УДК 004.056
DOI: 10.31673/2409-7292.2022.040008

Самко В.В.

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В статті розглянуто приклад автоматизації процесів управління вразливостями та ризиками ІБ. Визначено основні вимоги до системи автоматизації, та її завдання. Розглянуто найбільш популярні методи управління ризиками та проведено перевірку впливу інструментів автоматизації на методики управління. Розглянуто можливості запропонованого інструментарію автоматизації, та запропоновано рекомендації, щодо його впровадження та використання.

Ключові слова: автоматизація, ризики ІБ, вразливості, ідентифікація, аналіз, оцінка, спрощення.

Вступ і постановка задачі

В сучасних умовах швидкого розвитку інформатизації, повсякчас створюються нові програмні продукти, розроблюються нові функції, створюються патчі, нові вимоги, рекомендації. Усі ці нововведення призводять до підвищення ефективності інформаційних систем, надають можливість використання нових функцій, але і впливають на вже існуючі процеси. Велика швидкість розроблення нових технологій, та їх взаємодія між собою надає зловмисникам можливість знаходити слабкі місця у системах інформаційної безпеки та використовувати їх на свою користь, призводить до появи вразливостей у системах ІБ. Щоб запобігти можливості реалізації загроз з використанням таких вразливостей, зменшити затрати на процес и вразливостями інформаційної безпеки (УВІБ), пришвидшити його, збільшити його ефективність, пропоную розглянути можливості по автоматизації процесу УВІБ. В цій статті запропоную інструментарій для автоматизації УВІБ та підвищення ефективності суміжних процесів: управління загрозами; інцидентами; ризиками (УРІБ); тощо.

Критерії успішності для інструментів автоматизації

Для розгляду інструментів автоматизації процесу УВІБ необхідно зазначити, що цей процес можна вважати під-процесом більш високорівневого процесу – УРІБ, тому має сенс розглянути вплив автоматизації УВІБ також і на процес УРІБ. Для розгляду повноти покриття завдань представленим інструментарієм необхідно спершу визначити які завдання він повинен виконувати. В якості завдань до автоматизації процесу УВІБ можна визначити [1]:

1. Ідентифікація активів, оцінка їх цінності.
2. Ідентифікація, оцінка вразливостей системи ІБ та загроз активам.
3. Обчислення вірогідності реалізації загроз і їх впливу на бізнес.
4. Надання вичерпної інформації, рекомендацій для аналізу та прийняття рішень.
5. Надання інструментів автоматизації для спрощення впровадження рішень.

Згідно [2], процес управління ризиками ІБ в організації є неперервним процесом і у зв’язку з динамічною зміною стану систем ІБ та інформаційних продуктів, необхідно щонайменше раз на пів-року проводити переоцінку ризиків у системах ІБ. Так як стан та вірогідність реалізації ризиків можуть змінюватися. Ризики які вже були виявлені та оцінені повинні проходити переоцінку. Відповідним чином і оцінка вразливостей повинна проводитися на регулярній основі, бути постійним неперервним процесом, що дозволяє вчасно виявляти та попереджувати потенційні загрози до систем ІБ. Приймаючи до уваги неперервність процесів та необхідність постійного аналізу змін, що виникають в системах ІБ використання інструментів автоматизації може значно впливати на ефективність та швидкість виконання процесами поставлених завдань. Також окремо варто виділити проблему покриття інфраструктури організації обраними інструментами. В сучасному світі більшість організацій, що не підпадають під спеціальне нормативне регулювання, наприклад військові, використовують гібридний тип інфраструктури та мають системи ІБ у: хмарній; класичній; віртуалізованій; змішаній; типах інфраструктур. У зв’язку з цим важливою

вимогою до інструментів автоматизації буде можливість забезпечувати ефективне виконання завдань незалежно від: географічного розташування активів; їх зв'язку з корпоративною мережею; типу інфраструктури в якому знаходиться актив.

Для перевірки повноти автоматизації з використанням запропонованих інструментів перевірю покриття засобами автоматизації таких методів управління ризиками:

1. Методика OCTAVE(Operationally Critical Threat, Asset and Vulnerability Evaluation);
2. Методика NIST 800-30(NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems).

Методика OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) розроблена в Університеті Карнегі-Мелон (США) і передбачає оцінювання критичності загроз, активів і вразливостей. Цю методику широко використовують в усьому 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 галузі 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 проектної групи [3].

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 [3]. Алгоритм методики зображено на рис. 1 [3].

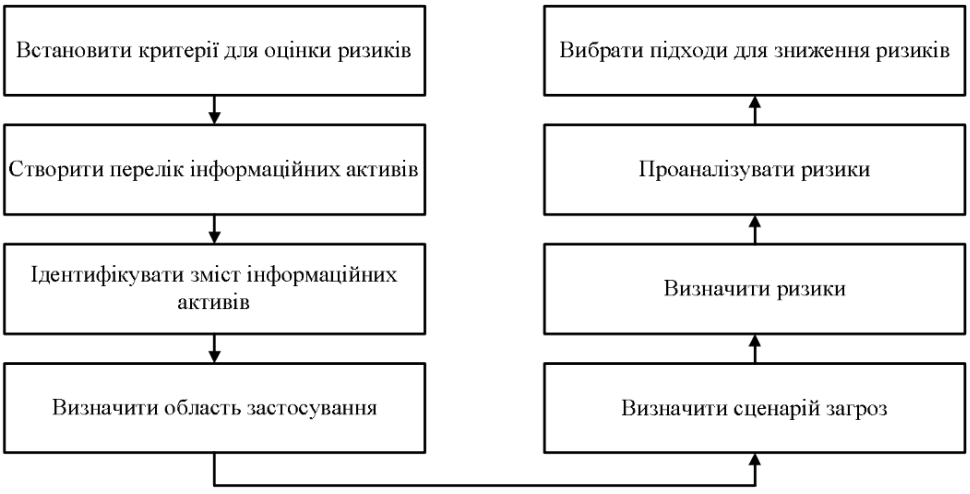

Рис. 1 Методика OCTAVE [3]

Однією з найпопулярніших та широковживаних методик управління ризиками є і методика Національного інституту стандартів і технологій США (National Institute of

Standards and Technology) NIST, зазначена в Керівництві з управління ризиками в інформаційних технологіях NIST 800-30 (NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems). Ця методика передбачає попереднє оцінювання двох параметрів: потенційного збитку та ймовірності реалізації загрози [3]. 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 800-30, охоплює широке коло завдань, що пов'язані зі стратегією управління ризиками і є основою для розроблення власної системи управління ризиками (рис. 2) [3]:

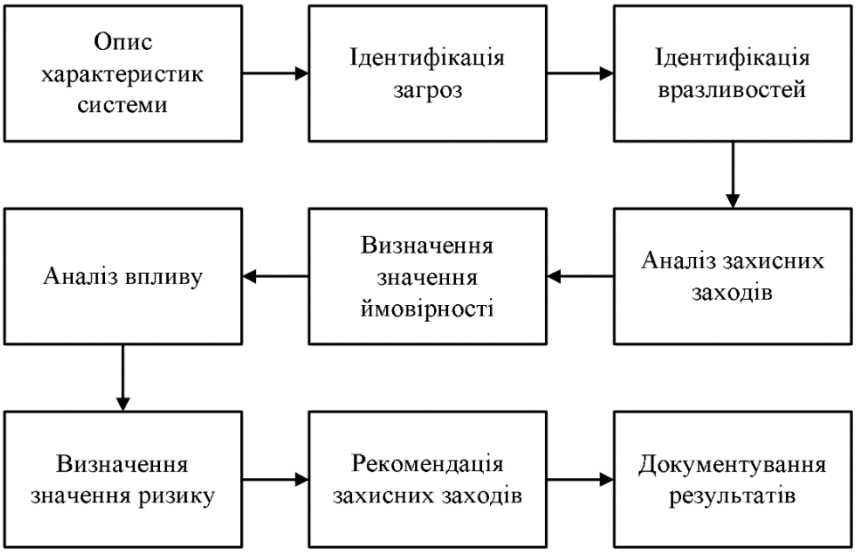

Рис. 2 Методика NIST 800-30 [3]

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.

Розгляд інструментарію та можливостей автоматизації процесів управління вразливостями та управління ризиками

В якості інструментів автоматизації, для виконання завдань визначених у попередньому пункті оберу платформу від компанії "Qualys, Inc." До інструментарію платформи входять більш ніж 25 додатків, які допомагають повністю контролювати та оцінювати інфраструктуру підприємства починаючи від ризиків та вразливостей, і закінчуючи автоматизованою перевіркою відповідності нормативним вимогам та стандартам накшталт PCI DSS [4].

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 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.

Можливості платформи дозволяють визначити:

1. Наявні вразливості.
2. Тип вразливостей.
3. Особливості активу.
4. Потенційні можливості по реалізації загроз.
5. Налаштування та конфігурацію активів.
6. Цінність активу для бізнесу.
7. Загальну оцінку рівня ризику активу або вразливості.
8. Нормалізацію та представлення даних для аналізу.
9. Рекомендації по виправленню вразливостей.
10. Автоматизовану систему розгортання патчів та управління конфігурацією.
11. Багато інших функцій.

Інструмент володіє можливостями по проведенню пріоритезації вразливостей на основі обраних критеріїв та дозволяє відображати найбільш актуальну інформацію для прийняття рішень (рис. 3).

Рис. 3 Пріоритизація вразливостей [4]

Платформа володіє можливостями для **узагальненого** розрахунку рівня ризику, що становлять активи в організації. Для такого розрахунку використовують значення критичності та ризику вразливостей активу, показник критичності активу для бізнесу, його розташування, особливості конфігурації, тощо (рис. 4, рис. 5).

Використовуючи можливості платформи Qualys можна значно спростити процес збору та аналізу інформації для прийняття управлінських рішень у процесах УВІБ, УРІБ, та навіть використати її для спрощення впровадження змін використовуючи можливості розгортання патчів та управління конфігурацією.

Розглянувши можливості інструментів можна відобразити покриття методів УРІБ на відповідних етапах.

Згідно алгоритму оцінки ризиків методики OCTAVE (рис 6) платформа Qualys дозволяє автоматизувати або напів-автоматизувати кожен з показаних в алгоритмі кроків. Продемонструю можливості автоматизації (рис. 6), які складають 95%.

Помітка Q – автоматизовано платформою. Q/E – частково автоматизовано, вимагає контролю людини. E –не автоматизовано, виконується спеціалістом.

Розглянуто вплив автоматизації за допомогою платформи Qualys на методику управління ризиками NIST 800-30 (рис. 7).

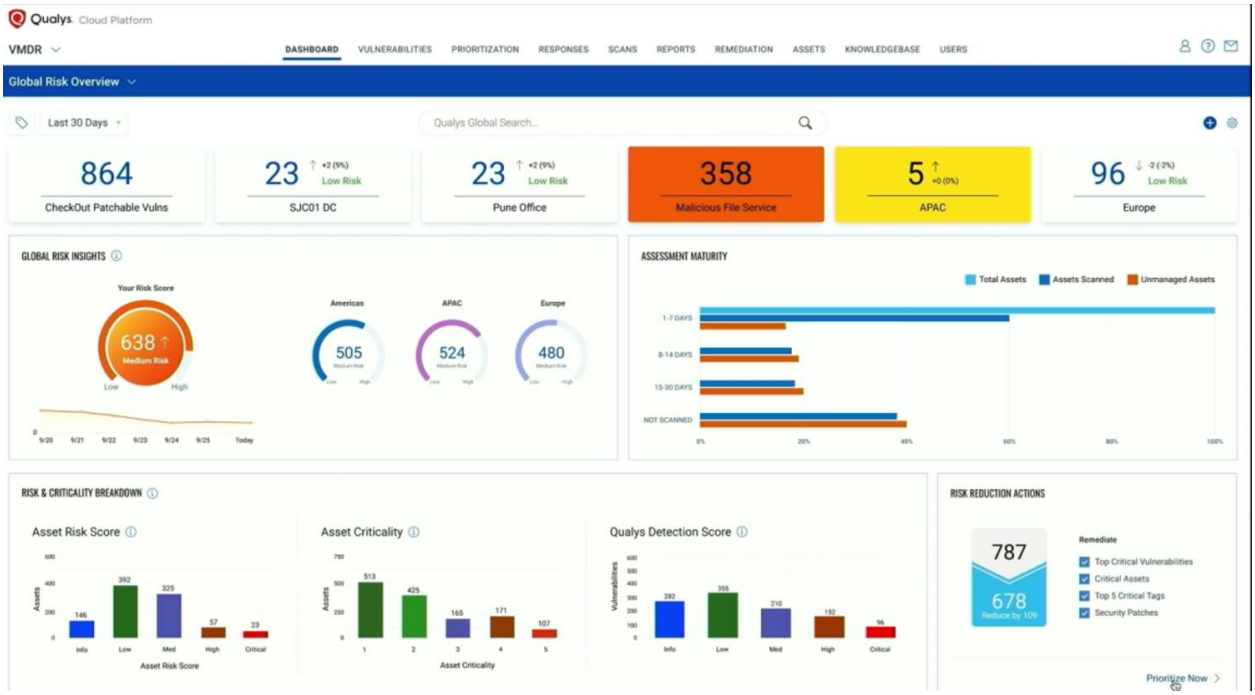

Рис. 4 Загальний огляд інфраструктури (ризики) [4]

Таким чином платформа Qualys дозволяє автоматизувати більшу частину розглянутих методик управління ризиками та надає найбільш повну інформацію для аналізу спеціалістами організації, що несуть відповідальність за прийняття управлінських рішень. Платформа Qualys дозволяє автоматизувати процес управління ризиками для методики OCTAVE майже повністю, але при цьому не забирає у спеціалістів можливість контролювати процес. Як показано на рис. 6 найважливіші частини алгоритму накшталт створення переліку активів для оцінки та виправлення, вибір методів виправлення, залишаються під контролем спеціалістів. Отже при використанні платформи спеціалісти лише отримують рекомендації та можливості, але вибір способів управління ризиками, методів їх закриття, пріорітету проведення робіт залишається повністю під їх контролем. Для методики NIST 800-30 майже повністю автоматизовано процес збору та оцінки даних для подальшого прийняття рішень. Інструментами автоматизації надано можливості автоматичного визначення способів закриття ризику, та інструментів для проведення виправлень.

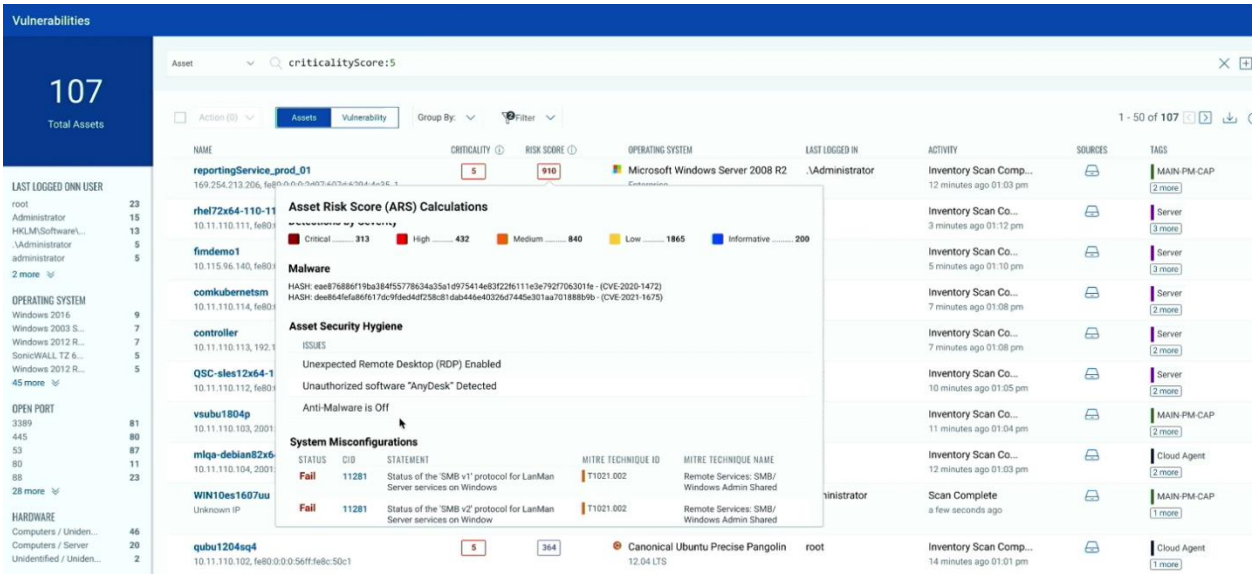

Рис. 5. Критичність та рівень ризику активів [4]

Рекомендації використання платформи Qualys

При використанні платформи для автоматизації процесів УВІБ та УРІБ варто враховувати особливості нормативного регулювання під яке потрапляє організація, брати до уваги особливості організаційних політик, а також враховувати вплив інших процесів та систем. Так, використовуючи платформу для управління вразливостями активів, що потрапляють в область дії стандарту PCI DSS лише сама організація несе відповідальність за повне покриття області PCI DSS інструментарієм платформи Qualys.

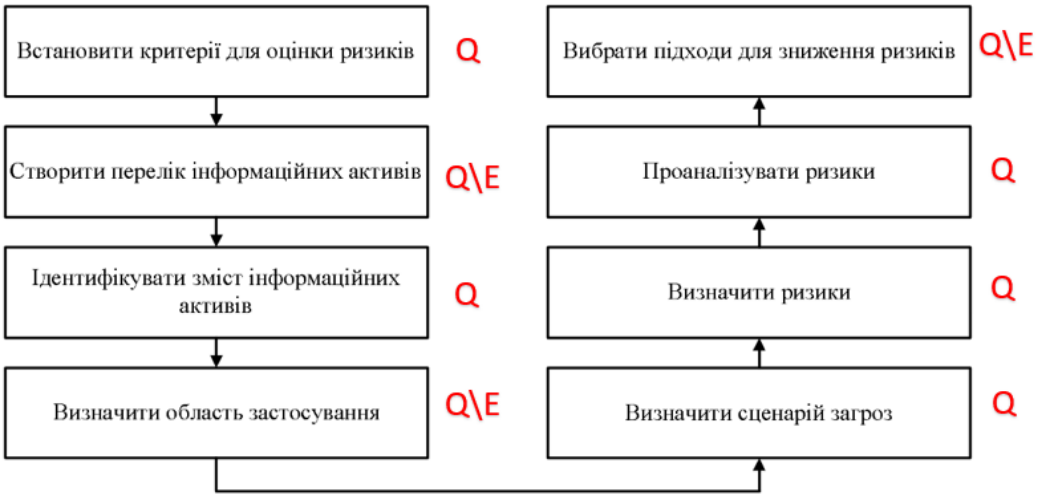

Рис. 6 Вплив автоматизації на методику OCTAVE

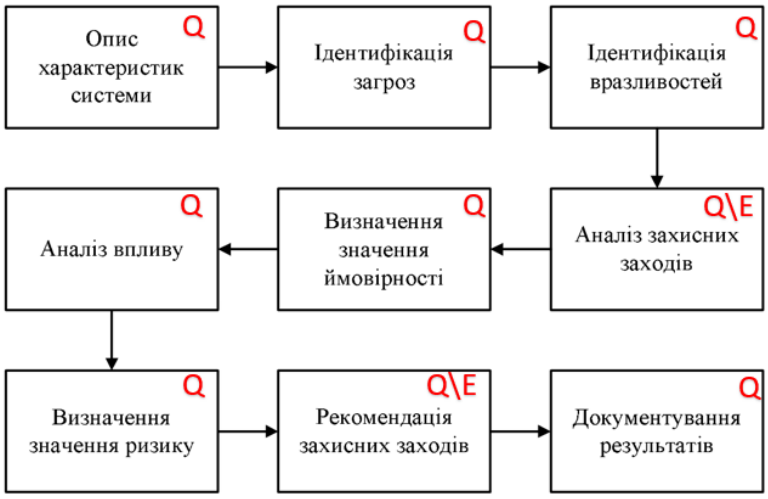

Рис. 7 Вплив автоматизації на методику NIST 800-30

При впровадженні системи рекомендовано провести аналіз наявних в інфраструктурі інструментів для роботи з ризиками, вразливостями, патчами, інструментів кореляції даних та централізованого управління інформаційною безпекою. До таких інструментів можна відносити системи безпеки кінцевих точок, системи оркестрації даних, SIEM-системи, тощо. В залежності від політик інформаційної безпеки організації інструментарій доступний в платформі Qualys може бути поєднаний з наявними інструментами для покращення ефективності проведення процесу управління ризиками. Платформа володіє якісним API

(Application programming language) який дозволяє інтегрувати та синхронізувати дані платформи з іншими інструментами безпеки.

Також рекомендовано при впровадженні автоматизації чітко визначити область її дії, не дивлячись на необхідність у сучасному світі контролювати та аналізувати усю інфраструктуру підприємства, деякі її частини можуть мати особливі вимоги щодо проведення будь-яких робіт по збору інформації та встановленню програмного забезпечення. Для таких систем варто розглянути роботу з приватним сегментом хмарної платформи Qualys, що розроблена "Qualys Inc." спеціально для підприємств з підвищеним рівнем вимог до захисту інформації. Наприклад для підприємств, що працюють з державною таємницею. Цей варіант платформи дає користувачеві повний контроль над місцем зберігання усіх даних, та зменшує їх розпорошеність. Такий підхід знижує швидкість обчислень, але збільшує рівень контролю підприємства за порядком обробки даних.

При використанні можливостей інструменту по управлінню патчами та контролем конфігурації варто провести аналіз можливостей інтеграції цих функцій з вже існуючими в організації практиками. Також варто використовувати можливість системи віддалено розгортати скрипти для змін конфігурації, а також додаткових перевірок наявності індикаторів вразливостей, що дозволить зменшити кількість потенційних "false positive" спрацювань.

Висновки

Платформа Qualys є підходящим рішенням для проведення автоматизації процесів УВІБ та УРІБ. Можливості інструменту дозволяють майже повність автоматизувати завдання по збору та нормалізації інформації необхідної для прийняття управлінських рішень, пришвидшують, підвищують ефективність відповідних процесів ІБ. Надають можливість повністю покривати будь-які типи організаційної інфраструктури, та отримувати видимість активів не залежно від їх географічного розташування. Велика кількість різноманітних інструментів системи дозволяє не лише виконувати збір інформації, а і надає інструменти для автоматизації впровадження патчів, управління конфігурацією, проведення перевірок на відповідність систем ІБ нормативним вимогам. Таким чином використання хмарної платформи Qualys в якості основи для автоматизації процесів УВІБ та УРІБ є доцільним.

Перелік посилань

1. Управление рисками информационой безопасости. Основные понятия и методология оценки рисков. [Електронний ресурс] // - Режим доступу: https://www.securityvision.ru/blog/upravlenie-riskami-informatsionnoy-bezopasnosti-chast-1-osnovnye-ponyatiya-i-metodologiya-otsenki-ri/ (10.10.2022)

2. ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements.

3. Ю.Р. Гарасим, В.А. Ромака, М.М. Рибій. Аналіз процесу управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем. [Електронний ресурс] // - Режим доступу: http://ena.lp.edu.ua:8080/bitstream/ntb/23330/1/16-90-99.pdf (10.10.2022)

4. Qualys Cloud Platform. Public Site [Електронний ресурс] // - Режим доступу: https://www.qualys.com/ (10.10.2022).

Надійшла: 29.11.2022 Рецензент: д.т.н., професор Кожухівський А.Д.