ШИФР «СВІТЯЗЬ»

«Розробка моделі центру управління мережею»

Київ – 2021 року

ЗМІСТ

АНОТАЦІЯ

ШИФР РОБОТИ «СВІТЯЗЬ»

ТЕМА РОБОТИ: «РОЗРОБКА МОДЕЛІ ЦЕНТРУ УПРАВЛІННЯ МЕРЕЖЕЮ»

Для ефективного управління комп’ютерною мережею необхідно контролювати стан кожного її елемента з можливістю змінювати параметри його функціонування. Постійний контроль за роботою мережі необхідний для підтримки її в працездатному стані. Зазвичай мережа складається з різних за своїм фізичним змістом та функціональним змістом елементів, ефективне керувати якими і являє собою найголовнішим завданням. Оскільки кожен з елементів мережі розуміє виключно свою систему команд то виникає необхідність в єдиному способі побудови та управління мережевими ресурсами, який буде використовуватись в системі управління мережею для ефективної взаємодії між пристроями.

Мета: розробка моделі центру управління мережею для забезпечення виконання визначених функцій на основі NOC.

Об’єктом розгляду даної роботи є процес управління мережею з заданою якістю.

Предметом дослідження є розробка моделі центру управління мережею на основі NOC.

Завдання:

– проведення аналізу принципів побудови та управління комп'ютерними мережами в контексті забезпечення їх кібербезпеки;

– дослідження організаційної структури центру управління мережею для побудови її функціональної моделі;

– практична реалізація центру управління мережею, відповідно етапам розробки моделі з метою забезпечення його функцій на основі NOC.

Використана методика дослідження: розробка моделі центру управління мережею, формулювання основних функцій та етапів процесу управління

мережевою інфраструктурою з використанням програмного забезпечення на основі NOC.

Загальна характеристика роботи: зміст, перелік умовних скорочень, анотація, вступ, основна частина (3 питання), висновки, список літератури, додатки.

Обсяг роботи: 30 сторінок.

Кількість схем: 6.

Кількість використаних наукових джерел:17.

Ключові слова: забезпечення кібербезпеки, інформаційний простір, центр управління мережею, NOC, інформаційна безпека.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АС – Автоматизована інформаційна система

ІБ – Інформаційна безпека

ІТС – Інформаційно-телекомунікаційна система

API – ApplicationProgrammingInterface(інтерфейс прикладного програмування)

DLP – DataLossPrevention (запобігання витоків конфіденційної інформації)

ISCM – InformationSecurityCntinuousMonitoring (програма безперервного моніторингу інформаційної безпеки)

NOC – NetworkOperationsCenter (центр управління мережею)

SIEM – SecurityInformationandEventManagement (управління інформацією про безпеку і подіями безпеки)

SLA – ServiceLevelAgreement (угода про рівень обслуговування)

SNMP – SimpleNetworkManagementProtocol (простий протокол мережевого управління)

SOC – SecurityOperationsCenter (операційний центр безпеки)

ВСТУП

Науково-технічна революція початку XXI сторіччя спричинила в усьому світі глибокі системні перетворення. Передусім завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем, сформувалися принципово нові глобальні субстанції – інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в розвитку кожної країни світу.

Для успішного адміністрування мережі необхідно знати стан кожного її елемента з можливістю змінювати параметри його функціонування. Постійний контроль за роботою мережі необхідний для підтримки її в працездатному стані. Зазвичай мережа складається з пристроїв різних виробників і керувати нею було б нелегким завданням якби кожен з мережевих пристроїв розуміло тільки свою систему команд.Тому виникла необхідність у створенні єдиного способу управління мережевими ресурсами, який буде використовуватись в системі управління мережею для взаємодії з конкретними пристроями.

Для вирішення поставленогозавдання використовується поняття NetworkOperationsCenter– центр управління мережею, який вирішує поточні завдання функціонування мережі: здійснює цілодобовий моніторинг і управління мережевою інфраструктурою, дозволяє знижувати аварійність, забезпечувати високу продуктивність мережі, підвищуючи ефективність надання послуг при одночасному зниженні ризиків.

РОЗДІЛ І
АНАЛІЗ ПРОБЛЕМАТИКИ УПРАВЛІННЯ КОМП'ЮТЕРНИМИ МЕРЕЖАМИВ КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ЇХ КІБЕРБЕЗПЕКИ

1.1 Забезпечення кібербезпеки в ІТС

Науково-технічна революція початку XXI сторіччя спричинила в усьому світі глибокі системні перетворення. Передусім завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем, сформувалися принципово нові глобальні субстанції – інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу.

Протягом останніх років Україна, як і більшість інших країн світу, робить впевнені кроки в напрямку розбудови інформаційного суспільства, забезпечення кібербезпеки та боротьби з кіберзлочинністю.Такий стан справ фактично означає, що Україна поступово нагромаджує важливий досвід у захисті власної ІТ-інфраструктури від кіберзагроз сучасності та протидії проявам кібертероризму. Утім протистояти фізичному руйнуванню технічних засобів, дезорганізації роботи інформаційних систем і мереж, порушенню функціонування об’єктів нападу, а також протиправній діяльності соціальних інженерів в умовах інтенсифікації кібервтручань з дня на день стає все важче.

Вочевидь, чинити дієвий опір таким агресивним діям дуже складно. Адже заходи з ефективного запобігання небажаним витокам інформації мають крім суто технічних механізмів спиратися на методи й засоби соціального інжинірингу. Поступове й доволі умовне поєднання віртуального і реального просторів за допомогою ІТС і мережних технологій різного функціонального призначення, які в процесах обробки, передавання та зберігання інформації

використовують електромагнітний спектр і діють як єдине ціле, а також відповідного програмного забезпечення призвело, зрештою, до формування кіберпростору (рис. 1.1) – високорозвиненої моделі об'єктивної реальності, в якій відомості щодо осіб, предметів, фактів, подій, явищ і процесів [3]: подаються в деякому математичному, символьному (як сигнали, знаки, звуки, рухомі або нерухомі зображення) або в будь-якому іншому вигляді; розміщуються в пам'яті будь-якого фізичного пристрою, спеціально призначеного для зберігання, обробки й передавання інформації; перебувають у постійному русі по сукупності ІТ-систем і мереж.

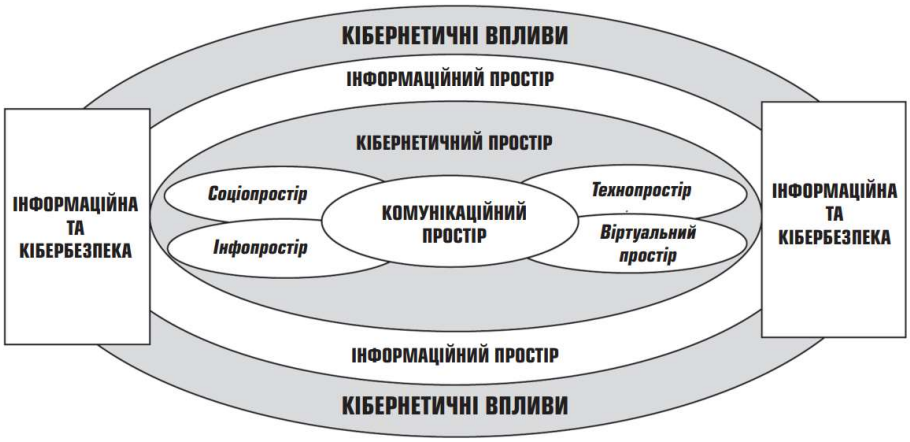

Рисунок 1.1 – Взаємозв'язок інформаційного та кіберпросторів

Сфера дії терміну «кіберпростір» перебувала під впливом загальних механізмів правового регулювання суспільних відносин, обмежуючись специфічними об'єктами й інтересами суб'єктів правовідносин, а також комп'ютерними мережами, за допомогою яких можна брати участь у відповідних правовідносинах. Відповідно до міжнародного стандарту, кіберпростір – це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення і послуг в інтернеті за допомогою технологічних пристроїв і мереж, під'єднаних до них, якого не існує в будь-якій фізичній формі. З урахуванням характерних особливостей кіберпростору як сфери вчинення заздалегідь спланованих деструктивних дій на кшталт проникнення в ІТС один одного, блокування або виведення з ладу найбільш

уразливих елементів цих систем, дезорганізації оборонних автоматизованих систем управління протилежної сторони, систем управління її транспортом і енергетикою, економікою й фінансовою системою і своєрідної сполученої ланки між такими поняттями, як інтернет і кібернетика, усе це, у свою чергу, дає змогу: виокремити в цьому просторі систему певних відношень між суб'єктами та об'єктами інформаційної й кібернетичної інфраструктури; схарактеризувати злочини, втручання і загрози, пов'язані з особливостями існування та передавання інформації; визначитись із можливими його дійовими особами (рис. 1.1); тощо.

З огляду на сказане, під кіберпростором розмітимо середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет або інших мереж передачі даних [3].

Рисунок 1.1 – Дійові особи кіберпростору та їх вплив на інформаційну і кібербезпеку

При цьому інформаційну безпеку (ІБ) у найзагальнішому розумінні можна визначити як такий стан захищеності інформаційного простору держави, за якого неможливо завдати збитку властивостям об’єкта безпеки, що стосуються інформації та інформаційної інфраструктури, і який гарантує безперешкодне формування, використання й розвиток національної інфосфери в інтересах оборони.Спектр інтересів ІБ щодо інформації, інформаційних систем та інформаційних технологій як об’єктів безпеки можна поділити на такі основні категорії (рис. 1.2).

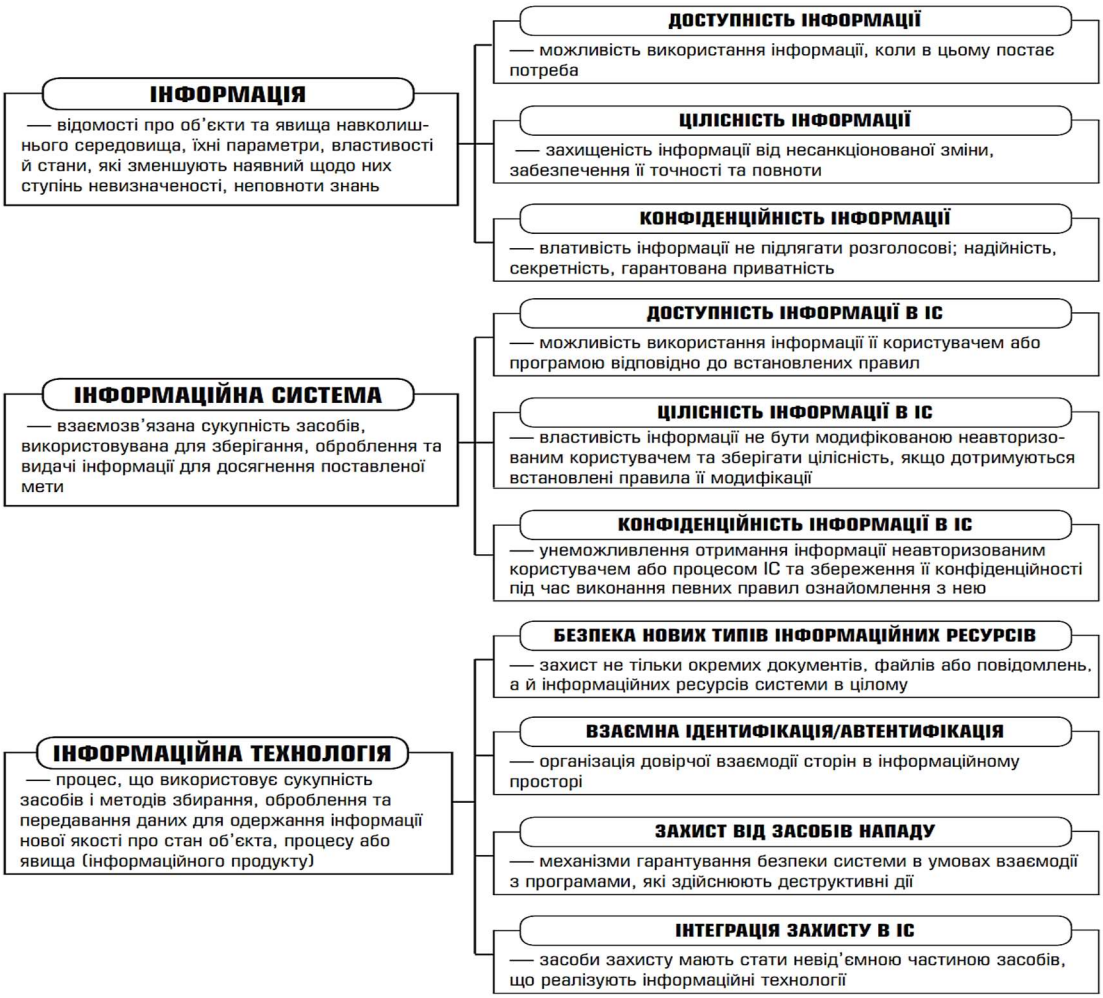

Рисунок 1.2 – Інформаційні системи та технології як об’єкти ІБ

Головні загрози, які можуть спричинити порушення цих категорій, а також негативно вплинути на компоненти інформаційної системи, призвівши навіть до їх втрати, знищення чи збою функціонування, такі: розголошення інформації, її витік або несанкціонований доступ до такої інформації:розголошення, витік, несанкціонований доступ.

Методи, завдяки яким цьому можна запобігти, забезпечивши відповідний рівень ІБ, доцільно класифікувати так: сервіси мережної безпеки;інженерно-технічні методи;правові організаційні татеоретичні методи забезпечення.

Кібербезпека – стан захищеності кіберпростору держави в цілому або окремих об’єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам.

Такі дії спрямовуються на досягнення і утримання потенційними протиборчими сторонами переваги у протидії новим загрозам безпеці для власних об’єктів критично важливої фізичної, інформаційної та кіберінфраструктури. Головні проблеми забезпечення кібернетичної безпеки постають з таких причин: термінологічна та нормативно-правова неврегульованість у сфері кібербезпеки; залежності держави від програмних і технічних продуктів іноземного виробництва;відсутності належної координації діяльності відповідних відомств; тощо.

Сутність кібербезпеки за таких умов зазначає схема, подана на рис. 1.3.

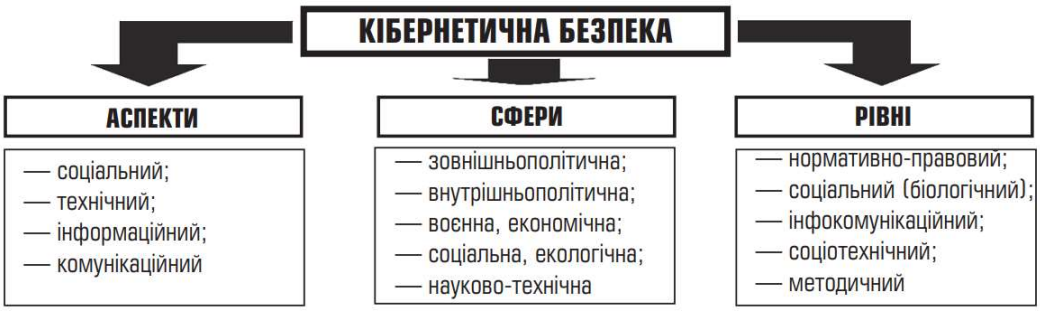

Рисунок 1.3 – Сутність кібернетичної безпеки

1.2 Забезпечення кібербезпеки ІТС операційним центром безпеки.

Більшість компаній прийняли стратегію кібербезпеки "моніторинг та реагування". Ця стратегія, як правило, має місце в операційному центрі безпеки (SOC) абовцентрі управлінні мережею(NOC). У більшості організацій SOC та NOC доповнюють функції один одного [14].

Ролі SOC та NOC не є тонкими, а принципово різними. SOC та NOC несуть відповідальність за виявлення, дослідження, визначення пріоритетності, розширення та вирішення питань, але типи питань та їх вплив значно відрізняються.

Метою NOC є підтримка оптимальної продуктивності та доступності мережі та забезпечення постійного часу роботи. NOC обробляє інциденти та попередження, які впливають на ефективність та доступність. Завданням NOC є управління інцидентами таким чином, що скорочує час простою. Він зосереджений на доступності та продуктивності.

SOC зосереджується на інцидентах та попередженнях, які впливають на безпеку інформаційних активів. Його головна роль – захист інтелектуальної власності та конфіденційних даних про клієнтів – фокус на безпеці.

Сучасний операційний центр безпеки (SOC) повинен включати в себе всі елементи, необхідні для забезпечення повноцінного захисту підприємства в умовах постійно розвиваються IT-технологій. Сюди входить великий набір передових методів виявлення і попередження кіберзагроз, інструменти формування звітності та доступ до швидко зростаючої базі талановитих IT-фахівців. SOC – це центр реагування на критичні інциденти інформаційної безпеки, який дозволяє здійснювати запобігання атак і повний моніторинг на всіх рівнях: мережевих пакетів, мережевих потоків, активності операційної системи, контенту, поведінки користувачів. Платформа SOC зазвичай базується на відмовостійкої конфігурації SIEM, до якої додатково підключені джерела даних про актуальні загрози інформаційної безпеки (що не викликають довіри IP, URL, бот-мережах), одержувані від провідних лабораторій, які займаються виявленням атак і протидією кіберзлочинності. Це дає можливість агрегувати інформацію про погрози, виявляти більше інцидентів і виявляти атаки нульового дня в найкоротші терміни.

SIEM (SecurityInformationandEventManagement) у комп'ютерній безпеці є програмними продуктами, які об'єднують управління інформаційною безпекою SIM (SecurityInformationManagement) та управління подіями безпеки SEM

(SecurityEventManagement). Технологія SIEM забезпечує аналіз в реальному часі подій (тривог) безпеки, отриманих від мережевих пристроїв і додатків. SIEM представлено додатками, приладами або послугами, і використовується також для журналювання даних і генерації звітів.

Типова задача SOC середнього рівня зазвичай включає запобігання інцидентів кібербезпеки:безперервний аналіз загроз;сканування мереж і вузлів для пошуку вразливостей;координація розгортання протидії;консалтинг в області політики безпеки і архітектури;моніторинг, виявлення і аналіз потенційних вторгнень в режимі реального часу і через відстеження трендів із значущих джерел даних в області безпеки; реагування на підтверджені інциденти шляхом координації ресурсів та контролю за використанням своєчасних і відповідних ситуації захисних заходів; надання відповідним організаціям актуальної інформації про поточну ситуацію, а також звітів про статус кібербезпеки, інциденти та тенденції в поведінці зловмисників; розробка і управління засобами захисту комп'ютерних мереж.

Основні завдання, які повинен вирішувати SOC:

- Інвентаризація та контроль інфраструктури.На базі центрів SOC досить часто забезпечується вирішення актуальних для кожної компанії завдання з управління інформаційними активами компанії, таких як:

- моніторинг IT-інфраструктури, збір даних про обладнання і його характеристиках (інвентаризація), контроль складу IT-систем, побудова зв'язків взаємодії між компонентами;
- складання переліку критичних активів і проведення оцінки їх цінності;
- контроль облікових записів користувачів, управління доступами і привілеями;
- управління вразливими.

Управління уразливими в рамках контролю інфраструктури, в свою чергу, полягає не тільки в їх виявленні, а й в реєстрації відповідно до типу і рівнем критичності, з подальшим автоматичним призначенням відповідальних і

термінів усунення, а також винятком тих вразливостей, які в ході вивчення визнаються помилкові спрацьовування.

Консолідація інформації про інциденти ІБ. Коли в організації немає єдиного центру моніторингу, інформація про інциденти розрізнена і не систематизована, ця обставина ускладнює, як оперативне реагування на інцидент, так і швидке і якісне його розслідування. Тому потрібна єдина база для збору інформації про всі інциденти ІБ, що відбулися в організації.

Робота з обробки інцидентів відбувається поетапно:

- Виявлення інцидентів. На цьому етапі інформація про інциденти збирається централізовано з різних джерел, класифікується, аналізується.
- Реагування. Призначення відповідальних осіб і групи реагування, контроль термінів і дій.
- Розслідування інциденту. На даному етапі збирається доказова база, свідоцтва, виявляються причини і обставини інциденту.
- Аналіз і статистика. Формуються статистичні дані по відділах, філіях, по типам. Виявляються основні зв'язки і залежності.
- Звітність. Формування і висновок різного виду звітів.

Інформація про інциденти при цьому може надходити в централізовану базу даних різними способами. В рамках фіксації інцидентів, як правило, реєструються такі параметри інцидентів як: рівні критичності, рівні збитку, джерело інциденту, ступінь навмисності, статус реалізації, ймовірність повторного виникнення, пріоритет тощо.

Координація та автоматизація реагування на інциденти ІБ. У сфері ІБ вкрай важлива автоматизація процесів реагування на інциденти, щоб кожен раз групі реагування не доводилося вигадувати якісь «відповідні заходи» заново. У SOC, як правило, закладена «адаптивна логіка», це означає, що існують певні конструктори, за допомогою яких, з огляду на конкретні бізнес-процеси в компанії можна задати ряд правил, за допомогою яких збирається інформація про інциденти за заданими критеріями, налаштовуються доступи до ній, а

також автоматично призначаються відповідальні особи з розслідування даного інциденту. Група реагування на інциденти ІБ організовується на базі SOC, функції всіх членів групи заздалегідь строго прописані процедурами SOC, формується автоматична звітність на всіх стадіях реагування та розслідування інцидентів ІБ.

Інтеграція з зовнішніми джерелами і обмін інформацією по інцидентах. Це можуть бути повідомлення, що надходять з систем збору і кореляції подій безпеки – SIEM, DLP(DataLossPrevention) –систем, антивірусних пакетів, сканерів уразливості тощо. Повідомлення можуть надходити і з зовнішніх джерел через прикладний програмний інтерфейс API або навіть по електронній пошті. Головне, щоб вони оброблялися за певними правилами, заснованим, наприклад, на регулярних виразах або тегах.

Збір показників ефективності системи захисту (метрик). Важливий блок SOC – це «метрики», тут подано звітність за типами інцидентів, термінів реагування і по величині матеріальних збитків від них. У хорошій системі повинні бути налаштовані, як мінімум, наступні метрики:середній час реагування на інцидент,кількість інцидентів в роботі,середній час закриття інциденту,ставлення закритих інцидентів до зареєстрованих інцидентів.

Крім вище зазначених параметрів, можуть бути представлені і інші показники, такі як «збиток від реалізації інцидентів» і ін. Всі метрики представляються візуально у вигляді графіків і схем.

Архітектори з безпекиНаціонального інституту стандартів і технологій (NIST), визнають, що мережева безпека поширюється на п'ять ключових етапів управління загрозами: ідентифікація, захист, виявлення, реагування та відновлення. Хоча ці етапи визначені як дискретні процеси, насправді вони часто виконуються як безперервно, так і одночасно.

Це ускладнює факт, що деякі процеси, такі як ідентифікація та виявлення, зазвичай здійснюються в SOC, тоді як інші, такі як реагування та відновлення, знаходяться в компетенції NOC. Кожна команда використовує власні

інструменти для збору та управління даними про мережеві активи. Обмін даними між командами – це ручний процес, який особливо вичерпує обмежені технічні ресурси, коли дані застаріли. Це також занадто повільно – дозволяє погрози завдати шкоди та поширити розповсюдження.

Адресація всіх п’яти етапів NIST постійно та ітеративно вимагає узгодженої перспективи, яка одночасно дає оперативний контекст SOC та усвідомлення безпеки NOC.

1.3 Основні поняття, завдання та функції NOC

Центр управління мережею (NOC) – це централізоване середовище, яке вирішує поточні завдання функціонування мережі. Центр здійснює цілодобовий моніторинг і управління мережею, дозволяє знижувати аварійність, забезпечувати високу продуктивність інфраструктури, підвищуючи ефективність надання послуг при одночасному зниженні ризиків. Він виступає першою лінією захисту від зривів та збоїв у мережі [9].

NOC розміщує обладнання та персонал для моніторингу мережі комп’ютерів, серверів, мобільних пристроїв та пристроїв Інтернету речей, також розумних пристроїв із централізованого місця. NOC має високофункціональну інфраструктуру з автоматичними оповіщеннями, які сповіщають техніків про проблеми по всій мережі. NOC здійснює нагляд за інфраструктурою та обладнанням, бездротовими системами, базами даних, брандмауерами, різними пов'язаними мережевими пристроями. Її послуги з управління також включають моніторинг викликів підтримки клієнтів та систем обслуговування квитків та інтеграцію з мережевими інструментами клієнтів, тому NOC відіграє величезну роль у забезпеченні позитивного досвіду роботи з клієнтами.

Метою NOC є підтримка оптимальної продуктивності та доступності мережі та забезпечення постійного часу роботи. NOC керує низкою важливих заходів, включаючи:

- Моніторинг мережі щодо проблем, які потребують особливої уваги, у тому числі тих, що надходять із зовнішніх джерел.
- Керування сервером, мережею та пристроями, включаючи встановлення програмного забезпечення, оновлення, усунення несправностей та розповсюдження на всіх пристроях.
- Реагування на інциденти, включаючи управління відключеннями живлення та проблеми зв'язку.
- Безпека, включаючи моніторинг, аналіз загроз та розгортання інструментів у поєднанні з операціями з безпеки.
- Резервне копіювання та зберігання;
- Система управління міжмережевими екранами, запобігання вторгнень та антивірусна підтримка.
- Забезпечення політики безпеки.
- Удосконалення послуг за допомогою збору відгуків та рекомендацій користувачів.

В цілому потрібно відзначити, що NOC – це не зовсім система моніторингу. Основне завдання – автоматизація повсякденної роботи центру управління мережею. Управління мережею та моніторинг продуктивності ніколи не було складніше вирішити. Сьогоднішні організації мають справу зі все складнішими мережами – у них є офіси, що охоплюють земну кулю, співробітники, що працюють з дому, і все більшу кількість пристроїв для управління та моніторингу.

Обсяг користувачів, трафік та зловмисне програмне забезпечення можуть впливати на ефективність роботи мережі, тому потенціал виникнення проблем може з’являтися практично з будь-якого місця. Навіть на перший погляд невеликі проблеми можуть призвести до простоїв, які можуть спричинити загрозу продуктивності та вашій здатності задовольняти потреби клієнтів.

Зважаючи на це, NOC створені спеціально для запобігання несправності простоїв, так що клієнти та внутрішні кінцеві користувачі навіть не усвідомлюють цього, коли трапляються неминучі інциденти або відключення.

Співробітники NOC потребують конкретних наборів навичок щодо моніторингу, підтримки та швидкого вирішення питань щодо продуктивності в мережі. Цей рівень знань, як правило, виходить за межі неспеціалізованого IT-професіонала. У NOC може бути персонал, який встановлює маршрутизатори або програмне забезпечення, наприклад, брандмауери, але вони не функціонують як служба підтримки. Служба підтримки IT-служб та команда NOC різні, і терміни не можуть бути взаємозамінними. Вона працює безпосередньо з клієнтами, тоді як команда NOC забезпечує підтримку роботи клієнта.ЗазвичайNOC буде застосовувати ієрархічний підхід до управління інцидентами.

Завдання NOC полягає у дотриманні домовленостей про рівень обслуговування (SLA) та керуванні інцидентами таким чином, що скорочує час простою – іншими словами, зосередження уваги на доступності та ефективності. SLA – це договори між кінцевим користувачем та постачальником, які визначають послуги, які надаватимуться NOC, та засоби захисту або штрафні санкції, якщо узгоджений рівень обслуговування не буде досягнуто. SLA розроблені для того, щоб визначити, що отримуватимуть клієнти, а також окреслити стандарти, яким потрібно дотримуватися під час надання послуг клієнтам. Зазвичай угода про рівень обслуговування складається між споживачами та постачальниками, але вони також можуть бути між двома відділами в межах організації.

Угода про рівень обслуговування повинна містити не лише опис послуг, які надаватимуться, та очікуваного рівня їх обслуговування, а й показники, за допомогою яких вимірюються послуги, обов'язки та відповідальність кожної сторони, засоби правового захисту або штрафи за порушення, а також протокол додавання та видалення показників.

Поєднання потужного обладнання та висококваліфікованого персоналу, що працює за дуже специфічними протоколами, дозволяє NOC працювати безперервно. Високий функціональний NOC допомагає фахівцям у виявленні проблем по всій мережі до її виникнення.

І NOC, і SOC виконують найважливіші функції для організації – виявляти, досліджувати та вирішувати проблеми, вони наполегливо працюють над тим, щоб швидко вирішити проблеми, перш ніж вплинути на бізнес. Крім того, обидва прагнуть діяти аналогічно, використовуючи ієрархічний підхід до вирішення інцидентів. Однак вони зосереджуються на дуже різних питаннях. Як результат, вміння, знання та підходи персоналу в обох групах також відрізняються.

Також варто зазначити, що NOC можуть і самі виявляти загрози безпеці, оскільки вони стосуються продуктивності мережі і навчений персонал може ефективно реагувати на них. Цей останній момент є ключовим. Системи SIEM збирають, аналізують і класифікують дані з широкого спектру у мережі та аналізують їх для роботи в режимі реального часу. Це призводить до зменшення помилкових реакцій на інциденти, полегшуючи NOC належним чином контролювати та вирішувати проблеми безпеки, що робить її розробку більш актуальним.

Висновки до розділу

Отримані результати встановлюють, що для підтримання належного рівня інформаційної безпеки та кібербезпеки, моніторингу, прогнозування та виявлення кібератак, своєчасного прийняття управлінських рішень застосовуються центри управління мережею та центри реагування на критичні інциденти інформаційної безпеки.

РОЗДІЛ ІІ
ОРГАНІЗАЦІЯ ФУНКЦІОНУВАННЯ ЦЕНТРУ УПРАВЛІННЯ МЕРЕЖЕЮ

2.1 Функціональна модель NOC

Розглянувши організаційну структуру управління мережею, визначивши сукупність функцій та видів діяльності, побудовано функціональну модель центру управління мережею в нотації IDEF0.

IDEF0 – нотація графічного моделювання, яка використовується для створення функціональної моделі, що відображає структуру і функції системи, а також потоки інформації і матеріальних об'єктів, що зв'язують ці функції.

Контекстна діаграма процесу управління мережею зображена на рис. 2.1.

Рисунок 2.1 – Контекстна діаграма процесу «Управління мережею»

На вхід блоку поступають обладнання та кінцеві пристрої мережевої інфраструктури. Функція управління мережею здійснюються інженерами, аналітиками за допомогою використання прикладного програмного забезпечення – елементами механізму виконання, керуючись угодою про рівень обслуговування, посадовими інструкціями, корпоративною політикою, протоколами управління та політиками безпеки – елементами управління. В

результаті виконанні функції управління мережею вихідними елементами є забезпечення стабільної роботи мережевої інфраструктури, надання послуг та звітність.

Проведено декомпозицію контекстної діаграми, що дозволить відобразити основні етапи процесу управління мережею (рис. 2.2).

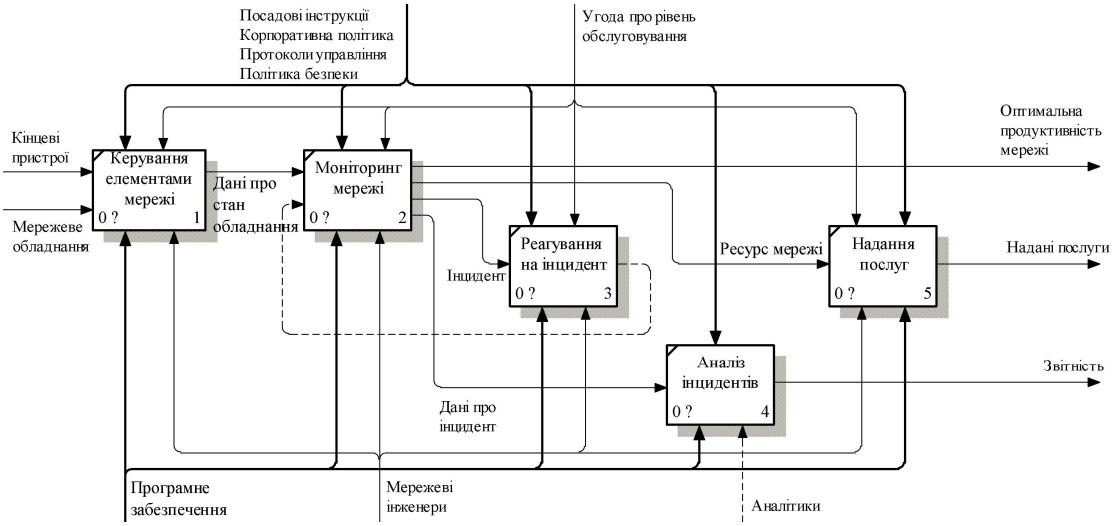

Рисунок 2.2 – Декомпозиція процесу «Управління мережею»

На етапі блоку «Керування елементами мережі» відбувається налаштування мережевого обладнання та кінцевих пристроїв. Дані про стан обладнання обробляються на етапі «Моніторинг мережі». Якщо показники мають нормовані значення – отримана оптимальна продуктивність мережі. При дотриманні цього критерія можливе виконання наступного блоку «Надання послуг», на виході якого отримано послуги, що описані в угоді про рівень обслуговування. При виявленні інциденту на етапі моніторингу, дані про нього передаються до блоку «Реакція на інцидент», на етапі якого персонал приймає певні рішення, керуючись керівними документами або політиками безпеки організації. Нові дані про стан обладнання поступають в блок «Моніторинг мережі» та продовжується виконання етапів процесу. Дані про інцидент обробляються аналітикам на етапі блоку «Аналіз інцидентів», вони складають звітність, статистику та наповнюють базу знань.

Аналіз організаційної структури управління мережею, дозволив побудувати її функціональну модель. Проведено декомпозицію контекстної діаграми, що дозволило відобразити основні етапи процесу управління мережею та полегшило розуміння роботи всієї системи в цілому. Отримані результати будуть використані для практичної реалізації центру управління мережею.

2.2 Побудова NOC

NOC складається з наступних модулів:

- NOC Console: консоль моніторингу та управління подіями, яка дозволяє NOC отримувати, підтверджувати та обробляти події – сповіщення, дзвінки, електронні листи тощо;
- Система обробки квитків: комплексні функції управління квитками про інциденти.
- Система управління мережею: надає систему обміну інформацією за допомогою керованих додатків, автоматизації завдань управління пристроями, обстеженням стану мережі, а також виявлення та визначення мережевих несправностей;
- Системи управління елементами мережі: програмне забезпечення призначене для управління і контролю окремого мережевого елемента групи однотипних елементів, отримує дані про події через SNMP або API;
- База знань NOC: система для зберігання та оновлення процесів та процедур підтримки клієнтів, робочих процесів та документації;
- База безпеки: прикладне програмне забезпечення зберігає інформацію про мережу, ієрархічні зв'язки, пов'язане обладнання та інформацію про порти.
- Система графічного відображення: надає підсумкові дані у вигляді інформаційних панелей, а також детальну інформацію про діяльність з підтримки NOC, стан мережі та продуктивність у режимі реального часу,

стандартні та спеціальні звіти на основі даних про події, випадки та результати діяльності.

- Система інтеграції зі сторонніми прикладними програмами: надає інтеграційну підтримку, щоб допомогти NOC працювати з підключеними наборами інструментів, прикладних програм та систем моніторингу та управління.

Перелічені інструменти повинні запропонувати повну видимість у всій мережі та дати змогу детальніше проаналізувати, дослідити проблеми, покращити загальну реакцію на інцидент із часом, а також забезпечують наступне:

- Комплексний вигляд інфраструктури: фізичної, віртуальної чи хмарної.
- Автоматизацію: щоб скоротити багаторазові завдання, звільнити персонал I рівня та зосередитись на питаннях з вищими пріоритетами.
- Управління квитками: з’являється можливість переглядати інформацію, що стосується відкритих квитків, включаючи пріоритетне завдання та призначеного фахівця, щоб забезпечити швидке вирішення внутрішніх та зовнішніх проблем.
- Повідомлення про випадки: забезпечує візуальний аналіз, графічне зображення порогів, сигналів тривоги, індикаторів та тенденцій, полегшує дослідження проблем та документування їх на майбутнє.
- Простий інтерфейс та розгортання: вирішення питання тривалого, складного та довгого процесу розгортання та навчання персоналу.
- Масштабованість: при розширенні мережі або системи NOC повинен впоратися з масштабом.

Важливо мати NOC, здатний запобігати катастрофічним перебоям і максимізувати час роботи всіх IT-сервісів. Багато організацій мають NOC, але можуть боротися за те, щоб він був повністю укомплектований, правильно навчений та добре обладнаний найкращими інструментами та

автоматизацією. Організації, які не можуть підтримувати ефективний NOC, можуть мати більший успіх с замовленням послуг у сторонніх постачальників.

2.2.1 Автоматизація IT-процесів NOC

Автоматизація IT-процесів – це процес автоматизації ряду завдань, пов'язаних з IT, для вирішення бізнес-ситуації або експлуатаційних вимог. Мета автоматизації IT-процесів – скоротити трудомісткі ручні завдання, впорядкувати робочий процес, прискорити процеси, усунути затримки та зменшити людські помилки. Необхідно знайти спосіб швидко визначити, проаналізувати та вирішити будь-яку кількість інцидентів, оскільки вони виникають якомога своєчасно для задоволення рівнів обслуговування [13].

Для успішних IT-операцій потрібно досягти якомога більшої ефективності. Завдяки автоматизації IT-процесів з’являється спосіб виконати більшість робіт нижчого рівня без використання ресурсу персоналу. Це називається підтримкою нульового рівня, і це може потенційно революціонуватиIT-операції.

Операції NOC 1 рівня, як правило, перші контактують з кінцевим користувачем, коли виникає IT проблема. Як результат, команда 1 рівня справляється з багатьма завданнями, які стають звичайними та повторюваними, що в кінцевому підсумку займає багато часу, яке може бути ефективніше розподілено в іншому місці. Автоматизація IT-процесів усуває цю марну трату часу та ресурсів, приймаючи ці повторювані ручні завдання та автоматизуючи їх, фактично звільняючи персонал NOC першого рівня, щоб мати можливість зосередитись на інших завданнях, які неможливо автоматизувати. Фактично, до 80% операцій NOC першого рівня можуть бути автоматизовані.

Для керівників NOC автоматизація IT-процесів також значно полегшує роботу з персоналом своїх відділів. Коли в організації є правильний інструмент автоматизації IT-процесів, наймання команди IT-фахівців більше не вимагає наявності всіх навичок та можливостей, як це було б, якби завдання

виконувалися вручну. Оскільки так багато ручних завдань обробляється програмним забезпеченням, працівники не обов'язково повинні мати довгий перелік навичок та досвіду, який вони повинні мати для того, щоб отримати кваліфікацію.

По суті, технологічні інструменти можуть замінити необхідність пошуку працівників, які володіють багатьма навичками, необхідними раніше для цих видів роботи. Це дозволяє менеджерам шукати кандидатів, які мають інші важливі ділові навички, створюючи більш надійну команду професіоналів.

Автоматизація IT-процесів дозволяє керованим постачальникам послуг максимально збільшувати свою продуктивність. Автоматизація загальних трудомістких ручних процесів зменшує витрату часу і ресурсів. IT-фахівці вільні зосередитись на інших, більш критичних питаннях, а це набагато кращий розподіл ресурсів.

Завдання полягає в розробці та впровадженні робочого процесу, який оптимізує всі наявні ресурси найбільш ефективним способом. Автоматизація дозволяє централізовано керувати та підтримувати велику кількість віддалених центрів обробки даних з одного єдиного NOC. Це не тільки покращує час роботи, але і без цього ви стикаєтесь з можливістю дорогих людських помилок. Автоматизація IT-процесів використовує двосторонні кроки зв'язку для віддаленого керування просуванням або виконанням будь-якого кроку в межах певного процесу, наприклад повторного запуску сервера. Віддалене спілкування може здійснюватися через SMS, чат, електронну пошту чи телефон.

Впровадження процедур автоматизації процесів покращує час відновлення після критичного IT-випадку. Менше простоїв означає покращений рівень обслуговування та менший ризик втрати для користувачів.

Автоматизація завдань не означає відмовитися від контролю. Керівництво може залишатися повністю контрольованим автоматизацією завдань IT, вбудовуючи точки людського вирішення в процесі робочого процесу. Коли процес досягає критичної точки вирішення, в якій вимагається

людське судження, власнику процесу представляється наявна інформація, який в свою чергу приймає рішення.

Однією з найприємніших особливостей якісного продукту автоматизації IT-процесів є те, що він притаманний гнучкості та настроюється для кожного користувача. Організації мають можливість використовувати вже розроблені робочі процеси автоматизації для автоматизації своїх найпоширеніших IT-функцій, а також налаштувати інших для вирішення конкретних унікальних больових точок їх конкретної організації. В результаті виходить індивідуальне рішення, яке допоможе впорядкувати внутрішні процеси роботи, тим самим значно покращивши послугу, що надається кінцевому користувачеві.

В цілому, це зводиться до того, що технологія автоматизації процесів IT може стати фундаментом підтримки – інакше називається підтримкою нульового рівня. Це робить роботу інших рівнів, а також керівництво, відповідальне за складання високоефективних команд, набагато простішими та ефективнішими. Це може принести користь всій організації в цілому та кінцевому користувачеві.

Висновки до розділу

Під часдослідження в другому розділі було розглянуто організаційну структуру центру управління мережею, визначено його завдання та функції. Побудовано функціональну модель центру управління мережею, що дозволило відобразити основні етапи процесу управління мережею та полегшило розуміння роботи всієї системи в цілому.

Проведений аналіз встановив необхідність комплексу програмного забезпечення та розробку інструкцій для побудови NOC. Для вирішення завдання запропоновано використовувати масштабовану, високопродуктивну систему з відкритим вихідним кодом NOC Project.

РОЗДІЛ III
ПРАКТИЧНА РЕАЛІЗАЦІЯ ФУНКЦІОНАЛЬНОЇ МОДЕЛІЦЕНТРУ УПРАВЛІННЯ МЕРЕЖЕЮ

3.1 Апаратно-програмне забезпечення NOC

Проведений аналіз відкритих джерел виявив наступну проблему, що у відкритому доступі відсутні готові рішення, тобто набір прикладного програмного забезпечення, інструкцій по налаштуванню та керівництва з експлуатації, що можуть використовувати операторами телекомунікацій, компанії, підприємства, установи чи організації для побудови власного центру управління мережевою інфраструктурою без замовлення послуг у сторонніх постачальників.Чимала кількість приватних компаній, пропонують коштовні послуги налаштування центру управління мережею. Замовлення дорогих послуг є недоцільним для організацій, з розгорнутою мережевою інфраструктурою.Комерційні організації будують NOC користуючись власним опитом та розробленим програмним забезпеченням. Вони не розкривають етапи побудови, тому і виникла необхідність у створенні єдиного способу управління мережевими ресурсами, який буде використовуватись в системі управління мережею для взаємодії з елементами мережі різних виробників.

Для забезпечення виконання функції центру управління мережею, які визначені в функціональній моделі, необхідний набір програмного забезпечення. Потрібні хороші інструменти для виконання задач організації мережевої інфраструктури, таких як управління конфігурацією мережі, моніторинг, збір показників, пошук та усунення несправностей і діагностика, автоматизація розгортання, резервне копіювання, хмарне сховище, розподіл і планування задач, безпека, ведення статистики та інші. Тому на етапі побудови була б зібрана велика кількість програм, кожну з якої необхідно встановити, налаштувати та навчитися керувати. Також виникає проблема з об’єднанням

програм в єдину функціонуючу систему для їх взаємодії, оскільки вони розроблені різними виробниками, відрізняються архітектурою побудови, мовою програмування, способами керування тощо.

Перспективу для вирішення даної проблеми відкриває масштабована, високопродуктивна система з відкритим вихідним кодом NOC Project. Вона об’єднує в собі сервіси, що виконують визначені функції управління мережею.

3.2Загальні відомості про систему NOC Project

NOCProject–масштабована, високопродуктивна система з відкритим вихідним кодом для управління мережею, яка здійснює цілодобовий моніторинг і управління мережевою інфраструктурою, дозволяє знижувати аварійність, забезпечувати високу продуктивність мережі, підвищуючи ефективність надання послуг при одночасному зниженні ризиків. Основна мова програмування – Python. Як баз даних використовується зв'язка PostgreSQL і MongoDB. Web-інтерфейс реалізований на Django. Розповсюджується за ліцензією BSD – ліцензія на вільне програмне забезпечення. Підтримує наступні операційні системи: Debian 9,Ubuntu 18,Centos 7, FreeBSD 10, RHEL 7 та Oracle Linux 7

Конфігурації NOC розрослася настільки сильно, що налаштування і оновлення NOCна крупній інсталяції власноруч представляло собою трудомістку задачу. НещодавнорозробникирозділилиNOC на окремі сервіси, якими управляє служба supervisord. У зв'язку зі зміною архітектури системи NOC, змінився і спосіб встановлення. Доданий засіб для автоматизації розгортання NOC –Tower, який централізовано зберігає настройки та поширює ці настройки на кінцеві інсталяції NOC, які називаютьсяNodes. Встановлення стало набагато зручніше, наочне та контрольоване.

Tower може зберігати різні настройки для різних Node. При необхідності вносити зміни в налаштування на Node, спочатку вносяться зміни в

конфігурацію на Tower, потімкомандою«Deploy»настройкионовлюються на Node.

Практична реалізація виконана на віртуальній машині – це модель обчислювальної машини, створеної шляхом віртуалізації обчислювальних ресурсів: процесора, оперативної пам'яті, пристроїв зберігання та вводу і виводу інформації. Віртуальна машина, на відміну від програми емуляції конкретного пристрою, забезпечує повну емуляцію фізичної машини чи середовища виконання. В якості платформи для NOC, за допомогою Microsoft Hyper-V – системи апаратної віртуалізації, на віртуальну машину встановлена операційна система CentOS 7Minimal з мінімальним набором пакетів та без графічної оболонки.

Встановлення та налаштування NOC Towerзазначено у (Додаток А), аналаштування NOC Project зазначено у (Додаток Б).

Висновки до розділу

В ході виконання третього розділу розглянуті загальні відомості NOC Project, а саме архітектуру побудови, системні вимоги та описані можливості його сервісів. Практично реалізовано центр управління мережею, а саме крок за кроком розписаний процес встановлення системи NOC Project та налаштування необхідних сервісів, які забезпечують виконання функцій NOC.

ВИСНОВКИ

В роботі запропоновано розробка моделі центру управління мережею на основі NOC. Розглянуті загальні відомості програмного забезпечення NOC Project: архітектуру побудови, системні вимоги та описані можливості його сервісів.

Практично реалізовано модель центру управління мережею, та крок за кроком описаний процес встановлення системи NOC Project та налаштування необхідних сервісів, які забезпечують виконання функцій NOC.

Дивлячись на сучасні тенденції щодо забезпечення кібернетичної безпеки треба надавати можливість ситуаційним центрам інтегруватися в загальну систему забезпечення кібербезпеки та підвищувати загальний рівень інформаційної безпеки та кібербезпеки.

Застосування запропонованої моделі забезпечить єдиний спосіб побудови та управління мережевими ресурсами, який буде використовуватись в системі управління мережею для покращення ефективної взаємодії між пристроями, спростить програмну складність процесу побудови та забезпечить виконання мети розробки даної моделі.

Подальша робота буде направлена на розробку методів оцінки стану захищеності інформаційних ресурсів центрів управляння мережевими ресурсами в системі забезпечення кібербезпеки та з урахуванням особливостей обробки IP в комунікаційних системах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про інформацію», редакція від 16.07.2019 [Електронний ресурс] // ВідомостіВерховноїРадиУкраїни (ВВР). – 1992. – № 48. – с. 650. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12

2. Закон України «Про захистінформації в інформаційно-телекомунікаційних система», редакція від 19.04.2014 [Електронний ресурс] // ВідомостіВерховноїРадиУкраїни (ВВР). – 1994. – № 48. – с. 650. – Режим доступу: https://zakon.rada.gov.ua/laws/main/80/94-вр

3. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.

4. Вороб'єнко П.П.. Телекомунікаційні та інформаційні мережі : Підручник [для вищих навчальних закладів] / Вороб'єнко П.П., Нікітюк Л.А., Резніченко П.І. – К.: САММІТ-Книга, 2010. – 708 с.

5. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы // Учебник для вузов. —3-е изд. СПб. : Санкт-Петербург, 2006. — 958 с

6. Чирков Д.В., Сєрєнко В.С. Правові аспекти створення та введення в експлуатацію інформаційно-телекомунікаційної системи і контексті захисту інформації— К. : Науково-технічний журнал «Захист інформації» №4, 2016

7. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28 квітня 1999 р. № 22.

8. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній

системі, затверджений наказом ДСТСЗІ СБ України від 8 листопаду 2005 року № 125;

9. Dr. JimMetzler. TheNextGenerationNetworkOperationsCenter, NetQoS, Austin, TX, 78746 UnitedStates, 2018;

10. NelsonHernandez. NOC/SOC Integration:OpportunitiesforIncreasedEfficiencyinIncidentResponsewithinCyber-Security, SANS Institute, Swansea, SA3 9BB, UnitedKingdom, 2019;

11. NetworkOperationsCenterservices. CienaCompany, 7035 RidgeRoadHanover, Maryland 21076 USA

12. Комплексныйподход к управлениюсетью (NOC) [Електронний ресурс] – Режим доступу: https://habr.com/ru/post/125034/(Дата звернення10.10.2019);

13. Сетеваяинфраструктура и центр управлениясетью в дата-центре [Електронний ресурс] – Режим доступу: https://www.comarch.com/trade-and-services/ict/it-outsourcing-integration/global-operations-center/ (Дата звернення30.09.2019);

14. Bridgingthe NOC-SOC divide[Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/ebook/bridging-the-noc-soc-divide.pdf (Дата звернення14.11.2019);

15. GlobalOperationsCenter, IT MonitoringServices[Електронний ресурс] – Режимдоступу: https://habr.com/ru/post/125034/(Дата звернення12.11.2019);

16. NOC BestPractices: TakingYourOperationsTeamfromZerotoHero[Електронний ресурс] – Режимдоступу: https://www.enableip.com/noc-technology-resources/noc-best-practices/(Дата звернення12.11.2019);

17. Whatisnetworkoperationscenter? [Електронний ресурс] – Режим доступу: https://www.extnoc.com/network-operations-center/ (Дата звернення27.10.2019);

Додаток А

Встановлення та налаштування NOC Tower

1) **Створення каталогу NOC Tower**:

- # mkdir /opt/tower
- # cd /opt/tower

2) **Створення virtualenv**–віртуальна середа мови програмування Python:

- /opt/tower# virtualenv .

3) **Завантаження та встановлення NOC Tower** :

- /opt/tower# ./bin/pipinstall --upgradepip
- /opt/tower# ./bin/pipinstall https://cdn.getnoc.com/tower/noc-tower-latest.zip
- /opt/tower# chown -R towervar/

4) **Створення ssh ключа для NOC Tower**:

- /opt/tower# su – tower -c "ssh-keygen -t rsa -b 4096"

5) Підготовка NOC Nodes:

Створення користувачаansible (за замовчуванням) та визначити пароль для користувача:

- useradd -d /home/ansible -s /bin/bash -m ansible`
- passwdansible

Користувачеві ansibleнеобхідно надати привілеї sudo (ansible ALL=(ALL) NOPASSWD:ALL в файлі /etc/sudoers) та скопіювати відкритий ключ sshTower (/opt/tower/var/tower/data/deploy_keys/id_rsa.pub) для нього:

- /opt/tower# docker-composeexectowerssh-copy-id -f -i/opt/tower/var/tower/data/deploy_keys/id_rsa.pub ansible@192.168.168.42,

де 192.168.168.42– IP-адреса серверу (віртуальної машини).

6) Вхід до веб оболонкиNOC Towerздійснюється за допомогоювеб-браузера. В адресній стрічці браузера потрібно ввести http://192.168.168.42:8888. У вікні авторизації ввести логін та пароль за

замовчуванням (admin/admin). Необхідно відразу змінити пароль адміністратора NOC Tower– натиснути верхнє меню праворучта«Changepassword» (Рис. А1)

Рисунок А1 – Вікно зміни паролю адміністратора

7)Додавання середовищаNOCTower:

Середовища потрібні для розділення різних інсталяції NOC.В одній системі NOCTower можливо здійснювати керування декількома інсталяціями NOC та конфігурувати їх окремо.Додати нове середовище потрібно на вкладці Environmentsнатиснув «Createnew»та вказати наступні параметри: ім’я середовища, опис, url (або ip-адрес) за яким буде доступне середовище. Тип, репозиторій та метод встановлення залишити за замовченням. На рис. А2 відображена сторінка додавання середовища NOC Tower із заповненими параметрами.

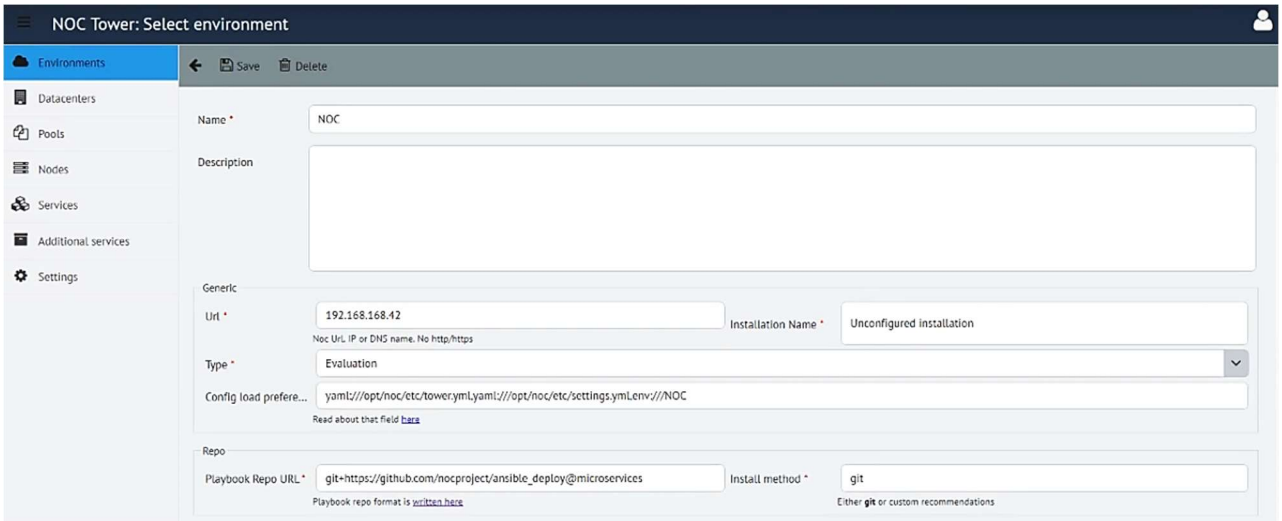

Рисунок А2 – Сторінка додавання середовища

Для створеного середовища виконати команду «Pull» (рис. А3). Вона завантажує оновлення конфігурацій на NOCTower.

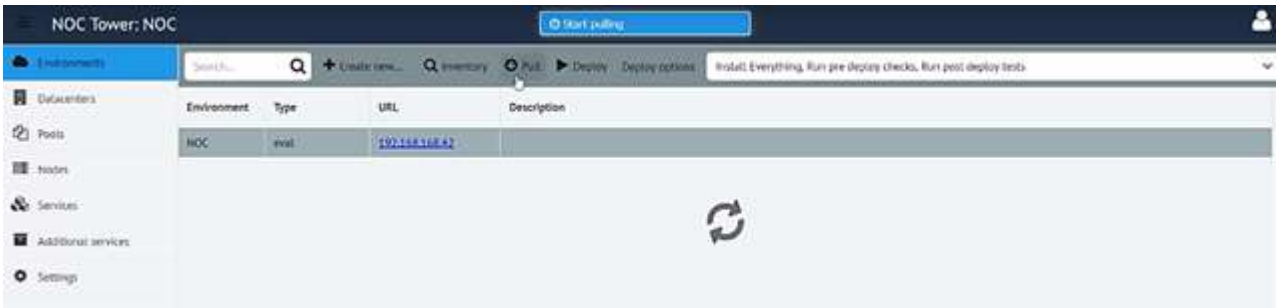

Рисунок А3 – Виконання команди «Pull»

8) Додавання дата-центру:

NOCNodes можуть розміщуватись в декількох дата-центрах, в яких може бути свій проксі-сервер який забезпечує доступ до зовнішніх інтернет-ресурсів з локальної мережі, тобто виступає посередником для доступу до ресурсів, прямий доступ до яких неможливий або з якихось причин небажаний.

На вкладці Datacenterscтворити новий дата-центр та у полі «InternetProxy» вказати проксі-сервер, якщо такий існує (рис. А4).

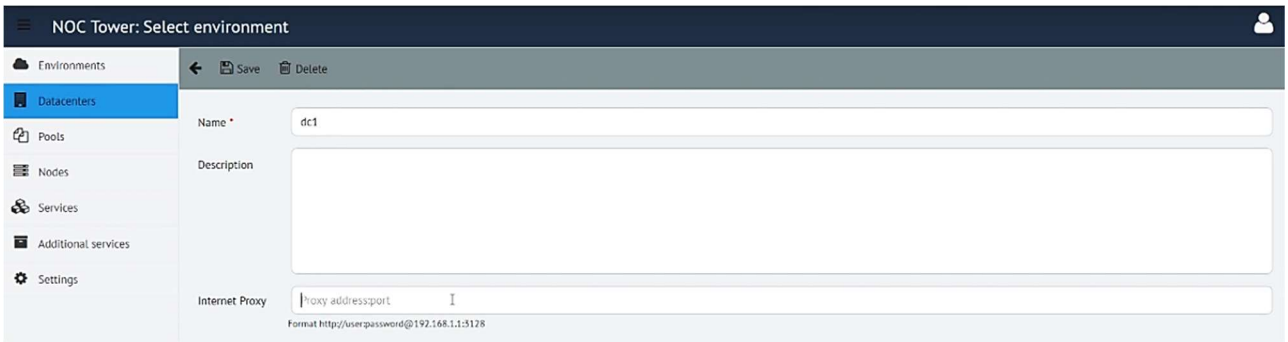

Рисунок А4 – Сторінка додавання дата-центру

9) Додавання Nodes:

Node–це сервер, на якому встановлено NOC. Було додано лише одну Node, оскільки в ході виконання практичного завдання NOCвстановлено на одній віртуальній машині. На сторінці додавання вказано ім’я Node, дата-центр, що використовується,опис, типопераційної системи, на якій встановленоNOC, ip-адреса серверу та логін користувача, якого було створено напочатку (рис. А5.).

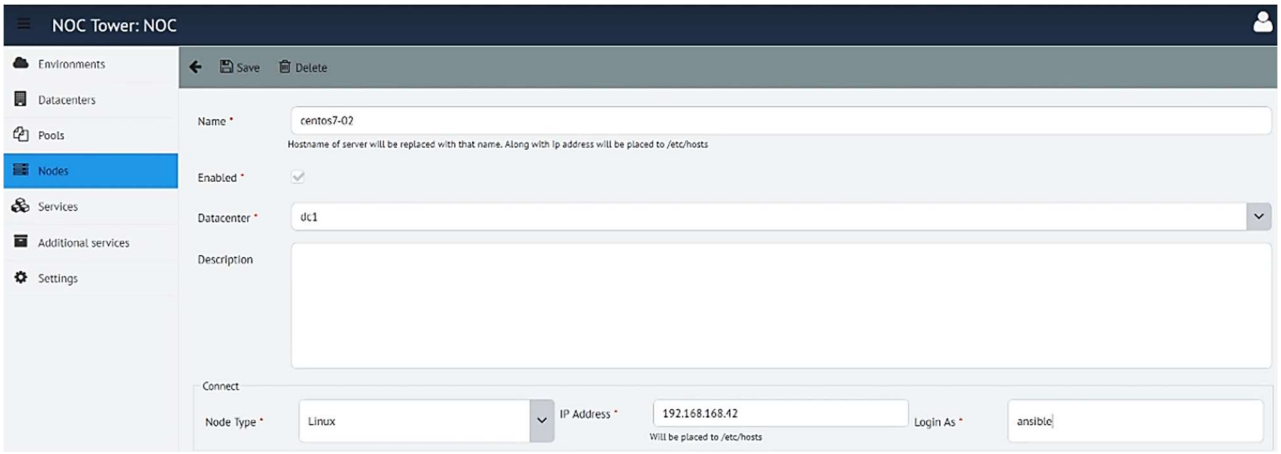

Рисунок А5 – Сторінка створення Node

10) Вибір необхідних сервісів:

На вкладці «Services»перелік всіх сервісів NOC Project. Не всі сервіси є обов’язковими для встановлення, тому є можливість відключити їх. У кожного є свої налаштування та короткий опис:

- Activator – відповідає за збір та обробку даних із мережевого обладнання;
- Card – відповідальний за альтернативний веб-інтерфейс – картки. Це сторінки, що показують інформацію про мережеве обладнання, сегменти та аварії;
- Ch_datasource– використовується для завантаження даних з баз даних mongo або postgres у словники Clickhouse;
- Clickhouse– це система управління базами даних, яка може створювати аналітичні звіти даних у реальному часі за допомогою SQL-запитів;
- Classifier– відповідальний за класифікацію потоку вхідних повідомлень згідно з правилами, записаними в NOC;
- Datastream– використовується для передачі змін до NOCсервісів;
- Discovery– запускає завдання на активаторах, аналізує результати, записує в бази даних;
- Goss– серверна перевірка;
- Grafana– відкрита платформа дляаналітики та моніторингу. Зберігає дані в базі данхихpostgres;

- Grafanads– відображає анотації на графіках Grafana з інформацією про тривогу;
- Login– служба внутрішньої аутентифікації;
- Mib– запускає і контролює виконання команд програми Runcommands;
- Mongod– первинна база даних. Використовується для більшості операцій.
- Nbi– сервіс для інтеграції зовнішніх систем;
- Nginx– веб-сервер і поштовий проксі-сервер;
- Noc– налаштування NOC;
- Nsqd– демон NSQD, який отримує, зберігає та доставляє повідомлення клієнтам;
- Ping– пінг мережевого обладнання з ICMP. Створює події на змінах стану;
- Postgres–база даниxPostgresSQL;
- Selfmon– відображає анотації на графіках Grafanas з інформацією про тривогу;
- Syslogcollector– прослуховуйте події syslog з мережевого обладнання та додайте їх до черги nsqd;
- Trapcollector– прослуховуйте події SNMP з мережевого обладнання та додайте їх до черги nsqd;
- Tgsender– сервіс відправки повідомлення в Telegrambot;
- Web– сервіс для показу веб-інтерфейсу.

Після того, як був обраний набір необхідних сервісів, необхідно зберегти конфігурування натиснув «Save», перейти на вкладку Environments та запустити команду «Deploy», яка почне автоматично розгортати систему з заданими параметрами. Результат виконання розгортання відображено на рис. А6. Повідомлення в останній стрічці повідомляє про успішність завершення розгортання, кількість виконаних операцій, змін, невиконаних операцій та помилок.

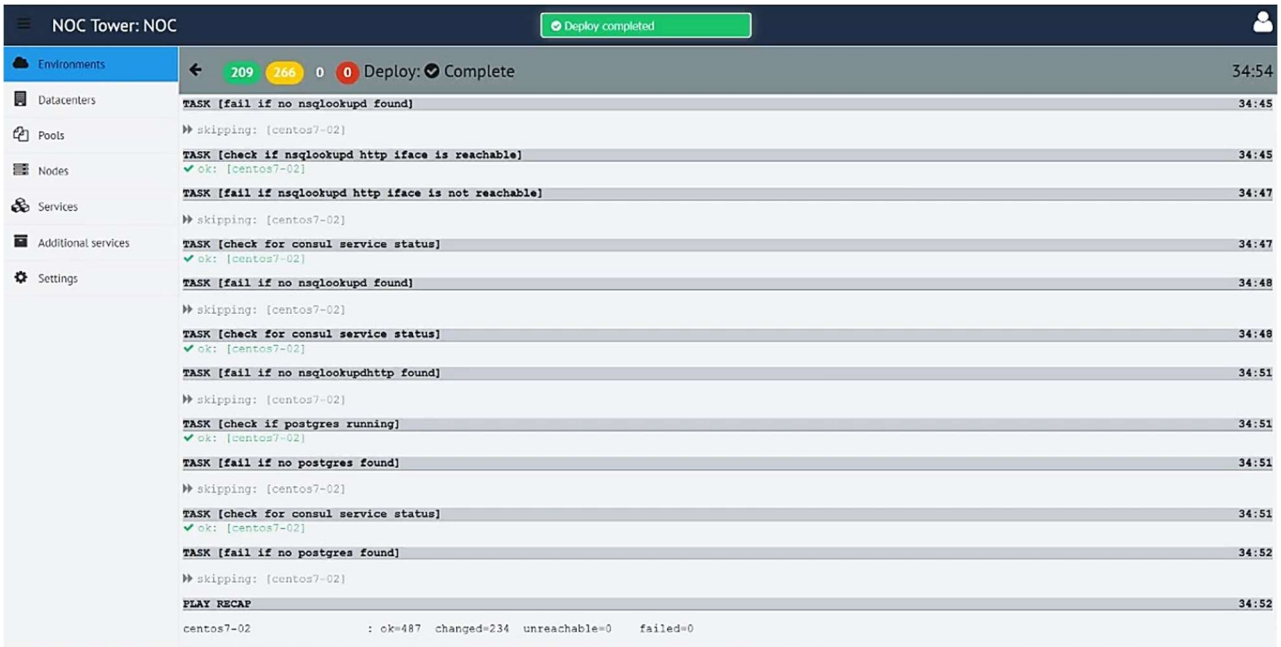

Рисунок А6 – Завершення розгортання системи NOC

Додаток Б

Налаштування NOC Project

Для входу в NOC Project за допомогою браузера перейти за ip-адресоюNode, але на відміну від Tower адреса Nodeпрацює під протоколом HTTPS.У вікні авторизації ввести логін та пароль за замовчуванням (admin/admin). Необхідно відразу змінити пароль адміністратора NOC Tower– натиснути верхнє меню праворуч та«Changepassword».

Відкривається початкова сторінка системи NOC Project. Робоча область при вході в систему містить інформацію про систему, а також посилання на інформаційні ресурси. При роботі з модулями і об'єктами в робочій області відображаються їх параметри і засоби управління ними. Відповідно літерам на рис. Б17:

1 – Документація та технічна підтримка NOC Project;

2 – Переглянути версію системи, налаштувати профіль, змінити пароль, вийти з системи;

3 – Панель навігації містить список модулів з ієрархічною структурою об'єктів.

Рисунок Б1 – Початкова сторінка NOC Project

Serviceactivation – основний модуль NOC, він забезпечує збір технічної інформації про мережу та абстрагує її для інших модулів від типу і виробника устаткування.

Модуль ServiceActivation розділений на дві частини:

- ServiceActivationEngine (SAE) – центральний процес, єдина точка входу для всіх завдань, які повинні бути виконані на обладнанні, розподіляє всі поступаючі завдання між доступними активаторами
- Activator– процес, який безпосередньо виконує підключення до обладнання.

ManagedObjects – основний розділ для створення, видалення і перегляду конфігурацій пристроїв. Згодом записів для пристроїв з'явиться багато і тут можна зручно сортувати ці записи різними фільтрами.

Для додавання нового обладнання необхідно виконати наступні дії:

1) Зліва в панелі навігації натиснути на ServiceActivation.
2) У списку, натиснутина рядку ManagedObjectSelector.
3) У вікні, ManagedObjectSelectorнатиснутинаAdd. Відкриється форма CreateManagedObjectSelector.
4) Заповнити наступні елементи форми: Name – найменування обладнання, прапорецьIsManaged – якщо цим обладнанням можна управляти; У списку ObjectProfilevибрати профіль збору даних з устаткування (задається в ServiceActivation→Setup→ManagedObjectProfiles). У списку Shapeвибрати позначення значка, яким обладнання буде позначатися намережевій карті. Приклад представлений на рис. Б2.

Рисунок Б2 – Опис обладнання

5) У групі елементів Locationзаповнити поля AdministrativeDomain (адміністративний домен – група серверів, маршрутизаторів і мереж, керованих однією організацією), Activator (активатор – служба управління обладнанням), VRF, VC Domain (в якому домені створювати VLAN). Приклад представлений на рис. Б3

Рисунок Б3 – Група елементів Location

6) В групі елементів Access заповнити поля SA Profile, Scheme, Address, Port, AuthProfile, User, Password, SuperPassword, Path (використовується, якщо на обладнанні є кілька контекстів або для комутаторів в кластері). Приклад представлений на рис. Б4.

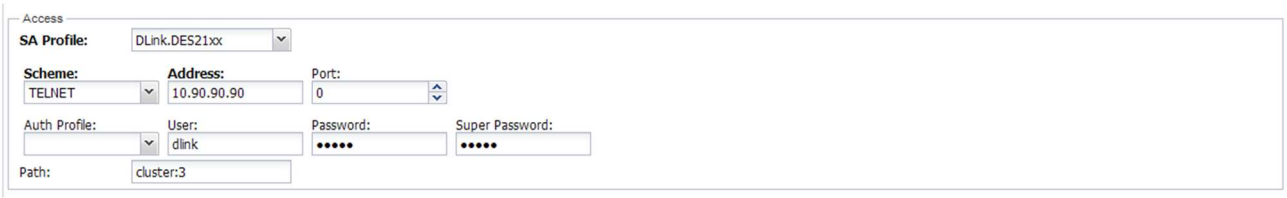

Рисунок Б4 – Група елементів Access

7) В групі елементів SNMP (Простий Протокол Мережевого Управління) заповнити поля TrapSource IP, TrapCommunity – пароль, яким будуть підписуватися повідомлення, відправлені обладнанням.
8) В групі елементів Rules (скрипти) за допомогою вибору значень зі списків заповнити поля: ConfigFilterpyRule – скрипт, який застосовується до конфігурації обладнання,ConfigDiffFilterRule – скрипт, який застосовується до різниці конфігурацій (тобто збирається конфігурація, потім робиться різниця поточної і попередньої, до результату застосовується скрипт), ConfigValidationpyRule – скрипт, який застосовується до конфігурації, для перевірки її на правильність.
9) В поліMax. Scripts задати максимальну кількість скрипів, які можуть бути запущені на обладнанні.
10) Група елементів Attributes доступна тільки користувачеві з привілеєм admin, заповнюється автоматично інформацією про версію і прошивці на обладнанні.
11) В панелі інструментів натиснути кнопку Save.

Для отримання інформації про конфігурацію обладнання виконайте наступні дії:

1) Зліва в панелі навігації перейти до вкладкиServiceActivation.
2) У списку, натиснути на рядку ManagedObjects.
3) У вікні ManagedObjects двічі натиснути на рядку з даними обладнання.Відкриється форма з даними обладнання.

Якщо панелі інструментів натиснутиDiscovery, відкриється таблиця зі списком методів виявлення інформації про конфігурацію обладнання з їх поточними статусами і датою останнього запуску (рис. Б5).

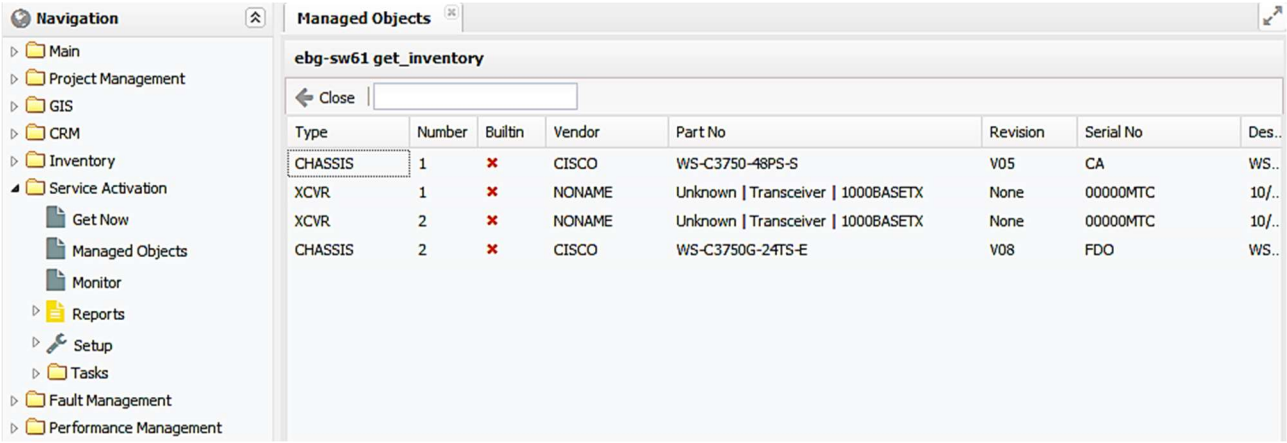

Рисунок Б5 – Вікно ManagedObjects

За допомогою команди Run запускається цей метод перевірки (рис. Б6). Після запуску методу відображається результат, якщо все в порядку – OK, якщо є помилки – Fail. В останньому випадку в пункті меню ServiceActivation→Reports→StateDiscovery буде описана причина помилки.

Close | Refresh | Run | Disable

Name	Profile	Status	Last Run	Last Status	Next Run	Links Found
ping	✔	OK				
version_inventory	✔	OK	2021-01-13 20:49:08	OK	2021-01-13 20:59:13	
id_discovery	✔	OK	2021-01-13 20:49:30	Fail	2021-01-13 20:55:18	
config_discovery	✔	Wait	2021-01-13 20:49:23	Fail	2021-01-13 20:59:47	
interface_discovery	✔	Wait	2021-01-13 20:49:02	Fail	2021-01-13 21:03:36	
asset_discovery	✖					
vlan_discovery	✖					
lldp_discovery	✔					
udld_discovery	✔					
bfd_discovery	✔					
stp_discovery	✔	Wait	2021-01-13 20:49:38	Fail	2021-01-13 21:02:44	
cdp_discovery	✔					
oam_discovery	✖					
rep_discovery	✔					
ip_discovery	✔	Wait	2021-01-13 20:49:17	Fail	2021-01-13 20:58:37	
mac_discovery	✔					

Рисунок Б6 – Таблиця зі списком методів

GetNow–сервіс для отримання інформації про обладнання. Можливо переглянути конфігурацію пристроїв, її останнєоновлення, поточний статусі загальну кількість (рис. Б7).

Get Now

Managed object: | By SA Profile: | By Adm. domain: | Reset filter | Get config NOW | Raw

ID	Managed object	SA Profile	Last success	Last update	Status	Last status
431	SAE	NOC.SAE	about 2 h	about 2 h	Wait	Wait
522	acc-Gov52-sw1	Zyxel.ZyNOS	about 2 h	about 3 h	Wait	Stop
518	acc-Rjk26-sw1	Zyxel.ZyNOS	about 2 h		Wait	Stop
519	acc-Rjk26-sw2	Zyxel.ZyNOS	about 2 h	about 2 h	Wait	Fail
520	acc-Rjk26-sw3	Zyxel.ZyNOS	about 2 h	about 2 h	Wait	Fail
521	acc-Rjk28-sw1	Zyxel.ZyNOS	about 4 h	about 4 h	Wait	Fail

Reload | Version: | Compare: | Day | Week | Month

Рисунок Б7 – Вікно GetNow

FaultManagement– модуль управління помилками в NOC може зберігати всі мережеві події, класифікувати їх, виводити повідомлення про помилки за пріоритетом, виконувати певні дії при будь-яку подію.

Для перегляду веб-події в NOC необхідно відкрити вкладку FaultManagement → Events та в розділі ManagedOdjectSelector встановити параметри, відповідно яких будуть виводитись повідомлення про помилки (рис. Б8).

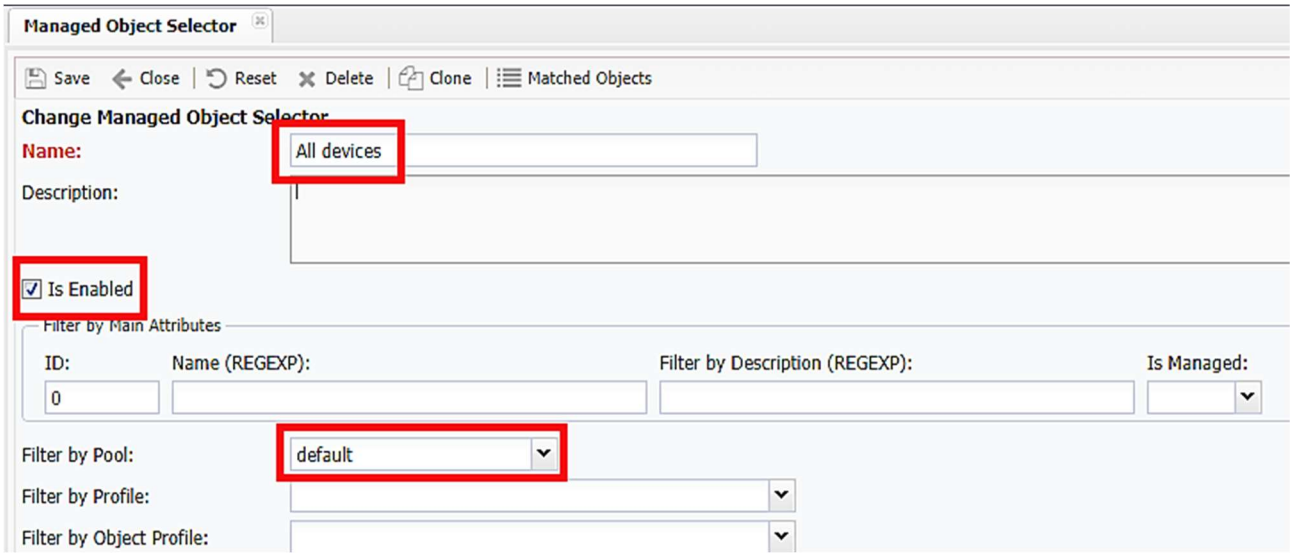

Рисунок Б8 – Вікно ManagedOdjectSelector

Після збереження результатів та початку роботи FaultManagement, список подій та інформація про них виглядає так (рис. Б9):

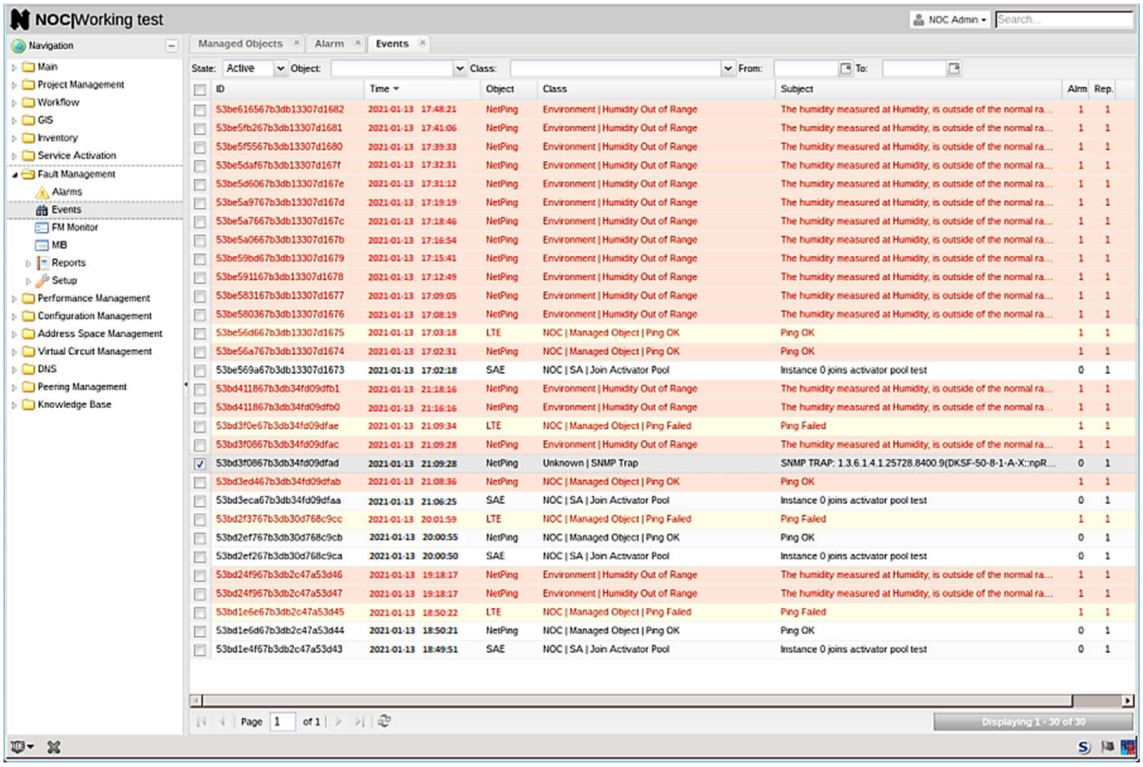

Рисунок Б9 – Вікно FaultManagement

Існує можливість фільтрації помилок: по об'єктах, класам, тимчасовим інтервалах.

NetworkMaps– сервіс для відображення схеми мережі зі зв'язками між об'єктами та їх поточним статусом. Для її отримання необхідно перейти в Inventory → NetworkMaps. Приклад побудованої мапи мережі зображено на рис. Б10.

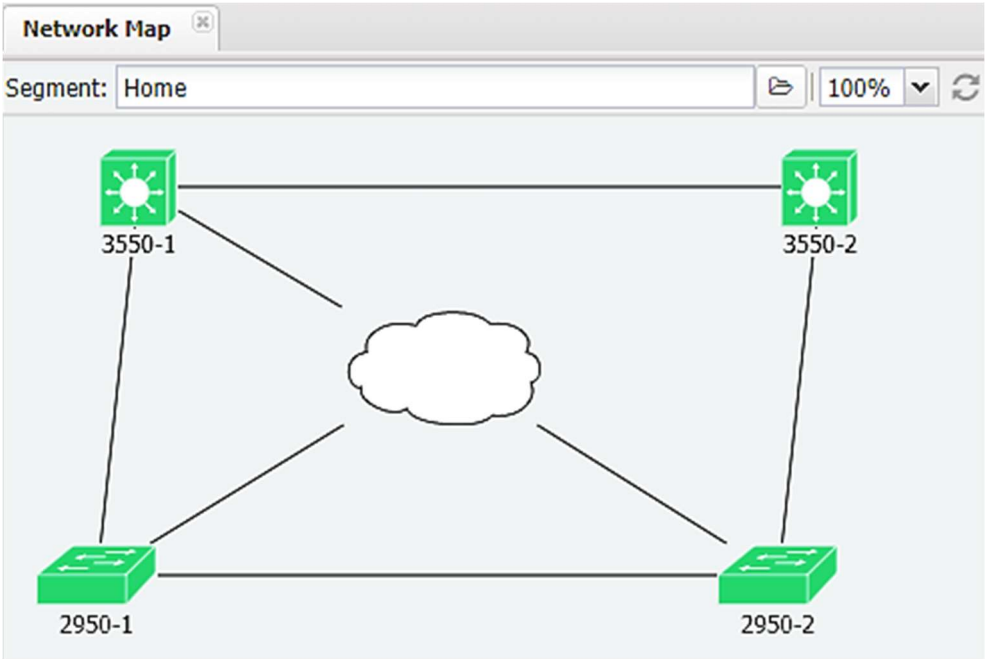

Рисунок Б10 – Вікно NetworkMaps

NetworkMaps корисний для візуальної оцінки стану підмережі сегмента – видно які пристрої недоступні та в якому елементі є відкриті помилки. Крім цього наочно видно проблеми з зв’язками. У разі недоступності об'єкта він змінить колір на червоний, а в разі аварії на об'єкті – на жовтий, детальніше про позначення елементів на рис. Б11.

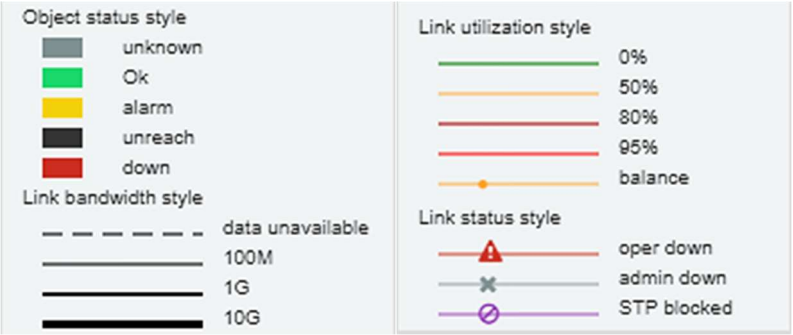

Рисунок Б11 – Позначення елементів NetworkMaps відповідно критеріям

PerformanceManagement – сервіс для управляння продуктивністю, відповідає за збір метрик з обладнання і контроль їх значення. Сервіс збирає метрики по SNMP, записує метрики в базу даних ClickHouse (можлива підтримка інших БД), відображає метрики за допомогою Grafana, відпрацьовує пороги та попереджує про перевищення встановленого значення.

Метрика – деякавеличина що змінюється в часі та підлягає фіксації. Формально кажучи, метрикою може бути будь-яка величина: швидкість інтерфейсу, число вільної пам'яті, статус інтерфейсу і т.д. Досить, щоб вона змінювалася в часі і представляла якийсь інтерес.

Архітектурно PerformanceManagementскладається з джерела даних, збирача (колектора), передавача, записувача і сховища. Туди ж, можна додати інтерфейс для відображення графіків і інтерфейс для аналітики (звітів).

- Джерело даних може бути зовнішнім (пристрій) або внутрішнім (сервіси Ping, Discovery тощо)
- В якості збирача виступає активатор. Він запускає скрипти для збору метрик.
- Ініціатором збору –сервісDiscovery. Тобто з боку Discoveryприходить запит на активатор, він відпрацьовується і повертає результат Discovery, який вже відправляє його в сторону записувача з передавача.
- Передавачем для метрик виступає HTTP (між Discoveryі активатором) і NSQ у всіх інших випадках.
- ЗаписувачChwriterслухає, що надходять повідомленняі, у міру їх накопичення, записує в базу даних. Для кожного сховища свій записувач.
- Як сховище для метрик використовується база даниxClickHouse.
- Інтерфейс для графіків та діаграм – Grafana.

Grafana дозволяє користувачам створювати Dashboardз панелями, кожна з яких відображає певні показники протягом встановленого періоду часу. Кожен Dashboardуніверсальний, тому його можна налаштувати для конкретного проекту або з урахуванням будь-яких потреб розробки.

Налаштування збору метрик з інтерфейсів:

Інтерфейсні метрики додаються на вкладці Metrics профілі InterfaceProfile (Inventory → Setup → InterfaceProfile).

У ньому необхідно обрати або додати необхідні метрики (рис. Б12)

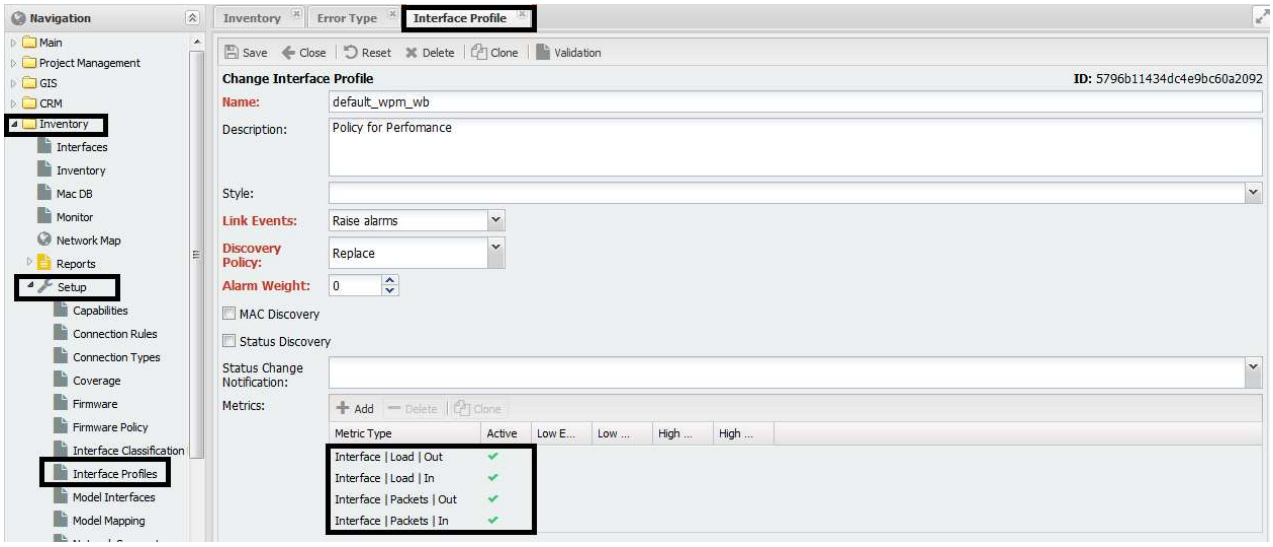

Рисунок Б12 – Вікно налаштувань InterfaceProfile

Перегляд метрик відбувається через Dashboard. Він доступний з інтерфейсу ManagedObjects: в цьому випадку, він автоматично, налаштовується на відображення всіх метрик.

Для настройки джерела даних необхідний доступ адміністратора до Grafana. Перейти до опції«DataSources»та натиснути кнопку Add у верхньому меню.При додаванні вказуємо наступні опції(рис. Б13):

- Name– ім’я Dashboard;
- Обов'язково вказуємо Default (за замовчуванням);
- Type вибираємо ClickHouse (або подібнубазу даних);
- В URL – адреса ClickHouse (якщо стоїть на окремому хості–необхідно вказати адресу цього хоста), порт 8086 –за замовчуванням;
- Access–Proxy – це режим доступу до даних;
- Спосібаутентифікації виставляємо BasicAuth;
- BasicAuthDetails вказуємо відповідно до тих, які прописували при розгортанні NOC.

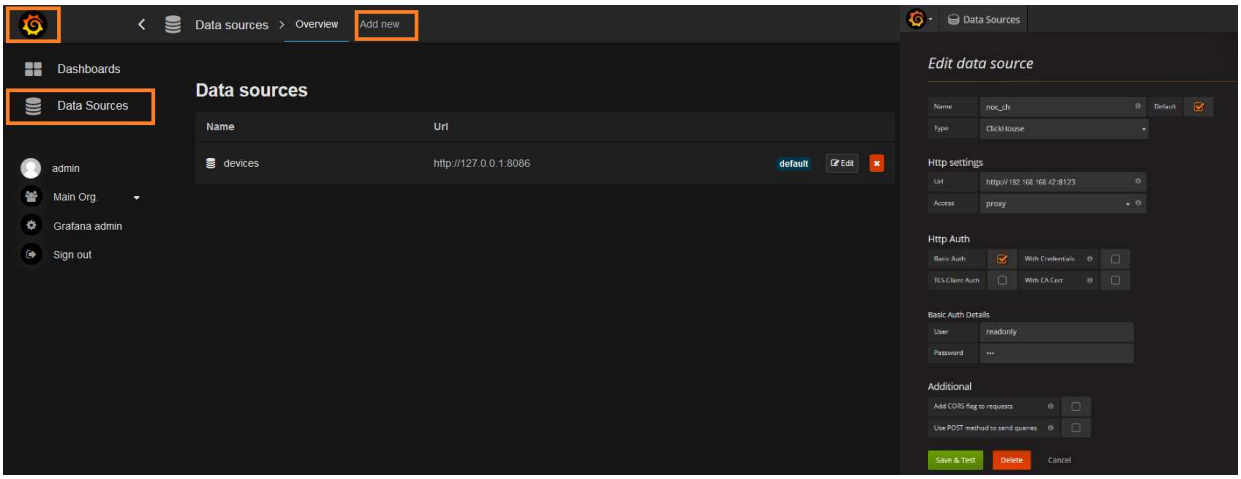

Рисунок Б13 – Додавання та налаштування DataSources в Grafana

Після налаштування необхідно провести тестування заданих параметрів «TestConnection» та зберегти їх.

Grafana налаштована та відображає показники в реальному часі на Dashboard. Для їх перегляду необхідно перейти на головну сторінку Grafana, результат відображено на рис. Б14.

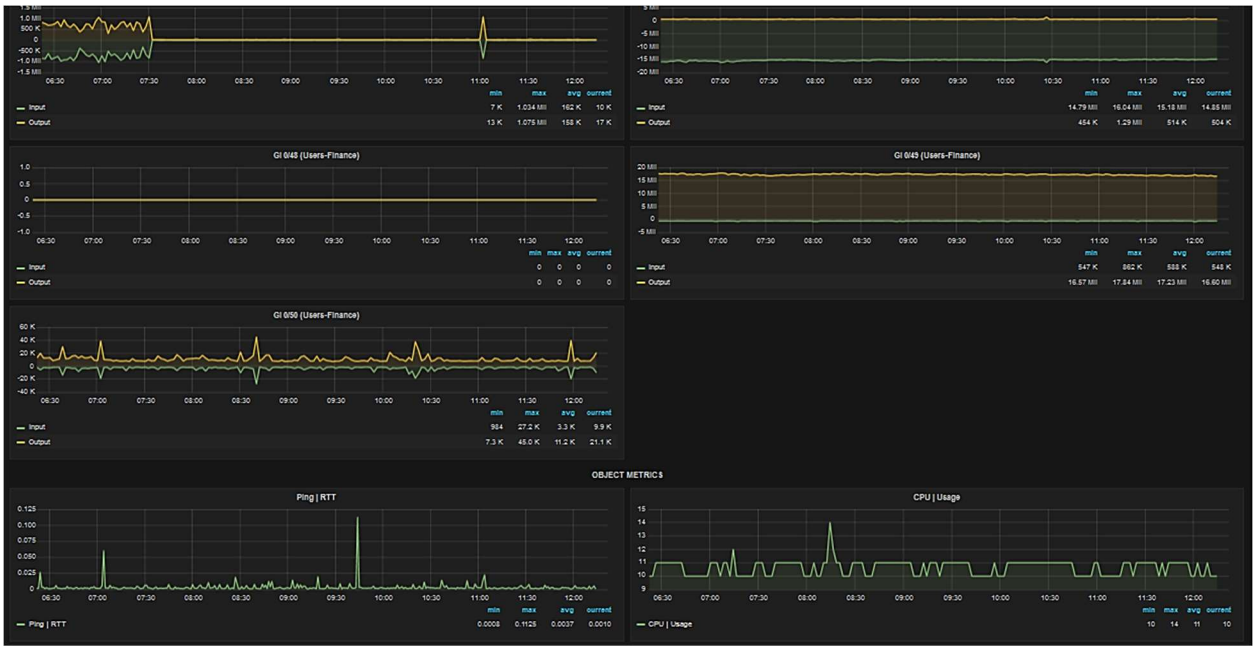

Рисунок Б14 – ІнтерфейсDashboardвсередовищіGrafana

Аналогічно налаштуванню збору метрик з інтерфейсів додається збір метрик об'єкта на вкладці в профілі ObjectProfile (ServiceActivation → Setup) та метрик SLA (SLA → Setup → SLA Profile).