовану в попередньому підрозділі необхідно згенерувати кілька помилок відповідно до створеної метрики використавши наступну команду в Cloud Shell:

«timeout 120 bash -c -- 'while true; do curl $(kubectl get

services -n gmp-test -o

jsonpath='{.items[*].status.loadBalancer.ingress[0].ip}')/error;

sleep $((RANDOM % 4)) ; done'»

Ця команда поєднує декілька утиліт Unix і Kubernetes і її дію можна було спостерігати на часовому графіку починаючи з 22:25 (рис. 3.3.)

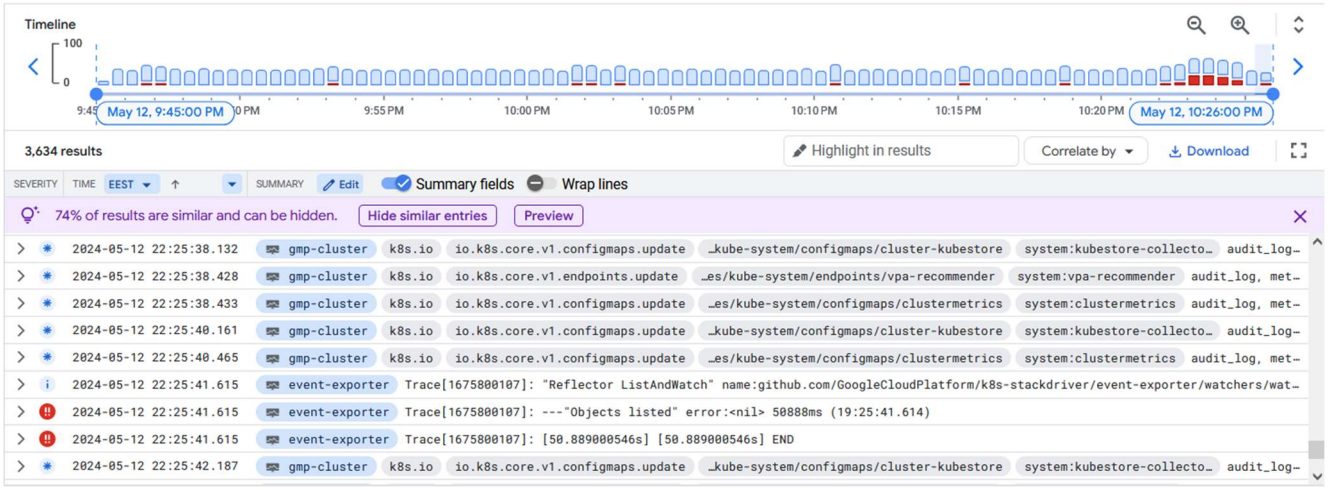



Рисунок 3.3 — Візуалізація поширенння помилок

Для того щоб глибше дослідити помилки необхідно перейти в розділ «Серйозність» далі «Помилки». На сторінці можна побачити переважно «404 Error Not Found». Щоб переглянути додаткову інформацію, потрбно розгорнути одне з повідомлень про помилку 404, (рис. 3.4). Цей запис вказує на те, що 12 травня, 2024 року, о 7:24:45 за східноєвропейським часом, з IP-адреси 10.84.0.1 був зроблений запит до URL-адреси "http://104.196.63.124/error". У відповідь на нього сервер за цією адресою видав відповідь "404 Помилка, сторінка не знайдена". Це може бути пов'язано з неправильно введеною URL-адресою, видаленою сторінкою або неправильною конфігурацією на сервері. Адже налаштування стосувались кінцевої точки «/metrics» не «/error».

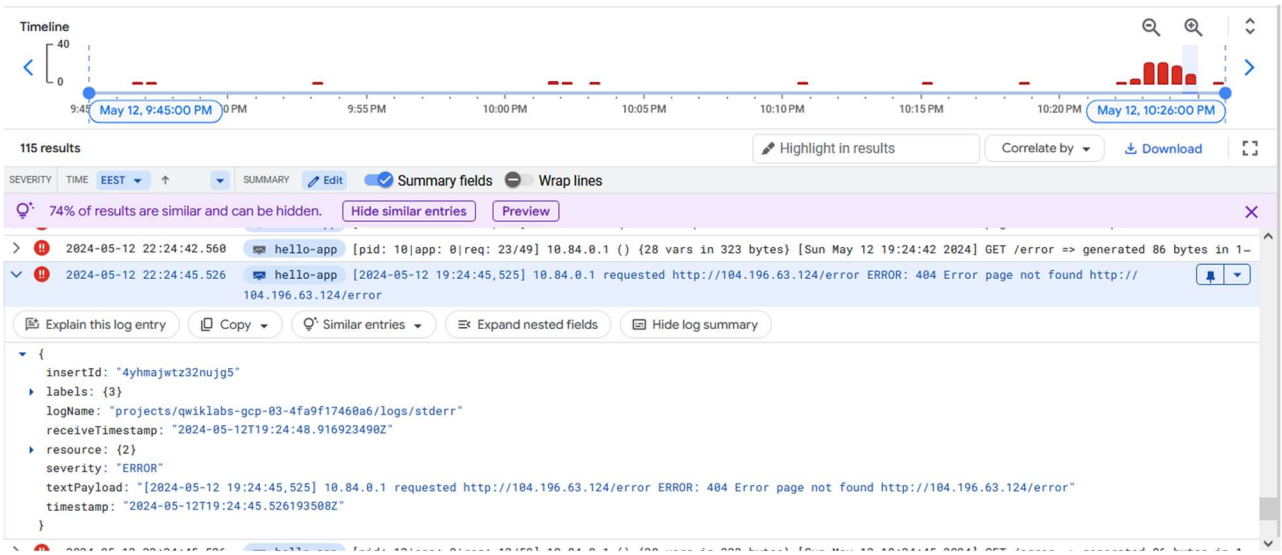



Рисунок 3.4 — Деталі одного з записів

# ВИСНОВКИ

У кваліфікаційній роботі досліджено концепцію ситуаційної обізнаності (далі СО) в контексті мережевої безпеки та виявлення аномалій. Адаптуючи відомі моделі ситуаційної обізнаності, було розглянуто, як мережеві аналітики можуть використовувати інфраструктуру для покращення розуміння кіберзагроз та визначення пріоритетів реагування на них.

Зокрема, проаналізовано складність ландшафту кіберзагроз, підкреслено важливість збору, аналізу даних та етичних міркувань при моніторингу мережі. Інтеграція людського досвіду з автоматизованими інструментами, особливо в інтерпретації мережевих потоків і виявленні аномалій, була визначена як вирішальна для ефективної СО.

За допомогою практичних демонстрацій на хмарній платформі Google було продемонстровано можливості хмарних віртуальних машин і механізмів логування для створення та виявлення аномальної поведінки. Ці приклади підкреслюють потенціал хмарних платформ у підтримці ініціатив з мережевої безпеки.

Подальші дослідження можуть бути спрямовані на вивчення більш досконалих методів виявлення аномалій, алгоритмів машинного навчання і розробку комплексних фреймворків СО, пристосованих до конкретних мережевих середовищ. Зрештою, мета полягає в тому, щоб надати мережевим аналітикам інструменти і знання для проактивної протидії кіберзагрозам і забезпечення безпеки і стійкості цифрової інфраструктури.

# ПЕРЕЛІК ПОСИЛАНЬ


1. Gilson R. D. Special Issue Preface. Human Factors: The Journal of the Human Factors and Ergonomics Society. 1995. Т. 37, № 1. С. 3–4. URL: https://doi.org/10.1518/001872095779049426 (дата звернення: 06.05.2024).

2. Jensen R. S. The Boundaries of Aviation Psychology, Human Factors, Aeronautical Decision Making, Situation Awareness, and Crew Resource Management. The International Journal of Aviation Psychology. 1997. Т. 7, № 4. С. 259–267. URL: https://doi.org/10.1207/s15327108ijap0704_1 (дата звернення: 06.05.2024).

3. Norman D. A. The ‘problem’ with automation: inappropriate feedback and interaction, not ‘over-automation’. Human Factors in Hazardous SituationsProceedings of a Royal Society Discussion Meeting held on 28 and 29 June 1989. 1990. С. 137–146. URL: https://doi.org/10.1093/acprof:oso/9780198521914.003.0014 (дата звернення: 06.05.2024).

4. Adams M. J., Tenney Y. J., Pew R. W. Situation Awareness and the Cognitive Management of Complex Systems. Human Factors: The Journal of the Human Factors and Ergonomics Society. 1995. Т. 37, № 1. С. 85–104. URL: https://doi.org/10.1518/001872095779049462 (дата звернення: 07.05.2024).

5. Owen T. Tasks, Errors And Mental Models by L.P. Goodstein, H.B. Andersen and S.E. Olsen, Taylor & Francis, London, U.K., 1988 (Price £35). Robotica. 1988. Т. 6, № 3. С. 259. URL: https://doi.org/10.1017/s0263574700004446 (дата звернення: 07.05.2024).

6. Reason J. Human error. Cambridge : Cambridge University Press, 1990. 302 с. (дата звернення: 07.05.2024).

7. Endsley M. R. Design and Evaluation for Situation Awareness Enhancement. Proceedings of the Human Factors Society Annual Meeting. 1988. Т. 32, № 2. С. 97–101. URL: https://doi.org/10.1177/154193128803200221 (дата звернення: 07.05.2024).

8. Klein G., Crandall B. Recognition-Primed Decision Strategies. Fort Belvoir, VA : Defense Technical Information Center, 1990. URL: https://doi.org/10.21236/ada226887 (дата звернення: 07.05.2024).

9. Bedny G., Meister D. Theory of Activity and Situation Awareness. International Journal of Cognitive Ergonomics. 1999. Т. 3, № 1. С. 63–72. URL: https://doi.org/10.1207/s15327566ijce0301_5 (дата звернення: 08.05.2024).

10. Smith K., Hancock P. A. Situation Awareness Is Adaptive, Externally Directed Consciousness. Human Factors: The Journal of the Human Factors and Ergonomics Society. 1995. Т. 37, № 1. С. 137–148. URL: https://doi.org/10.1518/001872095779049444 (дата звернення: 08.05.2024).

11. Osinga F. ‘Getting’ A Discourse on Winning and Losing: A Primer on Boyd's ‘Theory of Intellectual Evolution’. Contemporary Security Policy. 2013. Т. 34, № 3. С. 603–624. URL: https://doi.org/10.1080/13523260.2013.849154 (дата звернення: 08.05.2024).

12. A Discourse on Winning and Losing Col John R. Boyd, USAF, Retired Edited and Compiled by Dr. Grant T. Hammond Apendix the OODA Loop. cc. 384-385. Air University Press. Maxwell AFB, Alabama. March 2018. (дата звернення: 09.05.2024).

13. Schwartz J. T., von Neumann J., Burks A. W. Theory of Self-Reproducing Automata. Mathematics of Computation. 1967. Т. 21, № 100. С. 745. URL: https://doi.org/10.2307/2005041 (дата звернення: 09.05.2024).

14. Hauben M., Hauben R. Behind the Net: The Untold Story of the ARPANET and Computer Science (Chapter 7). First Monday. 1998. Т. 3, № 8. URL: https://doi.org/10.5210/fm.v3i8.612 (дата звернення: 07.05.2024).

15. 2014 Index IEEE Communications Surveys & Tutorials Vol. 16. IEEE Communications Surveys & Tutorials. 2014. Т. 16, № 4. С. 2286–2301. URL: https://doi.org/10.1109/comst.2014.2374511 (дата звернення: 07.05.2024).

16. Basili, V. R., & Yawn, J. (2003). Cybersecurity situational awareness: A collaborative approach. Proceedings of the 10th IEEE International Workshop on

Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003. WETICE 2003., сс. 239-244. (дата звернення: 08.05.2024)

17. National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity Version  A Multi-Criteria Decision Analysis Framework for Cybersecurity Risk Assessment" by Wu et al. (2019)

18. Addendum to ISO 7498 covering connectionless mode transmission. / ред. Great Britain. Department of Trade and Industry. IT Standards Unit. London : IT Standards Unit, 1984. (дата звернення: 09.05.2024).

19. Information Society Policy Link, linking European policies / ред. European Commission. Information Society DG. [Luxembourg : Office for Official Publications of the European Communities, 2005. (дата звернення: 09.05.2024).

20. Freire-Garabal y Núñez M. General Vision of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016. Al-Khalifa Business School. 2020. URL: https://doi.org/10.21428/18d9181c.39ae71fc (дата звернення: 10.05.2024).

21. Directive 2002/58/EC of the European Parliament and of the Council. Fundamental Texts On European Private Law. 2016. URL: https://doi.org/10.5040/9781782258674.0020 (дата звернення: 10.05.2024).

22. Samarati P. Protecting respondents identities in microdata release. IEEE Transactions on Knowledge and Data Engineering. 2001. Т. 13, № 6. С. 1010–1027. URL: https://doi.org/10.1109/69.971193 (дата звернення: 10.05.2024).

23. Mell P. M., Grance T. The NIST definition of cloud computing. Gaithersburg, MD : National Institute of Standards and Technology, 2011. URL: https://doi.org/10.6028/nist.sp.800-145 (дата звернення: 10.05.2024).

Додаток А

# ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ.
*Інститут інформаційних технологій. Кафедра Комп'ютерної інженерії.*


## БАКАЛАВРСЬКА РОБОТА

на тему: «Система ситуативної обізнаності: аналіз логів та виявлення аномалій мережі на базі платформи Google Cloud»

Виконав студент групи КІД-41
Рекун Денис Сергійович

Керівник дипломної роботи:
Кондратюк Борис Ігорович,
викладач кафедри КІ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ.
*Інститут інформаційних технологій. Кафедра комп'ютерної інженерії.*

## МЕТА РОБОТИ

Розгляд доступності технологій ситуативної обізнаності для застосування під час експлуатації мережевої інфраструктури.

## ОБ'ЄКТ ДОСЛІДЖЕННЯ

Адаптація загальних принципів ситуативної обізнаності до мережевого аналізу.

## ПРЕДМЕТ ДОСЛІДЖЕННЯ

Ідентифікація та інформування про аномальну поведінку мережі на хмарній платформі Google Cloud.

# Еволюція кіберзагроз




ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ.
*Інститут інформаційних технологій. Кафедра комп'ютерної інженерії.*

# Класи комп'ютерних атак

### Хробак

самовідтворюється і поширюється через *мережеві сервіси*

### Вірус

самовідтворюється і заражає систему *без відома або дозволу* користувача.

### Троян

виглядає *як корисна програма*, але насправді має секретний код, який може створити чорний хід до системи

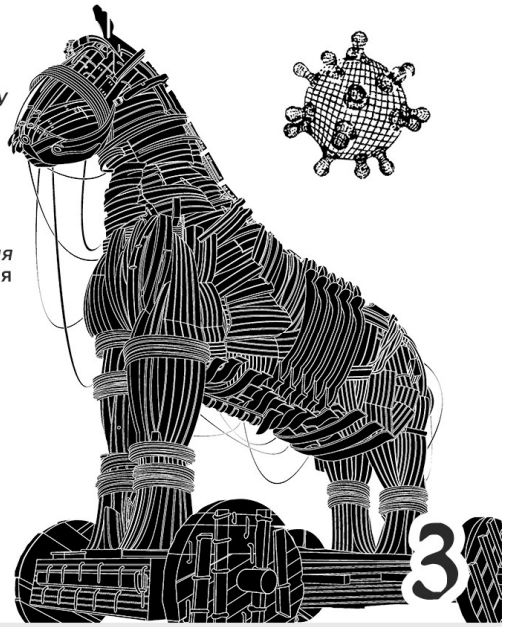
### DoS

примусового *перенавантаження* комп'ютера шляхом споживання *апаратних* обчислювальних *ресурсів*

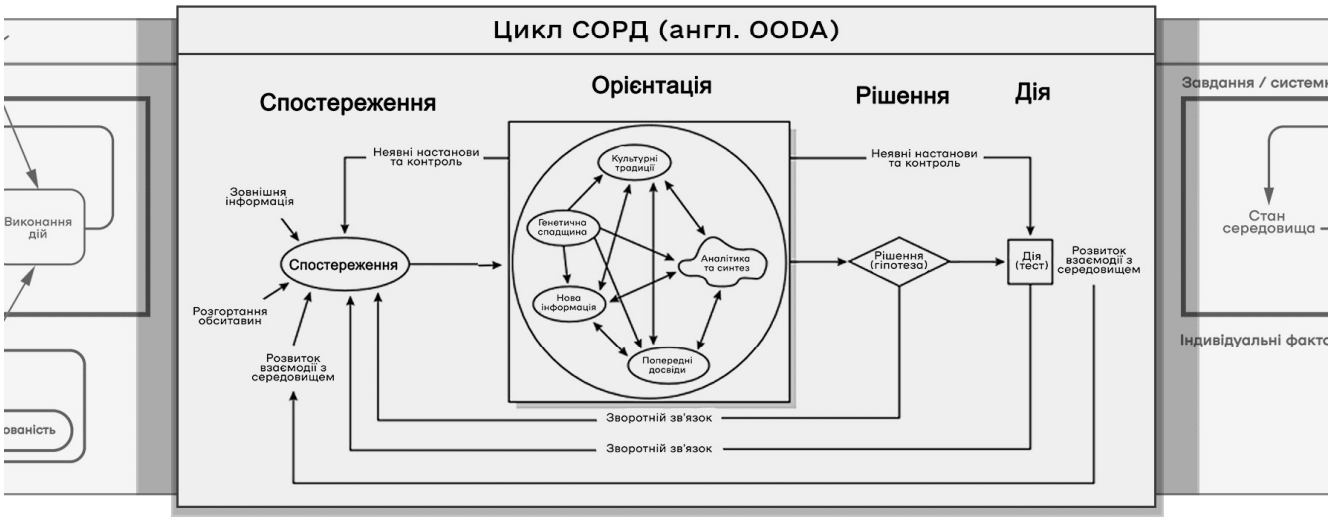
### Пакетна ін'єкція

процес *конструювання пакетів* так, щоб вони виглядали як частина нормального потоку зв'язку

...



# Моделі ситуативної обізнаності




4

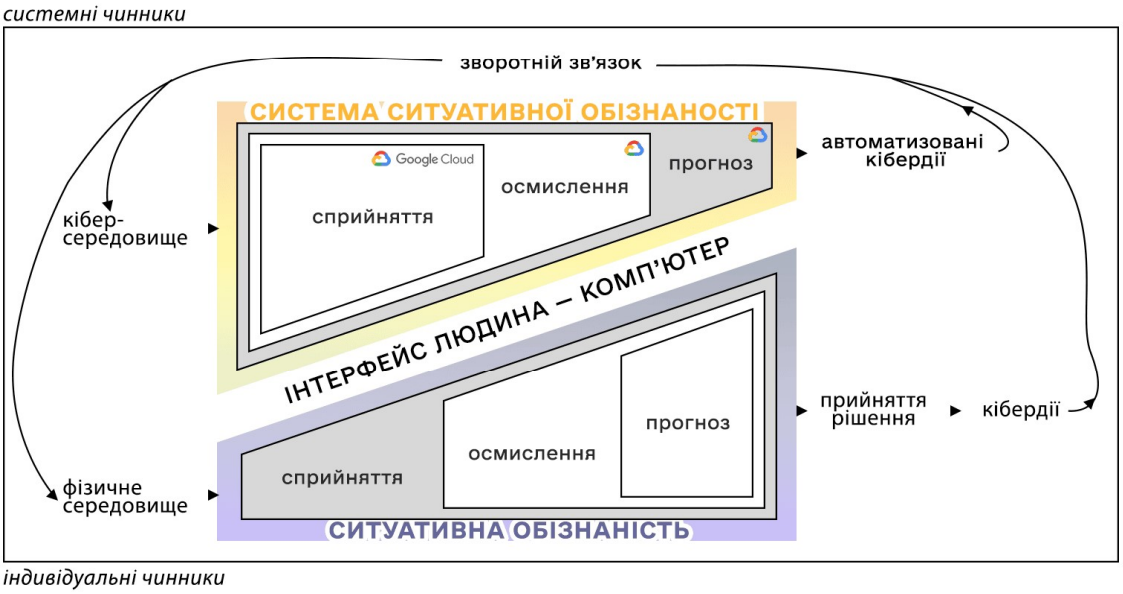


ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ.
*Інститут інформаційних технологій. Кафедра комп'ютерної інженерії.*

# Моделі ситуативної обізнаності


5

# Адаптація трирівневої моделі




6



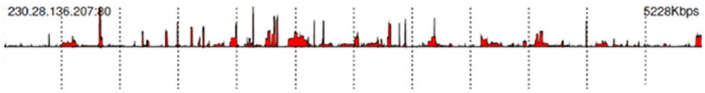


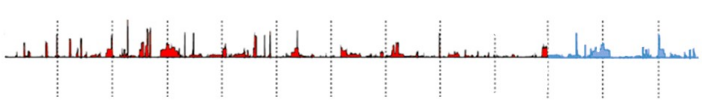
# Мережевий потік

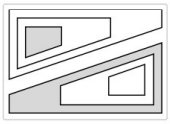

7

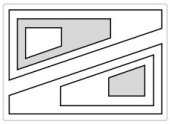
# Приклади роботи системи СО

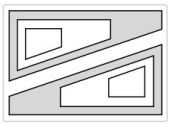
```
          sIP|          dIP|sPort|dPort|pro|packets|flags|initF|  type|
192.168.1.105| 198.51.100.6|49152|   80|  6|      4| SRPA| S   |outweb|
 198.51.100.6|192.168.1.105|   80|49152|  6|      3| S PA| S  A| inweb|
```





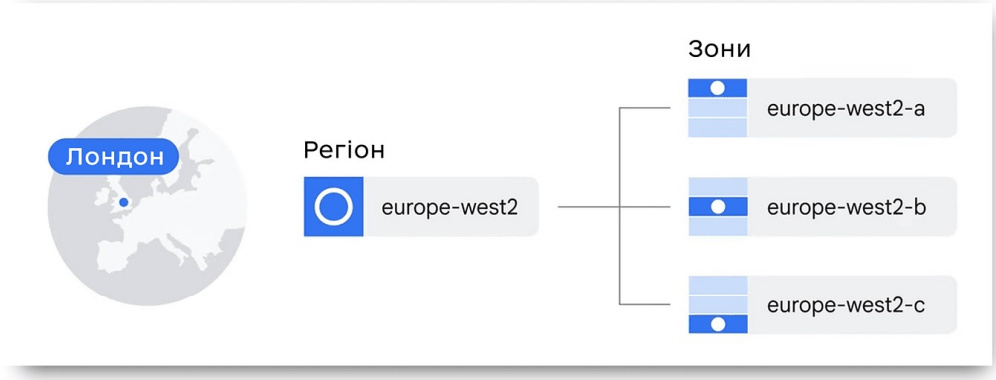








# Google Cloud Platform




cloud.google.com/about/locations.

# Google Cloud Platform

### 1. Належний колектор

***VPC Flow Logs***
Працює на рівні підмережі збирає TCP, UDP, ICMP, ESP та GRE кожної віртуальної машини.

***Packet Mirroring***
Копіювання мережевого трафіку з джерела

### 2. Фільтр та консолідація

***Cloud Logging***
Зберігає та обробляє VPC Flow Logs

***BigQuery***
потужне сховище даних для аналізу великих обсягів даних.

### 3. Візуалізація

***Cloud Monitoring***
Створює власні інформаційні панелі та діаграми для візуалізації показників мережевого трафіку з журналів VPC Flow Logs

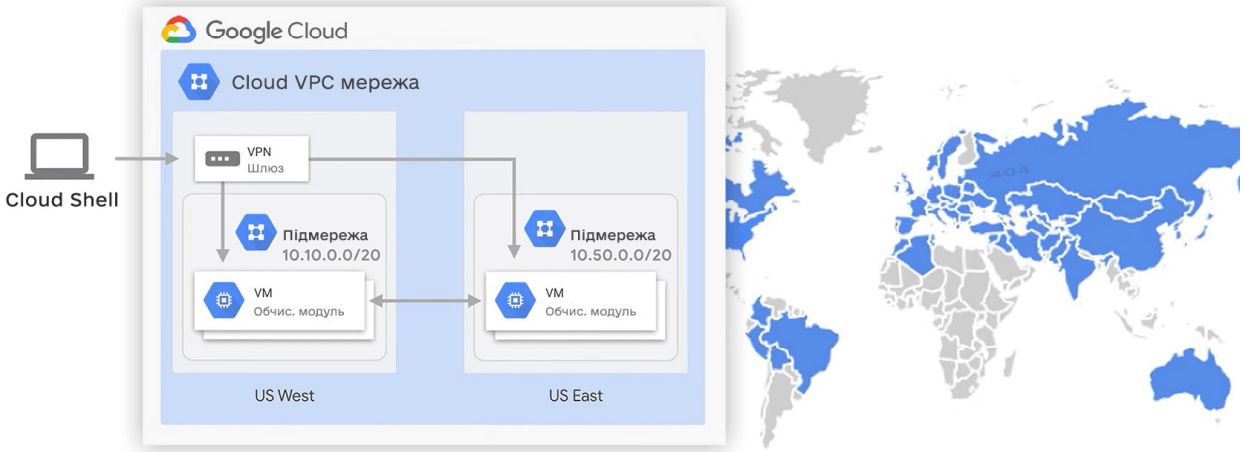
### 4. Генерація звітів

***Cloud Logging***
Дозволяє налаштувати повідомлення про аномалії.



ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ.
*Інститут інформаційних технологій. Кафедра комп'ютерної інженерії.*

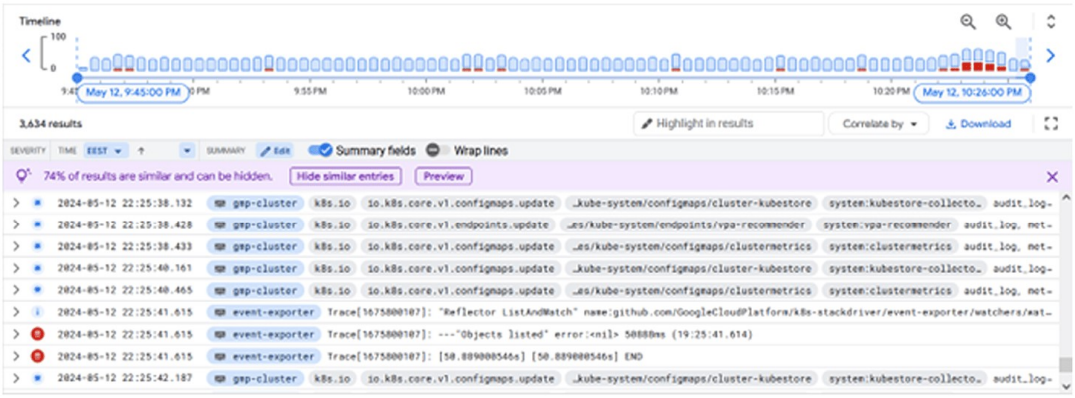
# Конфігурація VPC*




*VPC — Virtual Private Cloud (укр. приватна віртуальна хмарна мережа)

# Генерація аномалій

```
timeout 120 bash -c -- 'while true; do curl $(kubectl get
services -n gmp-test -o
jsonpath='{.items[*].status.loadBalancer.ingress[0].ip}')/error;
sleep $((RANDOM % 4)) ; done'
```




Зміни часового графіку подій у мережі





# Висновки

## 1. Концепція ситуативної обізнаності

У кваліфікаційній роботі досліджено концепцію ситуаційної обізнаності (далі СО) в контексті мережевої безпеки та виявлення аномалій. Адаптуючи відомі моделі ситуаційної обізнаності, було розглянуто, як мережеві аналітики можуть використовувати інфраструктуру для покращення розуміння кіберзагроз та визначення пріоритетів реагування на них.

## 2. Кіберзагрози

Проаналізовано складність ландшафту кіберзагроз, підкреслено важливість збору, аналізу даних та етичних міркувань при моніторингу мережі. Інтеграція людського досвіду з автоматизованими інструментами, особливо в інтерпретації мережевих потоків і виявленні аномалій, була визначена як вирішальна для ефективної СО.

## 3. Хмарна платформа Google Cloud

За допомогою практичних демонстрацій на хмарній платформі Google було продемонстровано можливості хмарних віртуальних машин і механізмів логування для створення та виявлення аномальної поведінки. Ці приклади підкреслюють потенціал хмарних платформ у підтримці ініціатив з мережевої безпеки.

# Продовження висновків

## 4. Подальші дослідження

можуть бути спрямовані на вивчення більш досконалих методів виявлення аномалій, алгоритмів машинного навчання і розробку комплексних фреймворків СО, пристосованих до конкретних мережевих середовищ. Зрештою, мета полягає в тому, щоб надати мережевим аналітикам інструменти і знання для проактивної протидії кіберзагрозам і забезпечення безпеки і стійкості цифрової інфраструктури.