МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації

На рецензію
Завідувач кафедри УІКБ
доктор економічних наук, професор
_____ С.В. Легомінова
«___»_____2022 р.

До захисту
Завідувач кафедри УІКБ
доктор економічних наук, професор
_____ С.В. Легомінова
«___»_____2022 р.

КВАЛІФІКАЦІЙНА РОБОТА
другого магістерського рівня вищої освіти
на тему:

ІНТЕЛЕКТУАЛІЗАЦІЯ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА (УСТАНОВИ, ОРГАНІЗАЦІЇ)

СТУДЕНТ: Самко Владислав Васильович _____
(підпис)

КЕРІВНИК: д.е.н., проф. Легомінова Світлана Володимирівна _____
(підпис)

НОРМОКОНТРОЛЕР: к.в.н., доц. Якименко Юрій Михайлович _____
(підпис)

Київ – 2022

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою
Спеціальність 125 Кібербезпека
Спеціалізація Управління інформаційною безпекою
Другого магістерського рівня вищої освіти

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В. Легомінова
«_____»_____ 2022 р.

ЗАВДАННЯ
на кваліфікаційну роботу

студенту Самку Владиславу Васильовичу
Тема роботи «ІНТЕЛЕКТУАЛІЗАЦІЯ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА (УСТАНОВИ, ОРГАНІЗАЦІЇ)», затверджена наказом по університету № 122 від «12» жовтня 2022 р.

1. **Термін здачі** студентом оформленої роботи «22» грудня 2022 р.
2. **Об'єкт дослідження:** Інтелектуалізація процесу управління ризиками інформаційної безпеки підприємства (установи, організації).
3. **Предмет дослідження:** особливості інтелектуалізації процесу управління ризиками інформаційної безпеки підприємства (установи, організації).
4. **Мета дослідження:** розробка сценаріїв та алгоритмів управління ризиками інформаційної безпеки підприємства (установи, організації).
5. **Перелік питань, які мають бути розроблені:**
   5.1 Дослідити теоретичні засади інтелектуалізації управління ризиками інформаційної безпеки підприємства (установи, організації).
   5.2 Проаналізувати методичне забезпечення інтелектуалізації управління ризиками інформаційної безпеки підприємства (установи, організації).
   5.3 Розробити та запропонувати сценарії та алгоритми інтелектуалізації управління ризиками інформаційної безпеки підприємства.
6. **Дата видачі завдання «**«19» вересня 2022 р.

Науковий керівник _____ С.В. Легомінова
підпис
Завдання прийнято до виконання _____ В.В. Самко
підпис

КАЛЕНДАРНИЙ ПЛАН
виконання кваліфікаційної роботи

студентом Самко Владиславом Васильовичем

Дата видачі завдання: «19» вересня 2022 р.

№ з/п	Етапи роботи	Термін виконання етапів	Примітка
1.	Визначення об'єкту, предмету, мети та завдань дослідження.	26.09.2022	
2.	Збір та аналіз літератури.	03.10.2022	
3.	Написання розділу 1.	17.10.2022	
4.	Написання розділу 2.	31.10.2022	
5.	Написання розділу 3.	14.11.2022	
6.	Формулювання висновків за результатами проведеного дослідження	01.12.2022	
7.	Оформлення роботи	08.12.2022	
8.	Оформлення презентації	15.12.2022	
9.	Отримання рецензії на роботу	23.12.2022	
10.	Захист в ДЕК	17.01.2023	

Студент В.В. Самко

(підпис)

Науковий керівник С.В. Легомінова

(підпис)

РЕФЕРАТ

Кваліфікаційна робота присвячена розгляду та інтелектуалізації процесу управління ризиками інформаційної безпеки. Робота складається з переліку скорочень, вступу, трьох розділів, що містять 28 рисунків та 2 таблиці, висновків та списку використаних джерел.

Об’єкт дослідження – Інтелектуалізація процесу управління ризиками інформаційної безпеки підприємства (установи, організації).

Предмет дослідження – особливості інтелектуалізації процесу управління ризиками інформаційної безпеки підприємства (установи, організації).

Мета роботи – розробка сценаріїв та алгоритмів управління ризиками інформаційної безпеки підприємства (установи, організації).

Для досягнення кінцевої мети в роботі було розглянуто міжнародний досвід, підходи до побудови процесу управління ризиками інформаційної безпеки та методи управління ним. На прикладі підприємства(організації, установи) застосовано підходи та методи для аналізу її особливостей, бізнес-функцій, завдань. Запропоновано відповідний інструментарій інтелектуалізації та рекомендації по організації управління системою. Розглянуто та проаналізовано потреби такої системи та інфраструктурні особливості, її можливості та функції. Розглянуто та обґрунтовано ефективність створеної системи. Надано рекомендації з побудови подібних інтелектуалізованих систем, впровадження, налаштування та підтримки запропонованого у роботі рішення.

Галузь використання – Продемонстрований в роботі приклад проектування інтелектуалізованої системи управління ризиками можна використовувати для створення подібних систем на підприємствах(організаціях, установах). Використані підходи та методи проектування є універсальними і підходять для більшості типів організаційного управління. Надані відомості про технології інтелектуалізації інформаційної безпеки можна використовувати при підборі та поєднанні інструментів інтелектуалізації, при створенні систем інформаційної безпеки різноманітних профілів.

Ключові слова: РИЗИК, ІНТЕЛЕКТУАЛІЗАЦІЯ, УПРАВЛІННЯ, СИСТЕМА, АВТОМАТИЗАЦІЯ, АРХІТЕКТУРА, ІНФРАСТРУКТУРА, УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СИСТЕМА УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІБ – інформаційна безпека

ПЗ – програмне забезпечення

СУРІБ – система управління ризиками інформаційної безпеки

СУІБ – система управління інформаційною безпекою

УІБ – управління інформаційною безпекою

УРІБ – управління ризиками інформаційної безпеки

MTTD – mean time to detection (переклад укр.мовою)

MTTR – mean time to remediation

MTTI – mean time to identify

SIEM – security information and event management

SOAR – security orchestration and response

SaaS – service as a service

IaaS – infrastructure as a service

PaaS – platform as a service

VMDR – vulnerability management detection and response

WAS – web application security

CS – container security

PC – policy compliance

SAQ – security assessment questionnaire

GAV/CSAM – global asset view/Cybersecurity asset management

SEP – Symantec endpoint protection від компанії “Broadcom Inc.”

DLP – Symantec data loss prevention від компанії “Broadcom Inc.”

BF – HCL BigFix від компанії “HCL Software”

SMG – Symantec messaging gateway від компанії “Broadcom Inc.”

ВСТУП

А к т у а л ь н і с т ь т е м и. У сучасному світі швидкість розвитку технологій та різноманітних сфер діяльності зростає з кожним днем. В результаті пришвидшення прогресу більшість актуальних та прибуткових сфер діяльності приймають динамічний характер та мають тенденцію розвивати методи, ідеї, засоби, які дозволяють їм отримувати перевагу у швидкості, зручності, універсальності, якості свого функціонування. Отже, інформаційні технології повинні адаптуватися під реалії сучасного світу та забезпечувати швидке, ефективне та надійне задоволення вимог у динамічному середовищі. В свою чергу це призводить як до прогресу та покращенню існуючих систем так і до створення нових. Збільшується кількість технологій, розміри IT інфраструктур, з'являються нові задачі та вимоги до IT. Такий швидкий розвиток технологій призводить до появи вразливостей, помилок , загроз, конкуренції та інших факторів які можуть стати причиною виникнення ризиків інформаційної безпеки. Інтелектуалізація управління ризиками інформаційної безпеки покликана захистити організацію від негативного впливу таких ризиків, зробити це ефективно, вчасно, та з мінімальними затратами.

М е т а і з а в д а н н я д о с л і д ж е н н я. **Мета роботи** - розробка сценаріїв та алгоритмів управління ризиками інформаційної безпеки підприємства (установи, організації).

Для досягнення поставленої мети необхідно виконати такі завдання:

1. Дослідити теоретичні засади інтелектуалізації управління ризиками інформаційної безпеки підприємства (установи, організації).
2. Проаналізувати методичне забезпечення інтелектуалізації управління ризиками інформаційної безпеки підприємства (установи, організації).
3. Розробити та запропонувати сценарії та алгоритми інтелектуалізації управління ризиками інформаційної безпеки підприємства.

Об'єкт дослідження - інтелектуалізація процесу управління ризиками інформаційної безпеки підприємства (установи, організації). **Предмет**

дослідження - особливості інтелектуалізації процесу управління ризиками інформаційної безпеки підприємства (установи, організації).

Наукова новизна одержаних результатів. Запропоновано та продемонстровано спосіб створення інтелектуалізованої системи управління ризиками на прикладі організації. Розглянуто та запропоновано набір інструментів та спосіб їх поєднання на прикладі гібридної, розгалуженої інфраструктури чого. Проаналізовано особливості інструментів та їх вплив на обрані методи управління ризиками інформаційної безпеки.

Практичне значення одержаних результатів. Продемонстрований в роботі приклад проектування інтелектуалізованої системи управління ризиками можна використовувати для створення подібних систем на підприємствах (організаціях, установах). Використані підходи та методи проектування є універсальними і підходять для більшості типів організаційного управління. Надані відомості про технології інтелектуалізації інформаційної безпеки можна використовувати при підборі та поєднанні інструментів інтелектуалізації, при створенні систем інформаційної безпеки різноманітних профілів.

Галузь застосування. Управління ризиками інформаційної безпеки. Проектування систем інформаційної безпеки. Інтелектуалізація процесів інформаційної безпеки. Аналіз та вибір актуальних інструментів та продуктів забезпечення інформаційної безпеки.

Розділ 1
ТЕОРЕТИЧНІ ЗАСАДИ ІНТЕЛЕКТУАЛІЗАЦІЇ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА (УСТАНОВИ, ОРГАНІЗАЦІЇ)

1.1 Сутність ризику інформаційної безпеки підприємства, його інтелектуалізація в процесі управління

Управління ризиками інформаційної безпеки (УРІБ) – процес завданням якого є виявлення, ідентифікація, оцінка ризиків та прийняття рішень щодо захисту інформаційних активів підприємства відповідно до визначеного прийнятного рівня ризику.

Інтелектуалізація управління ризиками інформаційної безпеки – це процес покликаний спростити, пришвидшити, автоматизувати та адаптувати існуючі системи та методи управління ризиками для створення максимально ефективного процесу УРІБ під потреби організації, установи, підприємства.

УРІБ – це комплексна задача, яка вимагає активності на всіх рівнях управління. Так вище керівництво бере відповідальність за стратегічне бачення управління ризиком та його кореляцію з бізнес інтересами та цілями організації, підприємства чи установи. Середня ланка керівників бере відповідальність за управління, проектами та процесами необхідними для ефективного управління ризиком. На операційному рівні спеціалісти забезпечують якість роботи та надійність виконання всіх необхідних функцій.

Організація – група людей чи процесів діяльність яких свідомо координується для досягнення загальної цілі чи цілей, може бути формальною і неформальною, складається з керуючої, та керованої підсистеми [1].

Так як організація це об’єднання активів для досягнення кінцевої цілі, яким властивий певний метод управління та ієрархія, надалі використано поняття організація в широкому контексті, включаючи також різноманітні типи управління та регулювання у тому числі підприємство та установу. В контексті

даної роботи буде наголошено на необхідності проведення процесу УРІБ для усіх типів організації та видів управління. Це зумовлено загальними рекомендаціями, а також алгоритмами та процесами аналізу і побудови УРІБ. В залежності від особливостей законодавства та сфери, задач та функцій організації, кожна з них буде по своєму унікальна, що зумовлює необхідність використовувати універсальні методи та підходи до формування процесу УРІБ, в якості основи. Надалі можлива їх модифікація та адаптація в залежності від потреб кожної унікальної організації та її зобов'язань. Надалі розгляну найкращі практики та уніфіковані методи УРІБ та підготовки до проектування Системи управління ризиками інформаційної безпеки (СУРІБ).

Ризик для організації може мати різний характер. В залежності від особливостей організації вона може бути більш сприйнятлива до одного типу ризику і менш сприйнятлива до іншого типу.

1.1.1 Класифікаційні ознаки ризиків інформаційної безпеки

Загалом ризики можна класифікувати за багатьма ознаками та однією з найбільш популярних є класифікація за джерелом:

1. IT інвестиції, прийняття управлінських рішень;
2. управління життєвим циклом програм та проектів;
3. підтримка систем;
4. IT інфраструктура;
5. несанкціоновані дії;
6. помилки ПЗ;
7. інциденти з апаратним забезпеченням;
8. кібератаки;
9. ризики від третіх сторін;
10. невідповідність нормативним вимогам;
11. геополітичні ризики;
12. помилки персоналу, некомпетентність;

13.природні катастрофи;

14.ризик інновацій;

15.ризики при управлінні даними та інформацією;

16.тощо.

Дана класифікація доводить, що джерелами ризику для інформаційної безпеки можуть бути як кіберзагрози так і фізичні загрози. Навіть політичні та нормативні зміни можуть бути джерелом ризику для ІБ організації. Така кількість потенційних джерел ризику для організації та постійний розвиток нових технологій призводять до утворення великої кількості ризиків які можуть наносити значні збитки організації. Такий збиток може нанести непоправну шкоду організації або окремим її функціям. Через це виникає необхідність побудови СУРІБ. В основу такої системи повинен бути закладений підхід, який дозволить ефективно оцінювати та оброблювати ризики з будь-якого джерела, так, щоб кінцевий результат такої оцінки був уніфікованим та простим для розуміння і надавав можливість для ефективного прийняття управлінських рішень. Інтелектуалізація УРІБ в свою чергу дозволяє визначити та інтегрувати в архітектуру та бізнес-процеси організації найбільш підходящий та ефективний процес УРІБ. Намагається пришвидшити, спростити, автоматизувати, уніфікувати процес УРІБ та адаптувати його під вимоги та потреби організації.

1.1.2. Метрики оцінювання ризиків інформаційної безпеки підприємства

Для забезпечення уніфікації процесу оцінки ризику, та розуміння його усіма учасниками процесу, організації рекомендовано визначитися з набором метрик які будуть використовуватися для вираження рівня ризику.

Метрики для оцінювання ризику можна розділити на дві основні категорії:

Кількісні – визначають рівень ризику на основі чисельного представлення параметрів ризику та збитків в результаті реалізації певного ризику. Такий метод є досить складним і в залежності від джерела та типу загрози, а також додаткових змінних у процесі розрахунку, може займати дуже багато часу. Проводити оцінку

ризиків цими методами вручну - є не ефективним у сучасних реаліях, тому він сильно залежний від методів автоматизації, а також від професіоналізму спеціалістів, що проводять таку оцінку. Від даного методу оцінки ризику очікується досить високий рівень точності розрахунку, а отже значні помилки можуть призводити до прийняття неправильних управлінських рішень.

Якісні - методи якісної оцінки замість фактичної оцінки фінансових втрат використовують абстрактне представлення ризику з використанням певної шкали рівня ризику. Наприклад визначення вірогідності реалізації ризику за шкалою від одного до десяти. Такі методи спираються здебільшого на досвід спеціалістів різних галузей, що входять в фокус групу для оцінки ризиків і використовують методи накшталт експертної оцінки. Якісні методи є менш точними ніж кількісні вони вимагають менших затрат часу, та є менш залежними від автоматизації. Проте вимоги до рівня кваліфікації спеціалістів, та особливо досвіду, при проведенні оцінки залишаються високими.

На практиці можна використовувати і комбінований метод, який передбачає якісну оцінку ризиків. Після проведення якісної оцінки, в залежності від отриманих даних та необхідності, можна додатково провести більш точну, але і більш затратну по ресурсам кількісну оцінку.

Відповідно до обраного методу оцінки також організація розробляє, або приймає вже існуючу метрику оцінювання. Метрика оцінювання ризику – універсальний спосіб вираження рівня ризику який покликаний забезпечити розуміння особливостей ризику усіма учасниками процесу оцінювання, та спростити процес прийняття ефективних управлінських рішень.

В якості прикладу метрики можна навести Common Vulnerability Scoring System v3 (CVSS v3), яка покликана оцінювати рівень критичності вразливостей інформаційних систем. Така метрика допомагає пріоритезувати виправлення вразливостей, а отже і загроз та ризиків, які можуть бути реалізовані шляхом їх експлуатації. CVSS v3 – є кількісною метрикою оцінювання.

Таким чином ризики для організації можуть з’являтися з великої кількості різноманітних джерел. На фактичний рівень ризику та його оцінку в організації

може впливати безліч факторів, таких як: способи оцінювання, метрики, бізнес інтереси, суміжні процеси, пріоритети, політики, конфігурація і навіть нормативні вимоги. Усі ці фактори потрібно враховувати та систематизувати для оцінювання ризиків та прийняття управлінських рішень, побудови ефективної СУРІБ.

1.1.3. Етапи управління ризиками інформаційної безпеки підприємства

Розглянуто з яких етапів складається типовий процес УРІБ (рис 1.1.). Основні етапи управління ризиком [2]:

Ідентифікація інформаційних активів – якими інформаційними активами володіє організація, які функції вони виконують, з якими саме даними працюють, які з них є критично важливими? На даному етапі виконується процес оцінки цінності інформаційних систем організації, визначення особливостей їх функціонування [2].

Ідентифікація вразливостей – після визначення цінності активів та встановлення пріоритетів з їх захисту необхідно визначити потенційні загрози, ризик реалізації яких може призвести до нанесення збитків організації. Для цього необхідно проводити процес управління вразливостями. Основним завданням управління вразливостями при забезпеченні процесу управління ризиками є визначення які саме вразливості, та в якій мірі, створюють ризик для конфіденційності, цілісності, доступності інформаційних ресурсів організації [3].

Ідентифікація загроз – наявність вразливості не обов’язково означає наявність загрози. Процес управління загрозами дозволяє не лише визначити наявність та критичність загроз, а також прогнозувати особливості їх появи в майбутньому, відслідковувати світові, або вужчі - організаційні тенденції. Процес управління загрозами допомагає в оцінюванні критичності та пріоритезації загроз, а також у пошуку способів боротьби з ними. Таким чином управління загрозами є невід’ємною частиною ефективного процесу управління ризиками[2].

Управління контролями (конфігурацією) – у процесі управління ризику його поява не прив’язана до початку функціонування системи чи до його кінця. Ризик може виникати у будь-який час і мати різноманітний характер. Таким чином під час виникнення ризику вже існує певна конфігурація або контролі, які впливають на його характеристики. Так вже існуючі політики, налаштування, системи можуть значно зменшити рівень ризику вже на етапі його виникнення, або навпаки збільшити вірогідність його реалізації. Таким чином ефективне управління та аналіз контролів є важливою складовою для підвищення ефективності управління ризиками, та є абсолютно необхідним для використання проактивного підходу до управління ризиками [2].

Оцінювання – процес поєднання отриманої інформації про вразливості, контролі, загрози, особливості систем, процесів та конфігурацій для оцінки ризику. Для проведення оцінки ризиків організація обирає метод оцінювання. Він може бути як кількісний так і якісний в залежності від потреб. При необхідності можливо використання декількох методів, та вибір декількох різних метрик оцінювання [2].

Наприклад для виконання якісної оцінки зазвичай використовують більш ускладнену версію такої формули [2]:

Ризик = (Загроза x Вразливість (Вірогідність експлуатації x Вплив експлуатації) x Цінність активу) - Контролі безпеки.

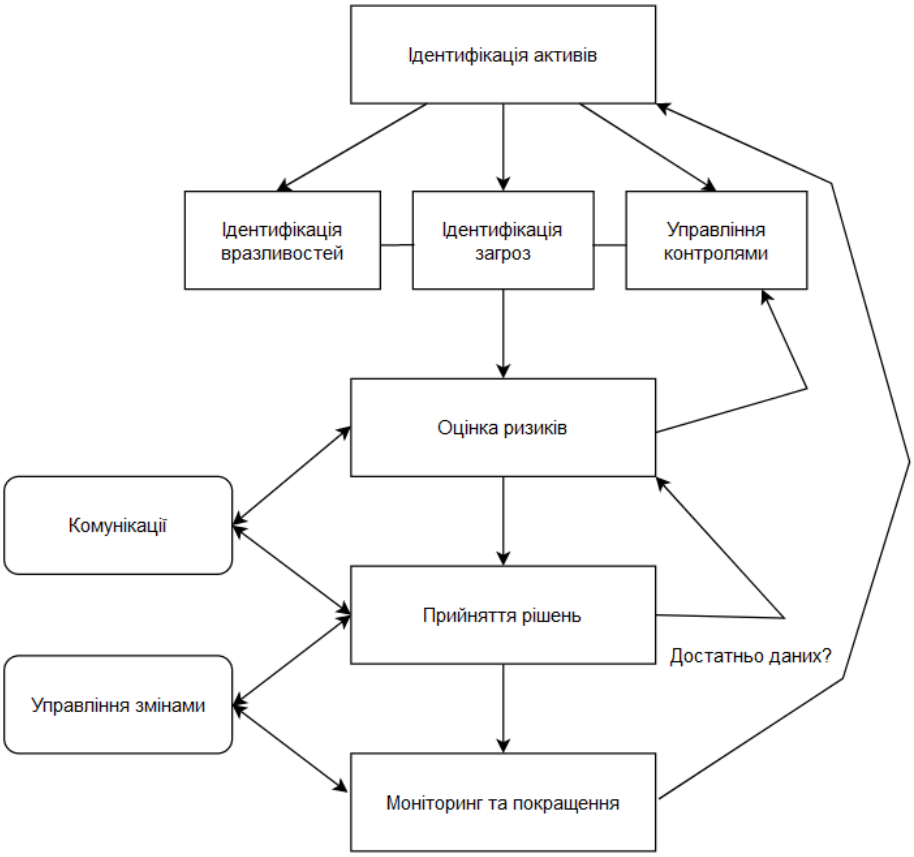
Прийняття рішення – етап управління ризиками на якому за результатами проведеної оцінки уповноваженими спеціалістами приймається рішення про те, як саме буде адресовано цей ризик.

- Закриття ризику – впровадження контролів які повністю, або частково виправляють ризик.
- Зниження ризику – зниження вірогідності реалізації ризику, але не повне його закриття.
- Перекладання ризику – передача відповідальності за обробку ризику на інший суб’єкт, таким чином в разі реалізації ризику відповідальність буде частково передана на цей суб’єкт, що дозволить зменшити втрати.

- Прийняття ризику – ризик не буде виправлено, найчастіше використовується коли збиток від ризику нижчий ніж затрати часу та ресурсів на його виправлення.
- Уникнення ризику – прибрати причини впливу ризику на організацію. Наприклад прибрати всі сервери Windows 2012 R2 з корпоративної мережі таким чином уникаючи будь-якого ризику пов’язаного з вразливостями цієї системи.

Комунікація – необхідна частина процесу управління ризиком завданням якої є забезпечення розуміння між усіма ланками та учасниками процесу. Ефективна комунікація пришвидшує процес прийняття рішень та забезпечує ефективність управління ресурсами і ризиками в цілому.

Моніторинг – постійний процес повторного оцінювання ризиків. За своєю природою ризик є динамічним, він має властивість змінюватися в залежності від багатьох факторів. Таким чином будь-які організаційні зміни можуть впливати як



Має бути посилання у тексті на рисунок та підпис під рисунком.

на нові ризики, так і на ті, які вже були адресовані раніше. Така властивість ризиків вимагає регулярно проводити аудити, повторні оцінки ризиків та прогнозування появи нових ризиків у майбутньому, для забезпечення надійності та ефективності функціонування СУРІБ.

Рис. 1.1. Типовий цикл УРІБ

При використання такого циклу управління ризиком організація здатна систематизувати оцінку ризиків та враховувати більшість факторів, що впливають на об’єктивність такої оцінки. Він дозволяє розставляти пріоритети та перш за все враховує особливості організації, та її ІС при прийнятті рішень. Комунікації між задіяними спеціалістами знижують вірогідність помилок та забезпечують об’єктивність оцінки, а моніторинг дозволяє підтримувати актуальність проведеної оцінки та самого циклу, надає можливості для його адаптації та покращення.

1.2 Практика та рекомендації підвищення ефективності циклу УРІБ

Важливим процесами забезпечення ефективності для такого циклу СУРІБ стає управління змінами та комунікації. Однією з основних задач управління ризиками, вразливостями, інцидентами та іншими важливими процесами інформаційної безпеки є закриття ризиків, введення змін в інфраструктуру безпеки, та її покращення [4]. Таким чином прийняті рішення по обробці ризику, окрім прийняття ризику, будуть призводити до проведення певних змін в організації. Такі зміни можуть бути досить незначними, або повністю змінювати особливості функціонування системи чи організаційної функції. Управління змінами – це процес управління людськими і технічними ресурсами що пришвидшує та спрощує планування, тестування і впровадження змін [4]. Процес управління змінами буде спрямований на: підвищення якості комунікації між спеціалістами до, та після прийняття управлінських рішень; зменшення часу

витраченого на впровадження змін; перевірку ефективності змін; сприйняття введених змін в організації, та зменшення опору змінам; тощо [4].

Так ефективний процес управління змінами підвищуватиме ефективність процесу управління ризиками, особливо при виконанні прийнятих рішень, та стане запорукою їх ефективності.

Для реалізації процесу управління змінами також можна використовувати інтелектуалізацію та інструментами автоматизації. В якості найпростішого прикладу такого інструменту можна навести систему ”Тікетів”. Уявімо, що в процесі управління ризиками була знайдена критична вразливість в системі ІБ. Така вразливість потребує швидкого реагування і закриття, що передбачає внесення певних змін до системи ІБ.

Завдяки системі “Тікетів” можна організувати комунікацію спеціалістів відділу ІБ та ІТ. Створивши в цій системі завдання для відповідних спеціалістів, можливо, надати їм всі необхідні дані для проведення робіт по її виправленню. За допомогою цієї системи можна встановити дедлайн виправлення, здійснювати контроль за процесом на кожному його етапі та отримувати інформацію у разі виникнення труднощів [4].

Також важливим елементом при функціонуванні СУРІБ є комунікації між усіма учасниками процесу, що його проводять. Так як ризики в організації можуть мати різноманітний характер та джерело, можуть впливати на різні організаційні функції або на організацію в цілому для ефективного виявлення та оцінки ризиків необхідно залучати до процесу спеціалістів різних напрямків та з різних рівнів організаційної ієрархії. Найнижча ланка у такому процесі може стати способом виявлення ризику, виконувати процес збору необхідної для аналізу та прийняття рішень інформації і таким чином буде численним та важливим активом СУРІБ. Середня ланка організаційного керівництва проводитиме аналіз даних та формуватиме рекомендації, прийматиме участь у прийнятті рішень. Вища ланка розподілятиме організаційні ресурси, та буде приймати управлінські рішення. Таким чином, виникає необхідність побудови ефективних комунікацій між спеціалістами різних рівнів, що забезпечить максимальну повноту та ефективність

отримання та обробки даних, спростить процес прийняття рішень та запобігатиме конфліктам інтересів між спеціалістами. На кожному рівні можливо створити засоби для спілкування з вищим рівнем, а також організувати спеціалістів у фокус групи в межах кожного рівня. Наприклад об'єднати керівників відділів ІТ, ІБ, фінансового відділу, відділу кадрів, тощо, у середній керівній ланці. Таким чином, забезпечивши можливість представлення виявлених ризиків з точки зору їх впливу на кожний відділ(організаційну-функцію). Такий підхід повинен спростити пріоритезацію ризиків та забезпечити розуміння випливу запропонованих рішень на усі організаційні-функції, таким чином підвищуючи їх ефективність. Також створення відповідних фокус груп є невід'ємною частиною використання якісних методів оцінювання ризиків які засновані на експертній оцінці.

Згідно багатьох найкращих світових практик організації СУРІБ рекомендується також проводити перевірку на відмову контролів. Цей процес дозволяє перевірити та прогнозувати рівень збитку отриманий у разі відмови або помилкового спрацювання інструментів використаних для закриття ризику. В результаті така оцінка буде залежною від ефективності управління інцидентами в організації, що може значно знизити збитки у випадку відмови. У випадку виявлення недостатньої ефективності використаних первинних контролів вони повинні бути замінені, підсилені, прибрані, або залишені як є в залежності від цінності активів, що захищаються. В залежності від типу контролів застосованих для закриття ризику та цінності активів, можливо створювати додаткові захисні механізми. Наприклад, ризик отримання несанкціонованого доступу до інформації, що зберігається у базі даних може бути захищений на основі доменного контролю доступу користувачів. Але у разі будь-якої помилки результатом якої буде підвищення привілеїв користувача такий ризик може бути реалізовано, тому в якості додаткового контролю можливо створити правила на локальному фаєрволі, які здійснюватимуть додатковий контроль доступу дозволяючи підключення до бази лише з певного переліку IP-адрес комп'ютерів та серверів, тощо. У свою чергу процес управління інцидентами ІБ покликаний

максимально знизити збитки від реалізації ризиків ІБ, а також попередити виникнення таких інцидентів. Таким чином превентивне управління інцидентами також впливає на виявлення змін у організації, та стає важливим для своєчасного та ефективного виявлення та аналізу ризиків.

Важливо зазначити, що засоби захисту та закриття ризиків ІБ також можуть бути джерелом ризику. Наприклад, при використанні програмного забезпечення для захисту певних організаційних функцій - це ПЗ так само може містити вразливість, і якщо вона не виявлена та не опрацьована – становити ризик для ІБ організації. Таким чином виникає необхідність постійної перевірки та покращення існуючих контролів ІБ. Також необхідно забезпечити ефективну інтеграцію між різними засобами та продуктами ІБ, щоб не створювати вразливості та ризики задля спрощення функціонування такої системи. Особливо це стосується самостійної розробки інтеграцій спеціалістами організації.

Наприклад: використання хмарних технологій, як відомо, має властивість розділення відповідальності за ризик між клієнтами хмарних провайдерів та самим постачальником послуг. Розглянемо ситуацію, де клієнт поставника хмарних послуг має в інфраструктурі певний додаток, у функції якого входить обробка та передача даних. У такому випадку для виконання обробки даних після їх отримання захищеними каналами необхідно їх розшифрувати, для відправлення далі – зашифрувати. Отже, криптологічні процеси будуть відбуватися в хмарі, на стороні поставника послуг. Як зазначає [5] для проведення таких процесів необхідно завантажувати ключі шифрування в оперативну пам’ять. Уявімо, що система віртуалізації хмарного провайдера має певні механізми захисту, які захищають її від ризиків переповнення буферу, шкідливого ПЗ, тощо. Такі механізми можуть виконувати процедуру сканування оперативної пам’яті і або впливати на якість проведення криптографічних операцій, або навіть порушити конфіденційність ключів шифрування які там використовуються [5]. Саме така поведінка є прикладом захисту від ризиків, який породжує інші ризики, проте в даному випадку – ризики компрометації ключів для клієнта, та втрати репутації для провайдера. В якості додаткового контролю, що попередить такий ризик

можна використати технологію Trusted Execution Environment (TEE), яка дозволить ізолювати частину ресурсів провайдера так, щоб доступ до середовища обробки інформації клієнта мали лише санкціоновані додатки. Забезпечить захист від багатьох ризиків хмарного середовища включаючи конфіденційність, а поєднання з іншими механізмами захисту дозволить максимально знизити ризики не лише при обробці, а і в процесі передачі інформації [5].

При проведені процесу управління ризиками також важливо враховувати складність реалізації загрози, а не лише потенційні збитки, яких вона може завдати. До того ж варто враховувати особливості організаційної інфраструктури, в якій відбувається експлуатація. З метою проведення перевірки стійкості контролів ІБ та перевірки складності експлуатації вразливостей в конкретному середовищі прийнято використовувати тестування на проникнення (далі - пентест).

Нажаль в Україні на даний час використання такої практики не є популярним. По-перше це пов’язано з певними ризиками, які представляє сам процес пентесту. Так, він може призводити до тимчасової відмови в обслуговуванні, зниження продуктивності певних систем або до помилок ПЗ. Задля цього прийнято перед початком виконання пентесту визначати область його дії та дозволені способи та інструменти проведення тестування. Часто критичні для бізнесу системи не потрапляють до цієї області, або сильно обмежують інструментарій спеціалістів, які проводять тестування. Також, проведення подібного процесу вимагає досить високого рівня кваліфікації спеціалістів і тому наймати на постійній основі штатного спеціаліста може бути досить витратно. Через це організації, які все ж проводять тестування на проникнення замовляють таку послугу у відповідних сторонніх компаній. Таким чином, пентест є необхідним та рекомендованим багатьма стандартами у тому числі [2,3] процесом, що має виконуватись регулярно, але на практиці не отримує достатньо уваги та фінансування, особливо в менших за розміром та бюджетом організаціях. В якості альтернативи такому процесу починають виникати автоматизовані системи для проведення тестувань на проникнення від різних виробників. На

даний момент такі системи не здатні повністю замінити проведення професійного пентесту, але вони здатні автоматизувати частину завдань з перевірки, та можливо знизити навантаження на штатних чи найманих спеціалістів. Також, подібні системи значно пришвидшують перевірку реалізованих контролів і надають можливість за рахунок автоматизації проводити такі перевірки набагато частіше, ніж вручну. З боку розробників продуктів гарантується прагнення досягти мінімального впливу на активи ІБ при проведенні автоматизованих тестувань, а також спроба максимально наблизити симуляцію до справжньої атаки або перевірки на проникнення. Це надає можливість актуальної перевірки систем захисту та їх реагування на аномалії і знижує вірогідність генерації false positive з боку активних систем захисту та моніторингу ІБ.

1.3 Підходи та методи побудови циклу управління ризиками

1.3.1 Підхід NIST SP 800-39

Підхід NIST 800-39. Відповідно до [3] запропоновано використання багаторівневого підходу до управління ризиками. Такий підхід передбачає розподіл процесу на три рівні, управління ризиками на кожному з яких буде проходити паралельно. Рівні процесу є такими: організаційний, бізнес-процесів, інформаційний рівень (рис. 1.2).

Перший рівень такого підходу визначає як саме буде проводитись управління ризиками в організації та напряму впливає на активності, що проводяться на другому та третьому рівнях. На першому рівні визначаються цілі та бізнес інтереси організації, що напряму впливає на розвиток СУРІБ та її функцій на інших рівнях процесу. Перший рівень процесу несе відповідальність за пріоритезацію і розподіл ресурсів організації. Другий рівень процесу розглядає ризик з точки зору функції, або бізнес-процесу. Завдання другого рівня включають: захист функцій та бізнес-процесів; пріоритезацію процесів та оцінку цінності інформації; визначення критичності інформації; побудову та підтримку

ефективної архітектури ІБ; тощо. Таким чином архітектурні рішення на другому рівні процесу напряму впливають на третій рівень. Наприклад, зміни на рівні архітектури ІБ організації можуть впливати на особливості конфігурації індивідуальних систем на третьому рівні. Третій рівень розглядає ризик з точки зору інформаційної системи. Його завдання включають: категоризацію інформаційних систем організації; встановлення контролів безпеки та конфігурацію ІС; підтримку ефективної взаємодії з існуючою архітектуро ІБ; управління, створення, встановлення, моніторинг, модифікацію конфігурації ІБ; тощо.

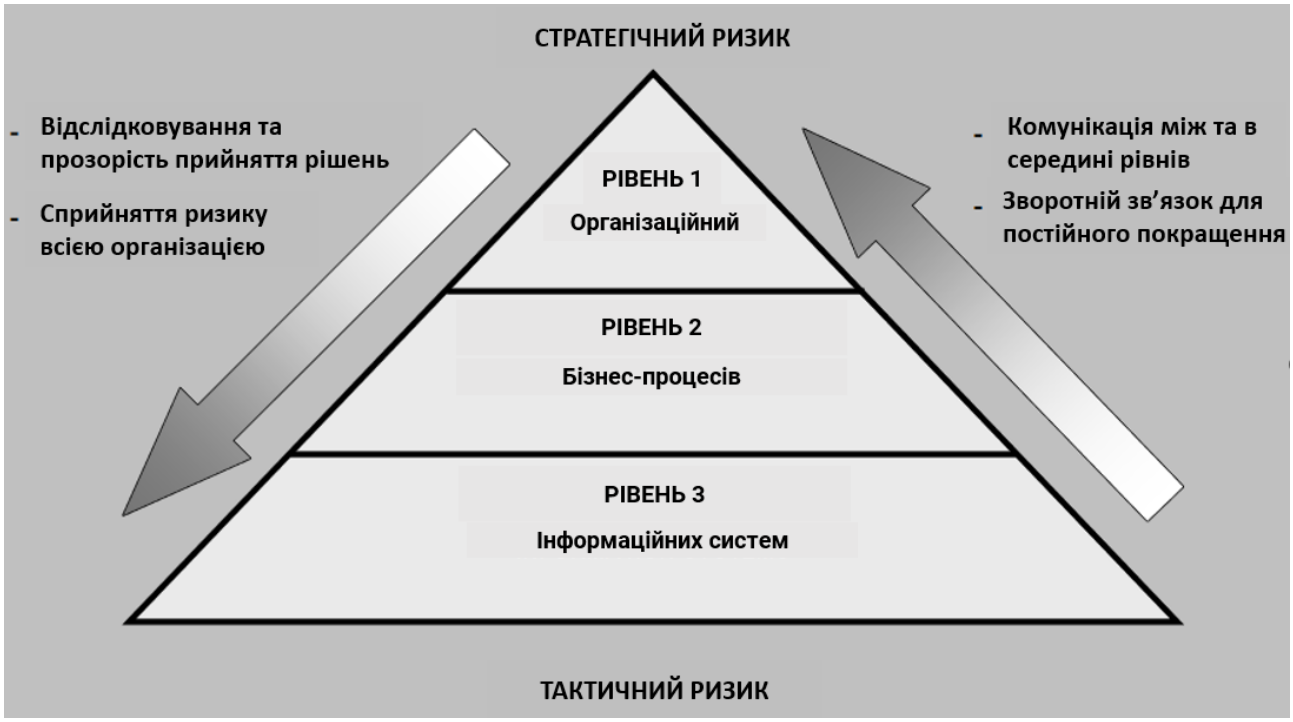


Рис. 1.2. Багаторівневий підхід до управління ризиком[3]

1.3.2 Підхід ДСТУ ISO/IEC 27005

ДСТУ ISO\IEC 27005. У свою чергу [6] пропонує наступний підхід до побудови процесу управління ризиками. Основні вимоги: процес управління ризиками інформаційної безпеки є необхідним для створення і підтримки ефективної СУІБ; СУРІБ має бути інтегрована у будь-які процеси УІБ та використовуватися як в процесі впровадження так і функціонування СУІБ; УРІБ має бути безперервним процесом; СУРІБ повинна визначати зовнішні та

внутрішні обставини, проводити оцінювання та оброблення ризиків відносно прийнятого в організації плану оброблення ризиків; УРІБ повинно надавати рекомендації щодо внесення змін та прийняття управлінських рішень, які стосуються обробки ризиків[6].

СУРІБ повинна:

- ідентифікувати ризики;
- оцінювати імовірність їх реалізації, появи та наслідки;
- встановлювати порядок пріоритетів оброблення;
- здійснювати моніторинг ефективності оброблення ризиків;
- здійснювати перегляд та покращення СУРІБ;
- тощо;

Також [4] наголошує на тому, що СУРІБ може бути впроваджена як для організації в цілому так і для окремих її частин. Це дає можливість поступової інтеграції розробленої системи з уже існуючими в архітектурі ІБ системами, а також дозволяє проводити адаптацію процесу під їх особливості. Згідно представлених вище вимог [6] надає наступний цикл УРІБ рис. 1.3.

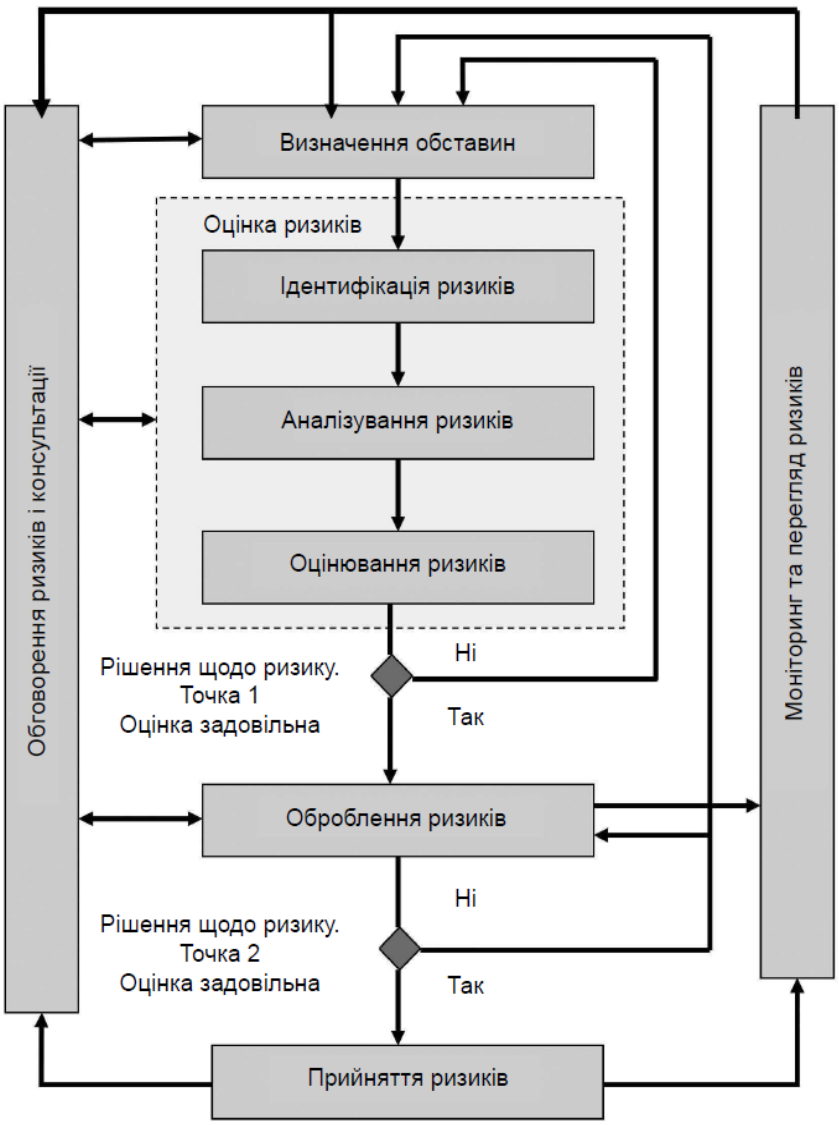


Рис. 1.3. Цикл управління ризиком згідно ISO/IEC 27005[6].

Першим етапом згідно циклу є визначення усіх обставин, що впливають на оцінювання ризику. Це можуть бути особливості ведення бізнесу, вимоги до систем, конфігурація, нормативне регулювання, тощо. Потім проводиться оцінка ризиків. Ітерації перших двох етапів виконуються доти, поки не буде зібрано достатньо інформації для виконання оброблення ризиків. У стандарті [6] відмічають важливість обговорення ризиків і консультації, що є процесом комунікації необхідним для ефективного проведення процесу УРІБ. Згідно [6] можна виділити, що СУРІБ являє собою систему завданням якої є проведення ефективного процесу УРІБ, а СУРІБ у свою чергу є частиною загальної СУІБ організації. Також рекомендується здійснювати регулярний моніторинг та

перегляд ризиків для контролю за потенційними змінами ризику які можуть і будуть відбуватись як реакція на значні зміни в організації. Останнім етапом є прийняття рішення по обробці ризику.

Документування – в результаті створення СУРІБ необхідно провести документування визначених організацією політик, методів, рівня прийнятного ризику для систем, метрик, впроваджених процесів тощо. Таким чином буде визначено регламент управління ризиком в організації та надано основу для розуміння особливостей процесів всіма відповідальними спеціалістами та їх учасниками.

Також варто відмітити важливість створення документації в процесі функціонування СУРІБ. При прийнятті управлінських рішень, внесенні змін в організаційні політики, інфраструктуру, активи, які захищаються, тощо. Відповідальне відношення до документування процедур, процесів та змін в організації дозволяє спростити їх розуміння, забезпечує ефективність моніторингу та покращення вже існуючих процесів, а також використовується для звітності під час проведення внутрішніх та зовнішніх аудитів та проходження СУІБ сертифікацій.

Для побудови СУРІБ на основі обраного підходу можна використовувати різні методи, які стануть основою процесу УРІБ. Проте такі методи мають здатність до адаптації в залежності від потреб організації та вимог які постають перед нею.

При виборі методу та підходу до УРІБ в організації необхідно враховувати, що створена СУРІБ буде під-системою, та частиною загальної СУІБ. Таким чином, вона повинна інтегруватися з уже існуючими процесами, та не використовувати протилежні підходи відносно тих, що використовуються у функціонування СУІБ. При створенні СУРІБ необхідно проводити визначення області її дії у загальній архітектурі організації.

Визначення області дії СУРІБ. Для забезпечення розуміння ризиків, які мають вплив на ІБ та повинні бути оброблені відповідним чином визначають області дії СУРІБ. Така область дії повинна включати всі активи, інформаційну

інфраструктуру, бізнес-процеси, або частини організації, які впливають на ефективне провадження ІБ в організації. Така область дії визначає елементи організації, які потрібно інтегрувати до СУРІБ та проводити повний цикл управління ризиками ІБ. При цьому для затвердження області дії СУРІБ необхідно враховувати такі фактори як: бізнес-задачі, бізнес-процеси, функції та структура організації, законодавчі, регуляторні, нормативні вимоги, політику ІБ організації, загальний підхід організації до управління всіма ризиками (не тільки ІБ), побажання зацікавлених сторін, кадрові особливості та соціальне середовище, тощо. Також при визначенні області варто враховувати не лише інтереси бізнесу та зацікавлених сторін, але і особливості активів які потраплятимуть в область дії. Для отримання актуальної інформації про такі активи на етапі планування системи варто проводити консультацію з володільцями активів.

Для кожного активу або групи активів обов'язково потрібно визначити володільця, це забезпечить наявність відповідальності за активи та їх підзвітність. Володілець активу не обов'язково має права власності на актив, але він є відповідальним за його виробництво, супроводження, розробку, захист та використання. Найчастіше він займає одну з керівних посад і має можливість визначити цінність активу для організації. Володілець активу повинен нести відповідальність за його визначення та класифікацію з точки зору ІБ, а також визначати права доступу до нього. Також володілець активу несе відповідальність за документування змін та особливостей активу. Корисним може бути документування контролів та правил використання активу, які описують дозволені та заборонені дії щодо активу. Таким чином, відповідальність за підтримку певного рівня безпеки активу може бути делегована іншим спеціалістам, але відповідальність за інвентаризацію та коректне використання активу залишається за його володільцем [7]. Так володільці активів можуть нести відповідальність за цілі кластери активів, мати інформацію про особливості роботи певного типу технологій в організації, та забезпечувати їх ефективність у підтримці бізнес-процесів. Отримання даних про критичні активи та особливості їх взаємодії з іншими елементами організаційної архітектури може стати

критично важливим при визначенні області дії СУРІБ а також методів та підходів, інструментів які будуть використані для створення СУРІБ.

1.3.3 Методика OCTAVE

Розглянуто декілька найбільш популярних методів УРІБ. Методика “Operationally Critical Threat, Asset and Vulnerability Evaluation”(OCTAVE) розроблена в Університеті Карнегі-Мелон (США) і передбачає оцінювання критичності загроз, активів і вразливостей. Цю методику широко використовують у всьому світі, виконуючи роботи з оцінки ризиків ІБ та впровадження процесів управління ризиками в компанії загалом. Методика має ряд модифікацій, які розраховані на організації різного розміру та сфери діяльності. Зміст методики OCTAVE полягає в тому, що для оцінки ризиків використовується послідовність відповідно організованих внутрішніх семінарів (workshops). Оцінка ризиків здійснюється в три етапи, яким передує набір підготовчих заходів: узгодження графіка семінарів, призначення ролей, планування, координація дій учасників проєктної групи [7].

На першому етапі, в межах практичних семінарів, здійснюється розроблення профілів загроз, що містять в собі інвентаризацію та оцінку цінності активів, ідентифікацію застосовних вимог законодавства та нормативної бази, ідентифікацію загроз та оцінку їх ймовірності, а також визначення системи організаційних заходів з підтримки режиму інформаційної безпеки. На другому етапі проводиться технічний аналіз вразливостей систем організації щодо загроз, чиї профілі розроблено на попередньому етапі, який містить ідентифікацію наявних вразливостей компанії та оцінювання їх величини. На третьому етапі виконується оцінка та оброблення ризиків інформаційної безпеки, що містить визначення величини та ймовірності завданої шкоди внаслідок реалізації загроз ІБ з використанням вразливостей, які ідентифіковано на попередніх етапах, визначення стратегії ІБ, а також вибір варіантів і прийняття рішень з оброблення

ризиків. Величина ризику визначається як середнє значення річних втрат компанії в результаті реалізації загроз ІБ [8]. Алгоритм методики зображено на рис. 1.4.

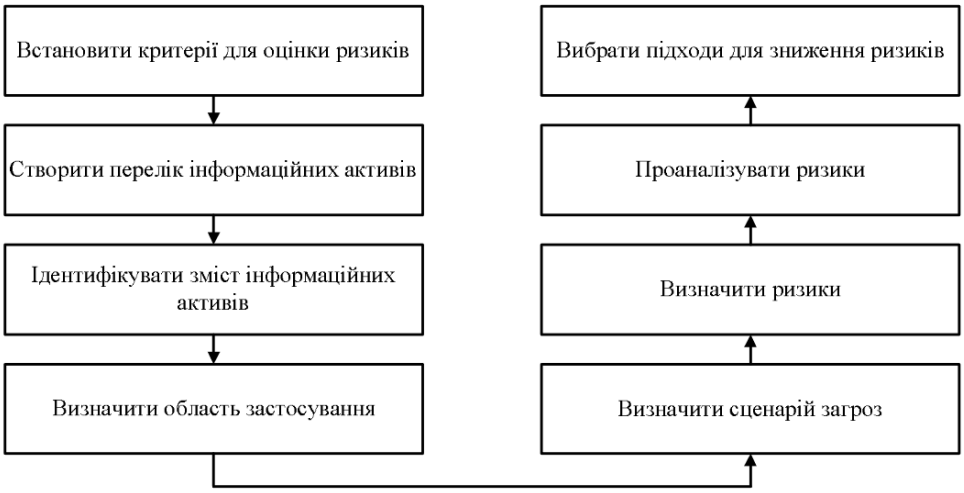


Рис. 1.4. Методика OCTAVE [8]

1.3.4 Методика NIST SP 800-30

Однією з найпопулярніших та широковживаних методик управління ризиками є методика Національного інституту стандартів і технологій США NIST, зазначена в Керівництві з управління ризиками в інформаційних технологіях NIST 800-30. Ця методика передбачає попереднє оцінювання двох параметрів: потенційного збитку та ймовірності реалізації загрози [8]. Призначення системи управління ризиками безпосередньо пов’язане з можливістю компанії виконувати свої основні функції за умов постійного розширення сфери використання інформаційних технологій. Методика оцінки ризиків, яка наведена в спеціальних рекомендаціях NIST SP 800-30, охоплює широке коло завдань, що пов’язані зі стратегією управління ризиками і є основою для розроблення власної системи управління ризиками [8].

Використання методики передбачає такі етапи:

1. опис характеристик системи;
2. ідентифікація загроз;

3. ідентифікація вразливостей;
4. аналіз наявних засобів/заходів захисту;
5. визначення значення ймовірності;
6. аналіз впливу;
7. визначення значення ризику;
8. вибір засобів/заходів захисту;
9. документування отриманих результатів.

Алгоритм цієї методики зображено на рис. 1.5.

Для успішного проведення оцінки ризиків будь-якою методикою основним завданням можна назвати збір даних для аналізу. Цей етап оцінки ризиків вимагає найбільших затрат часу та зазвичай проводиться на постійній основі, в процесі функціонування інформаційних систем. Тому якість проведеної оцінки ризиків напряму залежить від якості отриманих для цього аналізу даних, їх повноти та актуальності.

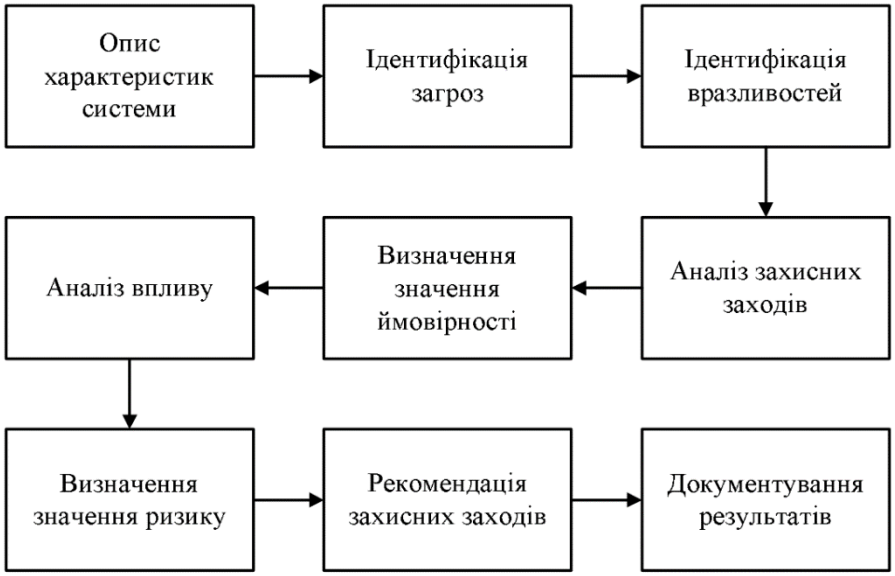


Рис. 1.5. Алгоритм методики NIST 800-30 [7]

Для забезпечення найбільш повних та актуальних даних для оцінювання ризиків запропоновано використовувати інструменти автоматизації.

Висновки до розділу 1

Отже, процес УРІБ є складним та трудомістким процесом, покликаним знаходити, аналізувати та як результат – попереджувати потенційні негативні наслідки для організацій. Завданням цього процесу стає виявлення та обробка ризиків з будь-яких джерел, залежно від особливостей організації. Існує багато підходів до побудови циклу УРІБ та багато методів його провадження, проте усі вони мають місце для впровадження інтелектуалізації. Інтелектуалізація покликана спростити провадження процесу УРІБ, пришвидшити його, підвищити ефективність та адаптивність, забезпечити неперервність процесу. На процес УРІБ та його побудову напряму впливає безліч факторів: ресурси, бізнес інтереси та функції, нормативне регулювання, особливості інфраструктури, особливості управління, тощо.

Виходячи з особливостей та потреб організації визначаються підходи та методи управління, будується процес УРІБ та всі необхідні для його функціонування системи та ресурси.

Складність УРІБ та особливості взаємодії з іншими процесами ІБ зумовлюють необхідність використання інтеграцій та інтелектуалізації процесів між собою для створення та підтримки ефективності процесу.

Розділ 2
МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ІНТЕЛЕКТУАЛІЗАЦІЇ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА (УСТАНОВИ, ОРГАНІЗАЦІЇ)

2.1 Методичні аспекти проектування інтелектуалізованої СУРІБ організації, архітектура рішень

Розглянуто послідовність дій та необхідних підготовчих етапів, що передують розробці, проектуванню та створенню СУРІБ. Не залежно від типу структурного управління для якого буде проектуватися СУРІБ кроки по аналізу та підготовці до проектування можна використовувати ті самі. Перед тим як проводити проектування системи для організації, підприємства чи то установи, згідно [4] необхідно в першу чергу визначити область її дії та зрозуміти яким чином вона буде інтегрована в загальну архітектуру організації, СУІБ. Для цього необхідне розуміння інфраструктури та її особливостей, а також потенційного впливу процесу УРІБ на бізнес-процеси. Використання інформації про архітектуру, активи, взаємодія з володільцями активів та створення ефективних комунікацій між керівництвом, що приймає рішення про створення системи, та виконавцями процесу проектування та її побудови, є критичним на даному етапі.

В залежності від нормативного регулювання організації, підприємства, установи, результати початкового аналізу та кінцевого проектування відрізнятимуться між собою, так само як на можливості по проектуванню системи впливатимуть і особливості архітектури, інфраструктура, географічне положення та розпорошеність активів, наявність спеціалістів та їх рівень кваліфікації , тощо. Надалі у даному розділі розглядатиму приклад організації процесу УРІБ та проектування СУРІБ для його виконання на основі прикладу організації, проте аналогічним чином можна проводити і проектування для інших структурних типів, залежно від результатів підготовки та початкового аналізу.

Далі у цьому розділі розділено процес проектування СУРІБ на декілька частин і продемонстровано створення проекту системи в залежності від особливостей організації.

В першу чергу для проведення такого проектування потрібно провести аналіз особливостей організації, її бізнес-процесів та цілей. Тож буде визначено особливості та функції організації для подальшого проектування системи.

Для визначення завдань до системи потрібно розуміти які задачі виконує організація і який кінцевий продукт виробляє, які функції та процеси існують в організації, тощо. В якому стані знаходиться ІБ організації в цілому, які існують політики ІБ, системи ІБ, тощо. Все це буде необхідним для визначення таких необхідних для проектування СУРІБ елементів як: область дії СУРІБ; ризик-апетит організації; нормативне забезпечення; план обробки ризиків; бюджет; тощо.

При проведенні проектування СУРІБ у реальних умовах певний набір таких даних може існувати вже на етапі початку проектування. Визначення цих необхідних елементів може займати досить багато часу, та потребує проведення повного аналізу особливостей організаційних функцій.

В даній роботі, в якості прикладу для організації процесу УРІБ використано типову організацію кінцевим продуктом якої є вироблення програмного забезпечення, та використання його у вигляді веб-додатків для надання інформаційних послуг користувачам. Організація активно розробляє різноманітні додатки, які можуть бути використані клієнтами за допомогою веб-порталу. Типовою особливістю організації вважатимемо те, що кількість таких додатків досить велика і їх призначення – різноманітне. Всі додатки незалежні один від одного та ізольовані з використанням технологій контейнеризації. Також використання багатофункціональної веб-платформи та ізоляції дозволяє використовувати не лише свої додатки на основі платформи, але і надавати її можливості для використання партнерами, або замовниками послуг хостингу. Тобто інші організації можуть використати платформу в якості способу надання своїх послуг певному колу споживачів.

Далі для розуміння особливостей організаційних процесів та архітектури визначимо основні процеси та функції які забезпечують бізнес-процеси організації.

Для софт-орієнтованої організації з роботою на основі веб-платформи виділено наступні основні бізнес-функції:

1. Функція розробки ПЗ;
2. Функція покращення ПЗ;
3. Функція підтримки користувачів;
4. Функція зберігання та обробки даних;
5. Функція реклами та просування продуктів;
6. Функція залучення партнерів до платформи;
7. Функція покращення та розвитку знань розробників;
8. Функція розробки дизайну додатків та платформи;
9. Функція розробки та покращення платформи, а також її модульної системи;
10. Функція підтримки інтеграцій партнерських додатків та простоти управління ними.

Розглядаючи ці 10 основних бізнес-функцій організації можна виділити наступні завдання до ІБ щодо підтримки таких функцій:

1. Забезпечення КЦД усіх критичних систем та інформаційних активів;
2. Забезпечення безпеки процесу розробки та самих додатків;
3. Управління вразливостями інфраструктури, додатків, платформи;
4. Управління інцидентами, захист даних споживачів;
5. Виявлення та попередження загроз ІБ;
6. Захист хмарної інфраструктури та інтеграцій;
7. Контроль доступу та управління патчами;
8. Контроль доступу, та захист від ризиків з боку користувачів;
9. Тощо.

Розглянуто поняття гібридної інфраструктури рис 2.1.

В першу чергу, перед тим як використовувати методи УРІБ, необхідно розуміти до якого типу інфраструктури буде застосовано той чи інший метод. Інформаційні інфраструктури можна розділити наступним чином:

1. Класична інфраструктура;
2. Хмарна інфраструктура;
3. Гібридна інфраструктура;

Рис. 2.1. Гібридна інфраструктура

Класична інфраструктура зазвичай включає апаратні, технічні, мережеві активи, такі яка комп’ютери, сервери, мережеве обладнання, тощо. Зазвичай такі активи розгорнуті фізично і знаходяться під прямим управлінням спеціалістів організації. Перевагою такого підходу можна назвати прямий контроль та підвищений рівень безпеки даних що циркулюють в такому середовищі. Організація має повний контроль над своїми активами, застосунками та даними. Але таке рішення є більш дорогим ніж інші види інфраструктури, та вимагає більшої кількості підтримки, ресурсів, спеціалістів для свого функціонування.

Хмарна інфраструктура передбачає оренду організацією апаратних ресурсів відповідного провайдера, що запобігає великим витратам на купівлю апаратного забезпечення, та знижує затрати на його обслуговування. Частково передається і навантаження по захисту інформації, що циркулює в таких системах. Саме через це, не для кожної організації припустимо використання даного типу інфраструктури, особливо при роботі з службовою або секретною інформацією.

Універсальним рішення цієї проблеми є гібридна інфраструктура, яка поєднує у собі класичну та хмарну і дозволяє використовувати як переваги захищеності класичної так і ресурсної ефективності хмарної інфраструктури. Наприклад комбінування даних інфраструктур в залежності від типу інформації яка циркулює в тому чи іншому сегменті IT-середовища, або в залежності від нормативних вимог.

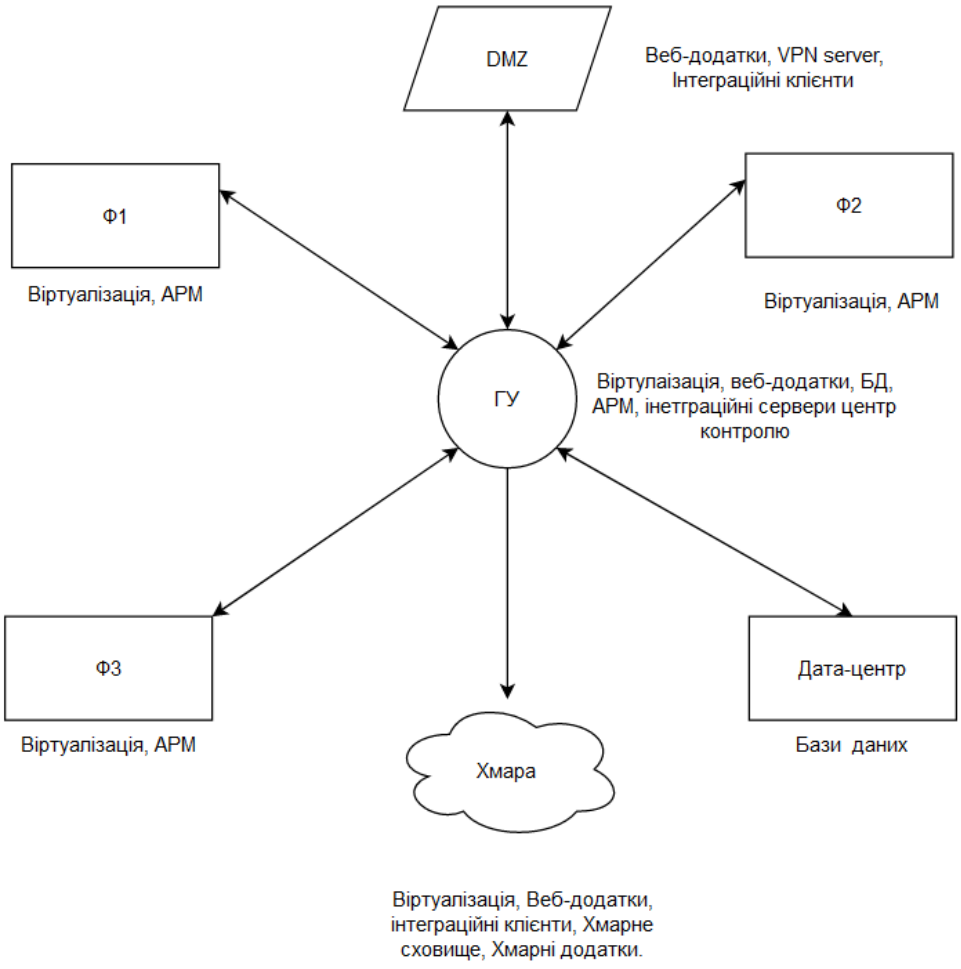
Також варто окремо виділити віртуалізовану інфраструктуру, яка являє собою ресурси, та програмне забезпечення, що створюється за допомогою розподілення технічних ресурсів певного активу на програмному чи апаратному рівні. Вона так само активно застосовується у гібридній інфраструктурі. Основною особливістю віртуалізованої інфраструктури можна назвати можливість ізоляції процесів, що є дуже цінним з точки зору безпеки, але призводить до обмеження видимості в такій інфраструктурі і може призводити до ускладнення УРІБ, що необхідно брати до уваги при її широкому використанні.

На практиці найпопулярнішою є саме гібридна інфраструктура, що дозволяє максимально гнучко комбінувати можливості IT-інфраструктури та ресурсів в залежності від потреб та нормативних вимог. Надалі пропоную розглядати УРІБ на прикладі гібридної інфраструктури.

На даний момент в світі такий тип інфраструктури є найбільш розповсюдженим, але в той же час може викликати певні складнощі при організації ефективної роботи СУРІБ. На даний момент в Україні гібридна інфраструктура стає все більш популярною. Частково причиною є останні події 2022 року, та прийняття нового закону [9], про віртуальні сервіси та легалізацію віртуальних активів, що значно спрощує переведення інформаційних активів

державних організацій у хмару. З практичного досвіду відомі випадки масового перенесення великих частин інфраструктури ІБ та ІТ в хмарне середовище, і така тенденція буде продовжуватися в майбутньому, тож у цьому розділі також розгляну особливості та виклики побудови СУРІБ для закриття завдання аналізу ризиків у хмарі.

На рис 2.2 продемонстровано узагальнену схему інфраструктури обраної організації. В даному випадку інфраструктура розділена на декілька частин: публічну віртуалізовану; внутрішню гібридну; та хмарну. Така інфраструктура є загальним представленням і може сильно відрізнятися в залежності від організації, але головне що потрібно відмітити на даній схемі – наявність ІТ інфраструктури усіх типів. Організація володіє активами, що існують як у класичній, віртуалізованій, так і у хмарній інфраструктурі. Таким чином завдання



до СУРІБ повинні виконуватися для всіх визначених активів, що входять в область її дії не залежно від того до якого типу інфраструктури належить актив. Звідси випливає необхідність ефективної організації виконання процесів СУРІБ в організації з гібридною інфраструктурою.

Рис. 2.2. Узагальнена схема гібридної інфраструктура організації

Використовуючи визначену схему інфраструктури організації, для проведення процесу проектування СУРІБ розділятиму її на структурні частини.

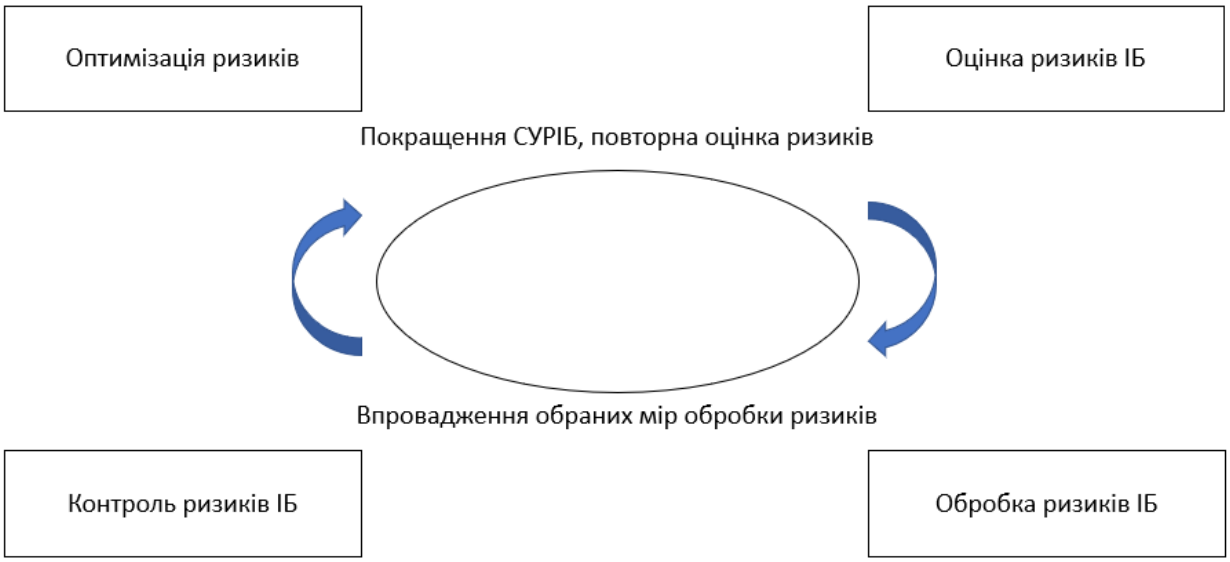
СУРІБ включає в себе три основні елементи:

1. Нормативне забезпечення, що включатиме: рекомендації, стандарти, метрики, методи, політику ІБ організації, план обробки ризиків, тощо.
2. Сукупність формалізованих, взаємопов'язаних процесів, що забезпечують ефективність УРІБ. Починаючи від аналізу і оцінки, закінчуючи перевіркою і покращенням системи
3. Кваліфіковані кадри, експерти, та організаційна структура управління, що складається з декількох рівнів.

2.2 Проектування та адміністративне регулювання СУРІБ

На першому етапі створення СУРІБ використовуючи визначений приклад організації, її особливості, архітектуру, пріоритетні процеси та функції оберу підхід до проектування системи, методи її створення, визначу область дії СУРІБ, також буде створено план обробки ризиків та обрано метрики оцінювання, визначено ризик-апетит організації, розглянуто типові політики, що впливають на проектування СУРІБ, тощо. В якості підходу до побудови СУРІБ обираю підхід представлений в ДСТУ ISO/IEC 27005. Серед розглянутих в цій роботі підходів обрав для побудови СУРІБ саме цей. В першу чергу [4] є державним стандартом України, що робить його більш привабливим для використання і побудови систем в нашій державі, так само він є і міжнародним стандартом у сфері, що сприяє визнанню систем побудованих саме за цим стандартом. Обираючи такий підхід спрощується інтеграція СУРІБ з СУІБ, за умови, що вони створені на основі

рекомендацій ДСТУ ISO/IEC 27001[10] – що надає рекомендації до побудови СУІБ і є міжнародним стандартом того ж сімейства. У зв'язку з актуальністю використання такого підходу в нашій країні та спрощення поєднання СУРІБ і



СУІБ побудованих згідно єдиної лінійки ДСТУ спробую використати такий підхід на прикладі розглянутої архітектури організації. Наприклад інтеграція СУРІБ з СУІБ як її підсистеми може проводитися на основі моделі PDCA та процесного підходу до функціонування і підтримки СУРІБ. Етапи циклу СУРІБ на основі моделі PDCA можна представити так – рис 2.3.

Рис. 2.3. Модель управління ризиком на основі циклу PDCA

Для інтеграції СУРІБ і СУІБ використання такого підходу вважаю актуальним за умови, що СУІБ використовує процесний підхід та модель циклу PDCA в якості основи для управління процесами ІБ. Що ж до методу УРІБ який буде актуальним для запропонованої системи вважаю можливим використання усіх методів які представлені в першому розділі. По-перше використання декількох різних методів у різних типах інфраструктури або для збільшення глибини аналізу даних є досить ефективним. Так використання різних методів може допомогти провести додаткову перевірку та виявити певні недоліки одного з них і мінімізувати втрати ефективності. По-друге динамічні зміни сфери ІБ, організаційної архітектури, політик, інструментів або навіть керівної ланки спеціалістів, що відповідають за УРІБ в організації може призвести до значних

змін у використовуваних методах УРІБ. Тому спробую створити на основі доступних інструментів ІБ автоматизовану систему, що надаватиме найбільш повну основу для проведення подальшого аналізу ризиків та прийняття управлінських рішень. Завданням системи буде покривати більшість вимог методів представлених в першому розділі та надавати максимально повні дані для прийняття рішень, або проведення додаткового раунду пріоритезації та аналізу даних, якщо це необхідно.

Таким чином розглянутий далі варіант СУРІБ буде надавати певний рівень гнучкості при виборі методів УРІБ, надаватиме можливості адаптації цих методів під особливості та потреби організації.

Далі розгляну типовий перелік нормативного регулювання, що може впливати на особливості системи УРІБ та організацію в цілому[11]:

1. Політики управління персоналом;
2. Політики навчання та тренувань;
3. Політики захисту та обробки даних;
4. Політики управління активами;
5. Політики управління змінами;
6. Політки інформаційної безпеки;
7. Регуляторні, стандартизація, ліцензування;
8. Налаштування та конфігурації систем\активів;
9. Політика класифікації даних;
10. Політика розподілу ролей та відповідальності;
11. Тощо.

У даному переліку представлено не повний обсяг типових політик які варто враховувати при проектування СУРІБ. Після аналізу всіх факторів нормативного регулювання та архітектури СУІБ, підходу до проектування та методу УРІБ перейду до визначення області його дії.

Відповідно до визначеної раніше архітектури організації розгляну на її основі область дії процесу УРІБ рис. 2.4. Відповідно особливостям роботи організації пропоную включати повну ІТ інфраструктуру в область дії процесу

УРІБ. Розгляну важливість процесу УРІБ для окремих елементів архітектури розділивши її на три основні частини більш детально, у порівнянні з рис 2.2:

1. Платформа;
2. Внутрішня мережа та ресурси;
3. Хмарне сховище та зовнішні репозиторії.

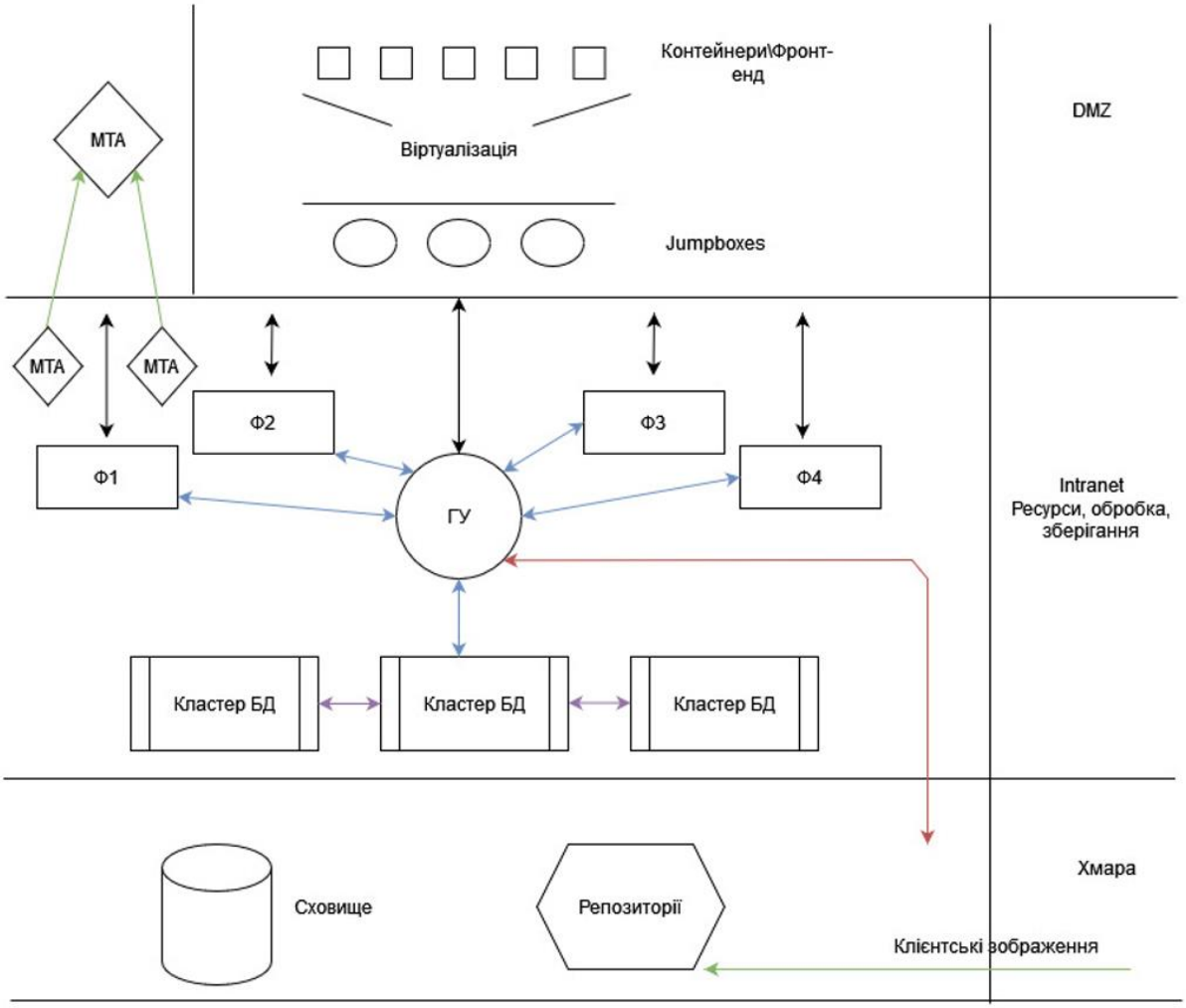


Рис. 2.4. Покриття інфраструктури процесом УРІБ

Першими розглянуто DMZ, віртуалізацію, публічно доступну частину платформи. Для цих елементів архітектури процес СУРІБ може різнитися та залежати від способу взаємодії з замовниками та користувачами платформи.

Наприклад в залежності від Service level agreement(SLA), та типу послуг які надаватиме організація відповідальність організації за управління ризиками може змінюватися. Так при наданні послуг Infrastructure as a Service(IaaS) організація

несе відповідальність лише за з управління ризиками відносно фізичної частини операцій. Так як замовникам надається апаратний ресурс та можливість контролю за способом його використання, то і управління ризиками тих продуктів та ПЗ яке ці ресурси використовує зазвичай покладається саме на користувачів. Таким чином відповідальність за перевірку ПЗ на вразливості, його оновлення, контроль інтеграцій та взаємодії з зовнішніми джерелами та іншими продуктами або сервісами контролюється користувачем. У випадку ж використання формату Service as a Service(SaaS) користувачеві буде надано ПЗ та його можливості які контролюються та захищаються організацією, де вже організація несе відповідальність за підтримку, пошук та аналіз вразливостей, оновлення ПЗ та апаратного забезпечення, забезпечення КЦД, тощо.

Таким чином для першого елементу архітектури запропоновано “плаваюче або часткове” покриття областю дії процесу УРІБ.

Друга частина архітектури яку можна назвати внутрішньою. Повинна мати найбільш повне покриття. В цій зоні знаходяться основні потужності, ресурси компанії, а також ІТ активи та способи моніторингу. Також в цій зоні існує велика частина центрів контролю та управління СУІБ, частиною якої можемо вважати створювану СУРІБ. Як результат для забезпечення безпеки внутрішніх систем, підтримки сервісів, контролю та попередження людських помилок, тощо, дану частину інфраструктури запропоновано покривати процесом повністю.

Третю частину інфраструктури яку можна охарактеризувати як зовнішнє сховище також рекомендовано покривати повністю. Дана інфраструктура є дуже важливою, так як надає функцію не лише полегшення доступу до ресурсів зовнішніх працівників, та можливість клієнтів надавати свої власні зображення та ПЗ для подальшого аналізу та розгортання, а є і способом реалізації розподіленого резервного копіювання даних, що є вимогою багатьох стандартів та вважається найкращою практикою. Також важливим для реалізації повного процесу УРІБ стає можливість користувачів надавати власні образи для розгортання на платформі віртуалізації. Така можливість безумовно є дуже зручною, так як знімає частину навантаження зі спеціалістів організації, а також надає більше

самостійності клієнтам при використанні своїх IaaS, Platform as a Service(PaaS) сервісів. Проте така можливість створює багато ризиків для організації і викликає необхідність аналізу та виявлення загроз і ризиків які можуть нести такі клієнтські завантаження. Тому третю частину архітектури теж рекомендовано повністю включити в область управління ризиками.

2.3 Процеси та інструменти функціонування СУРІБ (програмні продукти, інструменти автоматизації)

Після проведення початкового етапу проектування, враховуючи визначені там особливості СУРІБ та завдання до її створення потрібно розробити відповідні процеси СУІБ. Розглянути особливості їх поєднання та інструменти за допомогою яких можна реалізувати ці процеси. Такі процеси повинні поєднуватися з УРІБ та вносити свою лепту в правильну оцінку ризиків та прийняття рішень УРІБ. Згідно розглянутих у попередніх розділах рекомендацій, та особливостей організації і її бізнес-процесів для створення СУРІБ враховано такі процеси:

1. Процес управління вразливостями ІБ;
2. Процес управління загрозами ІБ;
3. Процес управління інцидентами ІБ;
4. Процес управління змінами;
5. Процес управління кадровими ресурсами та навчанням;
6. Процес управління фізичною безпекою;
7. Процес управління ресурсами;
8. Тощо.

Отже запропоновано набір інструментів, метою такого набору інструментів ІБ буде автоматизація та спрощення процесу УРІБ та можливість роботи з суміжними та під-процесами СУРІБ.

Для забезпечення ефективного захисту основних організаційних функцій запропоновано використання платформи “Qualys” від компанії “Qualys Inc.”[12]. Платформа Qualys це комплексний, хмарний інструмент завданням якого є

спрощення та автоматизація таких процесів як управління вразливостями, виконання перевірок на відповідність нормативним вимогам, автоматична оцінка ризиків та впливу активів на бізнес-процеси, управління виправленнями, контроль конфігурації, виконання завдань по адмініструванню активів, інвентаризація мережі та програмного забезпечення, контроль ліцензування та версій, тощо.

Можливості платформи “Qualys” дозволяють отримати повну видимість наявних в мережі організації активів незалежно від географічного розташування, зв’язку з корпоративною мережею, типу інфраструктури в якій знаходиться актив. Велика кількість спеціалізованих сенсорів Qualys, що надається платформою дозволяє проводити автоматизоване виявлення та оцінку вразливостей у гібридній інфраструктурі. Платформа Qualys рис 2.5 є хмарним рішенням, тому дозволяє легко збирати дані з будь-яких активів, що мають доступ до мережі інтернет, незалежно від особливостей їх зв’язку у корпоративній мережі. Платформа не потребує витрат на закупівлю апаратних ресурсів та проведення відповідних налаштувань.

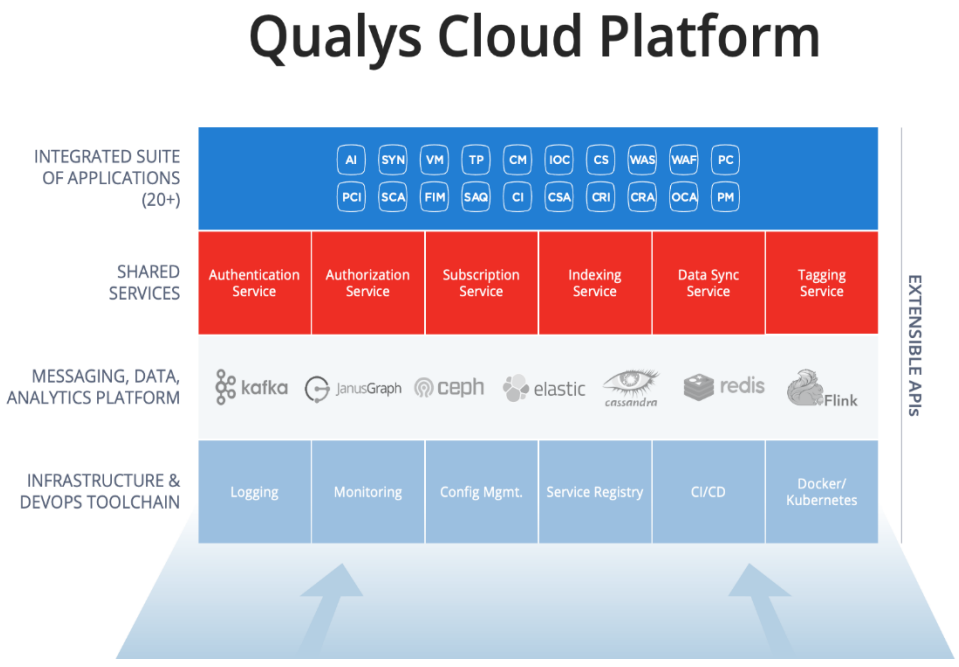


Рис. 2.5. Платформа Qualys [12]

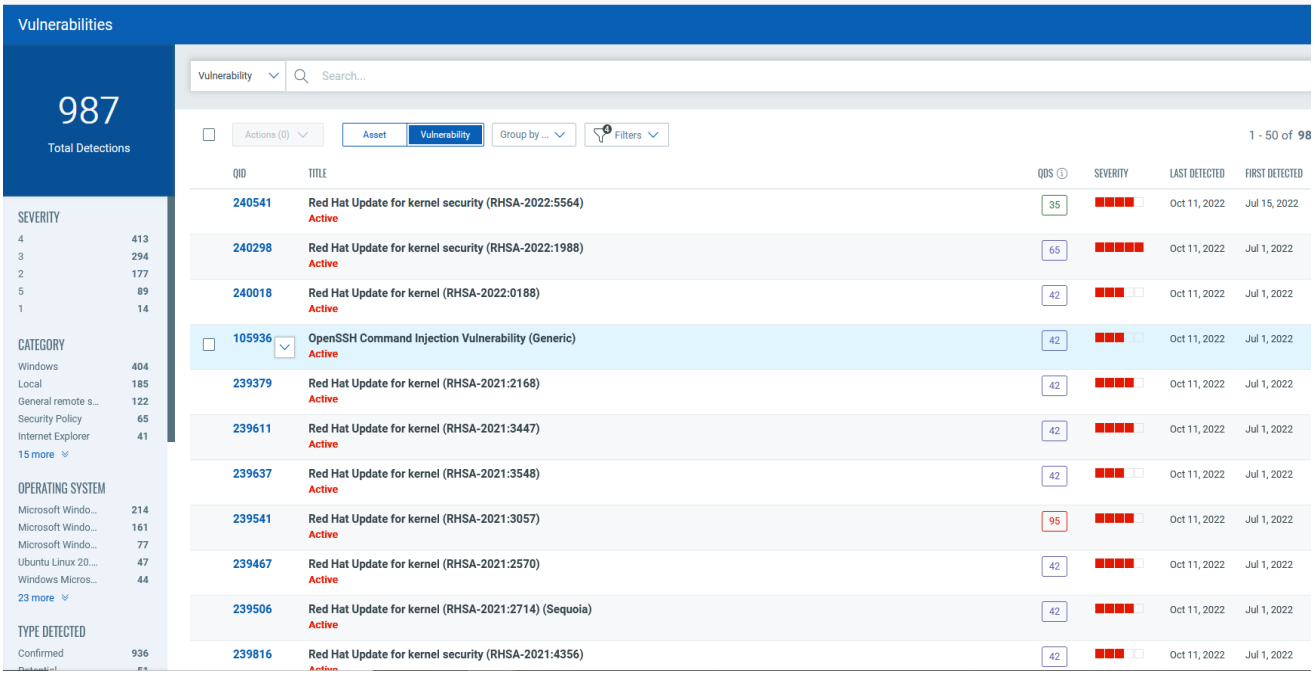
Згідно особливостей та організаційних функцій визначеної в даній роботі організації використано такі інструменти платформи Qualys для забезпечення ефективності УРІБ організації.

1. Модуль VMDR;
2. Модуль CM;
3. Модулі WAS, MD, WAF;
4. Модуль CS;
5. Модулі PC, SAQ;
6. Модуль GAV/CSAM;
7. Модуль CV, SDR;
8. Модуль EDR;
9. Модуль PM;

Основний модуль платформи Vulnerability management detection and response(VMDR) надає можливість отримання видимості в інфраструктурі організації за допомогою проведення інвентаризаційних сканувань. Надає інструменти для покриття інфраструктури скануваннями на виявлення вразливостей включаючи: внутрішні та зовнішні сканери вразливостей, локальні програмні агенти для регулярного сканування активів, хмарні конектори для виявлення та оцінювання вразливостей у хмарі, пасивні сенсори для аналізу трафіку мережі та пошуку загроз і ризиків таким чином, “out-of-band” сенсори для збору даних із мереж з обмеженим доступом до мережі інтернет. Надає нормалізовані дані про останні вразливості, їх оцінку згідно CVSS, а також власної критичності системи. Розраховує рівень ризику, що становлять інформаційні активи чи вразливості в залежності від їх важливості для бізнесу та особливостей конфігурації. Дозволяє відображати відсортовану та доповнену усіма необхідними даними інформацію яка потрібна для прийняття управлінських рішень. Наприклад: критичність активу, рівень його ризику, вразливості знайдені на машині, їх оцінку, вплив, спосіб виправлення, рекомендації, індикатори виявлення, посилання на патчі та офіційні статті виробників, тощо. Дозволяє використовувати автоматичний інтерфейс для проведення пріорітезації виправлення вразливостей. Володіє інструментами для ведення повноцінної звітності і представлення інформації у підходящому вигляді для кожної ланки

управління організації. Наприклад у вигляді глобальних звітів для керівництва, чи технічних звітів-завдань для керівників відділів або спеціалістів на місцях, тощо.

Використовуючи модуль VMDR рис. 2.6 організація зможе досягнути повного покриття своєї інфраструктури інвентаризаційними скануваннями та



скануваннями на виявлення вразливостей, зможе налаштувати перевірки сертифікатів безпеки активів в інфраструктурі, провести автоматичне оцінювання вразивостей та **узагальненого** розрахунку рівня ризику активів та вразливостей в інфраструктурі. Отримати дані для аналізу та прийняття рішення, провести пріорітезацію та підтримувати звітність та документацію, отримувати рекомендації по виправленню вразливостей та закриття ризиків, враховувати особливості конфігурації активів, тощо.

Рис. 2.6. Приклад інтерфейсу VMDR(вразливості, критичність, ризик)

Модулі Web Application Security (WAS) та Malware Detection (MD) – дозволять проводити виявлення та оцінку ризиків у веб-додатках організації, а також нададуть можливість виявляти шкідливе програмне забезпечення яке може розповсюджуватися через такі додатки. Додаток WAS дозволяє проводити сканування у складних, багатошарових додатках. Надає можливість сканувань з аутентифікацією, проводить перевірки на основні способи атак на веб-додатки,

здійснює пошук неправильної конфігурації, шкідливих посилань, надає рекомендації щодо виправлення проблем. У зв’язку з можливостями модулів визначати шкідливі посилання та ПЗ у веб-додатках організацій вони також дозволяють визначити ризики нанесення шкоди репутації організації та попередити її.

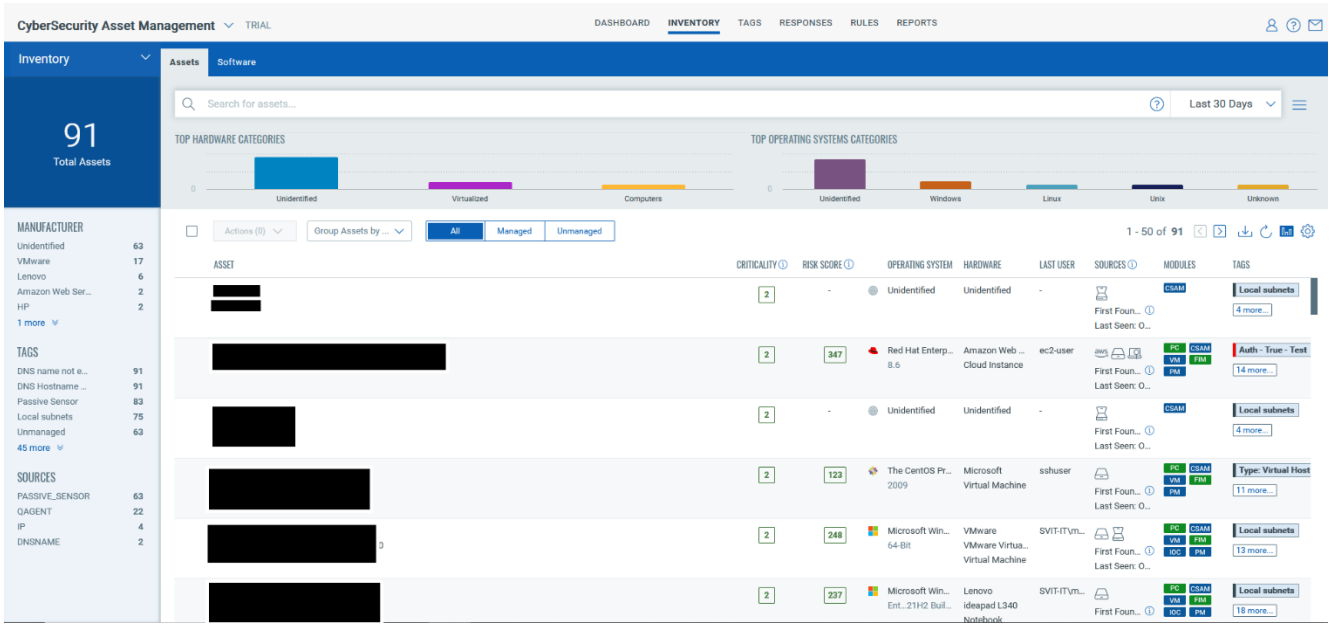
Модуль Container Security(CS) буде максимально актуальним для обраного типу організації, він дозволяє проводити виявлення вразливостей, та попереджувати виникнення загроз повністю покриваючи “CI/CD pipline”. Цей модуль може використовувати 3 різні типи сканерів. Перший проводить виявлення вразливостей на етапі створення та пакування зображень для контейнеризації. Другий контролює стан зображень та ПЗ що в них знаходиться під час перебування зображень в репозиторіях, та виявляє застарілі, вразливі, неактуальні зображення підтримуючи репозиторії а актуальному стані. Третій безпосередньо здійснює сканування та контроль за контейнерами на докер-хостах. Враховуючи особливості організації що розглядається, доцільним буде використання всіх 3 варіантів сканерів, що надає модуль CS.

Модуль Policy Compliance (PC) – дозволяє організації створювати або використовувати вже існуючі контролі для проведення автоматизованих перевірок на відповідність активів нормативним вимогам. Так організація наприклад може перевіряти відповідність своїх активів рекомендаціям CIS. Створювати власні вимоги та перевіряти всі активи в мережі на виконання встановлених політик. Такий функціонал дозволяє вчасно визначати порушення нормативного чи організаційного регулювання, проводити відповідну оцінку ризиків, виправляти та попереджувати інциденти пов’язані з порушенням нормативного регулювання.

Модуль Secure Assessment Questionnaire (SAQ) – це автоматизований спосіб проведення опитувань кадрової бази. Такий модуль можна використовувати під час проведення оцінки ризиків. Можливості модуля дозволяють проводити опитування відразу великої кількості респондентів залишаючи його зручним для них. Використовуючи такий інструмент працівники можуть проходити

опитування тоді коли їм зручно в поставлених часових рамках, що не буде відволікати від роботи та переривати процеси. При проведенні довгих опитувань працівники можуть перервати його та закінчити пізніше, прогрес зберігається. Використовуючи модуль SAQ можна не лише визначати додаткові ризики за допомогою опитування більшої аудиторії респондентів, а і проводити тестування цифрової грамотності спеціалістів, визначати слабкі ланки кадрових ресурсів, та визначати цілі для покращення ефективності спеціалістів і їх подальшого розвитку.

Модуль Global asset view(GAV) та його покращена версія Cyber security asset management(CSAM), рис. 2.7 – це основна система інвентаризації та надання видимості Qualys. Цей модуль надає максимум інформації про активи, ПЗ, ліцензії, налаштування. Дозволяє зручно групувати активи, розділяти їх по групам, аналізувати зібрану інформацію. Дозволяє контролювати життєвий цикл систем та програмного забезпечення. Має можливість контролю встановлення ПЗ.



Також використовується для створення звітності та є загальним центром аналізу актуальної інформації по IT-інвентарю організації. Для обраної організації, як і для будь якої іншої такий модуль є основою для проведення аналізу та прийняття рішень, управління активами ІБ. Тому платформа Qualys надає звичайний модуль інвентаризації GAV в якості безкоштовного функціоналу. CSAM у свою чергу додає функціонал відслідковування встановлення ПЗ та можливості по

додатковому створенню інвентаризаційних звітів, відслідковування життєвого циклу систем.

Рис. 2.7. Інтерфейс CSAM, активи, критичність, рівень ризику

Модуль Cloud View(CV) – створений для контролю та звітності по активам в хмарній інфраструктурі, використовує хмарні конектори які інвентаризують активи та збирають з них телеметрію надаючи актуальну інформацію про стан машин у хмарі, поєднуючись з можливостями сканувань активів на вразливості VMDR, та центом контролю активів GAV/CSAM дозволяють повністю контролювати та оцінювати захищеність хмарної інфраструктури.

Модуль SaaS Detection and Response(SDR) – Модуль який дозволить отримувати видимість ресурсів та ризиків у середовищі хмарних провайдерів, які надають послуги SaaS. Це дозволить контролювати стан, та наявність вразливостей використовуваних сервісів за умови не повного контролю на інфраструктурою поставника SaaS послуг.

Модуль Event detection and response(EDR) – дозволяє реалізувати функції систем EDR на основі хмарного агенту Qualys. Такі системи забезпечують виявлення загроз та ризиків, оповіщення про таке виявлення та надають можливості щодо часткового реагування на інциденти.

Модуль Patch management(PM), рис. 2.8 – один з найважливіших елементів системи, що в безкоштовному варіанті входить до базового пакету VMDR і надає інформацію про версії ПЗ, патчі для вразливостей, інформацію про особливості патчів та виробників, рекомендації по встановленню та налаштуванню, тощо. У платному варіанті розширює свої можливості дозволяючи віддалено виконувати скрипти на системах, керувати конфігурацією систем, автоматично встановлювати патчі та закривати вразливості і ризики, реалізує ці функції на основі хмарного агенту Qualys. Такий модуль може бути використаний не лише на етапі реалізації прийнятих рішень по виправленню ризиків, але і на этапі збору інформації та перевірки успішності прийнятих рішень. Його можливість запуску

скриптів на інформаційних активах дозволяє реалізувати безліч автоматизованих способів перевірки та зміни конфігурації систем.

Таким чином, запропоновано використовувати хмарну платформу Qualys в якості основи для побудови системи УРІБ. Також для посилення можливостей і функцій системи можна використати такий набір продуктів інформаційної безпеки:

1. IBM “Qradar SIEM”;
2. Symantec “Endpoint Protection”(SEP);
3. Symantec “Messaging Gateway”(SMG);
4. Symantec “Data Loss Prevention”(DLP);
5. HCL “BigFix”(BF);
6. IBM “SOAR”

IBM “Qradar SIEM” від компанії “IBM”[13](далі Qradar) – Security information and event management(SIEM) система моніторингу інформації та подій інформаційної безпеки. Така система є центром аналізу та моніторингу стану архітектури ІБ організації. Вона надає можливість збирати та автоматично аналізувати логи з усіх систем в архітектурі та має велику кількість методів та інтеграцій для збору подій, що робить її ефективною при роботі з розгалудженими та гібридними архітектурами. Використання даної системи дозволить централізовано та автоматично аналізувати, нормалізувати, корелювати системні події та повідомлення, виявляти кібератаки, загрози, ризики, а безліч додатків та розширень функціоналу стануть корисними при проведенні всіх визначених для організації функцій.

До функціоналу системи, який запропоновано використовувати віднесу:

1. Збір, нормалізація, кореляція системних подій;
2. Створення звітів;
3. Інструментарій для автоматичного аналізу подій;
4. Інструментарій управління джерелами та даними;
5. Можливість архівації та зберігання даних;
6. Можливості проведення розслідувань та реагування на інциденти;

7. Централізований інструмент управління;
8. Можливості по налаштуванню інтеграцій;
9. Тощо.

Використання даної системи дозволить захиститися від загроз, та допоможе проводити процес УРІБ. Наприклад функціонал системи дозволятиме відслідковувати зміни конфігурації на інших системах, дозволить контролювати активність користувачів та адміністраторів, попереджувати появу інцидентів, стане ресурсною базую для проведення розслідувань інцидентів. Надасть цінні дані для аналізу ризиків та прийняття управлінських рішень. Qradar також дозволить виконувати певні нормативні вимоги та надасть обширні можливості по документуванню та обробці прецедентів.

SEP від компанії “Broadcom inc.”[14]. - Продукт ІБ для захисту кінцевих точок та контролю користувачів. Додаючи цей продукт до СУРІБ використано такі його можливості:

1. Захист від шкідливого ПЗ;
2. Поведінковий аналіз активів;
3. Управління доступом локальних користувачів;
4. Захист цілісності файлів;
5. Репутаційні перевірки файлів;
6. Мережевий фаєрвол та функціонал IPS;
7. Можливість швидкої ізоляції скомпрометованих активів;
8. Централізоване керування.

Можливості системи дозволять підсилити систему УРІБ шляхом попередження загроз, та проактивного захисту активів. Інструметарій продукту дозволить виявляти ризики направлені на кінцеві точки та надасть можливості для реагування в тому числі автоматичного. Наприклад SEP здатний виявляти сканування портів активу і не лише сповіщати про це, а і автоматично блокувати спроби зловмисників виявити актив або його вразливості. Інтегрувавши цю систему з іншими отримаємо інструмент для локального контролю активів.

Також продукт надасть можливість контролювати використовувані сервіси та ПЗ, надасть статистику використання ресурсів на системі і дозволить досить просто контролювати доступ користувачів на активах. Попередить завантаження шкідливих файлів, а знизить ризик помилок користувачів.

SMG від компанії “Broadcom inc”[15] - це продукт створений для захисту поштової інфраструктури організації. Такий продукт пропонується використовувати для виявлення загроз та ризиків джерелом яких є поштова інфраструктура. Це може бути як попередження фішингу, розсилок з шкідливим ПЗ, так і виявлення інсайдерських загроз, попередження витоків інформації, загальне підвищення захищеності інформації, що передається через поштову інфраструктуру організації. Даний інструмент чудово підходить для забезпечення виконання організаційних політик, наприклад, шифрування поштових повідомлень, перевірка шифрування архівів що відправляються поштою, пошук ключових слів та попередження відправки повідомлень за наявністю недозволеного до відправлення контенту, тощо.

Також продукт має вбудовану інтеграцію з Symantec DLP. Що дозволяє проводити додаткові перевірки контенту поштових повідомлень та захищатися від ризиків витоку інформації.

Symantec DLP від компанії “Broadcom inc.”[16] – Це продукт ІБ створений для захисту від ризиків витоку інформації та контролю інформації, що передається. Даний інструмент дозволяє проводити інтеграцію з іншими представленими продуктами.

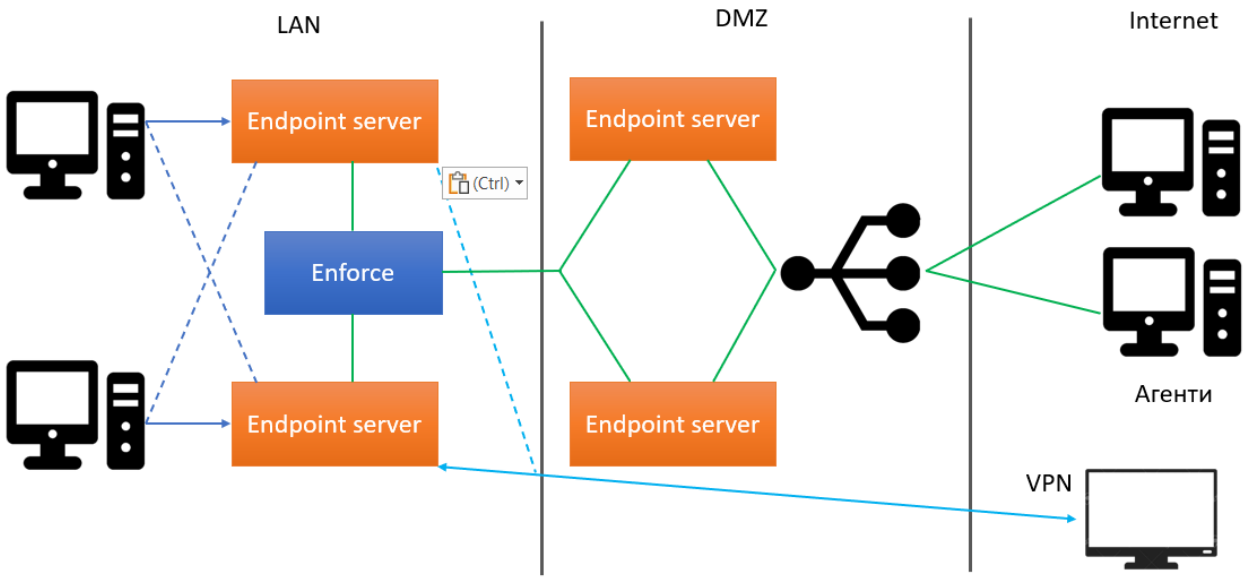
Symantec DLP надає наступні можливості:

1. Захист від втрат даних через хмарну інфраструктуру;
2. Захист від втрат даних з місця їх зберігання(файлові сервери, БД, тощо.);
3. Захист від витоку даних з мережі;
4. Захист від витоку з кінцевих точок, пошти, віртуальної інфраструктури;
5. Тощо.

Використання продукту дозволяє повністю покривати гібридні інфраструктури, та враховує такі потреби як: покриття віддалених працівників;

віртуальної інфраструктури; захист хмарних сховищ; контроль витоку даних через месенджери; управління доступом до хмарних ресурсів; контроль поштової інфраструктури; тощо. Наприклад на рис. 2.8. зображено можливості покриття класичної інфраструктури продуктом Symantec DLP.

Використовуючи сервери контролю кінцевих точок(Endpoint Server) можемо контролювати не тільки активи, що знаходяться в мережі, а і робочі



станції користувачів, що працюють віддалено. Для цього налаштовуємо контрольні сервери в DMZ або можемо використовувати VPN для підключення віддалених користувачів до корпоративної мережі. Контрольний центр Enforce забезпечує управління політиками та налаштуваннями системи, а також надає можливість проводити аналіз зібраних даних та інцидентів.

Рис 2.8. Покриття класичної інфраструктури Symantec DLP

Для проведення інтеграції з Symantec SMG або іншими поштовими системами використовуються сервери контролю та аналізу пошти. На рис. 2.9 представлено варіанти контролю простої та розгалудженої поштових інфраструктур.

Для реалізації захисту від витоку даних у хмару або з неї можна використовувати можливості Symantec DLP відповідно рис. 2.10. Також за

необхідності здійснення додаткового контролю доступу у хмарі можливе використання рішень класу CASB(Cloud access security broker).

Як можна бачити на рис. 2.10 для багатьох продуктів Symantec. Включно з представленими в цій роботі існують повністю хмарні варіанти рішень. В залежності від наявних ресурсів, потреб організації та її особливостей можна використовувати і їх хмарні аналоги. Проте з практики можу сказати, що навіть версії продуктів створені для розгортання в класичній інфраструктурі можуть бути перенесені в IaaS варіант хмарного середовища при виникненні потреби. Після початку військових дій в Україні практика перенесення баз даних та серверів централізованого управління продуктами в хмару набуває все більшої популярності.

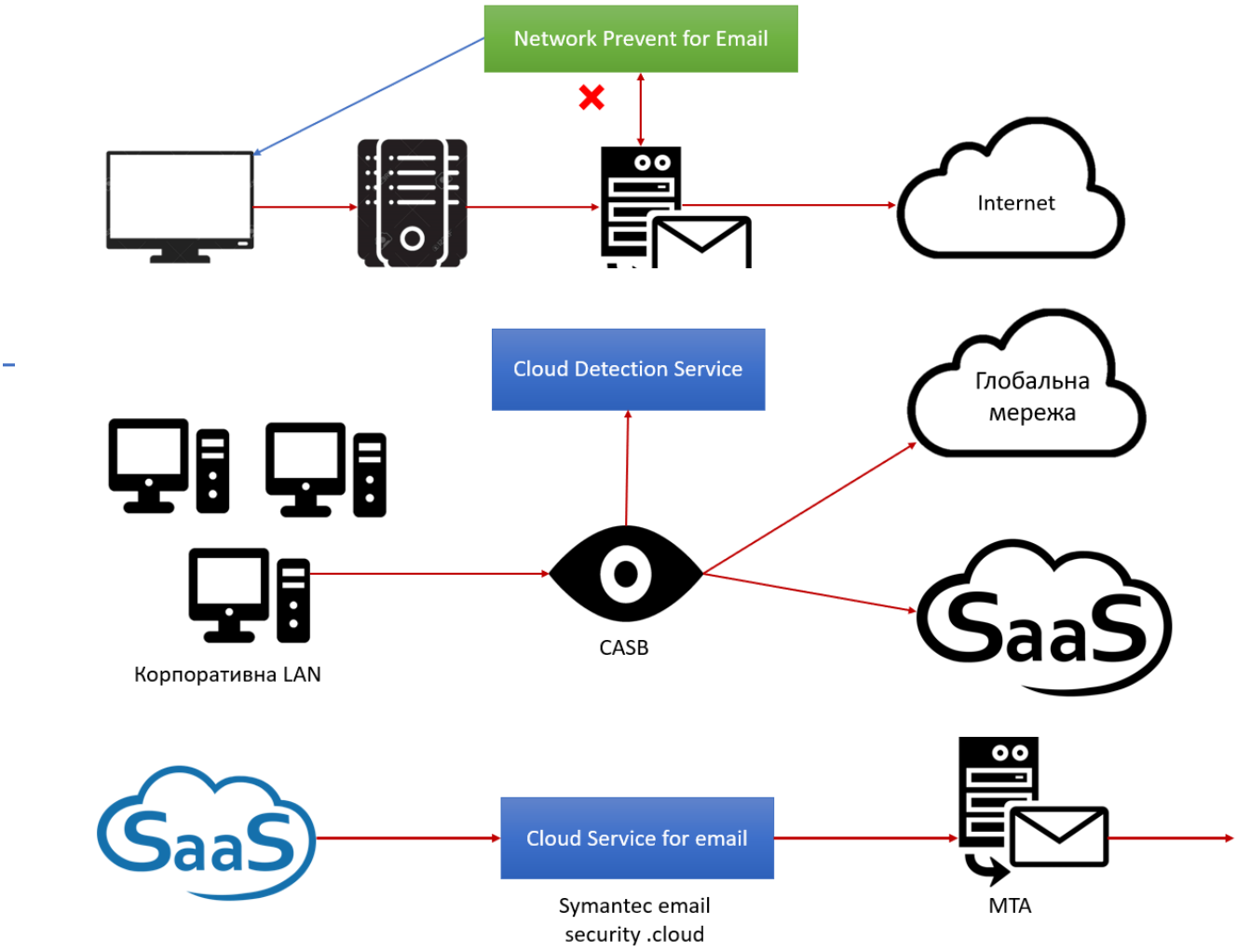


Рис. 2.9. Захист поштової інфраструктури

Рис. 2.10. Symantec DLP для захисту від витоку даних у хмарі

В результаті від цього продукту взято його можливості по контролю інфраструктури організації, та захисту від витоків даних, а також можливості контролю доступу до даних та поведінкового моніторингу. Так наприклад зможу визначати користувачів, які найчастіше порушують встановлені за допомогою продукту політики. Використавши статистику, можна визначити слабку ланку у кадровому забезпеченні, спеціалістів яким потрібно провести навчання, або навіть виявити потенційних інсайдерів. Таким чином Symantec DLP дозволить знизити ризики витоку інформації з багатьох джерел, а також дозволить покращувати СУРІБ та знизить ризик критичних помилок персоналу.

HCL BF від компанії “HCL software”[17] – платформа керування кінцевими точками, направлена на управління великою кількістю різноманітних ОС та активів. Система надає можливість працювати з більш ніж 90 видів ОС, здійснювати керування відповідністю, проводити автоматизацію, керувати ПЗ та ліцензіями, встановлювати патчі, тощо.

Інструмент BigFix планується використовувати для:

1. Інвентаризації ПЗ та АЗ;
2. Контролю ліцензій;
3. Аналізу та управління конфігурацією систем;
4. Можливостей по встановленню патчів;
5. Інструментарію виправлення та ізоляції систем;
6. Можливостей по роботі з ізольованими інфікованими системами;
7. Автоматизації завдань та дистанційного керування активами.

Найбільш корисною система буде для встановлення патчів та проведення змін конфігурації. На відміну від платформи Qualys вона є профільним інструментом, що націлений на управління конфігурацією активів і підтримує набагато більшу кількість різноманітних ОС. Так само існує і можливість розгортання системи BF у хмарному варіанті. Наявність вже готових інтеграцій від виробника з таким продуктами як Qradar та Qualys, спростить процес

поєднання систем між собою, та дозволить їм компенсувати недоліки одна одної. Таким чином можна, наприклад, використати інформацію про наявність вразливості в ПЗ встановленому на сервері яку надає система Qualys і провести її виправлення системою BF. Особливо корисною буде система BF завдяки її можливості віддалено проводити власні зміни та виправлення, навіть якщо такі не передбачені виробником. Система BF володіє власною мовою написання перевірок та запитів, яка дозволяє самостійно налаштовувати необхідні перевірки та зміни конфігурації.

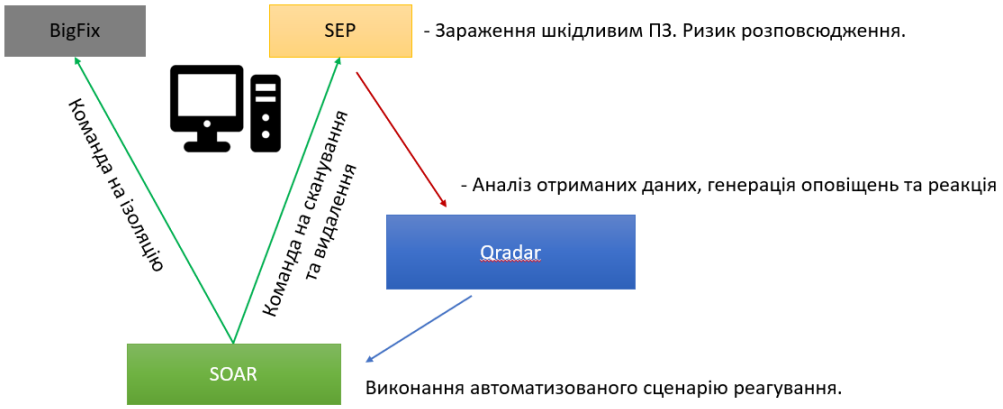
IBM SOAR[18] – Програмний продукт управління автоматичним реагуванням на події та інциденти ІБ покликаний спростити процеси УРІБ та управління інформаційною безпекою шляхом інтелектуалізації та автоматизації реагування.

Заплановано використовувати систему для підвищення здатності до інтеграції всіх інших систем, централізованого контролю інтеграції та її ефективності, а також загального підвищення швидкості реагування та введення змін до СУІБ та СУРІБ.

Основні можливості системи:

- Зменшення затрат часу на реагування;
- Оркестрація та автоматизація реагування;
- Спрощення завдань для спеціалістів завдяки динамічним алгоритмам реагування;
- Проактивний підхід до виявлення та реагування на події і інциденти ІБ;
- Та багато іншого.

За допомогою такого продукту можна забезпечити автоматичне виконання певних дій по реагуванню на події, або дані які отримані з інших елементів СУРІБ. В якості прикладу можна навести автоматичну ізоляцію кінцевої точки системою BF після отримання сигналу від IBM SOAR, що був згенерований в якості автоматичної реакції на порушення у системі Qradar, яке у свою чергу було виявлено продуктом Symantec Endpoint Protection на кінцевій точці рис 2.11 та



передано до системи Qradar в якості події. Спрацювання кореляційного правила в системі Qradar розпочне ланцюжок автоматичного реагування передаючи інформацію до IBM SOAR.

Рис. 2.11. Приклад автоматичного реагування

2.4 Організаційні аспекти інтелектуалізації СУРІБ

Для ефективного функціонування СУРІБ необхідно визначити структуру управління системою. Така система повинна складатися з декількох контрольних рівнів та надавати можливість ефективного прийняття управлінських рішень. В якості такої структури пропоную розділити людський ресурс організації на такі категорії:

- вище керівництво;
- функціональне керівництво;
- операційне керівництво;
- виконавча ланка.

До вищого керівництва можна віднести раду директорів, інвесторів, тощо. Це група людей, що розглядає найвищі, стратегічні інтереси організації, та визначає курс її розвитку. Функціональне керівництво забезпечує ефективну роботу організаційної або бізнес функції. До функціональної категорії можна віднести керівників відділів інформаційної безпеки, юридичного, фінансового відділу, тощо. Операційне керівництво відповідає за роботу окремих груп, підрозділів або працівників. Наприклад старший адміністратор, заступник

керівника відділу кадрів, тощо. До найбільш чисельної виконавчої ланки відносяться спеціалісти та рядові працівники які забезпечують виконання завдань у межах організаційних функцій. Виконавча ланка є найбільш важливим інструментом забезпечення ефективності роботи організації так як від якості її роботи напряму залежить ефективність виконання усіх організаційних функцій рис 2.12.

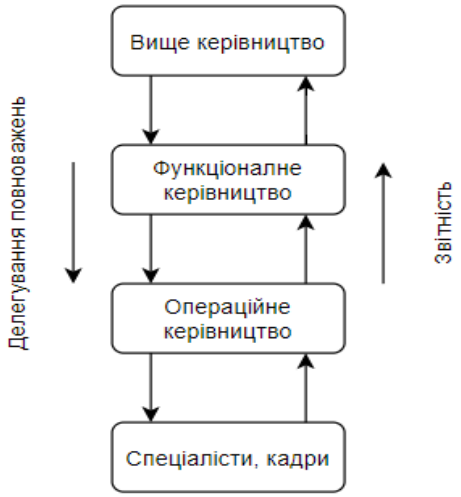


Рис 2.12. Ієрархія управління

При функціонуванні СУРІБ буде створено фокус групи, що включатимуть керівників різних категорії та організаційних функцій. Такий підхід дозволить розглядати і оцінювати ризики всебічно, що знизить вірогідність нанесення шкоди організації через прийняття рішень вплив яких на всі організаційні функції не розглянуто повністю. Але і залучення працівників виконавчої ланки до оцінки ризиків та їх виявлення є дуже важливим. Створення процедур та впровадження механізмів комунікації від нижчої до вищої ланки дозволяє зменшити затрати часу на виявлення ризиків, збільшити якість їх виявлення. А використання спеціальних автоматизованих інструментів для проведення опитувань спеціалістів виконавчої ланки надає можливість враховувати такі дані при прийнятті рішень:

- рівень опору змінам;
- прийняття управлінських рішень;
- думка спеціалістів на місцях;

- визначення рівня компетенції спеціалістів;
- прогнозування вірогідності людських помилок;
- виявлення слабкої ланки(організаційної функції);
- тощо.

В якості прикладу інструментів для контролю виконання робіт та зворотного зв’язку по ієрархії з низу в гору можна навести такі інструменти ІБ та ІТ:

- Qualys Remediation у модулі VMDR;
- Qualys SAQ;
- “Jira” від компанії “Atlassian Software”[19];
- “Omnitracker” від компанії ”Omninet Software Solutions”[20];
- Тощо.

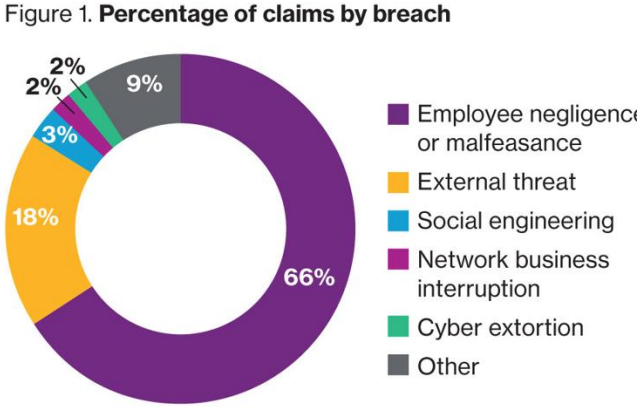
Також пропонується організувати контрольні групи висококваліфікованих спеціалістів. Завданням такої групи стане виконання найбільш термінових та складних завдань, з якими не може впоратися група операційних спеціалістів. Використовуючи ті самі інструменти комунікації представлені вище можна розділити найбільшу – операційну ланку на декілька рівнів кваліфікації. Де на нижчому рівні спеціалістами будуть виконуватись регулярні задачі по контролю та підтримці систем, а на вищому за допомогою використання функції ескалації від нижчого до вищого рівня закриватимуться більш складні, або унікальні задачі, інциденти. Також висококваліфікований сегмент спеціалістів може виступати в якості цінного джерела технічної інформації передаючи важливі для прийняття управлінських рішень аналітичні дані на вищі рівні управлінської ієрархії.

Ефективна структура управління системою УРІБ та персоналом, що забезпечує її функціонування є дуже важливою для УРІБ, так як людський фактор є найбільшим джерелом ризику згідно світової статистики рис. 2.13 [21].

Рис. 2.13. Статистика ризиків джерелом яких є людський фактор[21]

Для зниження такого ризику та ефективного управління персоналом міжнародний досвід [11] рекомендує створення та підтримку відповідних політик та процедур, практик:

1. On-Boarding Policy та Off-Boarding Policy – політики створені для попередження загроз КЦД. з боку мобільних девайсів які належать користувачам та використовуються по моделі Bring Your own Device (BYOD);
2. Делегування повноважень;
3. Acceptable User Policy (AUP) – Правила користування пристроями та системами організації. Наприклад правила віддаленого підключення до корпоративної мережі, тощо;
4. Non-Disclosure Agreement (NDA) – попереджує розголошення службової та секретної інформації встановлюючи відповідальність за порушення;
5. Вихідне інтерв'ю – визначення причини звільнення;
6. Обов'язкові відпустки – Можна використовувати як спосіб визначення участі працівника в інсайдерській діяльності;
7. Навчання користувачів;



8. Політика чистого столу – політика, що змушує працівників прибирати всі відкриті джерела не відкритої інформації коли вони не використовують їх з робочими цілями. Наприклад бокування АРМ коли працівник йде на обід;
9. Тощо

Використання таких практик дозволяє знизити кількість загроз та ризиків джерелом яких будуть користувачі використовуючи нормативне регулювання в організації. Проте такі ризики можливо зменшити ще більше за допомогою використання автоматизованих систем. Наприклад системи контролю доступу. Така система може складатися з двох частин – фізичної та віртуальної. Обидві частини будуть поєднані між собою та здійснюватимуть контроль за пересуванням працівників на території підприємства, а також контролюватимуть їх доступ до інформації та організаційних активів. При додаванні певних продуктів ІБ можна навіть відслідковувати сумлінність роботи спеціалістів та перевіряти їх на спроби реалізації шкідливих намірів. Також важливим джерелом ризиків ІБ є і фізична безпека організації. Створення систем фізичного захисту дозволить виявляти ризики НСД, пошкодження інформаційних активів, викрадення даних, промислової розвідки, тощо, та запобігати їх реалізації. Так як системи фізичної безпеки, управління доступом користувачів, та відслідковування їх активності у робочий час мають багато спільних завдань, їх можна об’єднати. Така систем дозволить не лише обмежити ризики які виникають в результаті помилок або шкідливих намірів працівників організації, але і захистити організацію від ризиків що створюються як антропогенними так і природніми факторами ззовні.

Висновки до розділу 2

Отже, у цьому розділі було розглянуто порядок підготовки та проектування СУРІБ для організації, підприємства чи установи. На прикладі організації обрано підхід до проектування та впровадження СУРІБ, а також розглянуто методику проектування. Запропоновано інструментарій автоматизації та способи

інтелектуалізації СУРІБ, розглянуто основні проблеми УРІБ та запропоновано шляхи їх вирішення за допомогою інструментів інтелектуалізації. Розглянуто можливості інструментів, та особливості їх функціонування. Запропоновано рекомендації з організаційних аспектів СУРІБ та розподілу відповідальності при проектуванні та під час функціонування системи.

Як результат запропоновано та проаналізовано приклад організації на основі якої буде створено СУРІБ та процес УРІБ. Створено ресурсну та інформаційну базу для проектування та створення такої системи.

Висновки бажано відкоригувати та додати конкретики. Зараз вони носять характер опису.

Розділ 3
КОНЦЕПТУАЛІЗАЦІЯ ТА ВПРОВАДЖЕННЯ ІНТЕЛЕКТУАЛІЗАЦІЇ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Системне поєднання інтелектуальних інструментів управління інформаційною безпекою підприємства

Відповідно до визначених у попередньому розділі області дії СУРІБ, підходу до проектування системи та визначених інструментів автоматизації буде створено варіант поєднання та розгортання СУРІБ. На рис 3.1 показано узагальнену схему розгортання та покриття інфраструктури обраними інструментами, де позначення інструментів автоматизації відповідають визначеним скороченням у другому розділі. Також окремо позначені консолі та менеджери централізованого управління інструментами автоматизації, мають позначку “/m”, Наприклад: Qradar/m – означає покриття інструментом Qradar і місце знаходження централізованої консолі управління інструментом. Пропонується розміщення центрів управління, інтеграції та агрегації даних у головному управлінні, звідки вони зможуть отримувати доступ до управління процесами та механізмами автоматизації. Таке положення елементів управління спростить можливості інтеграції між ними та забезпечить простіший контроль доступу до них. Використовуючи інструментарій кожного продукту автоматизації представленого на схемі буде реалізовано моніторинг, збір даних, та автоматичне реагування на виявлення ризиків ІБ. Деякі інструменти представлені на схемі, мають загальне покриття всієї інфраструктури: Qradar, VMDR. Для таких інструментів відображено лише положення центру управління. Деякі інструменти розгорнуті та використовуються дистанційно, у хмарі: SAQ, GAV/CSAM. Відповідно вони відображені у місці розгортання та не мають прямого впливу на архітектуру організації. Де SAQ використовується я хмарна платформа для проведення опитувань при проходженні аудитів, аналізі та оцінці ризиків, реагуванні на інциденти, перевірці знання організаційних політик, тощо. Де

GAV\CSAM є лише агрегатором інформації отриманим з інших елементів СУРІБ і створений для її аналізу, вся інформація зберігається в хмарі і модуль не має прямого впливу на архітектуру організації.

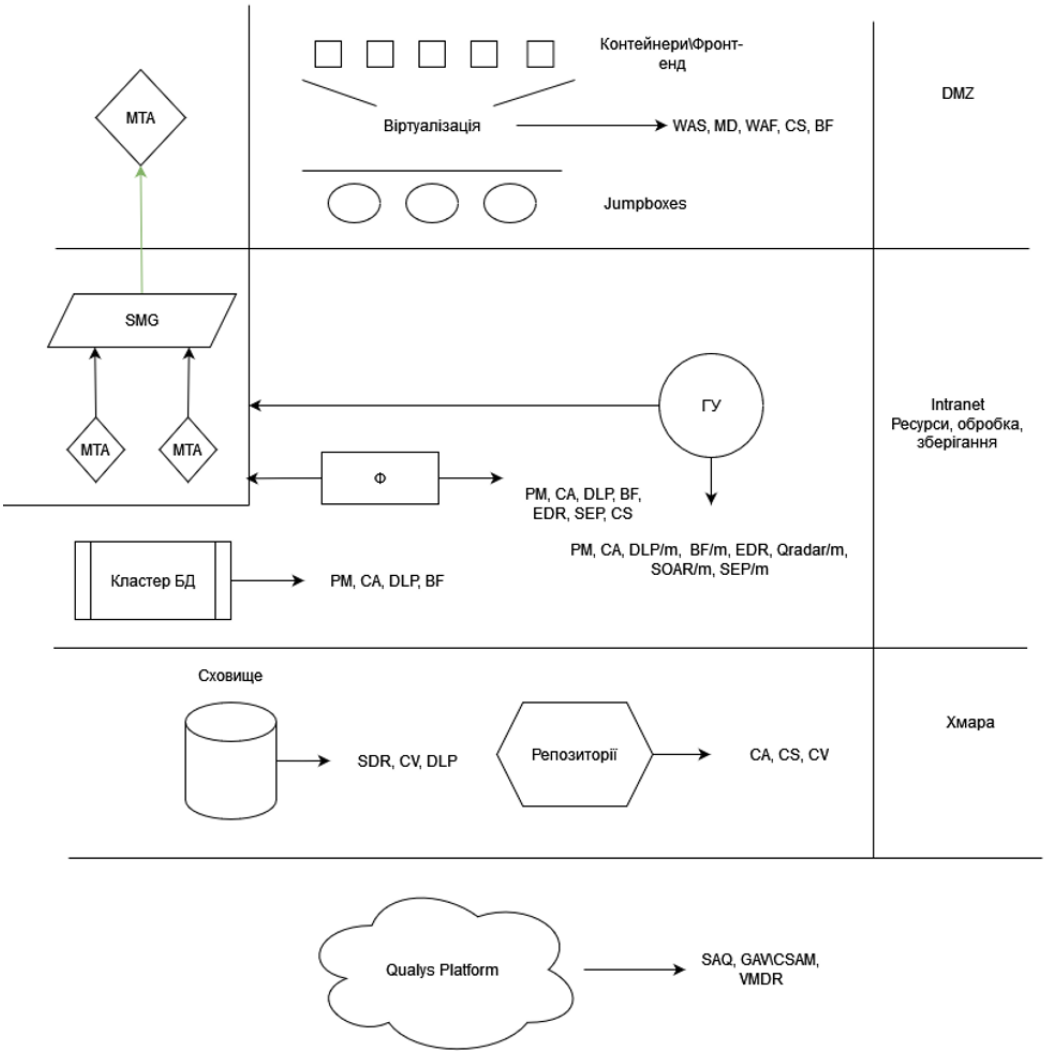


Рис 3.1 Узагальнена схема покриття інфраструктури

Далі розглянуто схему взаємодії інструментів між собою рис 3.2, ця схема відображає інтелектуалізацію процесу УРІБ. На схемі відображається в першу чергу взаємодія центрів управління інструментами. Де інструмент IBM Qradar та SOAR мають інтеграцію з усіма іншими інструментами і збирають події, та управляють виконанням автоматичних дій усіх інструментів захисту та управління конфігурацією, що відображені на схемі у групі.

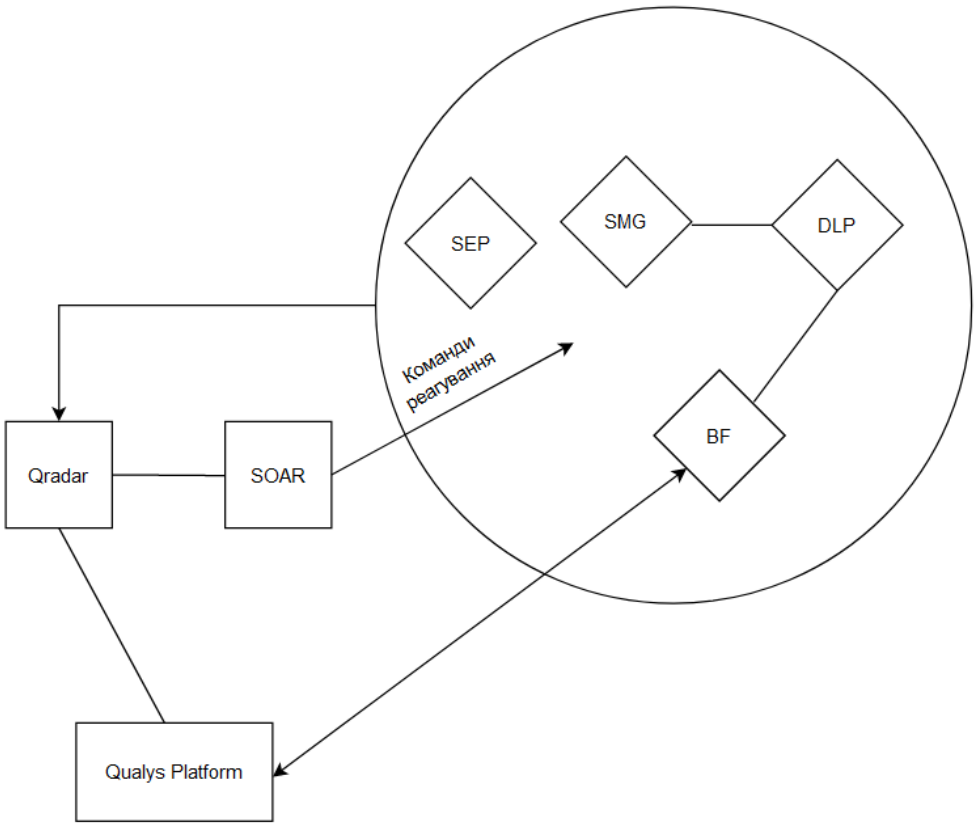


Рис 3.2 Узагальнена схема взаємодії інструментів

Після того як було розглянуто схему взаємодії інструментів між собою можна перейти до розгляду способу використання такого інструментарію інтелектуалізації УРІБ на прикладі. Відповідно до обраного у попередньому розділі процесного підходу до реалізації УРІБ на основі циклу PDCA розглянуто як можна реалізувати такий цикл на основі наявних інструментів.

1. Оцінка ризиків ІБ

Проведення виявлення та оцінки ризиків на даному етапі можна виконати за допомогою інструментарію Qualys, SMG, BF, DLP, SEP. Завданням інструментів буде сканування, пошук, виявлення ризиків, і створення бази інформації для його аналізу. Надалі використовуючи можливості інтеграції дані буде передано на аналіз системам Qualys та IBM Qradar де в залежності від типу ризику, його критичності, та швидкості з якою необхідно реагувати буде проведена його оцінка.

2. Обробка ризиків ІБ

В залежності від результатів оцінки на першому етапі, та визначеного плану реагування буде проведено роботи по обробці ризиків, які можуть виконуватися як в автоматичному режимі, так і в ручну в залежності від особливостей робіт та відповідних можливостей інструментарію інтелектуалізації. Для проведення автоматичного реагування використано систему IBM SOAR яка зможе централізовано та швидко керувати вбудованими функціями інших інструментів для виконання поставлених завдань. А також можна використати можливості інструментів контролю конфігурації, автоматичного розгортання патчів, ізоляції, тощо для повного, часткового чи тимчасового закриття ризиків.

3. Контроль ризиків ІБ

Використовуючи представлені інструменти та їх можливості про проведенню тестувань, контролю відповідності нормативним вимогам, а також інструментам написання власних автоматизованих перевірок можна протестувати успішність закриття ризиків, або виявити невідповідність, та створити завдання для виправлення. Так самі можливості інструментів та покриття ними всієї інфраструктуру організації, в тому числі покриття інструментами розгортань інших інструментів, дозволяють виявляти нові ризики, що породжені проведенням виправлень і невідповідності чи несправності самих інструментів інтелектуалізації. Наприклад: інструмент IBM Qradar зможе виявити неочікувану поломку інструменту Symantec DLP та повідомить про це відповідальних спеціалістів, а платформа Qualys зможе знайти вразливості інструментів інтелектуалізації, якщо такі з’являться та надасть рекомендації виробника по їх виправленню чи оновленню. Інструмент BigFix можна застосувати для контролю стану апаратного забезпечення, що використовується системами та попередити його вихід з ладу. Таким чином інструментарій інтелектуалізації також має і можливості самоконтролю, які покликані забезпечити неперервність процесу УРІБ в організації.

4. Оптимізація ризиків

Можливості по агрегації та зберіганню даних інструментами інтелектуалізації надають можливість для легкого і швидкого аналізу прецедентів

та буд-яких подій, що вже відбувалися в організації протягом визначеного організацією часу зберігання записів. Це дозволяє швидко розглянути інформацію про ризики, які вже були закриті, причини їх виникнення та прийняті рішення по їх закриттю. Часто організації мають певні вимоги, щодо зберігання даних і результатів процесу УРІБ. В залежності від нормативного регулювання можна налаштувати час зберігання подій та документації і надалі використовувати інструментарій інтелектуалізації для зручного перегляду та повторного аналізу таких матеріалів.

Так самі інструменти інтелектуалізації надають можливість швидкої повторної перевірки, пошуку, виявлення, та переоцінки як нових так і вже існуючих ризиків. Всі ризики, що існують в організації, незалежно від управлінських рішень прийнятих відносно цих ризиків, продовжують відслідковуватися, та автоматично переоцінюватися на постійній основі. Як тільки автоматизовані алгоритми визначають певну зміну стану ризиків, що вже наявні в організації, вони проводять відповідне реагування. Наприклад: в наслідок змін внесених на одному з активів, щоденне сканування вразливостей виявило, що для однієї з вразливостей стає доступним новий метод її експлуатації. В якості реагування така вразливість буде автоматично переоцінена платформою Qualys, отримає вищий рівень ризику і буде переведена в іншу ризик-категорію. В реакцію на це в залежності від налаштування інструментів в організації можливе продовження автоматичного реагування. Наприклад: автоматичні сповіщення, створення задач на відповідних спеціалістів, або за можливості автоматична зміна конфігурації, та виправлення вразливості.

Таким чином до зібраних інструментів інтелектуалізації можна застосувати процесний підхід PDCA та реалізувати процес УРІБ на його основі, що в свою чергу дозволить його інтеграцію до загальної СУІБ та зробить поєднання УРІБ з процесами та політиками СУІБ простішим, звісно, за умови функціонування СУІБ на основі циклу PDCA.

3.2 Оцінка запропонованої системи інтелектуалізації управління ризикам інформаційної безпеки організації

В якості основи для проведення етапів процесу УРІБ заснованого на циклі PDCA у попередньому розділі пропонував використовувати один з наступних методів УРІБ:

1. Метод OCTAVE[7];
2. Метод NIST SP 800-30[8].

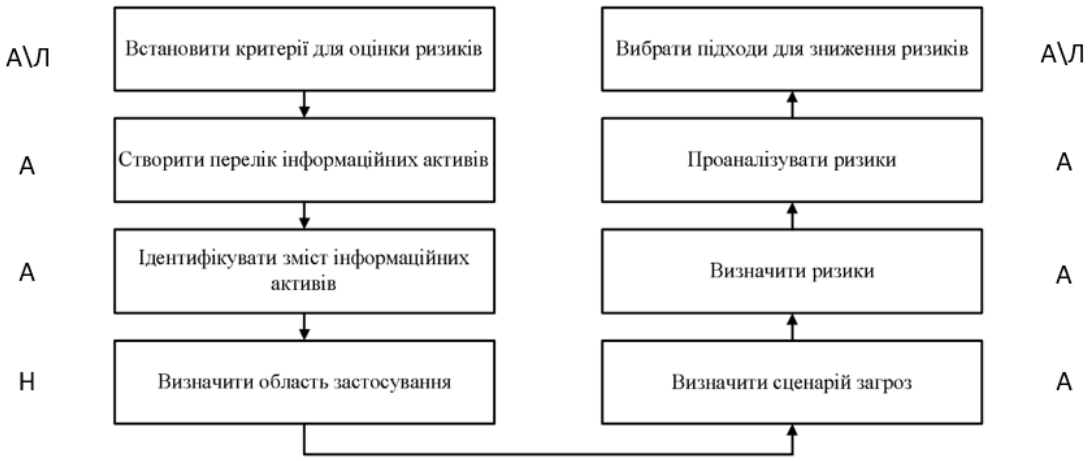
Пропонується визначити вплив запропонованих інструментів інтелектуалізації на визначені методи УРІБ, та розглянути повноту можливостей по автоматизації методик.

Відповідно до особливостей методики OCTAVE розглянутих у першому розділі роботи можна наголосити на прийнятті управлінських рішень на основі проведення серії практичних семінарів з участю відповідних спеціалістів. За такої умови важливою є подання та структура даних, аналіз яких буде проведено цими спеціалістами. А також необхідна гнучкість інструментів інтелектуалізації, яка дозволятиме контролювати процес автоматичного виконання завдань та змінювати його.

Головною перевагою обраного набору інструментів УРІБ для цього методу стане те, що він в ніякому разі не диктує як саме потрібно проводити ті чи інші операції, або приймати рішення. Зібраний інструментарій надає лише інформацію в максимально повному вигляді для прийняття цих рішень, та варіанти, інструменти для їх подальшої реалізації. Ті рішення, або будь-які дії, що будуть виконані в якості реагування на ризики ІБ повністю контролюються спеціалістами організації. Отже такий набір інструментів буде зручним для застосування в умовах динамічних змін в організації, її керівництві, та інтересах. Отже основним завданням інструменту є саме спрощення процесу УРІБ та його автоматизація, а не прийняття рішень замість відповідальних спеціалістів, що підтверджує

важливість висококваліфікованих спеціалістів, та управлінців, що в тому числі будуть керувати інструментами інтелектуалізації.

Покриття методу OCTAVE інструментами інтелектуалізації відображено на рис 3.3. Де, А – автоматизовано повністю; А\Л – автоматизовано частково, потрібна участь спеціалістів; Н – не автоматизовано. Набір інструментів дозволяє повністю автоматизувати пошук і збір даних для аналізу, а також надає повні можливості по застосуванню управлінських рішень. Процес оцінки автоматизовано, але існує і можливість самостійної реалізації оцінки ризиків за потреби. Також можна використати готові метрики інструментів для порівняння або переведення оцінки ризику в іншу метрику. Саме прийняття рішень та проведення практичних нарад і семінарів при використанні таких інструментів



залишається не автоматизованим, проте може пришвидшуватися за допомогою інструментів комунікацій розглянутих раніше, таких як відео зв’язок або Qualys SAQ модуль або Qualys Remediation.

Рис 3.3 Автоматизація методу OCTAVE

Щодо методики NIST SP 800-30 можливості автоматизації етапів цієї методики можна відобразити наступним чином рис 3.4. Можливості запропонованого інструментарію інтелектуалізації дозволяють автоматизувати задачі на всіх етапах циклу і надають можливість спрощувати УРІБ за допомогою цього методу від етапу опису та збору характеристик системи до документування і зберігання результатів проведення процесу УРІБ. Після розгляду можливостей

автоматизації методів УРІБ визначено результати перевірок ефективності створеної СУРІБ.

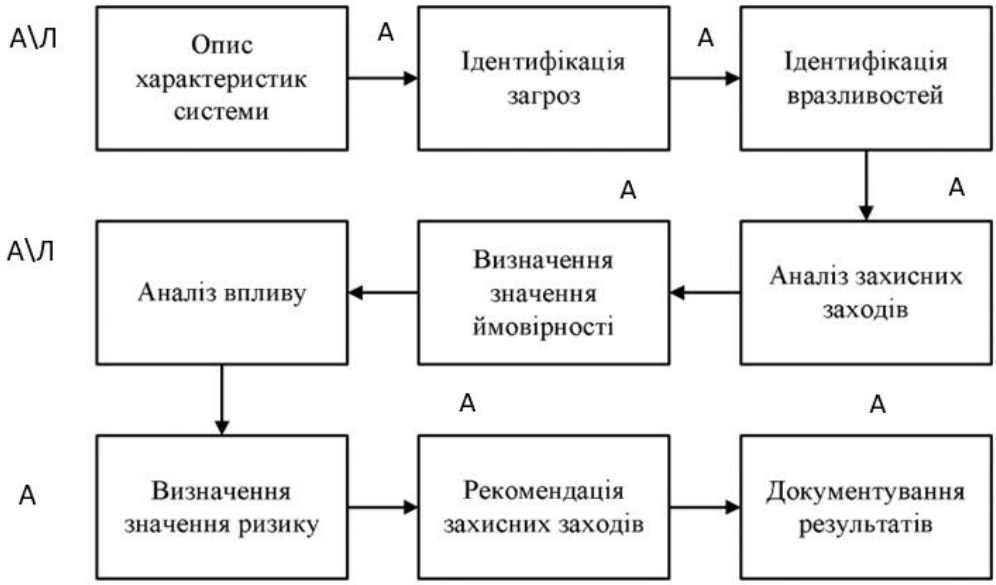


Рис 3.4 Можливості автоматизації методики NIST 800-30

Розглянуто статистичні дані по основним проблемам в сфері УРІБ та показники ефективності середньостатистичних СУРІБ. Згідно [21] основними недоліками практичного УРІБ є:

1. Лише 36% організацій справді мають побудовану програму і план УРІБ;
2. Більше 60% респондентів не впевнені в якості свої СУРІБ, основною проблемою виділяють їх здатність до адаптації та стійкість перед появою нових особливостей ризиків ІБ у майбутньому;
3. Більше 60% організацій протягом року мали інцидент ІБ, який виник в результаті експлуатації критичного ризику ІБ;
4. Найбільшими джерелами ризику та збитків називають: Продуктивність працівників(62% опитаних), операційну ефективність – поломки систем, процесів, простій виконання бізнес-функцій, поломки програмного та апаратного забезпечення(59%); втрату репутації(38%); стягнення за умисне чи випадкове порушення нормативного регулювання, складність проходження аудитів(28%);

5. Як показує опитування на управлінських нарадах високого рівня, на УРІБ виділяється досить малий відсоток часу – лише 9% від загального;
6. Лише 6% директорів впевнені в ефективності управління ризиком вищою ланкою керівництва;
7. Більше 60% організацій використовують реактивний підхід до УРІБ;
8. Більше 40% організацій прагнуть збільшити, оновити та покращити свої процеси і системи УРІБ;

Запропонована СУРІБ на основі обраних інструментів пропонує можливості по адресації усіх перерахованих вище проблем. Так її здатність до проактивного реагування та адаптації під найсвіжіші вразливості, загрози та ризик дозволяє легко підтримувати систему а актуальному стані. Інструменти управління доступом та комунікації дозволяють контролювати активність та навіть проводити їх навчання. Можливості відслідковування ризиків з боку порушення політик та нормативного регулювання дозволяють уникати відповідних стягнень а можливості вичерпного документування спрощують проходження аудитів. Здатність до самоконтролю захищає інструменти від поломок та підтримує їх в актуальному стані відносно останніх оновлень та рекомендацій виробників цих інструментів. Модульна структура запропонованої СУРІБ у свою чергу дозволяє не лише її розширювати, а і за потреби змінювати механізми вже існуючої системи. Так можна змінити механізми поведінки інструментів в залежності від ситуації, а за потреби і замінити інструмент повністю, використавши замість нього обраний аналог зі зміненим функціоналом.

Таким чином розглянута раніше СУРІБ здатна закривати більшість основних проблем УРІБ та покращувати відсоткові показники, що свідчить про її актуальність у сучасному середовищі ІБ.

Далі для вираження чисельного впливу запропонованої системи на стан ІБ організації використаю дві метрики: Mean time to remediation(MTTR), Mean time to detection(MTTD).

MTTR – Обсяг часу який проходить з моменту виявлення ризику до його обробки, тобто реалізації управлінського рішення[22].

MTTD - Обсяг часу який проходить від появи ризику в організації, до його виявлення[22].

Таке вираження ефективності також часто використовують для розрахунку аналогічних показників у процесах управління інцидентами, вразливостями ІБ.

Також на мою думку важливо враховувати і показник Mean time to Identify(MTTI)[23] – це показник, який демонструє час, що проходить від моменту виявлення ризику інструментами автоматизації до інформування відповідних спеціалістів та початку ними аналізу. Цю метрику можна вважати частиною MTTR, проте розгляну її окремо через значний вплив на загальну швидкість реагування.

На основі статистики [23, 24, 25, 26] визначено наступні середньостатистичні показники (табл.3.1):

Таблиця 3.1

Середньостатистичні показники MTTR, MTTD, MTTI

Ризики	MTTR	MTTD	MTTI
Зовнішні	50 днів	40 днів	7 днів
Внутрішні	60 днів	60 днів	14 днів
Апаратні\Мережеві	63 дні	70 днів	9 днів
ПЗ	40 днів	80 днів	7 днів
Критичні	30 днів	10 днів	3 дні
Середні	80 днів	40 днів	10 днів

Потрібно враховувати, що такі показники є середньостатистичними, вони зібрані на основі статистики та опитувань організацій з різними підходами, можливостями, ресурсами УРІБ. Такі показники можуть бути як значно меншими, так і значно більшими в залежності від ефективності процесу УРІБ в організації.

Під час проходження переддипломної практики, використовуючи ресурси та можливості бази практики, вдалося протягом місяця протестувати вплив створеної СУРІБ на основі запропонованих інструментів інтелектуалізації на показники MTTR, MTTD, MTTI.

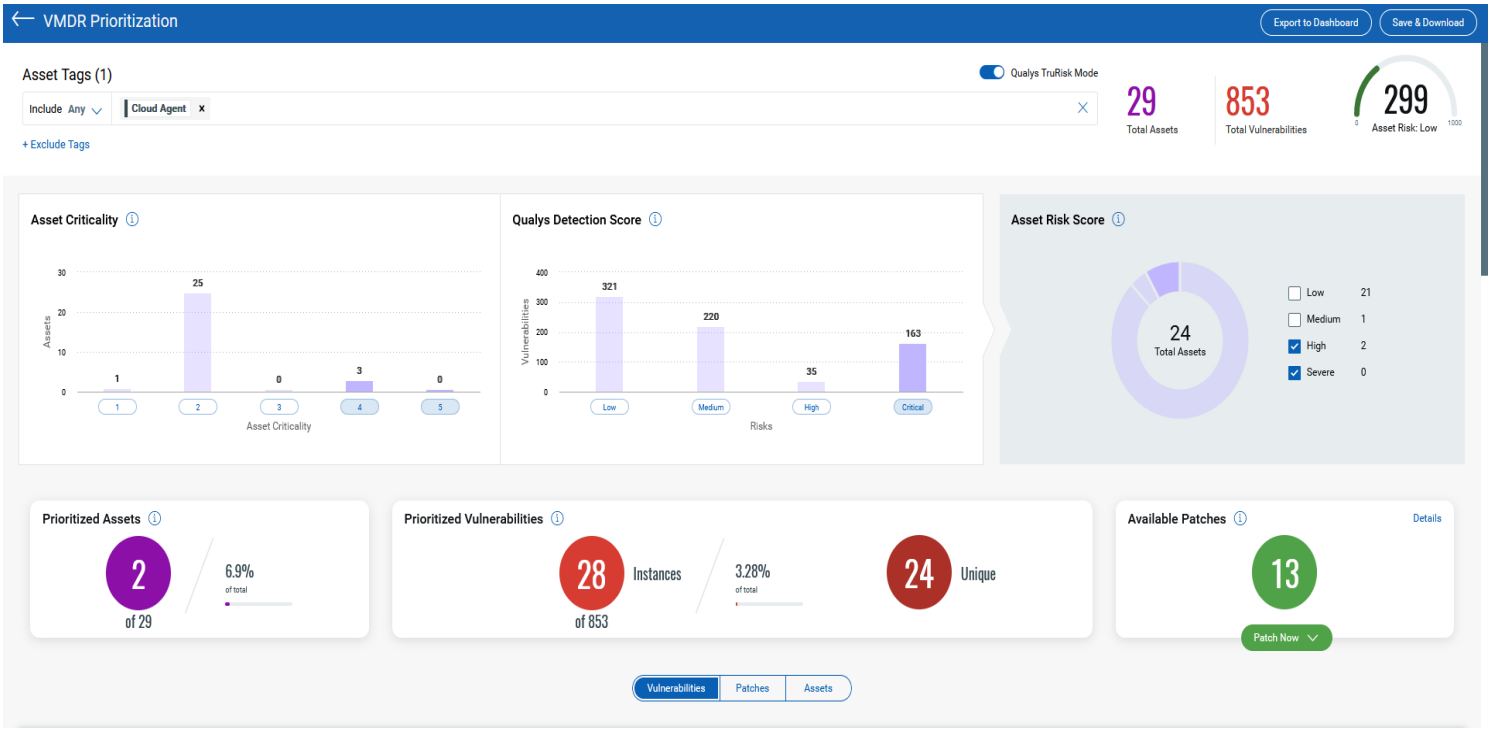
При побудові СУРІБ та обранні інструментів використовувалися рекомендації [25] по зниженню цих показників та підвищенню ефективності роботи системи. Коротко, основні рекомендації можна перерахувати так:

1. Побудова та вибір підходів, методів, політик управління ризиком. Чітке визначення циклу та контролів УРІБ;
2. Нормалізація, контекстуалізація та пріоритезація ризику;
3. Обізнаність, швидкість реагування, комунікації;
4. Швидке прийняття рішень та автоматизація реагування;

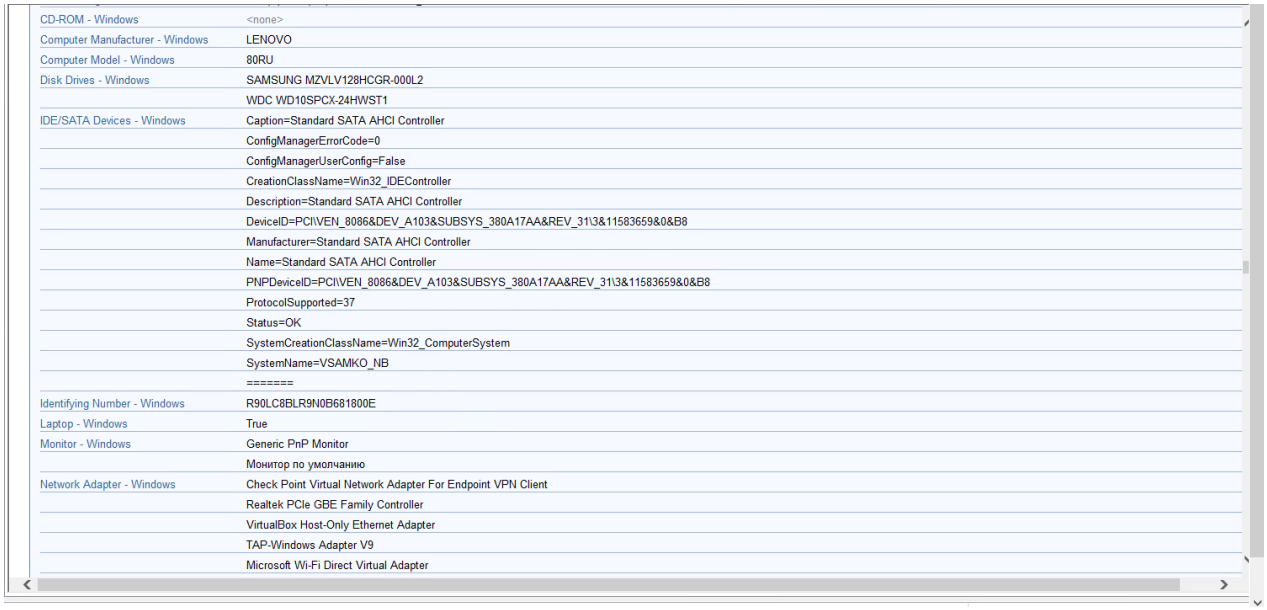
Таким чином для інтелектуалізації УРІБ та підвищення його ефективності у запропонованій системі було розглянуто політики та підходи, методи та цикли УРІБ. Запропонована СУРІБ побудована та адаптована згідно визначених підходів та методів управління. Також було створено автоматичні правила реагування та дій на основі визначених підходу та методів управління.

Використано можливості інструментів для спрощення подачі інформації до аналізу, та пріоритезації виправлень. Так наприклад інструмент Qualys VMDR дозволяє проводити пріоритезацію виправлення ризиків використовуючи автоматично розраховану критичність ризику вразливостей, активів, або навіть цілих груп активів, що значно зменшує час затрачуваний на аналіз та прийняття управлінських рішень рис 3. 5.

Рис 3.5. Qualys VMDR пріоритезація ризиків



Використання інструментів оповіщення, комунікації, підвищення кваліфікації, контролю відповідності політикам, автоматичного реагування, контролю конфігурації та налаштувань, самоконтролю та захисту від простою інстурментарію СУРІБ дозволяє значно знизити всі три показники забезпечуючи безвідмовність системи рис 3.6, 3.7, 3.8.



CD-ROM - Windows	<none>
Computer Manufacturer - Windows	LENOVO
Computer Model - Windows	80RU
Disk Drives - Windows	SAMSUNG MZVLV128HCGR-000L2
	WDC WD10SPCX-24HWST1
IDE/SATA Devices - Windows	Caption=Standard SATA AHCI Controller
	ConfigManagerErrorCode=0
	ConfigManagerUserConfig=False
	CreationClassName=Win32_IDEController
	Description=Standard SATA AHCI Controller
	DeviceID=PCI\VEN_8086&DEV_A103&SUBSYS_380A17AA&REV_31\3&11583659&0&B8
	Manufacturer=Standard SATA AHCI Controller
	Name=Standard SATA AHCI Controller
	PNPDeviceID=PCI\VEN_8086&DEV_A103&SUBSYS_380A17AA&REV_31\3&11583659&0&B8
	ProtocolSupported=37
	Status=OK
	SystemCreationClassName=Win32_ComputerSystem
	SystemName=VSAMKO_NB
	=======
Identifying Number - Windows	R90LC8BLR9N0B681800E
Laptop - Windows	True
Monitor - Windows	Generic PnP Monitor
	Монитор по умолчанию
Network Adapter - Windows	Check Point Virtual Network Adapter For Endpoint VPN Client
	Realtek PCIe GBE Family Controller
	VirtualBox Host-Only Ethernet Adapter
	TAP-Windows Adapter V9
	Microsoft Wi-Fi Direct Virtual Adapter

Рис 3.6. Контроль апаратного забезпечення системи

MicrosoftEdge_X64_97.0.1072.55_96.0.1054.62.exe;Mon, 10 Jan 2022 10:06:59 +0300;Mon, 10 Jan 2022 10:06:59 +0300;Mon, 10 Jan 2022 10:07:17 +0300;False;00:00:18.531;1
MSI6D56.tmp;Thu, 06 Jan 2022 13:28:14 +0300;Thu, 06 Jan 2022 13:28:14 +0300;Thu, 06 Jan 2022 13:28:33 +0300;False;00:00:18.922;1
wordpad.exe;Wed, 05 Jan 2022 16:56:05 +0300;Wed, 05 Jan 2022 18:31:30 +0300;Wed, 05 Jan 2022 18:31:54 +0300;False;00:00:33.610;4
OnVUE-3.75.26(1).exe;Thu, 30 Dec 2021 17:17:31 +0300;Thu, 30 Dec 2021 17:40:49 +0300;Thu, 30 Dec 2021 17:49:01 +0300;False;00:25:35.984;3
OnVUE.exe;Sat, 25 Dec 2021 11:14:08 +0300;Thu, 30 Dec 2021 17:40:57 +0300;Thu, 30 Dec 2021 17:49:01 +0300;False;00:27:35.812;5
igfxTray.exe;Fri, 20 Aug 2021 10:43:48 +0300;Wed, 29 Dec 2021 12:07:40 +0300;Thu, 30 Dec 2021 16:53:25 +0300;False;35 days, 04:52:08.055;132
OnVUE-3.75.26.exe;Sat, 25 Dec 2021 11:14:08 +0300;Sat, 25 Dec 2021 11:14:08 +0300;Sat, 25 Dec 2021 11:16:54 +0300;False;00:02:45.313;1
TestTakerSBBrowser.exe;Sat, 25 Dec 2021 11:15:58 +0300;Sat, 25 Dec 2021 11:15:58 +0300;Sat, 25 Dec 2021 11:16:32 +0300;False;00:00:33.547;1
QASetupHost_4.6.1.6.exe;Wed, 17 Nov 2021 10:49:54 +0300;Wed, 22 Dec 2021 10:19:10 +0300;Wed, 22 Dec 2021 10:19:10 +0300;False;00:00:19.578;6
nsw121F.tmp;Tue, 21 Dec 2021 13:28:36 +0300;Tue, 21 Dec 2021 13:28:36 +0300;Tue, 21 Dec 2021 17:01:48 +0300;False;03:33:12.422;1
MSIDC68.tmp;Tue, 21 Dec 2021 13:28:25 +0300;Tue, 21 Dec 2021 13:28:25 +0300;Tue, 21 Dec 2021 13:28:25 +0300;False;00:00:00;1
MicrosoftEdge_X64_96.0.1054.62_96.0.1054.57.exe;Mon, 20 Dec 2021 09:38:04 +0300;Mon, 20 Dec 2021 09:38:04 +0300;Mon, 20 Dec 2021 09:38:12 +0300;False;00:00:07.328;1
MicrosoftEdge_X64_96.0.1054.57_96.0.1054.53.exe;Thu, 16 Dec 2021 20:55:20 +0300;Sat, 18 Dec 2021 10:04:37 +0300;Sat, 18 Dec 2021 10:04:37 +0300;False;00:00:07.969;2
nsz462A.tmp;Fri, 17 Dec 2021 13:22:22 +0300;Fri, 17 Dec 2021 13:22:22 +0300;Fri, 17 Dec 2021 18:04:52 +0300;False;04:42:29.452;1
MSI1621.tmp;Fri, 17 Dec 2021 13:22:14 +0300;Fri, 17 Dec 2021 13:22:14 +0300;Fri, 17 Dec 2021 13:22:22 +0300;False;00:00:08.579;1
Windows-KB890830-x64-V5.96.exe;Fri, 17 Dec 2021 10:12:47 +0300;Fri, 17 Dec 2021 10:12:47 +0300;Fri, 17 Dec 2021 10:14:45 +0300;False;00:01:58.750;1
96.0.4664.110_96.0.4664.93_chrome_updater.exe;Thu, 16 Dec 2021 09:59:32 +0300;Thu, 16 Dec 2021 09:59:32 +0300;Thu, 16 Dec 2021 09:59:49 +0300;False;00:00:16.891;1
MicrosoftEdge_X64_96.0.1054.53_96.0.1054.43.exe;Sun, 12 Dec 2021 11:00:39 +0300;Mon, 13 Dec 2021 10:12:12 +0300;Mon, 13 Dec 2021 10:12:12 +0300;False;00:00:14.766;2
96.0.4664.93_96.0.4664.45_chrome_updater.exe;Thu, 09 Dec 2021 15:22:28 +0300;Thu, 09 Dec 2021 15:22:28 +0300;Thu, 09 Dec 2021 15:22:28 +0300;False;00:00:00;1
MicrosoftEdge_X64_96.0.1054.43_96.0.1054.41.exe;Sun, 05 Dec 2021 10:35:29 +0300;Sun, 05 Dec 2021 10:35:29 +0300;Sun, 05 Dec 2021 10:35:47 +0300;False;00:00:18.078;1
MicrosoftEdge_X64_96.0.1054.41_96.0.1054.34.exe;Fri, 03 Dec 2021 10:04:34 +0300;Fri, 03 Dec 2021 10:04:34 +0300;Fri, 03 Dec 2021 10:04:55 +0300;False;00:00:21.532;1
QualysCloudAgent.exe;Tue, 30 Nov 2021 12:19:54 +0300;Tue, 30 Nov 2021 15:29:35 +0300;Tue, 30 Nov 2021 15:29:45 +0300;False;00:00:10.188;17
QualysCloudAgent-2.0.6.1.exe;Tue, 30 Nov 2021 15:24:22 +0300;Tue, 30 Nov 2021 15:24:22 +0300;Tue, 30 Nov 2021 15:24:29 +0300;False;00:00:07.047;1
Uninstall.exe;Tue, 30 Nov 2021 15:07:29 +0300;Tue, 30 Nov 2021 15:22:36 +0300;Tue, 30 Nov 2021 15:22:36 +0300;False;00:00:00;2

Рис 3.7 – Контроль використання ПЗ

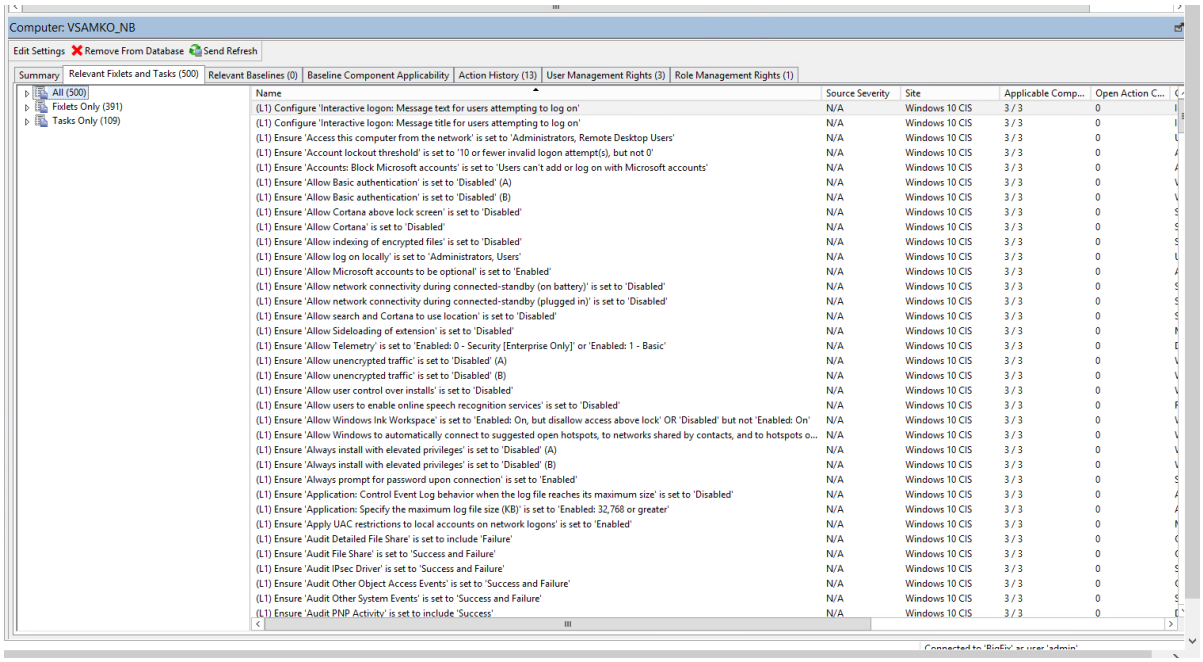


Рис 3.8 – Можливості контролю конфігурації

Інструменти автоматичного виявлення, аналізу та оцінки ризиків також значно впливають на всі визначені показники ефективності та у поєднанні з можливостями інформування надають можливість швидше переходити від аналізу інформації до впровадження виправлень рис 3.10, рис 3.11.

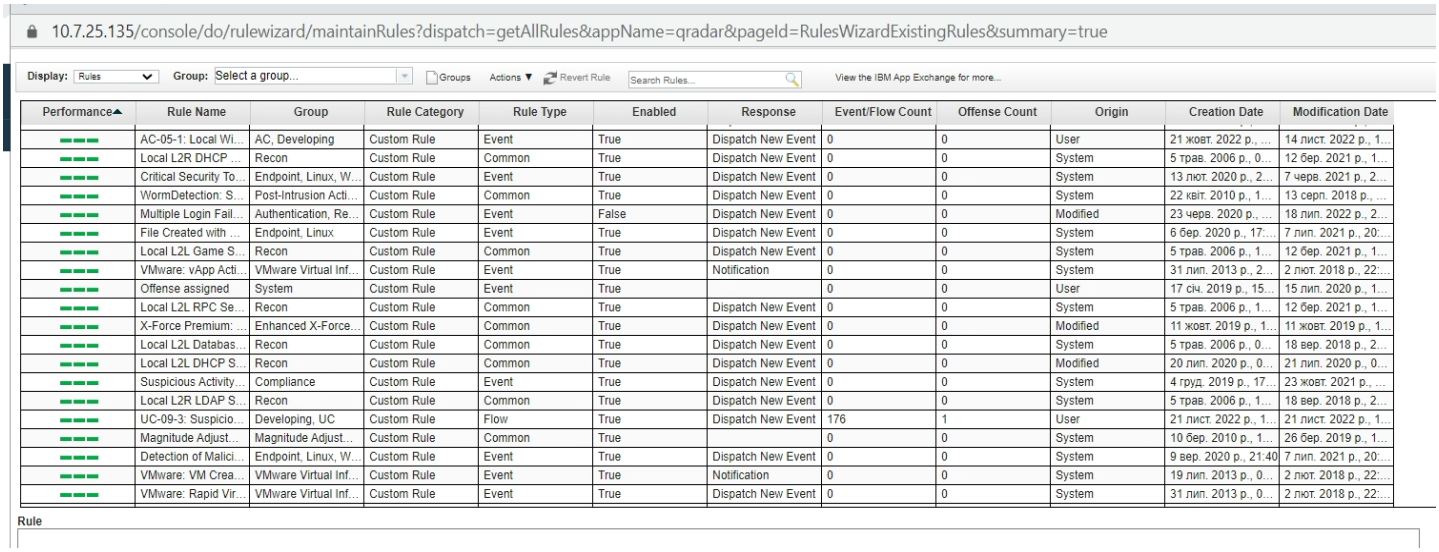


Рис 3.10. IBM Qradar SIEM правила реагування на події

В результаті використання рекомендацій та інструментів інтелектуалізації протягом тестового місяця вдалося досягнути наступних показників, що відображені в табл 3.2.

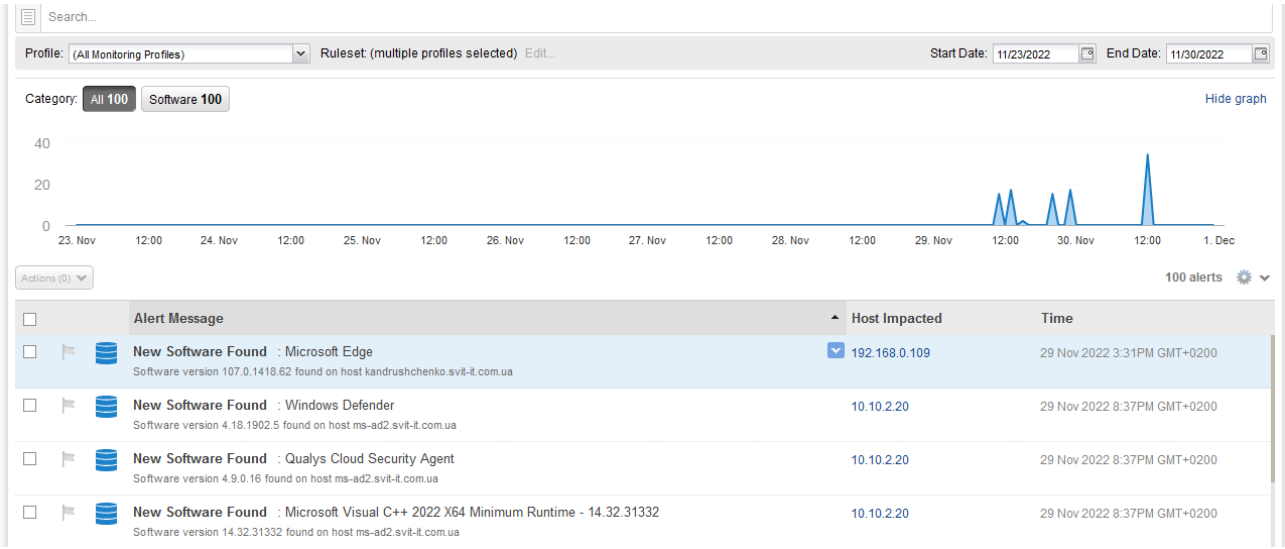


Рис 3.11 Qualys CM автоматичне оповіщення

Табл 3.2

Результуючі показники MTTR, MTTD, MTTI

Ризики	MTTR	MTTD	MTTI
Зовнішні	40 днів	30 днів	6 днів
Внутрішні	38 днів	30 днів	14 днів
Апаратні\Мережеві	58 дні	50 днів	9 днів
ПЗ	30 днів	35 днів	4 днів
Критичні	10 днів	10 днів	1 день
Середні	50 днів	15 днів	10 днів

Нажаль повна автоматизація такого громіздкого процесу як УРІБ є неможливою на даний момент і велика частина ефективності будь-якої СУРІБ буде залежати від якості роботи спеціалістів та ефективності керівництва. Таким чином найменше в результаті проведеного тестування вдалося знизити показник MTTI, швидкість реагування спеціалістів. Проте використання інструментів підвищення кваліфікації та комунікацій все ж дає досить відчутне підвищення ефективності роботи порівняно з середньостатистичними показниками. Показник MTTR який залежить від MTTD та MTTI але і від інструментів інтелектуалізації

та автоматичного реагування – знизився досить суттєво, у порівнянні з середньостатистичними даними. Показник MTTD продемонстрував найбільші скорочення затрачуваного часу, здебільшого повні можливості автоматичного виявлення та аналізу ризиків значно зменшили цей показник.

Таким чином створена СУРІБ з використанням обраних інструментів інтелектуалізації в результаті проведених тестувань демонструє показники MTTR, MTTD, MTTI нижчі ніж середньостатистичні. Це свідчить про загальне підвищення ефективності функціонування процесу УРІБ відносно середньостатистичних показників. Отже таку СУРІБ та процеси УРІБ можна вважати ефективними.

3.3. Рекомендації до впровадження системи інтелектуалізації управління ризиками інформаційної безпеки організації

При проведенні початкового аналізу організації(підприємства, установи, тощо) важливо визначити особливості її функціонування, основні інформаційні активи, бізнес-функції, очікування до процесу УРІБ та його область дії. Це є необхідним для обрання підходу до побудови процесу, методів УРІБ, а також вибору необхідного інструментарію інтелектуалізації УРІБ. Запропонований у цій роботі підхід можна використовувати для побудови СУРІБ та процесу УРІБ в організації, враховуючи унікальність кожної з них, та проводячи адаптацію підходу під конкретні особливості її функціонування. Варто зазначити, що у кожному окремому випадку існуватимуть унікальні особливості, що змінюватимуть: порядок нормативного регулювання; архітектуру IT інфраструктури та мережі; поставлені перед системою задачі, тощо. Саме якісний аналіз особливостей і потреб організації, як і її ресурсних можливостей є запорукою успішного створення процесу УРІБ в кожному окремому випадку.

При обранні інструментів інтелектуалізації варто враховувати наступне: функціональні можливості інструменту; вартість та його ліцензування; якість підтримки інструменту профільними інженерами виробника; рівень

ознайомленості персоналу організації у роботі з інструментом або подібними інструментами виробника; швидкість навчання власного персоналу; можливості інтеграції інструментів між собою; їх гнучкість у роботі з гібридними інфраструктурами та можливість покриття певних особливостей інфраструктури окремого випадку, якщо такий є; популярність, репутація, доступність на ринку ІБ країни, в які планується використовувати інструмент; тощо.

Необхідно враховувати наявні інструменти ІБ та процеси ІБ які вже функціонують в організації при створенні, або покращенні існуючого процесу УРІБ. Часто це може впливати не лише на вибір інструментів інтелектуалізації, а і розширювати процес, де для повноти функціонування процесу вже існуючі в організації інструменти також можуть інтегруватися до загального процесу, таким чином поглиблюючи його можливості та створюючи більш глибоку інтеграцію СУРІБ в СУІБ організації.

При підтримці інструментарію інтелектуалізації найважливішим завданням є забезпечення неперервності процесу УРІБ. Не дивлячись на здатність інструментарію проводити самостійну діагностику та попереджувати про потенційні проблеми, деякі з них можуть залишатися не поміченими. Навіть за умови автоматичного сповіщення про потенційну поломку однієї з систем залишатиметься завдання її виправлення адміністраторами такої системи. Тому необхідно проводити регулярний моніторинг стану систем для пошуку непомічених автоматичними засобами недоліків чи аномалій, а також побудувати процес виправлення відомих проблем таким чином, щоб це не вносило перебоїв та простою у функціонування СУРІБ та процесу УРІБ в цілому. Такий процес можна здійснити як вручну, спеціалізованими адміністраторами систем, так і використати додаткові інструменти попередження поломок системи. Наприклад досить популярним інструментом додаткового автоматичного моніторингу інструментів інтелектуалізації використовують SNMP v3. Це протокол який дозволяє віддалено за допомогою запитів до систем збирати інформацію про їх поточний стан: мережі; заліза; навантаження; процесів; тощо. За умови наявності

автоматичних інструментів опитування, аналізу та сповіщення такий спосіб моніторингу може стати досить ефективним додатковим джерелом захисту.

В деяких нормативних вимогах та стандартах рекомендується або вимагається зберігання даних протягом певного періоду часу, що є необхідною умовою для проходження сертифікації, аудитів, тощо. Особливу увагу варто приділити можливостям зберігання даних. За умови використання повної інтеграції, аналізу великих об’ємів даних з усіх елементів інфраструктури, їх документування та зберігання. Важливим є не лише забезпечення достатнього об’єму місця для зберігання даних у таких системах, а і можливість доступу різних інструментів до місць зберігання даних, що необхідно для повноцінної та функціональної інтеграції інструментів між собою. Також важливо забезпечити безперебійний доступ до сховищ даних на запис та читання інструментами за відсутності такого можливе виникнення помилок, колізій, та порушення неперервності їх функціонування. Часто для забезпечення цієї вимоги можна використовувати кластери високої доступності(HA – High availability), що дозволяють перемкнутися з одного активу зберігання даних на інший у разі його поломки або відсутності, тим самим забезпечуючи безперервну доступність середовища зберігання даних. Проте такі рішення є досить затратними.

Аналогічно безперервній доступності середовища зберігання даних, потрібно забезпечити і безперервність функціонування важливих елементів інструментів інтелектуалізації. Більшість інструментів мають модульну структуру, та не будуть виходити з ладу за умови відключення одного елементу, проте частково ефективність їх роботи буде знижуватися, можливі втрати даних для аналізу або зберігання, порушення графіків проведення сканувань, тощо. Для запобігання таким втратам можна використовувати HA технологію. Рекомендується визначити найбільш пріоритетні, важливі та навантажені елементи інструментарію та використовувати таких підхід до них. Особливої уваги заслуговують контрольні центри управління інструментів, вихід з ладу яких наноситиме найбільше шкоди ефективності функціонування системи.

У випадку з використанням хмарних рішень, таких як платформа Qualys. Відповідальність за забезпечення неперервної роботи інструментів буде покладена на поставника хмарного сервісу. В такому випадку з боку організації необхідно забезпечити доступ до хмарного середовища виробника, та підтримувати його у справному стані, в тому числі враховуючи інтеграційні потреби усіх інших інструментів. Проте жоден хмарний провайдер не зможе забезпечити сто відсотків доступності проятгом усього часу. Варто визначити умови, на яких надаватимуться послуги та враховувати зазначені там показники можливого простою у наданні сервісу, спонукати провайдера хмарної послуги дотримуватися визначеного в угоді рівня та якості обслуговування. Потрібно укладати відповідні договори SLA(Service Level Agreement) та за потреби забезпечити виконання зобов’язання сторін на юридичному рівні.

При функціонуванні інструментарію інтелектуалізації УРІБ варто також регулярно проводити оцінку ефективності його роботи та змінювати налаштування автоматизації, згідно актуальних потреб організації. В динамічному ІТ та ІБ середовищі здатність до адаптації та реагування на зміни є важливою запорукою підтримки ефективності функціонування створеного процесу УРІБ.

Для забезпечення такої адаптації та ефективності варто враховувати, що велика кількість інструментів інтелектуалізації і самі є динамічними. До таких інструментів постійно вносяться зміни, виходять оновлення, вводяться нові функції та можливості. Такий динамічний розвиток інструментів викликає як необхідність відслідковування оновлень так і навчання персоналу новим функціям, та за необхідності впровадження таких функцій у загальний процес. Окремі модулі різних інструментів можуть мати власні шляхи взаємодії із загальною системою, і як реакція на зміни такі шляхи можуть динамічно змінюватися. У свою чергу це вимагає наявності кваліфікованих спеціалістів та загального розуміння природи процесів УРІБ та їх функціонування в організації, для спрощення впровадження майбутніх покращень.

Також важливо зазначити, що в залежності від особливостей інструменту інтелектуалізації в ньому можуть виникати і помилки, які ніяк не пов’язані з

професійністю спеціалістів, що керують інструментом чи особливостями його використання в організації. Такі помилки найчастіше є наслідком помилок саме розробників продукту. Потрібно усвідомлювати можливість виходу з ладу певних функцій інструментів через помилки ПЗ та мати відповідний план реагування. Це може бути повідомлення виробника продукту для виправлення помилки, та розробки тимчасового рішення за умови, що продукт комерційний. Або виправлення таких помилок власними силами якщо інструмент створений самою організацією. У більшості випадків такі помилки будуть відбуватися неочікувано і матимуть різноманітний характер. Підготуватись до такої проблеми і розробити тимчасове рішення до її виникнення часто не вдасться. Таким чином при виникненні таких помилок виникатиме велика залежність від рівня кваліфікації спеціалістів організації у тому числі ефективності процесу управління інцидентами ІБ. При наявності кваліфікованих спеціалістів та підтримки виробника вдасться максимально зменшити негативні наслідки таких помилок. Тому рекомендується забезпечити наявність кваліфікованих спеціалістів для вирішення неочікуваних проблем, а за відсутності таких придбати підтримку продукції інженерами виробника.

Висновки до розділу 3

Отже, запропоновано набір інструментів інтелектуалізації та розглянуто спосіб їх поєднання в єдину СУРІБ на прикладі організації. Запропонована СУРІБ на основі інструментів інтелектуалізації здатна в повній мірі забезпечити автоматизацію процесу УРІБ, про що свідчать показники MTTD, MTTR, MTTI. Набір інструментів, що використано для створення системи є повним та покриває область дії процесу УРІБ в усіх типах організаційної інфраструктури. Можливості по інтелектуалізації методів провадження УРІБ є достатніми. Нажаль повної автоматизації методик досягти на разі неможливо, залишається залежність від висококваліфікованих спеціалістів. Як результат найгірше вдалося інтелектуалізувати процеси, які демонструють високу залежність від роботи

спеціалістів. Також надано актуальні рекомендації по впровадженню, інтеграції, та підтримці функціонування запропонованої або подібної системи.

ВИСНОВКИ

Отже, в результаті виконання кваліфікаційної роботи було проведено процес інтелектуалізації УРІБ організації, підприємства, установи. Створено інтелектуалізовану СУРІБ, яка поєднує в собі інструменти інтелектуалізації, цикл управління, методи та підходи до управління УРІБ, кадрове, ресурсне, нормативне забезпечення, що необхідне для ефективного та безперервного провадження процесу УРІБ.

В ході дослідження теоретичних аспектів інтелектуалізації УРІБ, було визначено основні рекомендації, вимоги, та особливості проведення процесу проектування. Розглянуто міжнародний досвід та особливості попереднього аналізу ІТ систем, бізнес-функцій та інтересів організації для побудови актуального процесу УРІБ.

В ході визначення необхідного методичного забезпечення та попереднього проектування СРУІБ було запропоновано приклад організації, розглянуто її особливості, обрано та застосовано підхід до проектування системи. Було розглянуто та обґрунтовано інструментарій інтелектуалізації для побудови системи та особливості організації її управління.

В ході впровадження інтелектуалізації та побудови інтелектуалізованої СУРІБ було запропоновано спосіб поєднання інструментів між собою, та управління визначеною системою. Розглянуто ефективність створеної СУРІБ у порівнянні з середньостатистичними показниками управління ризиками. Запропоновано рекомендації, щодо впровадження, інтеграції та підтримки СУРІБ та процесу УРІБ.

Розглянутий приклад інтелектуалізації процесу УРІБ може бути застосований на практиці для організацій будь-якого типу управління (установи, підприємства, тощо). З урахуванням їх особливостей та адаптацією набору інструментів та способу управління під особливості та потреби організації. Можна застосовувати наведені теоретичні відомості про різноманітні технології,

та інструменти ІБ, а також рекомендації інтелектуалізації та підтримці процесу УРІБ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Поняття організації. URL: https://buklib.net/books/31810/
2. Information Security Risk Management. URL: https://www.rapid7.com/fundamentals/information-security-risk-management/
3. NIST Special Publication 800-39. Managing Information Security Risk. Organization, Mission, and Information System View. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
4. Самко В.В. Управління змінами для підвищення ефективності управління ризиками та інформаційною безпекою підприємства. Матеріали Всеукраїнської науково-практичної Інтернет-конференції. м. Київ 24 лют. 2022 р. С. 28-31.
5. Моя стаття по Conf Computing + TEE десь має буть у виданні
6. ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки.
7. Ю. Р. Гарасим, В. А. Ромака, М. М. Рибій. Аналіз процесу управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем. URL: http://ena.lp.edu.ua:8080/bitstream/ntb/23330/1/16-90-99.pdf
8. Н.Г Милославская, М.Ю Сентаторов, А.И Толстой, Управление рисками информационной безопасности. Москва, «Горячая линия-Телеком», 2014.
9. Про віртуальні активи. Закон України від 07.04.2022. No 12/1-2022/60185. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/2698
10. ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT) Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги

11. Ian Neil. CompTIA Security+: SY0-601 Certification Guide Second Edition. Birmingham, «Packt Publishing Ltd.», 2021.
12. Qualys Cloud Platform. Public Site. URL: https://www.qualys.com/
13. IBM QRadar SIEM 7.5.0 documentation. URL: https://www.ibm.com/docs/en/qsip/7.5?topic=SS42VS_7.5/com.ibm.qradar.doc/c_qradar_pdfs.htm
14. Symantec Endpoint Protection. Related documents. URL: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Related-Documents.html
15. Symantec Messaging Gateway 10.7.3 – TechDocs. URL: https://techdocs.broadcom.com/us/en/symantec-security-software/email-security/messaging-gateway/10-7-3.html
16. Symantec Data Loss Prevention Help Center 15.8 – TechDocs. URL: https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/15-8.html
17. BigFix 10 Platform Documentation. URL: https://help.hcltechsw.com/bigfix/10.0/platform/welcome/BigFix_Platform_welcome.html
18. IBM Security QRadar SOAR. URL: https://www.ibm.com/docs/en/cloud-paks/cp-security/saas?topic=organization-soar
19. "Atlassian Software", "Jira". URL: https://www.atlassian.com/ru/software/jira
20. "Omninet Software Solutions". "Omnitracker". URL: https://www.omnitracker.com/
21. World Economic Forum. The biggest threat to your cybersecurity is hiding in plain sight. URL: https://www.weforum.org/agenda/2017/12/the-biggest-threat-to-your-cybersecurity-is-hiding-in-plain-sight/
22. MTTD and MTTR in Cybersecurity. URL: https://plextrac.com/mttd-and-mttr-in-cybersecurity/

23. Mean Time to Repair Explained. URL: https://www.crowdstrike.com/cybersecurity-101/observability/mean-time-to-repair-mttr/
24. Cyber Security Statistics. The Ultimate List of Stats. Data, & Trends For 2022. URL:https://purplesec.us/resources/cyber-security-statistics/
25. Cyber Risk Remediation: A Comprehensive Approach. URL: https://flare.systems/learn/resources/blog/cyber-risk-remediation-a-comprehensive-approach/
26. 166 Cybersecurity Statistics and Trends [updated 2022]. URL: https://www.varonis.com/blog/cybersecurity-statistics