**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**
**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**
**імені ІГОРЯ СІКОРСЬКОГО»**
**НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**
**Кафедра інформаційної безпеки**

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)

«_____»_____2022 р.

# Дипломна робота

**на здобуття ступеня бакалавра**

**за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»**
**спеціальності 125 «Кібербезпека»**

на тему: "Розробка методики автоматизації управління мережевими політиками безпеки"

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-83
(шифр групи)

Тущенко Денис Михайлович _____
(прізвище, ім'я, по батькові) (підпис)

Керівник к.т.н, доцент, Коломицев Михайло Володимирович _____
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент к.н., доцент, Южакова Ганна Олексіївна _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2022 року

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**
**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**
**імені ІГОРЯ СІКОРСЬКОГО»**
**НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 125 «Кібербезпека»

Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)
«___»_____2022 р.

# ЗАВДАННЯ

**на дипломну роботу здобувачу вищої освіти**

Тущенко Денис Михайлович

(прізвище, ім'я, по батькові)

1. Тема роботи: "Розробка методики автоматизації управління мережевими політиками безпеки",

керівник роботи Коломицев Михайло Володимирович, к.т.н, доцент,

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «  » _____ 2022 р. №

2. Термін подання здобувачем вищої освіти роботи 13 червня 2022 р.

3. Вихідні дані до роботи: попередні дослідження методів роботи з політиками інформаційної безпеки

4. Зміст роботи: дослідження сутності ПІБ, вивчення методів роботи з політиками безпеки, обґрунтування необхідності автоматизації за допомогою метода Монте-Карло та розробка економічної оцінки ризиків, огляд рішень для автоматизації роботи з ПІБ, розробка та застосування методики автоматизації управління мережевими політиками безпеки.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) “якась назва презентації” – презентація

6. Дата видачі завдання: 05.10.2021

Календарний план

| № з/п | Назва етапів виконання дипломної роботи | Термін виконання етапів дипломної роботи | Примітка |
|---|---|---|---|
| 1 | Отримання завдання | 05.10.2021 | Виконано |
| 2 | Вивчення та опрацювання літератури | 15.10.2021 – 30.12.2021 | Виконано |
| 3 | Вивчення сутності та причин використання ПІБ | 10.01.2022 – 23.01.2022 | Виконано |
| 4 | Аналіз принципів розробки ПІБ | 24.01.2022 – 06.02.2022 | Виконано |
| 5 | Дослідження роботи з ПІБ | 07.02.2022 – 23.02.2022 | Виконано |
| 6 | Аналіз проблем при ручному керуванні ПІБ | 13.04.2022 – 30.04.2022 | Виконано |
| 7 | Проходження переддипломної практики | 02.05.2022 – 29.05.2022 | Виконано |
| 8 | Обґрунтування необхідності автоматизації, розробка економічної оцінки ризиків та програмного коду для проведення розрахунків | 09.05.2022 – 20.05.2022 | Виконано |
| 9 | Огляд рішень для автоматизації управління ПІБ | 21.05.2022 – 25.05.2022 | Виконано |
| 10 | Розробка методики автоматизації управління мережевими ПІБ та її практичне застосування | 26.05.2022 – 31.05.2022 | Виконано |
| 11 | Оформлення дипломної роботи та презентації | 01.06.2022 – 10.06.2022 | Виконано |
| 12 | Передзахист дипломної роботи | 13.06.2022 | Виконано |
| 13 | Захист дипломної роботи | 20.06.2022 | |

Здобувач вищої освіти _____ Денис ТУЩЕНКО
(підпис) **(Власне ім’я, ПРІЗВИЩЕ)**

Керівник роботи _____ Михайло КОЛОМИЦЕВ
(підпис) **(Власне ім’я, ПРІЗВИЩЕ)**

# РЕФЕРАТ

Дипломна робота складається з 79 сторінок, має 42 ілюстрацій, 8 таблиць, 5 додатків до роботи та 20 посилань на джерела.

Метою роботи є поглиблене дослідження мережевих політик безпеки, аналіз та вибір методу для кількісної оцінки результатів змін політик для визначення необхідності автоматизації, а також розробка методики автоматизації управління мережевими ПБ.

Методами дослідження стали використання джерел зі статистикою, аналіз сучасних стандартів при роботі з мережевими ПБ, а також математичні методи попарних порівнянь та Монте-Карло.

Результатом роботи стало внесення розвитку у відносно нову тенденцію автоматизації керування мережевими політиками безпеки та удосконалення наявних у відкритих джерелах статей, що лише поверхнево описують тему роботи та розглядають її з точки зору маркетингу.

Ключові слова: політика інформаційної безпеки, автоматизація, ризик, оцінка, метод Монте-Карло, програмне забезпечення, Tufin.

# ABSTRACT

The work consists of 79 pages, contains 42 illustrations, 8 tables, 5 appendices and 20 references.

The aim of the work is to study carefully network security policies, analyze and select a method for quantifying the results of policy changes to determine the need for automation, and to develop methods for automating the management of network security policies.

The research methods were using sources with data and statistics, analyzing modern standards of working with the policies, and mathematical methods of pairwise comparisons and Monte-Carlo.

The results of the work were the development of a relatively new trend in the automation of security policy management and the improvement of existing open source articles that only superficially describe the topic of the work and consider it in terms of marketing.



Keywords: information security policy, automation, risk, evaluation, Monte Carlo method, software, Tufin.

**ЗМІСТ**

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ІТ – інформаційні технології

КБ – кібербезпека

ІБ – інформаційна безпека

ПІБ – політика(-и) інформаційної безпеки

ПЗ – програмне забезпечення

ОС – операційна система

SOC –Security Operations Center (перекл. “Операційний центр безпеки”)

SIEM – Security information and event management (перекл. “Менеджер управління безпекою інформації та подій”)

CIO – Chief Information Officer (перекл. “Директор з інформаційних технологій”)

CISO – Chief Information Security Officer (перекл. “Директор з безпеки інформаційних технологій”)

MAI – метод аналізу ієрархій

TOS – Tufin Orchestration Suite

ST – SecureTrack

SC – SecureChange

# ВСТУП

Керування політиками, правилами та конфігураціями мережевої безпеки вручну займає багато часу та може призвести до помилок, що збільшує експлуатаційні витрати та ризики, пов’язані з безпекою, особливо якщо IT-інфраструктура компанії стає все більш складною. Якщо політика безпеки мережі керується вручну (або за допомогою кількох несумісних інструментів), вплив на бізнес від складнощів, утворених всього кількома сайтами, пристроями, правилами, конфігураціями та моделями розгортання прикладних програм зростає експоненціально.

Саме тому автоматизація робочих процесів для змін конфігурації мережевої безпеки стає все більш важливою — і призначена для забезпечення високого рівня впевненості в тому, що ці важливі завдання виконуються точно й послідовно. Крім того, провідні рішення для керування політикою безпеки забезпечують постійний огляд фактичних політик, правил і конфігурацій, які зараз діють у поточній інфраструктурі безпеки мережі, в режимі реального часу, а також забезпечують необхідну інтеграцію з широким спектром продуктів мережевого брандмауера та моделей розгортання застосунків.

Актуальність роботи полягає в тому, що в умовах постійного розвитку технологій та методів атак на них, не зважаючи на критичну необхідність, багато спеціалістів досі не приділяють достатньої уваги ПІБ у своїх організаціях. І хоч, порівняно з минулим, вже не знайдеш адміністратора системи, який би не імплементував хоча би базові правила, постає серйозна проблема якісного керування політиками безпеки мережі на підприємствах. Звідси з’являється необхідність у автоматизації управління мережевими ПБ та поширенню необхідних для цього засобів.

Метою роботи є поглиблене дослідження мережевих політик безпеки, аналіз та вибір методу для кількісної оцінки результатів змін політик для визначення необхідності автоматизації, а також розробка методики автоматизації управління мережевими ПБ.

Завдання роботи: дослідити управління мережевими політиками безпеки; розробити алгоритм кількісної оцінки результатів змін мережевих ПБ; за результатами оцінювання, визначити необхідність автоматизації; розробити методику автоматизації управління мережевими ПБ у компанії.

Об’єктом дослідження є процес керування мережевими ПІБ в організації разом зі шляхами його автоматизації.

Предметом дослідження є полегшення процесу керування мережевими ПІБ за допомогою розробленої методики та її подальшої імплементації.

Методами дослідження стали використання джерел зі статистикою, аналіз сучасних стандартів при роботі з ПІБ, а також математичні методи попарних порівнянь та Монте-Карло.

Наукова новизна полягає в тому, що ця робота комплексно та детально присвячена відносно новій тенденції автоматизації керування мережевими політиками безпеки. Дане дослідження удосконалює наявні у відкритих джерелах статті, що лише поверхнево описували тему роботи та розглядали її з точки зору маркетингу.

Практичне застосування: дослідження з даної роботи та розроблена методика можуть бути використані в організаціях будь-якого розміру (малих, середніх чи ентерпрайзах) з метою покращення рівня безпеки своїх систем за допомогою автоматизації керування ПІБ.

# 1 ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 1.1 Сутність політики безпеки

Інформаційні технології на сьогоднішній день є невід'ємною і важливою складовою великої кількості бізнесів, що суттєво спрощує життя спеціалістів та значно підвищує прибутки при грамотному використанні. Однак, для запобігання ризиків втрати інвестицій, розробники пропонують все новіші методи захисту активів, керування якими здійснюється безпосередньо після затвердження необхідних документів, які прийнято називати політиками. Будь-яка політика безпеки спрямована на те, щоб IT-ресурси ефективно виконували основні бізнес-функції, забезпечували захист та стабільність електронних даних учасників, відповідали державним та іншим законодавчим нормам.

Узагальнюючи, політика інформаційної безпеки – це збірка різноманітних правил, процедур та інших політик, головним завданням яких є відповідність усіх кінцевих користувачів та мережі в певній організації мінімальним вимогам захисту IT та збережених даних. ПІБ повинні покривати усю інфраструктуру та повний спектр інформації, програм, наявних систем, працівників та клієнтів.

Насправді, існує надзвичайно велика кількість ПІБ, спрямованих на протидію всім відомим загрозам інфраструктурі та бізнесу. Існують ПІБ, розроблені для файлових систем, брандмауерів, служб, демонів та окремих файлів. Жодна система не є безпечною, тому захист цифрового середовища – це пріоритетне на дуже важливе завдання, яке потребує постійного вдосконалення та розробки нових шляхів захисту.

За значенням, політики інформаційної безпеки можна розділити на:

- спрямовані на захист від загроз;
- спрямовані на протидію загрозам та їх усуненню, коли ті відбулись.

Доцільно буде також дати визначення терміну “загрози” та навести певну класифікацію їх видів. В контексті КБ термін “загроза” застосовується для опису будь-якої події, що своїми діями може нести небезпеку та шкодити інформаційній системі шляхом її знищення, зміни, викрадення чи підробки даних, відмови обслуговування. Загрози можуть бути спрямовані на: безпосередньо фізичну будівлю, мережу компанії, кінцеві точки (сервери, комп'ютери), будь-які типи вразливої інформації.

Виділимо найпоширеніші види ПІБ [1]:

- Політика комп’ютерної безпеки – визначає цілі та елементи комп’ютерних систем.
- Політика захисту інформації – визначає вимоги щодо обробки, зберігання та розповсюдження чутливої інформації.
- Політика облікових записів – визначає поведінку з обліковими записами у компаніях.
- Мережева політика безпеки – містить правила доступу до мережі в організації і контролює політики, що застосовуються в її межах.
- Політика фізичної безпеки – запроваджує правила контролю фізичного доступу до приміщень та фізичних активів компанії.
- Політика контролю доступу – вимоги щодо контролю рівнів доступу в компанії.

Розуміючи загальну сутність ПІБ, необхідно детальніше вивчити мережеві ПБ в організаціях, яким присвячена тема даної роботи.

Політики безпеки мережі мають описувати рекомендації щодо доступу до мережі, її архітектури, визначати, які засоби контролю безпеки використовуються в організації, а також запобігати несанкціонованому доступу ззовні та зсередини компанії для зменшення ризикових ситуацій. Окрім цього, вони необхідні для визначення політик наявних в організації, надаючи користувачам доступ лише до тих частин мережі, на які вони мають дозволи.

Корисними для мережі вважаються політики, присвячені аспектам, як [1]:

- Управління рахунками
- Електронна пошта
- Управління інцидентами безпеки
- Управління журналами
- Використання VPN
- Контроль використання приватних девайсів
- Паролі облікових записів
- Безпека серверів

Перелічені політики мають зазначати поведінку користувачів під час доступу до мережі організації, чим забезпечувати конфіденційність, цілісність і доступність інформаційної системи. Розібравшись з цим, можна перейти до вивчення причин необхідності наявності мережевих ПБ у компаніях.

## 1.2 Основні причини створення мережевих політик безпеки

Аби мати змогу конкурувати на світовому ринку, всі організації, без винятку, користуються інформаційні системами та технологіями, а отже стають все більш залежними від їх стабільності, доступності та змоги використання. Окрім небезпеки від потенційних злочинців, програмне забезпечення постійно оновлюється та розвивається, що спричиняє необхідність якісної процедури підтримки безпеки та контролю інформації, якою оперують співробітники.

Враховуючи роль інтернету у сучасному світі, організації не можуть не користуватися ним для повсякденних операцій, що робить їх більш вразливими до загроз безпеки мережі. Атаки на мережу можуть вилитись у великі збитки, як фінансові, так і репутаційні. Тому організація, яка вибудувала якісну мережеву політику безпеки, не буде мати проблем із вчасним та успішним завершенням проектів, зменшуватиме ризики потенційних порушень через людський фактор чи недоброякісних працівників, унеможливить витік даних та їх використання третіми особами, а також допоможе уникнути безлічі інших небезпечних ситуацій. В сучасних умовах будь-яка компанія, що оперує людськими активами, чутливою інформацією чи іншими видами таких даних, має за найважливішу необхідність проробити комплекс мережевих політик безпеки. Саме наявність активної ПІБ мінімізує ризики та захищає організацію, встановлюючи правила поведінки користувачів, визначаючи та санкціонуючи наслідки порушення, і забезпечуючи їх дотримання.

Аналіз інфографіки поширення та використання ПІБ за 2010 та 2019 роки доводить, як сильно змінилась ситуація. У наведених нижче ілюстраціях будуть приведені статистичні дані порівняння безпеки інформаційних технологій в компаніях Європейського Союзу. Надана інформація отримана в результаті

щорічного анкетування спільноти, в ході якого збираються дані, пов'язані з IT та їх використанням на підприємствах малого (10-49 осіб), середнього (50-249 осіб) та великого (250 та більше осіб) розмірів [2-3]. Для даної роботи було оброблено інформацію в контексті інцидентів безпеки та заходів контролю для забезпечення організаціями цілісності, конфіденційності, та доступності даних/систем.

Так, графік на рисунку 1.1 ілюструє, що станом на 2010 рік, лише 27% організацій мали формально визначену ПІБ, тоді як у 2019 році цей показник виріс до 92%. Така звичайна річ, як наявність політики паролей, у 2010 році була наявна лише в 46% організацій, а у 2019 році – вже в 76%. Хоч відсоток використання іншого/додаткового засобу автентифікації зменшився на 4%, варто відмітити, що 12 років тому статистику збирали щодо розповсюдженості апаратних токенів (фізичні картки, як приклад), а з розвитком технологій, у 2019р., вже опитували про біометричні методи автентифікації (відбитки, сканування обличчя/сітчатки ока тощо). Відсоток працівників, що проходили детальне ознайомлення з наявними ПІБ, зріс із 48% до 61%. Також з 22% до 24% за 9 років збільшився регулярний перегляд ПІБ.

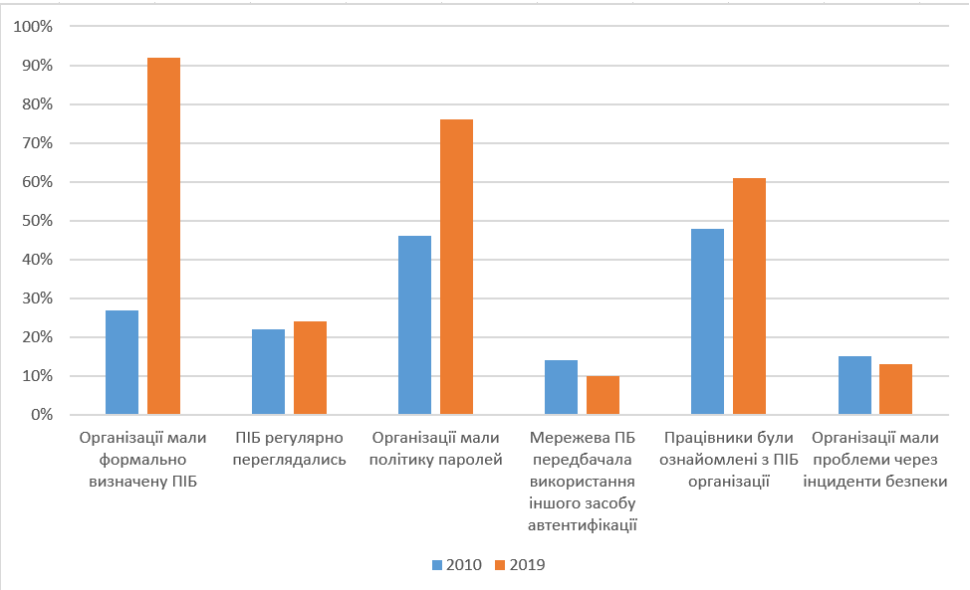



Рисунок 1.1 - Порівняння заходів безпеки IT на підприємствах в ЄС у 2010 та 2019 роках

Саме ці та інші міри допомогли знизити показник появи інцидентів безпеки в організаціях з 15% до 13%. Останні дві зміни можуть здатися не дуже суттєвими, тому пропонуємо розглянути їх детальніше. Рисунок 1.2 подає інформацію у більш конкретному вигляді, порівнюючи малі, середні та великі організації. Можна помітити, що з розміром компанії, зростають і поділки на графіку. Тоді як у значної кількості (57%) великих організацій перегляд усіх ПІБ відбувається в межах одного року, поміж середніх компаній – цей показник становить лише 38%, а серед малих – взагалі 21%. Що цікаво, те саме стосується і затримки у перевірці актуальності ПІБ – компанії-гіганти мають найбільші показники “Від 12 до 24 місяців” (13% проти 10% у середніх чи 5% у малих) та “>24 місяців” (4% проти 3% у середніх чи 1% у малих). На нашу думку, це пояснюється кількістю політик, які можуть бути наявні в межах організації, де працює більше 1000 осіб, та не рідко слабкою організацією їх підтримки.

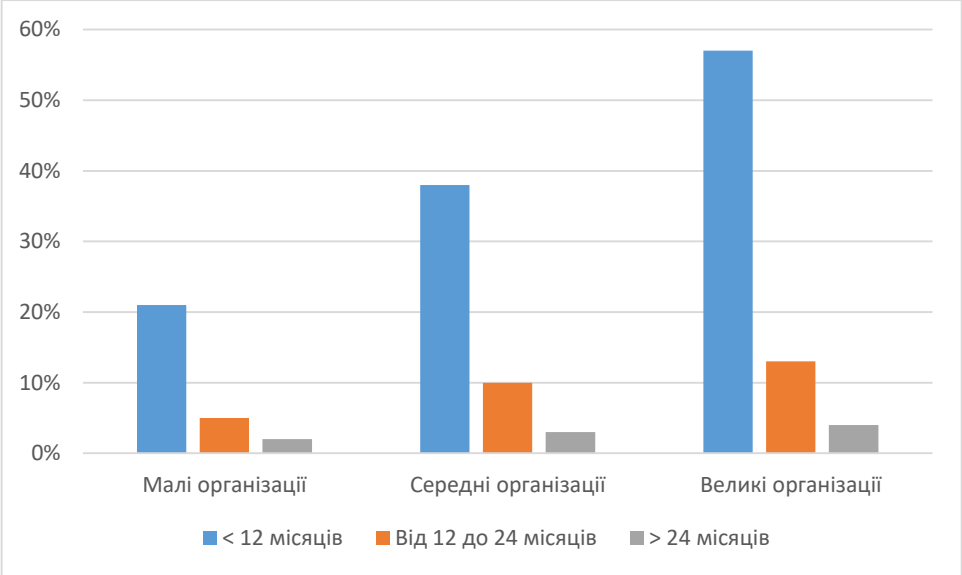



Рисунок 1.2 - Регулярність перегляду ПІБ на підприємствах в ЄС у 2019р.

Проте відсоток своєчасного нагляду за політиками все ще здається дуже незначним у малих організаціях, що може пояснити графік на ілюстрації 1.3. Він демонструє інформацію про виникнення інцидентів безпеки у компаніях різного розміру. В наведеному графіку найбільший інтерес для нас становить стовпець А, що подає загальну інформацію, оскільки в інших розподіл приблизно однаковий. Для малих компаній цей відсоток складає 12%, для середніх – 18%, а для великих – 25%.

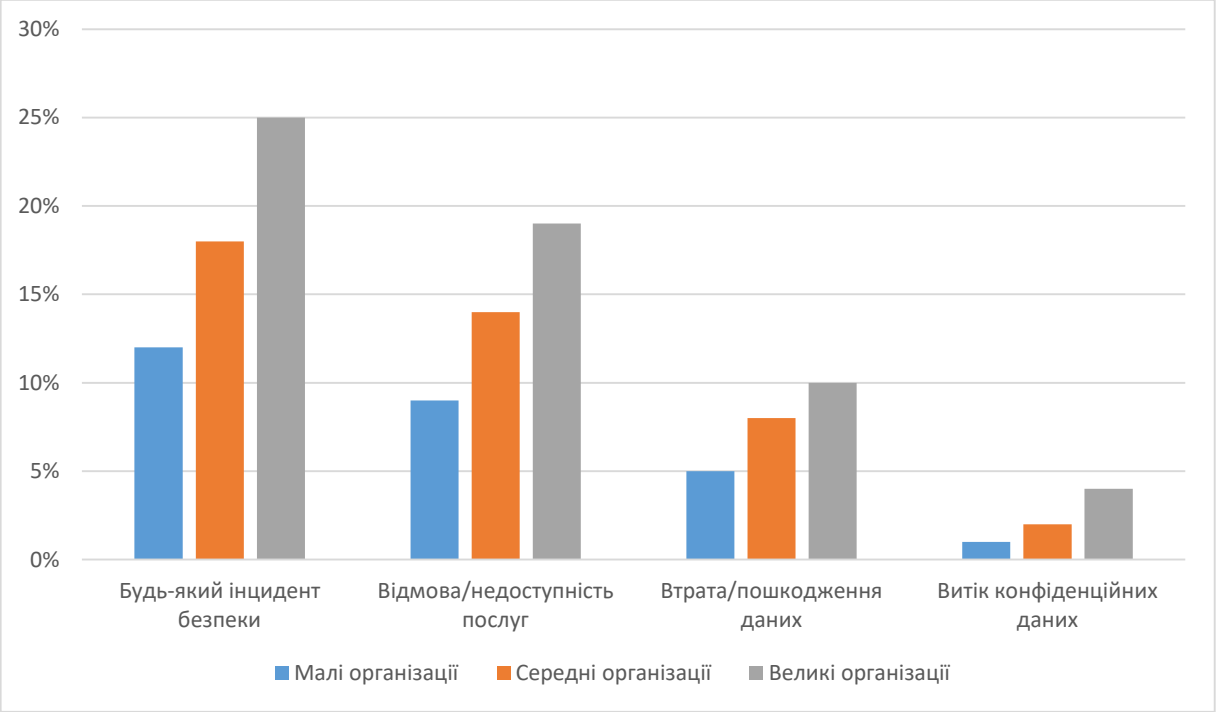



Рисунок 1.3 - Відсоток підприємств в ЄС, що хоча б раз мали проблеми з інцидентами безпеки у 2019р.

Виглядає цілком логічно, адже кількість невеликих організацій значно більша за ентерпрайзи та вони рідше складають цікавість для хакерів. Подібна безтурботність, на нашу думку, і стала однією з найвагоміших причин, чому використання ПІБ не набуло достатнього поширення серед малих компаній.

Компанії-гіганти ж, навпаки, маючи більше ризиків, як наприклад втрата значної кількості грошей, конфіденційної інформації та, як наслідок, довіри клієнтів, намагаються тримати під контролем ПІБ свою інтелектуальну власність.

Наостанок розглянемо ілюстрацію 1.4, дані якої доводять, що станом на 2019 рік підприємства ЄС використовують будь-які можливі заходи безпеки мережі своєї інфраструктури. Найпоширенішим є політика управління оновленнями (87%), далі йде політика паролей (76%), за ними – контроль доступу до мережі (65%). Менше половини компаній вели журнали логування (45%), використовували технології VPN (42%), та мали політику оцінки вразливостей (33%).


Рисунок 1.4 – Мережеві політики на підприємствах в ЄС у 2019р.

Після проведеного аналізу кількісних змін у використанні ПІБ, в якості висновку можна зазначити, що з кожним наступним роком відсотки на цих графіках будуть тільки зростати, адже все менше лишається людей, готових

зайвий раз ризикувати своїми активами, на тлі появи все більшої кількості технологій, що спрощують отримання доступу до незахищеної інформації.

Також необхідно зазначити, що, окрім спрощення повсякденних задач, без мережевих політик часто вже не можуть існувати певні цикли управління проектами з підтримкою IT. Отже, поєднання потреб бізнесу з вимогами безпеки та налагодження їх під затверджені стандарти ще на початку процесу дозволяє як прискорити завершення проекту, так і підвищити рівень його захищеності одночасно. У той час, як проектні групи розробляють фінансові стратегії, фахівці з безпеки займаються оцінкою ризиків, виявленням вразливостей, пошуком шляхів до їх усунення та інтеграцією в інфраструктуру ще на моменті розробки.

Головною причиною, чому така комбінація працює найкраще, є те, що компанія підвищує шанси виграти від даного підходу (не втратити конкурентоспроможність, підвищити продажі тощо), та водночас знижує шанси при цьому втратити чутливі дані клієнтів, конфіденційну/секретну інформацію, свої конкурентні переваги тощо.

Однак варто звернути увагу, що сама наявність ПІБ в організації не гарантує найвищий рівень безпеки мережі. Не менш важливим є сприяння ефективній інтеграції політик у команду компанії.

## 1.3 Ролі та обов’язки учасників у відношенні політики безпеки

Навіть якщо компанія ставиться серйозно до своєї безпеки, якісно оцінює ризики і має мережеві ПБ, де докладно прописано, що можна робити, а що – ні, це не означає, що вона не матиме серйозних проблем та інцидентів, що

призведуть до матеріальних або репутаційних втрат. Важливо запам’ятати, що політики, в першу чергу, розробляються спеціалістами з розділу ІТ. Останні, як правило, є одними з небагатьох, хто знає про існування ПІБ; і саме команда ІТ бере на себе пряму відповідальність за дотримання правил інформаційної безпеки.

Якісно розроблена політика ще не гарантує ефективності, адже вона досягається лише за умови, що всі працівники компанії будуть ознайомлені з її правилами, а найголовніше – дотримуватись прописаної поведінки. На жаль, поведінка співробітників дуже рідко повністю відповідає процедурам і методам ІБ, що значно підвищує ризики виникнення інцидентів на підприємствах.

За даними дослідження, що проводилось “B2B International” та “Kaspersky Lab”, близько 46% інцидентів з безпекою щороку трапляються через необачливих працівників, а на додачу до цього, майже 40% таких випадків намагаються приховати, щоб не отримати покарання, тим самим сильно погіршуючи наслідки [4]. Окрім цього, з майже половини співробітників, що вважають підтримку безпеки ІТ спільною відповідальністю, лише 12% були повністю обізнані з наявними в їхніх компаніях ПІБ. Зі статистики стає очевидно, що великий відсоток людей у організаціях міг ніколи не бачити політик, забути їх за час роботи чи спеціально ігнорувати через якісь свої причини (наприклад, це ускладнює стандартну задачу та вимагає виконати додаткові кроки). Вище керівництво, у свою чергу, не було дуже зацікавленим у заохоченні співробітників до обізнаності в правилах та їх дотриманні.

Отже, співробітники ІТ обов’язково мають залучати до розробки та виконання політик усіх членів команди. В першу чергу – директора та інших керівників, адже безпека стосується кожного. У кожного має бути своя роль та зона відповідальності, щоб чітко визначити задачі для досягнення безпеки

інформації, шляхом роз’яснення та координації дій для поширення ПІБ серед працівників.

Таблиця 1.1 містить список ролей та зон відповідальності, що мають вирішальне значення для ефективної взаємодії політик та стандартів ІБ [5]. Вказані ролі необхідні для забезпечення чітко визначених обов’язків та пояснення, як саме функціонує захист інформації. Їх мета – це інформування, розповсюдження, координація мір, необхідних для поширення та впровадження ПІБ.

Таблиця 1.1 – Ролі та зони відповідальності при роботі з ПІБ

| Роль | Відповідальність |
|---|---|
| Рада директорів | • Створення щорічного звіту стосовно ІТ та ризиків<br>• Зв’язок з виконавчим керівництвом, надання рекомендацій та узгодження задач |
| Виконавче керівництво | • Розрахунок витрат на ІБ<br>• Узгодження ПІБ на основі задач компанії |
| CIO | • Виділення фінансів для офісу ІБ, щоб був забезпечений сучасний захист<br>• Координація роботи з CISO для практичного втілення засобів безпеки |
| CISO | • Інформування керівництва про знайдені ризики ІБ<br>• Доведення ризиків до прийнятного рівня<br>• Координація розробки ПІБ<br>• Разом з офісом ІБ створює системи ІБ та поширює обізнаність |

Продовження таблиці 1.1

| | |
|---|---|
| Офіс інформаційної безпеки | • Проведення оцінки ризиків та створення документації<br>• Допомога в класифікації даних, обрання засобів контролю<br>• Розробка ПІБ для виявлених ризиків<br>• Співпраця з ІТ-відділом<br>• Спостереження за станом ІТ-інфраструктури<br>• Розробка програми управління вразливостями |
| Внутрішній аудит | • Проведення внутрішнього аудиту<br>• Допомога у проведенні зовнішнього незалежного аудиту |
| Менеджер з інцидентів безпеки | • Реагування на інциденти<br>• Розслідування причин та наслідків інцидентів |
| Співробітники | • Слідування визначеним ПІБ, щоб не створити загрози активам компанії<br>• Допомога у визначенні шляхів для створенні політик |

Розглянувши сфери відповідальності кожної з груп осіб, можна перейти до дослідження безпосередньо процесу створення мережевих політик безпеки в організаціях.

## 1.4 Принципи та основні етапи розробки мережевих політик безпеки

Сучасний рівень науки і техніки не пропонує жодного універсального засобу для виявлення та уникнення всіх можливих загроз інформаційній безпеці. Вважаючи на одночасний розвиток як атакуючих, так і захисників КБ, швидше за все, подібне універсальне рішення не вдасться винайти й у майбутньому.

Проте, в області аналізу було вироблено систематичний підхід оцінки інформаційної безпеки загалом [6]. Згадана ідеологія підвищення її рівня зводиться до того, що захист цільової системи забезпечується сукупністю заходів, реалізованих протягом усього життєвого циклу системи, що розробляється, а потім експлуатується. Тобто, починаючи з визначення вимог до системи, вибору архітектури та проектування, вибору інструментів розробки та підтримки життєвого циклу, повинні виконуватись роботи, спрямовані на підвищення рівня захищеності та довіри до цільової системи.

Будь-яка ПІБ має відповідати певним функціональним вимогам безпеки, які будуть її структурувати та подавати на різних рівнях деталізації. Одні з таких виконуваних умов мають бути [7]:

- Опис на різних рівнях деталізації.
- Опис архітектурних особливостей системи, поділу мережі та доменів.
- Забезпечення захисту функціональних вимог безпеки та неможливості його обходу.
- Відповідність між моделлю політики безпеки та функціональною властивістю.
- Модульність, розподіл на рівні та мінімізація складності.

Також сформована політика має відповідати двом властивостям. Перша з них полягає в тому, що певна функціональна можливість виконується правильно згідно задумки. Сенс другої полягає в унеможливленні використання об’єкту оцінки так, що це призведе до спотворення або обходу функціональних можливостей безпеки. Також, політика повинна чітко визначати, що вона захищає та що може очікувати від користувачів системою, бути орієнтиром для майбутніх оновлень безпеки при розробці нових програм чи розширень мережі. Вона має описувати дозволену поведінку користувачів (обережну поведінку з конфіденційною інформацією, задання складних паролів та їх періодичну зміну) і контроль своїх заходів безпеки, щоб мати можливість слідкувати за їх станом та спробами обходу.

Перед початком розробки мережевої політики безпеки треба окреслити цілі, яких необхідно досягти, серед основних можуть бути [8]:

1. Захист даних, окремих систем чи всієї інфраструктури організації. Гарантія, що лише користувачі з необхідним рівнем доступу зможуть отримати відповідну інформацію, а інфраструктура експлуатується за встановленими стандартами та практиками.
2. Запровадження безпеки інформації, якою оперує та зберігає організація.
3. Конфіденційність. Має вирішальне значення у питанні ІБ даних, виступає доказом, що інформація буде відомою тільки для довірених осіб.
4. Цілісність. Гарантія ідентичності інформації на будь-якому з етапів її обробки та зберігання з початково отриманою.
5. Доступність. Гарантія, що системою безпечно користуватись без ризику втратити будь-які активи компанії/користувача. Зазвичай, досягається завдяки цифровим сертифікатам, коли цифровий підпис необхідно поставити з обох сторін, тим самим підтвердивши здатність обміну.

Саме створення ж мережевої ПБ можна описати у такі етапи [9]:

1. Визначення відповідальних осіб/відділів. Опис їх ролей та обов’язків.
2. Опис основних цілей бізнесу для визначення масштабів створюваної політики безпеки та максимально економічно ефективної її розробки.
3. Визначення конфіденційних даних та систем організації, що підлягають захисту.
4. Окреслення та оцінка загроз для активу. Краще, щоб цей етап виконувався третьою стороною, яка знайде прогалини в безпеці мережі.
5. Створення плану дій, орієнтований на усунення знайдених загроз.
6. Розробка нової політики безпеки або розширення вже існуючої.
7. Визначення реакції на інциденти у мережі.
8. Визначення засобів контролю безпеки у мережі.
9. Затвердження ПІБ.

Після останнього етапу, можна приступати до практичного втілення політики та імплементації необхідних методів захисту. Серед цих кроків можуть бути ознайомлення та навчання команди, налаштування ПЗ, зміна інфраструктури системи, аналіз та переоцінка нових можливих ризиків, що можуть нести будь-яку загрозу активам компанії.

## Висновки до розділу 1

Спираючись на базові основи сутності політики безпеки, нами було розглянуто і виділено найпоширеніші види напрямків ПІБ. Було розглянуто мережеві політики безпеки, визначено найкорисніші з них, а також основні причини їх створення.

Проаналізовано інфографіку порівняння рівнів безпеки організацій за 2010 та 2019 роки, внаслідок чого визначено значний ріст показника поширення та використання політик усіх можливих типів.

Визначено властивості ПІБ, цілі та етапи створення мережевих політик в організації.

Оброблена нами інформація підтверджує необхідність створення та підтримка відповідного стану мережевих політик безпеки. Розглянуті дослідження інцидентів безпеки через людський фактор, в свою чергу, піднімають питання дослідження процесів роботи з ПІБ і визначення головних проблем. Це створює задачу з усунення недоліків, розв’язком якої пропонується автоматизація управління мережевими політиками безпеки. Таким чином, постає завдання вибору методу для кількісної оцінки результатів змін ПБ.

# 2 ДОСЛІДЖЕННЯ МЕТОДІВ РОБОТИ З МЕРЕЖЕВИМИ ПОЛІТИКАМИ БЕЗПЕКИ ТА НЕОБХІДНОСТІ АВТОМАТИЗАЦІЇ

## 2.1 Проблематика ручного керування мережевими політиками безпеки

Практика доводить, що за відсутності автоматизованого управління мережевими ПБ досить складним є своєчасне їх оновлення відповідно до найсучасніших практик, стандартів сертифікацій та нових правил, що постійно з'являються. Сучасний ринок пропонує багато рішень для керування політиками, відсутність яких у повсякденній практиці може призвести не лише до зменшення продуктивності праці, а й до катастрофічного росту числа інцидентів з безпекою.

За спостереженнями, найпоширенішими проблемами, що знижують ефективність при ручному керуванні мережевими політиками безпеки, є [10]:

1. Людський фактор.

   Як було зазначено раніше, майже половина усіх інцидентів з безпекою в організаціях відбувається за провини співробітників. Оскільки людина – це не машина, то навіть нескладна задача, як відкриття доступу працівнику до якогось сервера, буде вимагати затрат часу для перевірки рівнів дозволів, правил зонування та наявних політик на можливість доповнення.
2. Виявлення та контроль зайвих правил.

   За відсутності спеціалізованого програмного забезпечення, важко відслідковувати старі, непотрібні правила, множинні версії політики, чи правила з надмірними дозволами.
3. Надання та контроль доступу, використовуючи широкий спектр технологій.

Політики, процедури та процеси у мережі безпосередньо впливають на діяльність в компанії. Чи можуть співробітники легко отримати доступ до документів, коли це найважливіше? Чи доступна хмарна інфраструктура для тих, хто працює віддалено? Складно бути спеціалістом у всіх технологіях, що створюють мережу інфраструктуру, щоб мати змогу якісно та вчасно контролювати доступи співробітників до необхідних їм ділянок системи.

4. Відсутність видимості мережі.

   Через цю проблему не виникає відчуття цілісності мережі в організації, що зменшує ефективність при виконанні повсякденних задач, а також ускладнює інтеграцію нових розробок у неї.

5. Редагування політик різними групами людей.

   Процес управління ПІБ має контролюватися та відстежуватися. Зміни політик необхідно записувати та поширювати між іншими адміністраторами, щоб не руйнувалась цілісність. Замінювати старі версії на нові, а їх розповсюджувати серед співробітників, щоб ті в свою чергу дотримувались нових положень.

Використання інформаційних технологій при керуванні політиками, з іншого боку, створює безперервний та безпомилковий процес, забезпечуючи дотримання відповідності та вимог в організації. Деякими з методів автоматизації, що допоможуть компанії поліпшити контролювання ПІБ, є:

1. Автоматизація моніторингу – постійна перевірка стану безпеки та відповідності системи, яка дозволяє швидко знаходити та усувати недоліки.
2. Зменшення можливостей для людських помилок – функціонал засобів для управління ПІБ усуває необхідність обробляти великі масиви даних вручну, що зменшує ризики не догледіти помилку.

3. Надання повної прозорості для контролю – постійний збір інформації дозволяє спеціалістам легко проаналізувати стан девайсу, визначити неправильну роботу політики та історію її змін, тобто отримати повну видимість інфраструктури компанії.
4. Встановлення рівнів доступу для внесення змін – усуває помилкові зміни у системі та сповіщає про порушення спеціалістом наявних правил, що дозволяє швидко знаходити працівників, з якими необхідно провести роботу.
5. Підтримка відповідності з моменту початку розробки застосунку – дозволяє безпечно імплементувати в інфраструктуру системи ще не готове ПЗ, щоб одразу відстежувати можливі відхилення у роботі

Програмне забезпечення для керування мережевими ПІБ не лише полегшує робоче життя кожного окремого спеціаліста, а й захищає організацію в цілому. З огляду на розглянуті проблеми ручного управління політиками, постає завдання вибору методу оцінювання результатів змін політик для визначення необхідності автоматизації цього процесу як способу усунення недоліків.

## 2.2 Розробка алгоритму кількісної оцінки результатів зміни мережевих політик безпеки

В методиці, що розробляється в даній роботі, важливою складовою є обчислення кількісних показників, що характеризують поточний стан політик безпеки мережі у компанії. На основі отриманих розрахунків, можна порівнювати стани безпеки системи при різних налаштуваннях політик безпеки. Так можна виконати симуляцію загроз системі при очікуваних показниках та порівняти її

результати з тими, що були отримані за поточних умов. Внаслідок цього, можна отримати розуміння, чи необхідно покращувати робочі процеси шляхом автоматизації.

Надаючи співробітникам необхідні інструменти для активного дотримання стандартів, як обов'язкових, так і добровільних, керівництво заощаджує собі, своїй організації та юридичному відділу багато часу, та грошей. Щоб кількісно оцінити експлуатаційні витрати та ризики, пов'язані з безпекою, керуванням ПІБ мережі вручну (або за допомогою кількох суперечливих інструментів), можна скористатись методом Монте-Карло [11].

В аналізі Монте-Карло кожна змінна в обчисленні виражається не як єдине статичне значення, а як діапазон (нижня межа, верхня межа) і форма (розподіл ймовірностей). Відповідні розрахунки потім виконуються на основі випадково обраного значення з розподілу ймовірностей для кожної змінної протягом багатьох незалежних ітерацій. При цьому результати аналізу також виражаються у вигляді діапазону та розподілу (на відміну від єдиного статичного значення). Потім ітераційно обчислюються результати, щоразу використовуючи різний набір випадкових чисел між мінімальним і максимальним значеннями. У типовому експерименті Монте-Карло цю вправу можна повторити тисячі разів, щоб отримати велику кількість ймовірних результатів. Готові обчислення можна представити як ймовірність, так і як ступінь впливу, тобто з точки зору ризику.

Для доведення необхідності вчасної підтримки відповідності мережевих ПБ встановленим нормативам безпеки в організації, пропонується розрахувати оцінки загроз при двох станах політик у компанії – до внесення змін та після. За приклад буде взято умовну інфраструктуру з третього розділу даної роботи, що має девайси, на яких виявлено проблеми. Для математичного формулювання оцінки ризику мережевих політик безпеки пропонується гібридно поєднати метод попарних порівнянь [12] та раніше зазначений метод Монте-Карло.

Інформаційну систему організації можна оцінити з точки зору конфіденційності, цілісності та доступності [13]. При використанні метода Монте-Карло, ризики для системи можна розрахувати за наступною формулою:

$$Risk_j = \left(W_c C_j + W_i I_j + W_a A_j\right) * P\left(T_j\right) * P\left(V_j\right), \forall j \qquad (2.1)$$

де $W_c$, $W_i$, $W_a$ – це відносна вага факторів тріади CIA для системи j, отримана з експертної оцінки. $C_j$, $I_j$ та $A_j$ – це бінарні змінні, що приймають значення одиниці при вразливості j щодо C, I, A, або нуль при нечутливості. $P\left(T_j\right)$ – вірогідність виникнення загроз для j, $P\left(V_j\right)$ – вірогідність їх експлуатації.

У запропонованій розробці, відповідно до методу попарних порівнянь, для розрахунку ваги критеріїв необхідно сформувати порівняльну матрицю. Це необхідно для визначення рівнів важливості критеріїв та атрибутів. Можливі значення для $a_{ij}$ наведені в таблиці 2.1 – це індивідуальні оцінки, які можуть поставити експерти при оцінці переваги елемента і над j, що сприяє більш ефективному порівнянню при визначенні рівнів важливості атрибутів [13-14].

$$A = \begin{pmatrix} 1 & {}^{1}/_{a_{21}} & {}^{1}/_{a_{31}} \\ a_{21} & 1 & {}^{1}/_{a_{32}} \\ a_{31} & a_{32} & 1 \end{pmatrix} \qquad (2.2)$$

Після цього треба надати матриці А нормальний вид, використовуючи наступну формулу:

$$V_i = \frac{a_{ij}}{\sum_{j=1}^{n} a_j} \qquad (2.3)$$

Значення $W = (w_1, \dots, w_n)^T$ збільшується при обчисленні середнього значення власних векторів:

$$W_j = \frac{V_j}{\sum_{i=n}^{n} V_j} \qquad (2.4)$$

Таблиця 2.1 – Класична шкала оцінки експертів за методом попарних порівнянь

| **Важливість** | **Значення** |
|---|---|
| 1 | Рівноважливі |
| 3 | Слабка перевага |
| 5 | Сильна перевага |
| 7 | Дуже сильна перевага |
| 9 | Макс. перевага |

Метод Монте-Карло дозволяє фахівцям у галузях безпеки IT оцінити всі можливі результати впливу від ризиків в умовах невизначеності. Рисунок 2.1 ілюструє основну процедуру при використанні даного методу. Скориставшись ним, спробуємо розібрати на практиці, як запропонована модель працює для певного випадку (слід зазначити, що всі числа, якими ми будемо оперувати, є випадковими). Використовуючи формули (2.2) та (2.3), побудуємо порівняльну матрицю та її нормалізовану форму, що буде складатись з коефіцієнтів оцінки з незалежних точок зору. Через формулу (2.4) розрахуємо результати для ваг, які можна побачити у таблиці 2.2.


Рисунок 2.1 – Процедура використання методу Монте-Карло

Таблиця 2.2 – Результати методу попарних порівнянь для розрахунку ваг

| | | Матриця порівнянь | | | Нормалізована матриця | | | |
|---|---|---|---|---|---|---|---|---|
| **Назва** | **CIA** | **C** | **I** | **A** | **C** | **I** | **A** | **Ваги** |
| Мережеві політики безпеки | C | 1 | 0.143 | 0.111 | 0.06 | 0.023 | 0.085 | 0.056 |
| | I | 7 | 1 | 0.2 | 0.411 | 0.163 | 0.152 | 0.242 |
| | A | 9 | 5 | 1 | 0.529 | 0.814 | 0.763 | 0.702 |

Розглянувши початковий стан системи з наступного розділу, яка містить ризикові політики у мережі, можна оцінити рівні вразливостей та загроз. Нехай оцінку виносять три експерти і кожний з них має своє бачення рівня відповідності мережевих ПБ у системі. Враховуючи, що 70% від усіх ризикових політик, мають рівні небезпеки високий та критичний, нехай початковий рівень вразливості оцінюватиметься у 6, 7 та 9 балів, а можливі рівні загроз у 5, 8, 10. Ці дані можна подати у вигляді розподілів як (6, 7, 9) та (5, 8, 10). При цьому, експертна оцінка для бажаного випадку, коли всі вимоги підтримки стану політик безпеки виконуються вчасно спеціалістами, становить (2, 4, 5) та (1, 4, 6).

Таблиця 2.3 містить усі необхідні дані для кінцевих розрахунків. Наостанок, для методу Монте-Карло значення P(V) та P(T) приймають випадкові значення у раніше визначених проміжках. Розрахунок відбувається за формулою (2.1). Оскільки необхідно розглянути багато незалежних випадків, то було написано код мовою Python, що спрощує даний процес. Рисунок 2.2 містить його частину з функцією RandomCalc(), де виконуються основні розрахунки, такі як присвоювання випадкових значень змінним pv, pt, а також обчислення формули (2.1). Всі значення записуються в масиви для подальшої обробки.

Таблиці 2.4 та 2.5 демонструють декілька вихідних результатів моделювання для систем в умовах невідповідності стану мережевих ПБ та після внесення необхідних змін. Таблиця 2.6 містить усі фінальні дані, з яких можна робити висновки. Повний код, а також вміст масиву підрахунків ризиків можна подивитись у Додатку А та Додатку Б до роботи.

```
def RandomCalc():
    a1 = input()
    a2 = input()
    b1 = input()
    b2 = input()
    for x in range(0, 1000):
        y = random.randint(0,3)
        if y == 0:
            pv = random.randint(a1,a2)
            pt = random.randint(b1,b2)
        elif y == 1:
            pv = random.randint(a1,a2)
            pt = math.floor(random.uniform(b1,b2) * 1000) / 1000
        elif y == 2:
            pv = math.floor(random.uniform(a1,a2) * 1000) / 1000
            pt = random.randint(b1,b2)
        else:
            pv = math.floor(random.uniform(a1,a2) * 1000) / 1000
            pt = math.floor(random.uniform(b1,b2) * 1000) / 1000
        risk = math.floor((wc * c + wi * i + wa * a) * pv * pt * 1000) / 1000
        arr1.append(pv)
        arr2.append(pt)
        arr3.append(risk)
    print(arr1)
    print(arr2)
    print(arr3)
```

Рисунок 2.2 – Функція RandomCalc() з розробленого коду

Таблиця 2.3 – Попередні результати для фінальних розрахунків

| **Назва** | $W_c$ | $W_i$ | $W_a$ | **Стан** | **Рівень вразливості** | **Ймовірність загрози** |
|---|---|---|---|---|---|---|
| Мережеві політики компанії | 0.056 | 0.242 | 0.702 | Початковий (невідповідність умовам безпеки) | (6, 7, 9) | (5, 8, 10) |
| | | | | Фінальний (над ПБ виконані необхідні зміни) | (2, 4, 5) | (1, 4, 6) |

Таблиця 2.4 – Вихідні результати моделювання для початкового стану мережевих ПБ (при ручному керуванні)

| № | $C_j$ | $I_j$ | $A_j$ | Ймовірність експлуатації вразливості, P($V_j$) | Ймовірність виникнення загрози P($T_j$) | Розрахунок ризиків |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 7.11 | 8.145 | 57.91 |
| 2 | 1 | 1 | 1 | 8 | 7.404 | 59.232 |
| 3 | 1 | 1 | 1 | 6.174 | 5 | 30.87 |
| … | … | … | … | … | … | … |
| 1000 | 1 | 1 | 1 | 6 | 5.075 | 30.45 |

Таблиця 2.5 – Вихідні результати моделювання для бажаного стану мережевих ПБ (при автоматизації управління)

| № | $C_j$ | $I_j$ | $A_j$ | Ймовірність експлуатації вразливості, P($V_j$) | Ймовірність виникнення загрози P($T_j$) | Розрахунок ризиків |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 3.724 | 4 | 14.896 |
| 2 | 1 | 1 | 1 | 2.584 | 5.754 | 14.868 |
| 3 | 1 | 1 | 1 | 2 | 1.743 | 3.486 |
| … | … | … | … | … | … | … |
| 1000 | 1 | 1 | 1 | 2.085 | 5 | 10.425 |

Таблиця 2.6 – Фінальні результати симуляції Монте-Карло

| Назва | Стан | Мін. | Сер. | Макс. | Нижня межа | Верхня межа |
|---|---|---|---|---|---|---|
| Мережеві політики безпеки у компанії | Початковий (невідповідність умовам безпеки) | 30 | 56.46 | 90 | 0% | 25.8% |
| | Фінальний (над ПБ виконані необхідні зміни) | 2 | 11.83 | 30 | 31.2% | 9% |

Для висновку щодо результатів симуляції, слід брати максимальний рівень кожного випадку за 100%. Будемо вважати, що значення, які перетинають 75% від верхньої межі будуть становити серйозні загрози, а недобір до 25% - не критичні. Так ми можемо отримати показники відношення між появою різних загроз. Примітно, що при початковому стані середовища, при не відповідності мережевих ПБ необхідним умовам безпеки, більше чверті від усіх симуляцій становлять загрози максимального рівня, тоді як мінімальні взагалі відсутні. Результати симуляції за умови кінцевого стану системи, коли всі необхідні виправлення виконані, а мережеві ПБ відповідають нормативам компанії, демонструють набагато кращі результати. Третина від усіх можливих загроз знаходяться у нижній межі, а верхня налічує менше 10%.

Такий підхід надає спеціалістам з ІТ та безпеки необхідні дані для кількісної оцінки, а бізнесменам - корисний інструмент для вирішення фундаментальних питань, таких як [15]:

- Операційні витрати пов'язані з безпекою, керуванням ПІБ вручну, що будуються з урахуванням кількості взаємодій з політиками, затраченого часу та витрат на персонал.
- Ризики, наявні при повному обсязі роботи з ПІБ, які засновані на оцінках часу, коли мережа зазнає негативного впливу від проблем
- Цінність додаткових інвестицій у рішення з управління ПІБ для зниження операційних витрат і зниження ризику безпеки

Застосовуючи запропонований алгоритм оцінки результатів змін мережевих політик безпеки, можна зрозуміти, чи справляються спеціалісти ІБ в компанії з керуванням політиками. Якщо висновки незадовільні, то можливе рішення проблеми – це початок використання ПЗ для автоматизації управління мережевими ПБ.

## 2.3 Порівняння та вибір програмного забезпечення на ринку ІТ

Як було зазначено раніше, на сьогоднішній день існує велика кількість рішень, що допомагають автоматизувати роботу з безпекою в організації. Однак, саме це може стати проблемою при виборі єдиного, адже багато компаній-вендорів впроваджують схожий функціонал у свої продукти. Для подальшої роботи та розробки методики автоматизації ПІБ, нами було проаналізовано декілька продуктів, що конкурують між собою в ІТ секторі, і створено таблицю 2.7, що містить їх порівняльну характеристику [16-17].

Таблиця 2.7 - Функціонал засобів ПЗ для керування ПІБ

| **Рішення** | **Palo Alto** | **Tufin** | **FireMon** |
|---|---|---|---|
| Ринковий сегмент | Малі – 20%, середні – 33%, великі - 47% | Малі – 13%, середні – 6%, великі - 81% | Малі – 14%, середні – 14%, великі - 71% |
| Платформа | SaaS | SaaS | Windows, SaaS |
| Підтримка | Робочі години | Робочі години | Цілодобова |
| Переваги | Кластерізація системи, інтуїтивно-зрозумілий інтерфейс, автоматизація робочих процесів для створення політик, стабільність рішення, нескладне налаштування | Оцінка безпеки, можливість керування брандмауерами, підтримка багатьох рішень від третіх сторін, оптимізація непотрібних/не використовуваних правил, автоматизація політик, гнучка система звітування та API, дуже дружній інтерфейс, картографія мережі, надання видимості | Оцінка безпеки, ідентифікація не використовуваних правил, підтримка мови SQL, повне логування подій, нескладний інтерфейс |

Продовження таблиці 2.7

| | | | |
|---|---|---|---|
| Недоліки | Потрібно мати розуміння та навички для роботи, наявність багів, потребує покращення інтернет-з'єднання, слабка інтеграція з третіми сторонами, обмежені можливості звітування | Веб-інтерфейс потребує модернізації, використання всіх можливостей API потребує навичок, не найкраще рішення для глибокого аудиту | Закритість рішення та відсутність документації, проблеми зі стабільністю, необхідне покращення системи звітування, складність використання деяких функцій, відстає від конкурентів за функціоналом |

Враховуючи всі переваги та недоліки, для демонстрації реалізації на прикладному рівні було обране рішення від компанії Tufin. На нашу думку, воно найкраще підходить під цілі даної роботи, завдяки широкому спектру можливостей та несерйозним недолікам, що дозволяють автоматизувати роботу.

## Висновки до розділу 2

Досліджено методи управління та роботи з мережевими політиками безпеки, окреслено основні проблеми під час ручного керування мережними змінами, а також переваги від автоматизації.

Розроблено метод кількісної оцінки результатів змін мережевих ПБ в умовній інформаційній системі з наступного розділу роботи, на основі поєднання моделі Монте-Карло та методу попарних порівнянь. Для виконання головних розрахунків розроблено код мовою Python. Проведено аналіз отриманих результатів, мета яких - це зробити висновки чи необхідне застосування ПЗ для автоматизації управління мережевих ПБ в компанії.

Проаналізовано декілька програмних продуктів для автоматизації управління мережевими ПБ, серед яких пріоритет віддався продукту від компанії Tufin. Оскільки математична оцінка спонукає до автоматизації, то постає необхідність у розробці методики для виконання цього процесу та практичній демонстрації.

# 3 РОЗРОБКА МЕТОДИКИ ДЛЯ АВТОМАТИЗАЦІЇ УПРАВЛІННЯ МЕРЕЖЕВИМИ ПОЛІТИКАМИ БЕЗПЕКИ

## 3.1 Розробка методів для автоматизації роботи з політиками безпеки

Перед початком внесення будь-яких змін в мережу інфраструктури компанії, необхідно розробити список плану дій, необхідних для автоматизації управління політиками безпеки в організації. Це потрібно для того, щоб мати уявлення про хід майбутніх імплементацій. Отже, при практичному застосуванні варто притримуватись наступної методики:

**1. Аналіз поточного стану безпеки.**

Для оцінки початкового стану і впливу від змін мережевих політик безпеки, використовується розроблений у розділі 2.2 алгоритм оцінювання результатів. Треба проаналізувати початковий стан безпеки мережі, на основі якого оцінити поточні розподіли рівнів вразливостей та загроз. Після цього отримати значення очікуваних ризиків через пропущені зміни у політиках. Повторити симуляцію з бажаними розподілами і порівняти результати. Якщо вони незадовільні, то є необхідність звертатись до автоматизації.

**2. Ревізія мережевих політик безпеки**

По-перше, треба визначити, які правила повторюються, є взаємовиключними, вже непотрібні чи застарілі, мають багато привілеїв, можливо потребують нової сертифікації. Також варто поглянути на список девайсів, що обслуговуються, там так само можна знайти неактуальні IP-адреси чи сутності.

3. **Визначити дії, що будуть прийняті.**

Коли ми вже маємо список мережевих політик, що знижують рівень безпеки системи, то необхідно якимось чином їх змінити. Найпростішим рішенням буде видалити такі правила, скоріш за все ПЗ навіть не дасть зробити дію, що буде нести в собі зайві ризики, а отже можна не перейматись за зниження загального рівня захищеності. Окрім цього, можна позбавити політики сертифікації, модифікувати їх чи об’єднати з повторюваними.

4. **Створити запити на внесення змін.**

Проаналізувавши політики інфраструктури на вразливості та обравши відповідні стратегії щодо їх усунення, необхідно створити запити на внесення змін.

5. **Відправити на розгляд відповідальним за це адміністраторам.**

Оскільки одна людина фізично не може відповідати за безпеку всієї системи, має передбачатись можливість розділити зони відповідальності поміж різних адміністраторів. Це суттєво знижує ризики, виключаючи зайві помилки через людський фактор. Окрім цього, такий підхід дозволяє іншим працівникам створювати запити на доступ, після чого, більш відповідальні люди будуть аналізувати його складову та приймати відповідні рішення, що суттєво оптимізує роботу в компанії.

6. **Провести аналіз результатів, переглянути нову оцінку рівня безпеки.**

Після будь-яких змін варто проводити перевірку вагомості результатів - варто переглядати, як саме виправлена політика відрізняється від своєї попередньої версії. Окрім того, це дозволяє запевнитись, що запит був розглянутий та прийнятий. Після цього варто оцінити новий рівень безпеки

інфраструктури, який може бути задовільним, або спонукати повернутись до першого кроку даного плану. На додачу, можна знову повернутись до алгоритма оцінки результатів змін (розд. 2.2) та провести його вже на фінальному стані системи.

**7. Аудит.**

Для того, щоб не було плутанини у майбутньому, варто провести аудит та згенерувати репорт, що буде містити нещодавні зміни. Ним можна буде скористатись як і при наступній потребі у внесенні змін до політик, так і для звітування перед керівництвом організації.

Розроблений план надалі буде використаний для демонстрації автоматизації управління політиками в компанії на практиці.

## 3.2 Огляд застосунку Tufin Orchestration Suite

Tufin дає можливість організаціям із гібридними мультивендорними середовищами досягати видимості мережевих політик безпеки, організовувати автоматизації їх змін та постійно підтримувати відповідність, впроваджуючи нові рішення безпеки в робочі процеси.

Діаграма на рисунку 3.1 показує як Tufin Orchestration Suite взаємодіє з інфраструктурою в цілому. Згори схеми можна побачити програми, що є головними для кожної великої компанії. Знизу ж повна мережева інфраструктура: від звичайної фізичної мережі до приватного/публічного хмарного рішення. TOS – це проміжне ПЗ, що дозволяє розробникам застосунків і мережевим

адміністраторам вносити зміни до мережевої інфраструктури безпечно, точно та швидко.

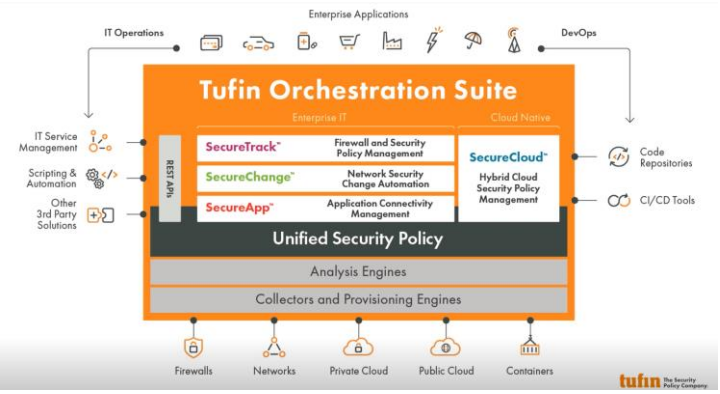



Рисунок 3.1 - Поєднання TOS з інфраструктурою [18]

Головними IT-рішеннями, з яких складається TOS наразі є:

1) SecureTrack
2) SecureChange

SecureTrack – це централізоване рішення керування брандмауером, яке потрібне для своєчасного забезпечення відповідності нормам та вимогам безпеки. ST надає видимість, підтримку і повний контроль підключень серед мережі організації, які необхідні для її захисту через брандмауери, маршрутизатори та комутатори.

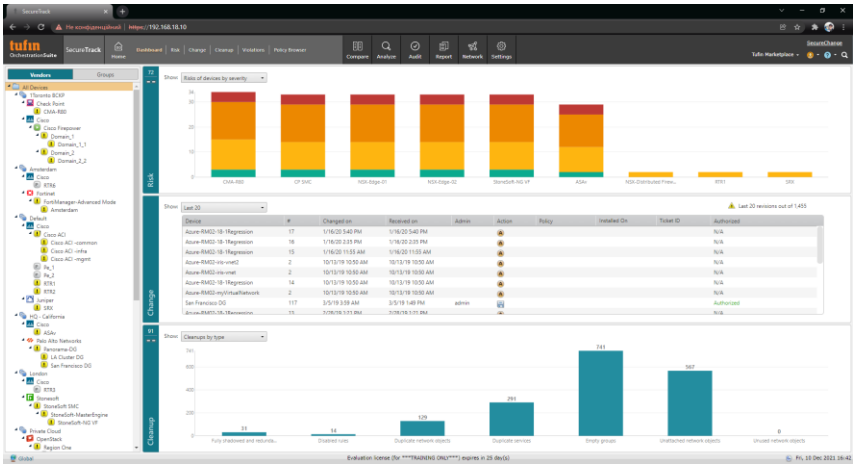


Рисунок 3.2 - Інтерфейс SecureTrack

Серед основних властивостей [19]:

- Надання повної видимості – візуалізація, що допомагає створити чітке уявлення про усі підключення у мережі.
- Створення центральної, єдиної бази ПІБ – дозволяє встановити розмежувальну лінію дозволеного та заблокованого трафіку між зонами безпеки.
- Готовність до аудиту в будь-який момент – дозволяє швидко створювати різноманітні налаштовані звіти, що будуть підходити під вимоги багатьох нормативних стандартів (PCI DSS, тощо).
- Керування політиками брандмауерів – пропонує окреме сховище для правил і об’єктів брандмауерів для подальшого спрощення їх керування.
- Встановлення та усунення несправностей з’єднань, відсутність яких заважає роботі бізнесу – забезпечує найточніше моделювання топології та аналіз шляху.
- Виявлення в режимі реального часу ризикованого доступу та порушень політик інформаційної безпеки.

Tufin SecureChange забезпечує автоматизацію та оркестрацію політик, даючи можливість технічним спеціалістам впроваджувати точні зміни мережі за лічені хвилини замість днів.

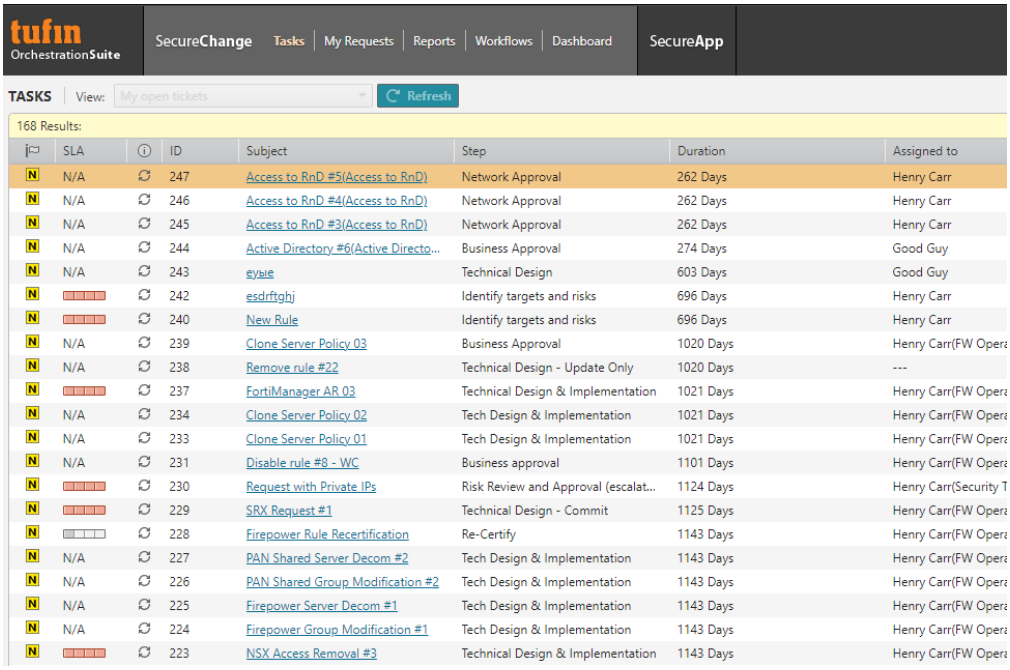



Рисунок 3.3 – Інтерфейс SecureChange

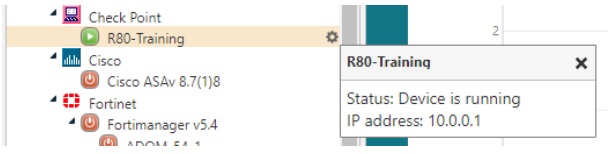
Основні властивості SC:

- Максимізує гнучкість керування змінами мережі, пропонуючи наскрізну автоматизацію їх впровадження.
- Підтримка відповідності політик завдяки активній оцінці ризиків.
- Аудит - система завжди готова до ревізії завдяки функціям автоматичного аудиту змін мережі.
- Гнучкі робочі процеси та параметри конфігурації – завдяки API можна легко розширити функції SC та інтегрувати їх із сторонніми рішеннями.

## 3.3 Практичне застосування розробленої методики

Встановивши операційну систему TufinOS та ПЗ TOS (методика підготовки та налаштування середовища для роботи розміщена у Додатку В до роботи), можна приступати до роботи. Згідно першого пункту розробленого нами плану - перед виконанням очистки нашої мережі від правил, які TOS вважає непотрібними, необхідно виконати підготовку. На рисунку 3.2 можна побачити наявні у системі проблеми з політиками, на основі яких визначались експертні оцінки розподілів рівнів вразливостей та загроз у розділі 2.2 даної роботи.

Використання методу показало, що для нашої інформаційної системи доречна автоматизація. Отже, для початку треба визначити ті самі неважливі правила та об’єкти, до яких вони застосовані. По-друге, посилити правила з надмірними дозволами. Найкращий шлях для виконання попередніх дій буде перейти до сторінки Home -> Dashboard, як на рисунку 3.4 (а, б), та вибрати об'єкт, що нас цікавить. В нашому випадку, це буде шлюз Check Point R80-Training. Обравши його, на ілюстрації 3.5 ми одразу бачимо ряд правил, що потребують корегування – перше використовує протокол SNMP та має забагато привілеїв, тоді як для другого не збираються логи. Окрім цього, перейдемо до вкладки Home -> Policy Browser (рис. 3.6), та знайдемо усі правила на цьому ж девайсі, що мають забагато привілеїв:

а) 

б) 

Рисунок 3.4 (а, б) – Інтерфейс панелі Dashboard для пристрою R80

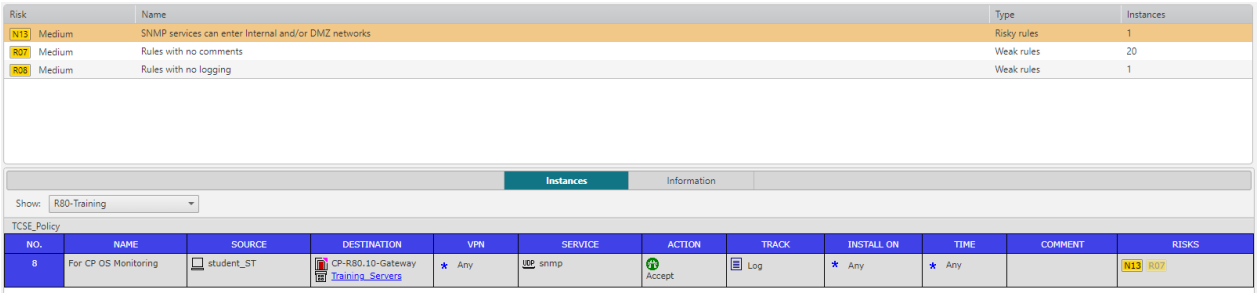



Рисунок 3.5 – Список ризикованих правил на пристрої R80

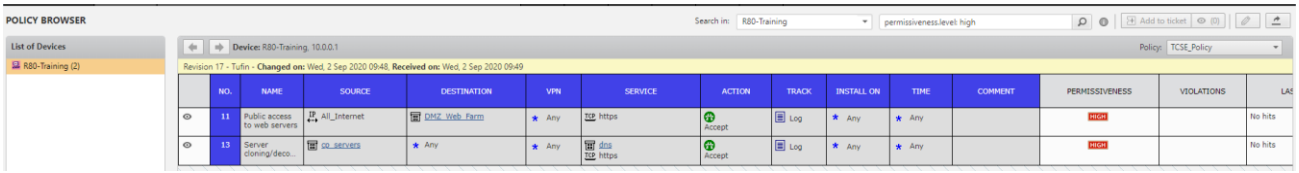



Рисунок 3.6 – Правила із завищеними привілеями

Визначивши вразливі політики у системі, ми звертаємось до другого пункту розробленої методики. Для зниження рівня дозволеності, перейдемо до Автоматичного генератору політик у вкладці Audit -> APG, створимо нове завдання, оберемо девайс, що нас цікавить, знайдемо правило з міткою High, як на рисунку 3.7, заповнимо поле для назви нашої роботи та налаштуємо збір логів. На ілюстрації 3.8 ми можемо побачити створене, але ще не виконане завдання. Тиснемо на Results, щоб дізнатись подробиці, та отримуємо граф, як на рисунку 3.9. На даному етапі пропонується вибір, що саме зробити з політикою. Як видно з рисунку графу, ми можемо навіть підвищити рівень до 100, зробивши з усіх правил одне глобальне, але треба обрати оптимальний варіант – нехай це буде збірка з 66 позицій, рівень дозволів кожної з яких не буде перевищувати 32. Налаштовуємо та завершуємо завдання, отримуючи результат, як на ілюстрації 3.10. Експортований звіт про всі зміни від завдання APG прикладається як Додаток Г до дипломної роботи.

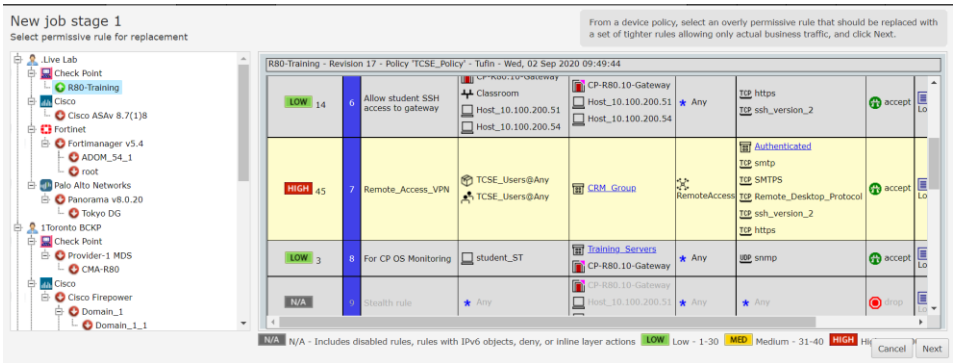



Рисунок 3.7 - Інтерфейс панелі APG для пристрою R80

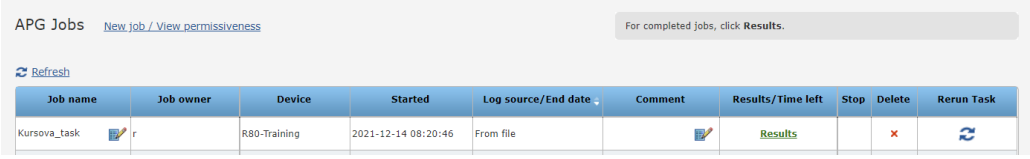



Рисунок 3.8 – Список створених завдань APG

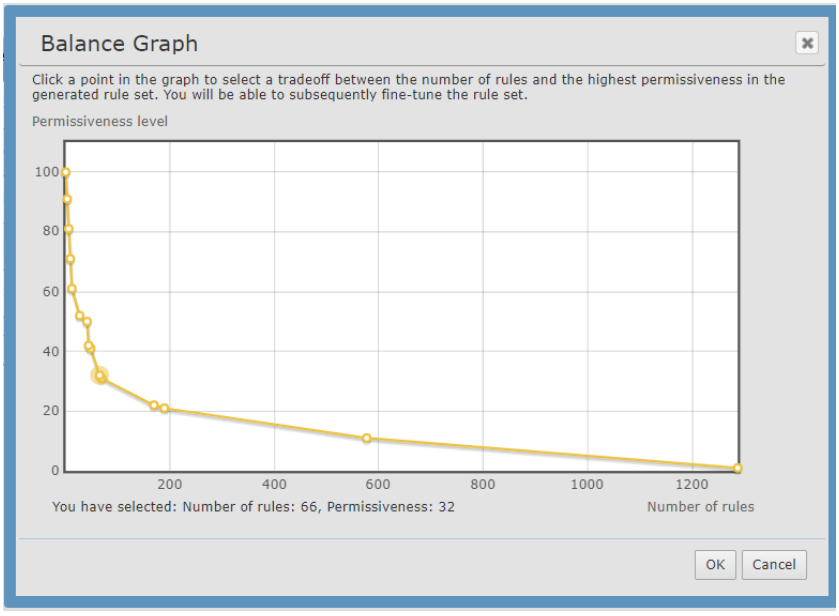



Рисунок 3.9 – Граф рівню дозволів політик

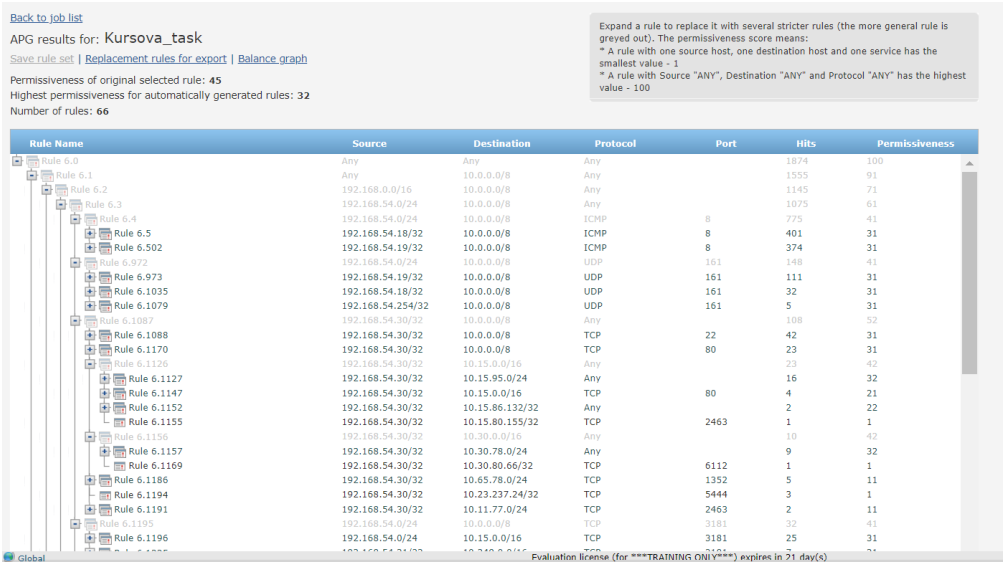



Рисунок 3.10 – Результат роботи функції APG

Згідно третього пункту плану, переходимо до створення запитів на внесення змін. Повертаємось до правил №8 та №4 з рис. 3.5, модифікуємо перше та видалимо останнє. Знайдемо їх, перейшовши до Policy Browser вікна. Почнемо з найпростішого – видалення. Оберемо правило, що нас цікавить, та натиснемо на Add to ticket (рис. 3.11). Після цього обираємо іконку ока та переходимо до наступної сторінки. Обираємо робочий процес для видалення політики та створюємо задачу (рис. 3.12). Запит створений, і оскільки можливості ST не дозволяють нам продовжити цей процес, то нас автоматично переводить на веб-інтерфейс SC. Підтверджуємо створену задачу, тим самим перенаправляючи її до відповідальних за мережеві політики осіб.


Рисунок 3.11 – Інтерфейс Policy Browser та правило №4

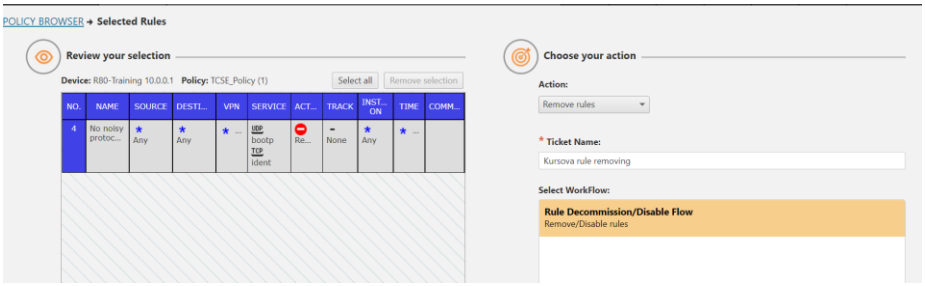



Рисунок 3.12 – Вибір робочого процесу для видалення політики

Отже, ми переходимо до четвертого пункту розробленого плану. Наступні ілюстрації потрібно вважати за дії технічного спеціаліста іншої зони відповідальності, тому змінюємо обліковий запис користувача та переходимо до панелі Tasks. На рисунку 3.13 видно, що ми отримали нове завдання. Переходимо до його виконання, що відбувається в декілька кроків, на кожний з яких, за бажанням, може бути назначена окрема особа (рис. 3.14). За замовчуванням використовується правило двох рук – одна й та сама особа, яка не є супер користувачем, не може створити та виконати свої ж зміни.

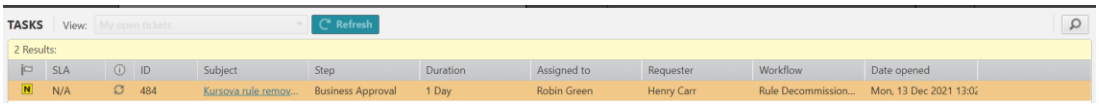



Рисунок 3.13 – Нове завдання для обробки

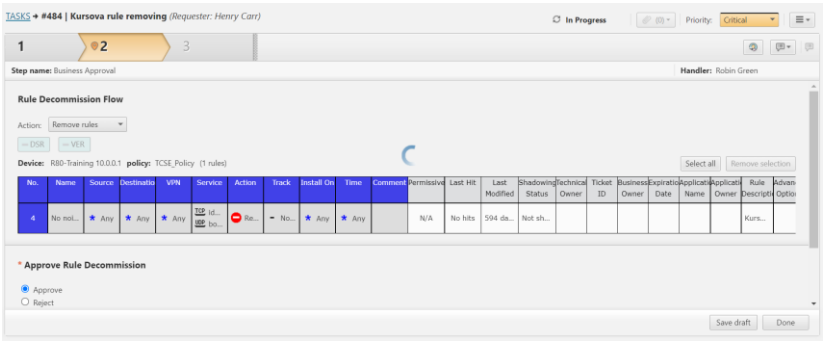
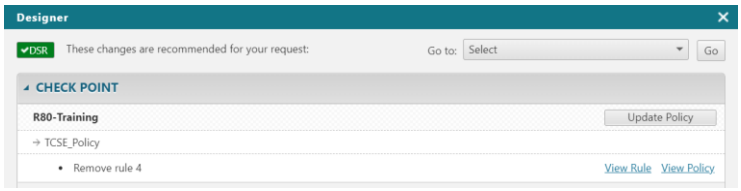



Рисунок 3.14 – Другий етап виконання завдання

На третьому етапі можна побачити дві дуже корисні функції від TOS, продемонстровані в ілюстрації 3.15 (а, б). Починати необхідно з дизайнера, що автоматично обчислює зміни правила, необхідні для реалізації запиту, а головне – які не створять нових вразливостей для інфраструктури. Другий – це верифаєр, який використовують після налаштування та імплементації політики в дизайнері, тим самим перевіряючи, чи внесені зміни успішно реалізовані.

а) 

б) 


Рисунок 3.15 (а, б) – Designer та Verifier при виконанні завдання

З видаленням завершено, тому повернемось до правила №8. В ньому треба модифікувати кінцеві точки призначення трафіку. Процес майже ідентичний з попереднім, але є пара відмінностей. Для початку, необхідно обрати інший робочий процес, а саме – модифікацію, як на рисунку 3.16. Окрім цього, з боку користувача, що створює завдання, з'являється додаткова задача – вказати які саме змінні його цікавлять (рис. 3.17). Це робиться за допомогою полів Source/Destination/Service. В нашому випадку обираємо поле Destination. Відправляємо завдання на обробку відповідальній особі та знову змінюємо обліковий запис користувача. На рисунку 3.18 також бачимо відмінність – є можливість не тільки відхилити завдання, а й додати свої корективи, після чого схвалити. Ми не будемо нічого змінювати, а просто приймемо.

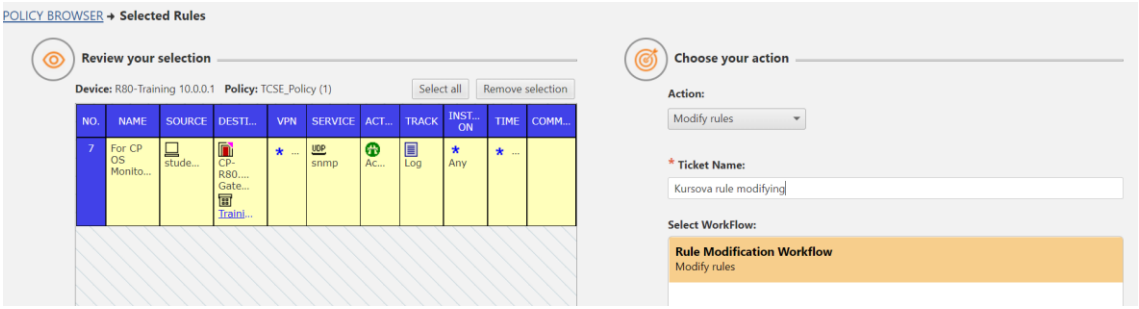



Рисунок 3.16 - Вибір робочого процесу для модифікації політики

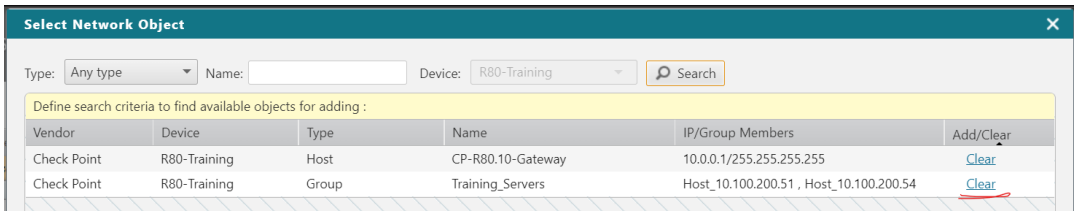



Рисунок 3.17 – Внесення корективів для зміни політики

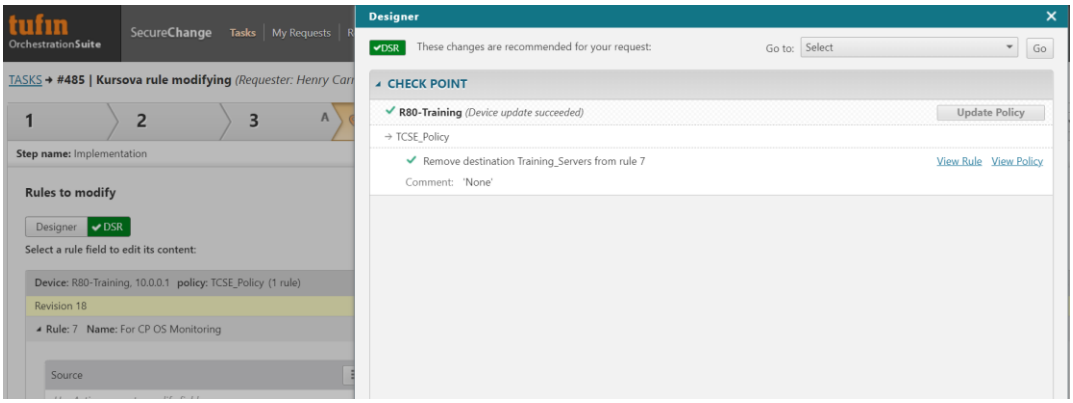



Рисунок 3.18 – Можливість зміни запиту модифікації політики спеціалістом

Згідно з п’ятим, передостаннім пунктом розробленої методики, необхідно переглянути результати дій. Для цього використаємо дві функції ST – стандартний моніторинг (рис. 3.19) та порівняння ревізій (рис. 3.20 та 3.21). Порівнявши діаграми до/після внесених змін, бачимо, що кількість вразливостей на девайсі знизилась з трьох до одної. Перейдемо до ревізій, де за датами

вирахуємо, що необхідні для аналізу – це три останніх. Ревізія №18 включає зміну з видаленням, а №19 – обидві зміни: і видалення, і модифікацію, отже доцільно одразу протиставити №19 з №17. На наступних скріншотах видно зміни, що потерпіли політики №4 та №8.

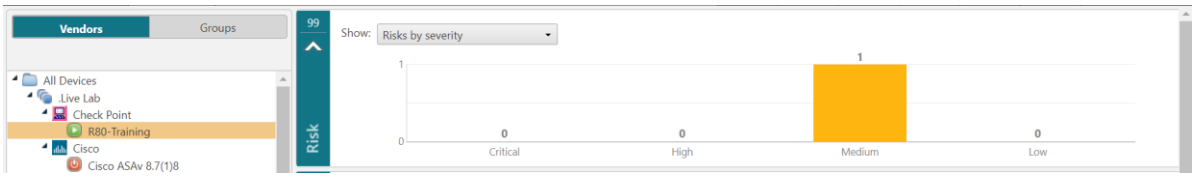



Рисунок 3.19 - Інтерфейс панелі Dashboard для пристрою R80 після внесених змін

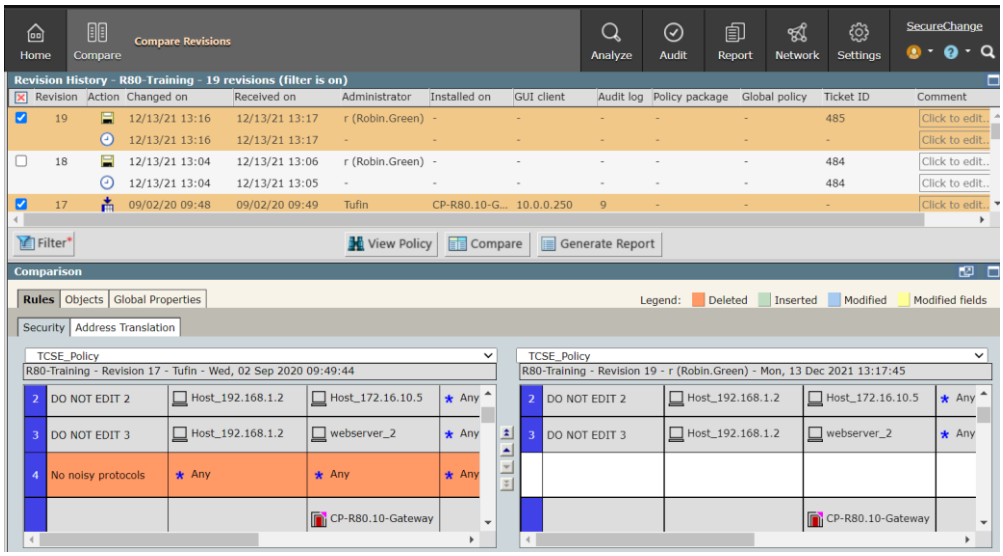



Рисунок 3.20 – Порівняння ревізій, політика №4


Рисунок 3.21 – Порівняння ревізій, політика №8

Вище була показана лише невелика частина того, які можливості надає використання зв'язки ST та SC під час роботи з ПІБ. Наприклад, адміністратор отримує завдання – позбавити сертифікації непотрібні правила за допомогою. В контексті Tufin це буде означати вимкнення дійсності правил до моменту повторного перегляду їх статусу. За допомогою гнучкого пошукового меню можна легко знайти політики, що не використовувались більше ніж півроку, але все ще залишаються сертифікованими, як на рисунку 3.22, після чого виконати задачу. Або інший варіант завдання – адміністратор дізнається, що певний сервер списується і більше нема потреби в обслуговуванні Tufin, його треба видалити. Завдяки робочому процесу Server Decommission Request, можна легко створити задачу на видалення непотрібної IP-адреси пристрою з топології, уникаючи проблем з розумінням у майбутньому (рис. 3.23).

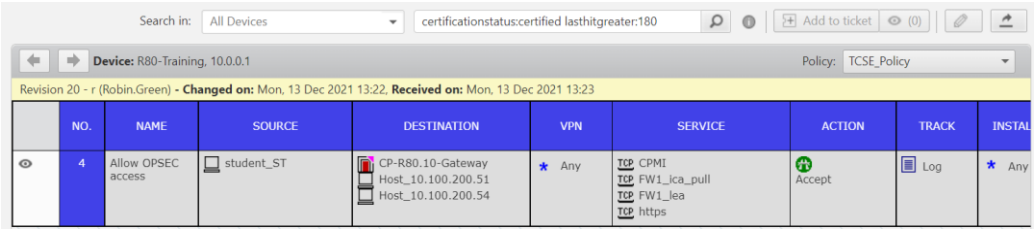



Рисунок 3.22 – Демонстрація можливостей пошуку

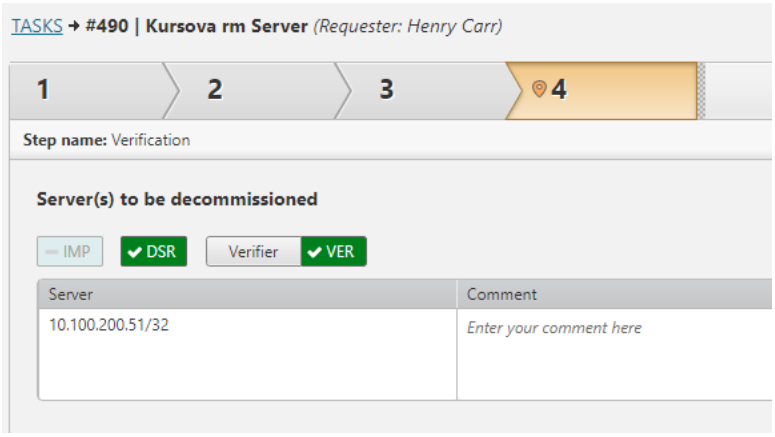



Рисунок 3.23 – Демонстрація робочого процесу Server Decommission Request

Згідно останнього пункту розробленої нами методики, необхідно згенерувати звіти щодо виконаної роботи. На ST в якості звіту буде порівняння ревізій, його можна побачити у Додатку Д до цієї дипломної роботи. На SC можна провести аудит оброблених завдань за певний проміжок часу. Також згенеруємо звіт, що буде містити всі зміни, які виконувались у рамках цієї дипломної роботи, та прикладемо у якості ілюстрації 3.24.

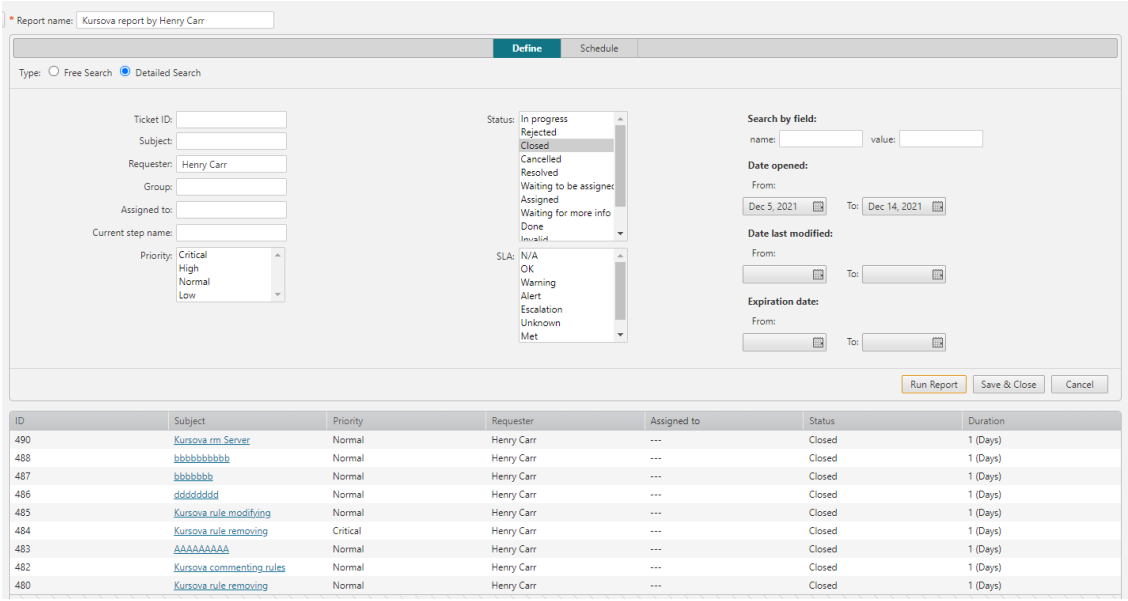



Рисунок 3.24 – Звіт з SecureChange

## Висновки до розділу 3

Розроблено методику автоматизації управління політиками інформаційної безпеки мережевих змін.

Оглянуто застосунок Tufin Orchestration Suite та його функціональні можливості.

Налаштовано середовище для виконання роботи в результаті інсталяції та налаштування операційної системи TufinOS, та встановлення ПЗ TOS.

На основі розробленої методики, продемонстровано її практичне застосування, використовуючи весь необхідний функціонал TOS ST та SC. В результаті зроблено висновки, що, використовуючи прописані методичні вказівки, вдається досягти поставленої цілі, а саме - провести автоматизацію управління ПІБ.

# ВИСНОВКИ

В ході написання роботи було підтверджено, що на сьогоднішній день однією з найголовніших завдань будь-якої організації є створення та впровадження ряду якісних політик інформаційної безпеки, включно з мережевими ПБ, а також найефективніше покриття повного спектру вразливостей системи завдяки грамотному поєднанню правил між собою.

Було проаналізовано статистичні дані, що стосуються імплементації політик та доводять стрімкий розвиток у використанні мережевих ПІБ, який збільшується з кожним роком. Враховуючи виявлену залежність між запровадженими засобами безпеки та успішними проєктами, що несуть прибуток, така тенденція зрозуміла та має заохочуватись надалі.

Під час дослідження було розглянуто загальні проблеми при ручному керуванні ПІБ. Такий підхід, безпосередньо пов'язаний із людським фактором, незмінно приводить до значних затрат уваги та часу. Після цього, для порівняння було розглянуто переваги від автоматизації, щоб запропонувати дане рішення як розв’язок для знайдених проблем.

Було обрано метод оцінки результатів змін мережевих політик безпеки через математичний підхід, а саме - спирання на метод попарних порівнянь та модель Монте-Карло, а також розроблено програмний код для розрахунку результатів. Аналіз отриманих висновків можна використовувати, щоб зрозуміти, чи варто використовувати автоматизацію для покращення стану безпеки.

В ході порівняння декількох застосунків, спираючи на відгуки від користувачів, для майбутньої практичної демонстрації було обрано рішення

Tufin Orchestration Suite, призначення якого спрямоване на автоматизацію управління політиками безпеки в організації.

В ході написання фінального розділу було розроблено та запропоновано методику автоматизації, спираючись на яку можна автоматизувати робочі процесу в компанії. Було інстальовано окрему систему Tufin OS, встановлено і налаштовано на ній TOS. Використання можливостей даної платформи цілком підтвердило наші припущення щодо суттєвого спрощення щоденної взаємодії системного адміністратора з мережевими ПІБ. За допомогою запропонованої нами сукупності взаємозв'язаних кроків було практично доведено і показано хід автоматизації, із використанням ПЗ від компанії Tufin.

Підсумовуючи все вищесказане, зазначимо, що запропонований підхід при роботі з політиками безпеки, а саме - перехід від ручного керування до автоматизованого, вважаємо необхідним та таким, що має великий потенціал для збільшення прибутків шляхом зменшення зайвих ризиків. Даний метод є гарним доповненням до інших засобів посилення безпеки в організації будь-якого розміру та формату, дозволяючи полегшити роботу інженерам безпеки та посилити її результативність.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ


[1] Network Security Policies Templates. [Електронний ресурс] : веб-сайт / PURPLESEC – Режим доступу: https://purplesec.us/resources/network-security-policies/

[2] Smihily M. ICT security in enterprises, EU-27, 2010 [Текст] / M. Smihily // Eurostat. – 2011. – с. 1-12.

[3] ICT security in enterprises, EU-27, 2019 [Електронний ресурс] : веб-сайт / EUROSTAT – Режим доступу: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises#Documents_on_measures.2C_practices_or_procedures_on_ICT_security

[4] Kaspersky Lab Survey, 2018 [Електронний ресурс] : веб-сайт / KASPERSKY – Режим доступу: https://usa.kaspersky.com/about/press-releases/2018_one-in-ten-employees-are-aware-of-their-organizations-it-security-policies

[5] Roles and Responsibilities Policy, 2019 [Електронний ресурс] : веб-сайт / WUSTL – Режим доступу: https://informationsecurity.wustl.edu/roles-and-responsibilities-policy/

[6] “Моделювання та верифікація політик безпеки управління доступом в операційних системах” [Текст]: навч. посібник / П.М. Девянін, Д.В. Єфремов, В.В. Кулямін, О.К. Петренко, О.В. Хорошилов, І.В. Щепетков. – М.: Гаряча лінія – Телеком, 2019. – с. 33-40

[7] Security Policy. Development and Implementation. [Електронний ресурс] : веб-сайт / NCES / National Center for Education Statistics – Режим доступу: https://nces.ed.gov/pubs98/safetech/chapter3.asp

[8] Security Policy and Objectives. [Електронний ресурс] : веб-сайт / IBM – Режим доступу: https://www.ibm.com/docs/en/i/7.1?topic=security-policy-objectives

[9] Developing a Security Policy. [Електронний ресурс] : веб-сайт / informIT – Режим доступу: https://www.informit.com/articles/article.aspx?p=25934

[10] Policy management problems. [Електронний ресурс] : веб-сайт / PowerDMS – Режим доступу: https://www.powerdms.com/policy-learning-center/five-policy-management-problems-and-their-solutions

[11] Monte Carlo Simulation. [Електронний ресурс] : веб-сайт / IBM / IBM Cloud Learn Hub – Режим доступу: https://www.ibm.com/cloud/learn/monte-carlo-simulation

[12] Saaty, T. L. Fundamentals of decision making and priority theory with the analytic hierarchy process [Текст] / T.L. Saaty. – Pittsburgh: Rws Publications, 2000. – 83-97с.

[13] Sheikhpour, R. M. N. Mapping Approach of ITIL Service Management Processes to ISO/IEC 27001 Controls [Текст] / R.M.N. Sheikhpour. – NY: Journal of Computing, 2011. – 117–124с.

[14] Multi-attribute evaluation and selection of sites for agricultural product warehouses based on an Analytic Hierarchy Process [Текст] / García, J., Alvarado, A., Blanco, J., Jiménez, E., Maldonado, A., & Cortés, G. – Amsterdam: Computers and Electronics in Agriculture, 2014. – 60–69с.

[15] Brink D.E. Operational cost, security-related risk: quantifying the value of network security policy management [Текст] / D.E. Brink // Aberdeen. – 2020. – с. 2-6

[16] FireMon vs. Tufin Report from PeerSpot. [Електронний ресурс] : веб-сайт / PeerSpot – Режим доступу: https://www.peerspot.com/products/comparisons/firemon_vs_tufin

[17] Palo Alto Networks Panorama vs. Tufin Report from PeerSpot. [Електронний ресурс] : веб-сайт / PeerSpot – Режим доступу: https://www.peerspot.com/products/comparisons/palo-alto-networks-panorama_vs_tufin

[18] “Introduction to Tufin Orchestration Suite - TOS Classic”. [Електронний відео-ресурс] : веб-сайт / tufin Academy – Режим доступу: https://lms.tufin.com/learn/lp/215/tcse-1-tos-classic-security-policy-management-basics

[19] Офіційна документація Tufin Orchestration Suite. [Електронний ресурс] : веб-сайт / tufin – Режим доступу: https://forum.tufin.com/support/kc/latest/Content/Suite/home.htm

[20] Tufin Portal: TCSE Training. [Електронний ресурс] : веб-сайт / tufin – Режим доступу: https://portal.tufin.com/

# ДОДАТОК А
# КОД РОЗРОБЛЕНОЇ ПРОГРАМИ

```
import random
from statistics import mean
import math
import numpy

c = 1
wc = 0.056
i = 1
wi = 0.242
a = 1
wa = 0.702
arr1 = []
arr2 = []
arr3 = []

def RandomCalc():
        a1 = input()
        a2 = input()
        b1 = input()
        b2 = input()
        for x in range(0, 1000):
                y = random.randint(0,3)
                if y == 0:
                        pv = random.randint(a1,a2)
                        pt = random.randint(b1,b2)
                elif y == 1:
```

```
                pv = random.randint(a1,a2)
                pt = math.floor(random.uniform(b1,b2) * 1000) / 1000
            elif y == 2:
                pv = math.floor(random.uniform(a1,a2) * 1000) / 1000
                pt = random.randint(b1,b2)
            else:
                pv = math.floor(random.uniform(a1,a2) * 1000) / 1000
                pt = math.floor(random.uniform(b1,b2) * 1000) / 1000
            risk = math.floor((wc * c + wi * i + wa * a) * pv * pt * 1000) / 1000
            arr1.append(pv)
            arr2.append(pt)
            arr3.append(risk)
        print(arr1)
        print(arr2)
        print(arr3)

def Math():
        minimum = min(arr3)
        maximum = max(arr3)
        average = mean(arr3)
        print(minimum)
        print(maximum)
        print(average)
        print('\n')
        lower_bound = maximum*0.25
        upper_bound = maximum*0.75
        low_risk = 0
        high_risk = 0
        for x in arr3:
            if x < lower_bound:
                low_risk = low_risk + 1
```

```
            elif x > upper_bound:
                high_risk = high_risk + 1
    print(low_risk / 10)
    print(high_risk / 10)

def main():
    RandomCalc()
    Math()

main()
```

# ДОДАТОК Б
# ВМІСТ МАСИВУ РОЗРАХОВАНИХ РИЗИКІВ

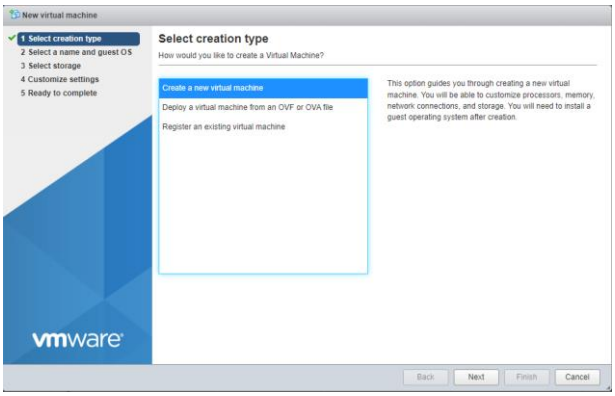
[20.0, 9.0, 15.0, 14.896, 14.868, 3.486, 2.0, 24.984, 11.333, 18.851, 15.66, 11.639, 10.0, 14.79, 12.0, 12.0, 3.0, 4.467, 18.119, 17.901, 9.217, 4.206, 10.0, 24.0, 19.622, 6.0, 18.492, 11.928, 3.876, 11.192, 4.0, 12.0, 15.137, 17.307, 18.816, 15.0, 23.255, 4.336, 3.363, 16.361, 24.036, 15.0, 9.0, 11.577, 2.486, 3.31, 5.822, 6.0, 6.144, 12.0, 16.736, 2.0, 3.0, 4.826, 8.855, 11.531, 22.755, 7.788, 10.05, 20.0, 16.9, 28.164, 14.489, 8.0, 4.43, 4.356, 6.792, 7.694, 12.0, 6.0, 6.471, 9.626, 12.218, 5.571, 3.878, 17.752, 5.636, 23.292, 18.692, 4.0, 10.0, 13.955, 18.42, 5.0, 14.91, 11.211, 11.275, 10.308, 19.73, 6.907, 17.088, 6.318, 5.0, 13.536, 10.0, 11.83, 28.955, 12.735, 16.565, 9.538, 3.0, 11.646, 16.05, 12.0, 4.83, 25.0, 21.595, 12.0, 18.004, 19.95, 6.013, 2.0, 8.882, 11.46, 15.612, 18.228, 24.544, 8.0, 4.408, 13.052, 15.582, 6.44, 20.465, 12.26, 25.0, 2.787, 11.52, 9.747, 8.0, 22.561, 9.305, 2.206, 14.579, 12.119, 11.997, 13.996, 10.944, 14.253, 10.0, 10.72, 10.485, 9.078, 3.942, 12.0, 5.144, 10.684, 27.235, 11.949, 12.0, 9.0, 16.32, 12.385, 7.4, 6.607, 16.0, 24.02, 20.903, 3.455, 20.0, 10.0, 9.228, 10.0, 15.109, 6.708, 8.86, 8.0, 20.555, 5.667, 2.974, 4.0, 12.984, 14.516, 4.531, 15.0, 14.086, 10.194, 16.269, 12.143, 19.46, 6.25, 8.876, 20.0, 6.902, 14.934, 10.256, 8.0, 18.0, 8.738, 5.0, 11.542, 4.09, 4.504, 5.23, 22.025, 2.843, 4.732, 6.0, 12.0, 5.856, 6.018, 14.508, 11.832, 12.696, 7.869, 10.363, 28.164, 3.268, 14.928, 4.148, 16.686, 8.0, 25.0, 9.716, 21.8, 2.56, 15.484, 20.0, 2.842, 4.0, 8.445, 18.645, 7.225, 16.812, 23.452, 26.386, 6.556, 2.0, 25.273, 4.518, 12.091, 18.0, 4.28, 3.169, 3.0, 20.619, 29.046, 29.994, 4.776, 22.905, 8.728, 26.465, 16.0, 11.895, 4.427, 17.634, 4.154, 14.82, 6.0, 3.012, 5.0, 8.0, 24.498, 10.022, 6.0, 12.297, 4.411, 21.669, 12.517, 16.4, 3.468, 4.0, 17.205, 12.0, 23.426, 10.0, 24.0, 16.695, 13.841, 7.432, 3.162, 3.808, 10.251, 9.003, 10.395, 10.854, 6.0, 8.874, 10.023, 6.801, 17.16, 2.101, 6.755, 2.46, 18.588, 29.352, 14.476, 20.06, 12.0, 5.98, 10.0, 13.4, 10.856, 12.676, 4.0, 21.906, 14.31, 19.047, 6.48, 16.0, 29.72, 3.714, 21.275, 9.0, 7.192, 17.652, 6.755, 4.984, 15.0, 18.124, 7.562, 9.624, 3.739, 11.162, 15.708, 12.0, 9.347, 10.209, 24.93, 23.788, 20.0, 21.78, 11.304, 19.995, 19.02, 6.0, 4.048, 4.0, 22.37, 12.0, 16.554, 7.7, 7.85, 4.0, 17.677, 8.0, 8.0, 12.443, 4.125, 6.201, 6.428, 16.365, 4.314, 9.488, 9.756, 2.0, 18.0, 4.287, 15.0, 16.944, 18.645, 11.22, 4.281, 24.0, 13.884, 22.2, 10.0, 5.488, 20.327, 4.83, 7.257, 10.0, 14.076, 4.0, 22.452, 2.285, 20.0, 7.854, 8.0, 6.743, 6.24, 9.099, 10.462, 28.17, 24.191, 4.215, 6.772, 23.028, 15.48, 12.578, 10.0, 5.0, 4.0, 6.962, 6.256, 6.0, 21.685, 15.0, 6.0, 11.611, 10.791, 2.0, 12.674, 9.02, 9.328, 6.156, 9.02, 7.809, 7.002, 14.2, 5.0, 5.338, 5.99, 24.121, 17.07, 16.656, 16.587, 20.346, 13.779, 3.336, 6.402, 15.184, 6.095, 23.522, 11.988, 19.12, 22.925, 5.794, 19.756, 10.77, 17.874, 12.0, 21.018, 10.0, 6.28, 15.954, 7.112, 11.804, 2.0, 22.582, 18.615, 6.04, 10.447, 9.416, 10.42, 7.164, 16.0, 10.83, 14.715, 13.235, 12.0, 9.111, 8.666, 2.938, 30.0, 15.873, 15.148, 4.0, 6.741, 5.846, 8.608, 24.663, 10.088, 10.575, 4.102, 4.653, 22.488, 22.425, 4.328, 7.182, 3.503, 21.909, 13.187, 12.0, 4.62, 11.075, 12.0, 20.0, 10.728, 3.354, 8.744, 12.0, 8.613, 24.0, 14.124, 11.214, 24.215, 8.0, 10.392, 19.315, 7.541, 10.159, 3.935, 22.494, 15.0, 9.0, 19.895, 5.559, 8.118, 9.878, 12.0, 12.234, 18.283, 5.0, 4.0, 13.02, 19.145, 7.901, 11.334, 12.0, 12.0, 18.03, 26.965, 17.133, 20.0, 4.511, 30.0, 6.88, 11.572, 11.168, 17.811, 28.868, 2.054, 14.43, 2.872, 19.548, 15.0, 10.0, 16.0, 15.168, 19.14, 5.0, 15.0, 26.178, 3.65, 5.62, 3.875, 15.0, 5.695, 18.448, 3.298, 9.705, 8.0, 8.734, 6.0, 6.0, 12.633, 21.124, 11.552, 28.404, 8.715, 22.867, 12.15, 21.009, 12.421, 17.488, 10.379, 22.812, 17.392, 12.776, 18.0, 19.689, 11.608, 12.0, 25.0, 18.0, 30.0, 25.0, 11.472, 17.81, 10.0, 8.0, 11.51, 2.908, 12.0, 5.683, 11.876, 10.85, 6.486, 8.0, 5.0, 13.264, 6.619, 2.55, 3.0, 9.69, 15.0, 19.56, 10.36, 6.0, 26.935, 11.884, 13.02, 30.0, 17.884, 4.942, 12.0, 3.0, 3.618, 25.0, 9.0, 7.39, 4.388, 16.0, 8.379, 6.0, 4.428, 5.038, 8.722, 10.332, 12.0, 26.269, 8.019, 14.47, 3.0, 18.583, 20.0, 3.0, 6.278, 7.482, 8.908, 8.128, 18.702, 3.0, 15.0, 12.904, 6.83, 3.737, 11.68, 4.0, 3.134, 16.484, 7.354, 7.341, 10.646, 5.575, 10.599, 20.0, 21.169, 22.41, 14.456, 2.753, 4.0, 10.0, 15.0, 7.959, 13.067, 17.073, 20.0, 7.071, 10.0, 27.189, 10.22, 10.0, 3.0, 12.0, 6.14, 10.986, 10.804, 4.0, 7.804, 3.268, 6.376, 13.904, 2.916, 11.048, 21.456, 23.53, 9.465, 10.368, 15.48, 4.0, 3.61, 6.82, 12.0, 3.0, 2.0, 6.803, 14.16, 8.0, 5.396, 11.852, 24.0, 8.853, 6.0, 6.328, 27.06, 24.0, 24.0, 14.133, 20.629, 15.1, 14.787, 16.0, 23.412, 4.775, 25.758, 6.53, 10.497, 3.0, 21.556, 18.732, 5.052, 15.0, 21.422, 26.205, 20.644, 18.648, 18.0, 25.0, 9.324, 16.324, 22.888, 3.919, 10.009, 8.157, 19.97, 13.804, 6.493, 14.477, 17.241, 29.52, 20.095, 19.596, 2.964, 7.324, 17.424, 11.71, 6.336, 9.138, 14.787, 3.0, 7.416, 12.0, 20.059, 7.655, 5.166, 5.694, 10.0,

17.628, 9.0, 13.069, 17.436, 10.461, 19.836, 15.966, 11.142, 2.0, 16.86, 2.82, 14.096, 16.0, 4.0, 20.285, 25.0, 4.025, 9.304, 4.111, 7.366, 16.72, 28.544, 9.849, 14.1, 9.058, 6.996, 12.244, 6.564, 2.462, 9.747, 8.0, 10.0, 9.244, 20.0, 25.0, 7.908, 12.851, 9.3, 9.462, 15.42, 12.0, 19.208, 9.273, 19.87, 15.0, 11.406, 12.732, 19.08, 13.824, 5.934, 4.0, 26.298, 6.0, 22.361, 26.795, 12.591, 5.04, 5.0, 12.953, 4.892, 12.0, 20.0, 17.044, 12.594, 5.764, 9.99, 23.464, 9.562, 25.0, 4.425, 27.665, 4.0, 5.0, 23.27, 21.556, 29.645, 6.0, 11.018, 14.643, 2.115, 9.024, 12.735, 15.917, 16.0, 10.0, 12.0, 5.0, 8.763, 9.116, 14.644, 10.616, 2.0, 4.821, 11.258, 15.0, 4.311, 15.0, 2.0, 6.44, 6.552, 5.18, 5.252, 16.236, 14.751, 28.086, 2.0, 17.79, 15.0, 13.205, 3.782, 3.794, 13.895, 7.43, 13.41, 7.324, 11.902, 9.052, 24.849, 16.87, 8.738, 30.0, 8.0, 12.567, 16.762, 19.57, 6.0, 5.643, 5.0, 6.0, 4.878, 7.598, 3.537, 10.825, 2.626, 4.0, 5.082, 10.754, 11.883, 8.379, 6.0, 2.59, 19.605, 5.88, 11.953, 10.996, 5.281, 8.54, 14.62, 11.295, 18.092, 5.0, 8.652, 13.048, 12.213, 4.54, 14.424, 28.896, 16.0, 4.086, 17.586, 7.199, 4.359, 16.726, 8.0, 3.0, 4.0, 14.306, 6.312, 4.851, 15.685, 3.0, 6.124, 24.0, 4.0, 20.094, 6.2, 23.439, 7.23, 6.508, 13.496, 10.483, 6.0, 9.942, 8.43, 12.0, 12.0, 20.0, 15.77, 18.0, 20.0, 13.597, 30.0, 5.439, 21.292, 5.0, 18.724, 3.335, 8.293, 20.0, 12.591, 4.266, 17.406, 15.26, 13.123, 29.748, 4.0, 17.556, 13.792, 18.49, 9.5, 9.0, 9.42, 13.86, 2.0, 24.0, 10.617, 14.744, 5.121, 12.0, 17.418, 19.085, 8.337, 6.166, 25.0, 8.592, 21.996, 10.945, 9.198, 10.526, 14.328, 14.448, 6.389, 8.138, 5.112, 9.63, 9.67, 8.432, 10.0, 13.657, 20.0, 15.0, 14.396, 8.0, 4.058, 21.312, 6.0, 24.505, 5.943, 9.536, 10.224, 6.0, 4.469, 23.629, 20.924, 5.298, 12.42, 26.262, 11.166, 5.45, 17.125, 21.006, 15.6, 7.914, 6.0, 5.03, 3.0, 6.802, 16.405, 3.666, 20.0, 4.096, 10.425]

# ДОДАТОК В
# МЕТОДИКА ПІДГОТОВКИ ТА НАЛАШТУВАННЯ СЕРЕДОВИЩА ДЛЯ РОБОТИ

## В.1 Попередні налаштування

Для створення середовища використовуємо VMware ESXi 6.5, інтерфейс якого можна побачити на ілюстрації В.1 (а,б). Додаємо нову віртуальну машину, обираємо назву та майбутню встановлювану версію операційної системи (ОС). TufinOS написана на базі CentOS 6, тому обираємо її. Для роботи було виділено наступну кількість ресурсів: 380GB HDD, 32GB RAM, 24 CPUs.

а) 

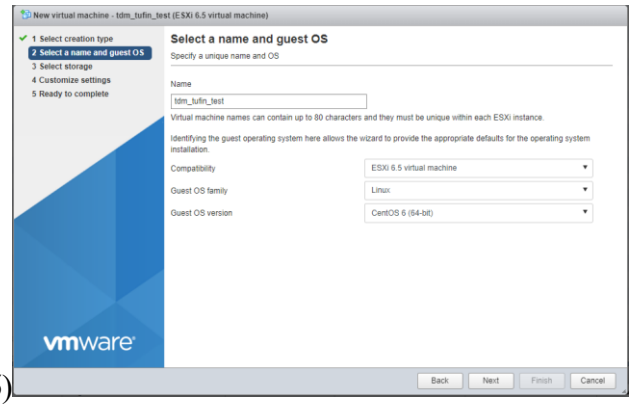

б) 


Рисунок В.1 (а,б) – Інтерфейс VMware ESXi 6.5

## В.2 Інсталяція Tufin OS

Запускаємо віртуальну машину, після чого одразу починається процес інсталяції операційної системи TufinOS (рис. В.2 (а,б)). Обираємо KVM, щоб отримати можливість здійснювати керування за допомогою клавіатури, та починаємо процес, що майже не потребує втручання. Після успішного завершення установки ОС виконується процедура першої авторизації користувача та зміни стандартного пароля (рис. В.3):

а)


б)

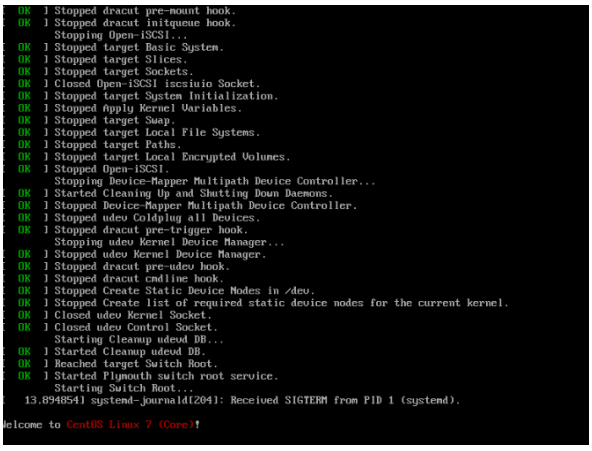



Рисунок В.2 (а,б) – Процес інсталяції ОС TufinOS

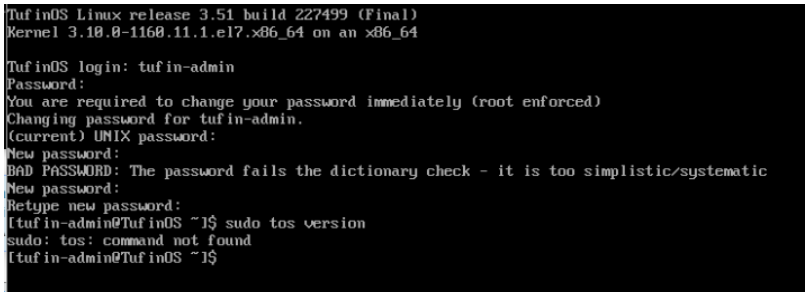



Рисунок В.3 – Процедура першої авторизації

Маючи готову систему, необхідно інсталювати саме ПЗ Tufin Orchestration Suite. Перед цим налаштуємо потрібну IP-адресу, за допомогою якої користувач буде потрапляти на веб-інтерфейс програми (рис. В.4(а)).


Рисунок В.4 – Налаштування IP-адреси

## В.3 Інсталяція Tufin Orchestration Suite

Нами заздалегідь з офіційного порталу [20] був скачаний та завантажений через FTP скрипт для установки. Розархівуємо, надамо права на використання та запустимо його, як на рисунку В.5 (а,б). Дочекавшись завершення, виконаємо команду #tos version, щоб отримати поточні версії TufinOS та Tufin Orchestration Suite та переконатись в успішності (рис. В.6 (а)), після чого перейдемо на веб-інтерфейс програми для остаточних налаштувань (рис. В.6 (б), В.7):

а) б)

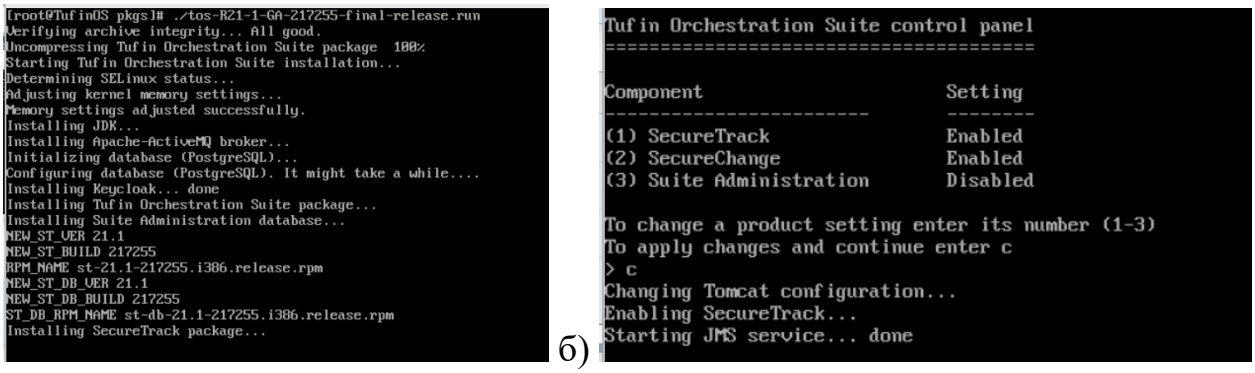



Рисунок В.5 (а, б) - Процес інсталяції TOS

а) б)

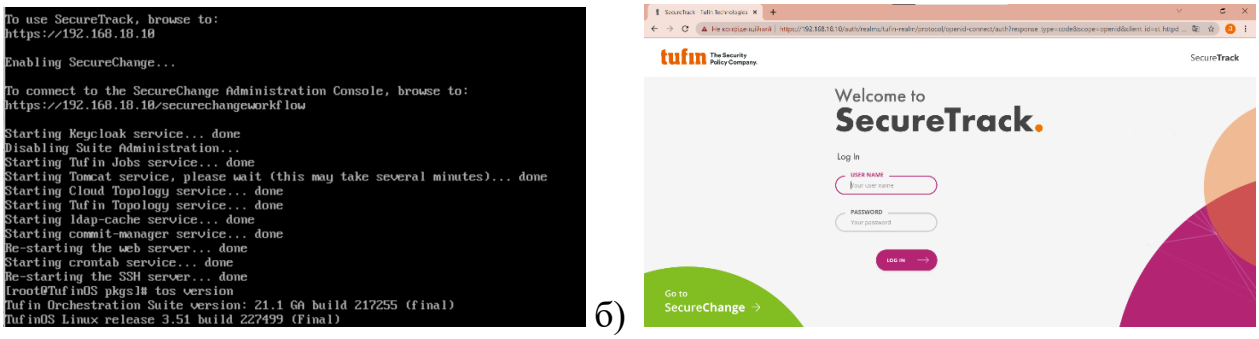



Рисунок В.6 (а, б) – Вивід команди #tos version та WebUI TOS

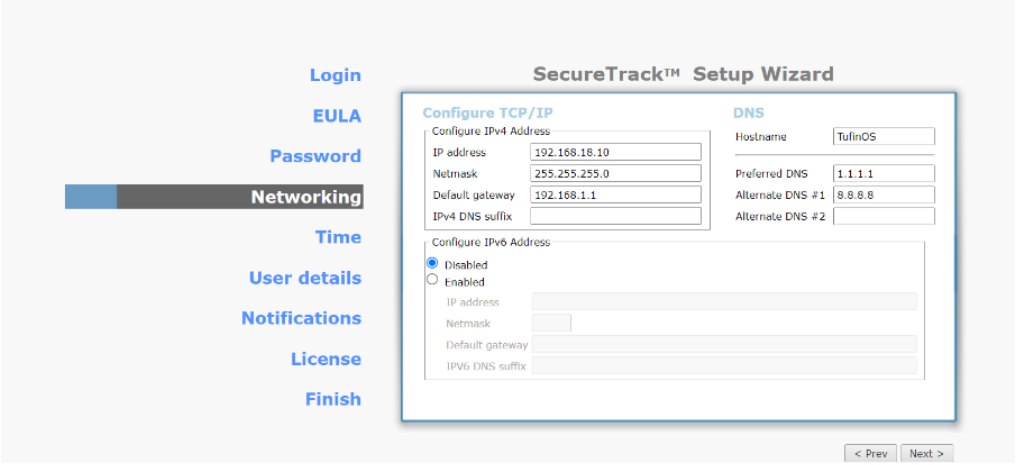



Рисунок В.7 – Остаточні налаштування TOS

## В.4 Завантаження тестової ліцензії та відновлення бази мережі

За відсутності можливості створити реальну мережу для даної роботи, було прийнято рішення використати заздалегідь заготовану демо-базу, яку можна знайти на офіційному порталі вендора. Там же було згенеровано тестову ліцензію та завантажено на TOS. Результати завантажень можна побачити на рисунках В.8, В.9 та В.10

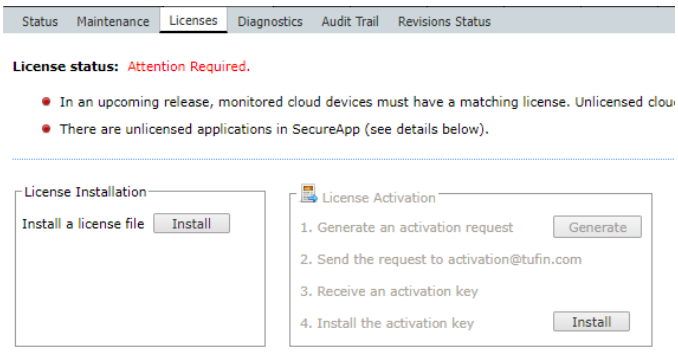



Рисунок В.8 – Вікно статусу ліцензії

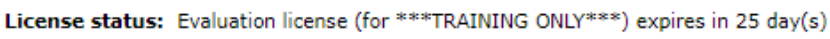



Рисунок В.9 – Успішно завантажена ліцензія

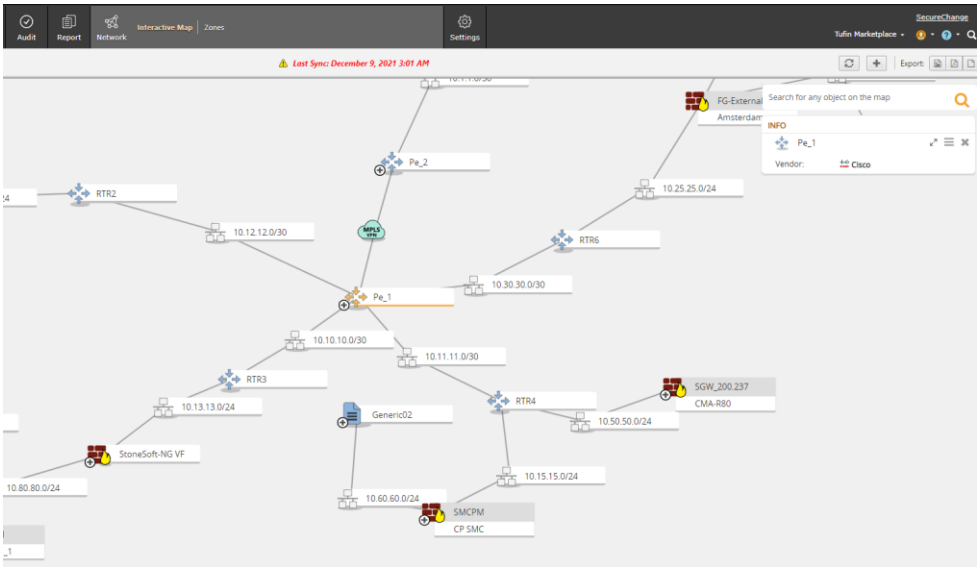



Рисунок В.10 – Мапа мережі демо-бази

# ДОДАТОК Г
# ЗВІТ РОБОТИ APG

APG task results:

Job Name,"Job Owner","Device Name","Policy Name","Rule Number","Revision"
Kursova_task,"r","R80-Training","TCSE_Policy","6","20"

Start Date,"End Date","Number of Generated Rules","Original Permissiveness","Generated Rulebase Permissiveness"

Generated Rulebase:
Name,"Source","Destination","Port","Protocol","Hits","Permissiveness"
Rule 6.5,"192.168.54.18/32","10.0.0.0/8","8","ICMP","401","31"
Rule 6.502,"192.168.54.19/32","10.0.0.0/8","8","ICMP","374","31"
Rule 6.1438,"172.16.11.33/32","10.0.0.0/8","8","ICMP","206","31"
Rule 6.1333,"172.16.11.33/32","10.0.0.0/8","161","UDP","200","31"
Rule 6.973,"192.168.54.19/32","10.0.0.0/8","161","UDP","111","31"
Rule 6.1597,"10.11.8.31/32","192.168.55.134/32","49","TCP","66","1"
Rule 6.1713,"172.16.2.100/32","192.168.55.134/32","49","TCP","61","1"
Rule 6.1628,"10.23.195.13/32","192.168.54.48/32","5529","TCP","49","1"
Rule 6.1088,"192.168.54.30/32","10.0.0.0/8","22","TCP","42","31"
Rule 6.1247,"192.168.55.0/24","10.30.0.0/16","8","ICMP","34","31"

Rule 6.1547,"10.0.0.0/8","192.168.55.9/32","21","TCP","33","31"

Rule 6.1035,"192.168.54.18/32","10.0.0.0/8","161","UDP","32","31"

Rule 6.1196,"192.168.54.0/24","10.15.0.0/16","3181","TCP","25","31"

Rule 6.1170,"192.168.54.30/32","10.0.0.0/8","80","TCP","23","31"

Rule 6.1290,"192.168.55.0/24","10.41.0.0/16","8","ICMP","22","31"

Rule 6.1652,"192.168.54.0/24","170.224.0.0/16","8","ICMP","20","31"

Rule 6.1573,"10.0.0.0/8","192.168.55.60/32","8530","TCP","17","31"

Rule 6.1563,"10.0.0.0/8","192.168.55.9/32","3803","UDP","16","31"

Rule 6.1127,"192.168.54.30/32","10.15.95.0/24","","Any","16","32"

Rule 6.1600,"10.15.0.0/16","192.168.54.0/24","162","UDP","10","31"

Rule 6.1157,"192.168.54.30/32","10.30.78.0/24","","Any","9","32"

Rule
6.1225,"192.168.54.21/32","10.249.0.0/16","3181","TCP","7","21"

Rule
6.1696,"192.168.55.144/32","170.224.0.0/16","8","ICMP","6","21"

Rule 6.1314,"192.168.55.141/32","10.0.0.0/8","8","ICMP","6","31"

Rule
6.1186,"192.168.54.30/32","10.65.78.0/24","1352","TCP","5","11"

Rule 6.1322,"192.168.55.140/32","10.0.0.0/8","8","ICMP","5","31"

Rule 6.1079,"192.168.54.254/32","10.0.0.0/8","161","UDP","5","31"

Rule 6.1632,"10.33.35.36/32","63.83.37.0/24","443","TCP","4","11"

Rule 6.1147,"192.168.54.30/32","10.15.0.0/16","80","TCP","4","21"

Rule 6.1613,"10.0.0.0/8","192.168.54.18/32","162","UDP","3","31"

Rule 6.1706,"172.16.11.33/32","32.83.13.0/24","161","UDP","3","11"

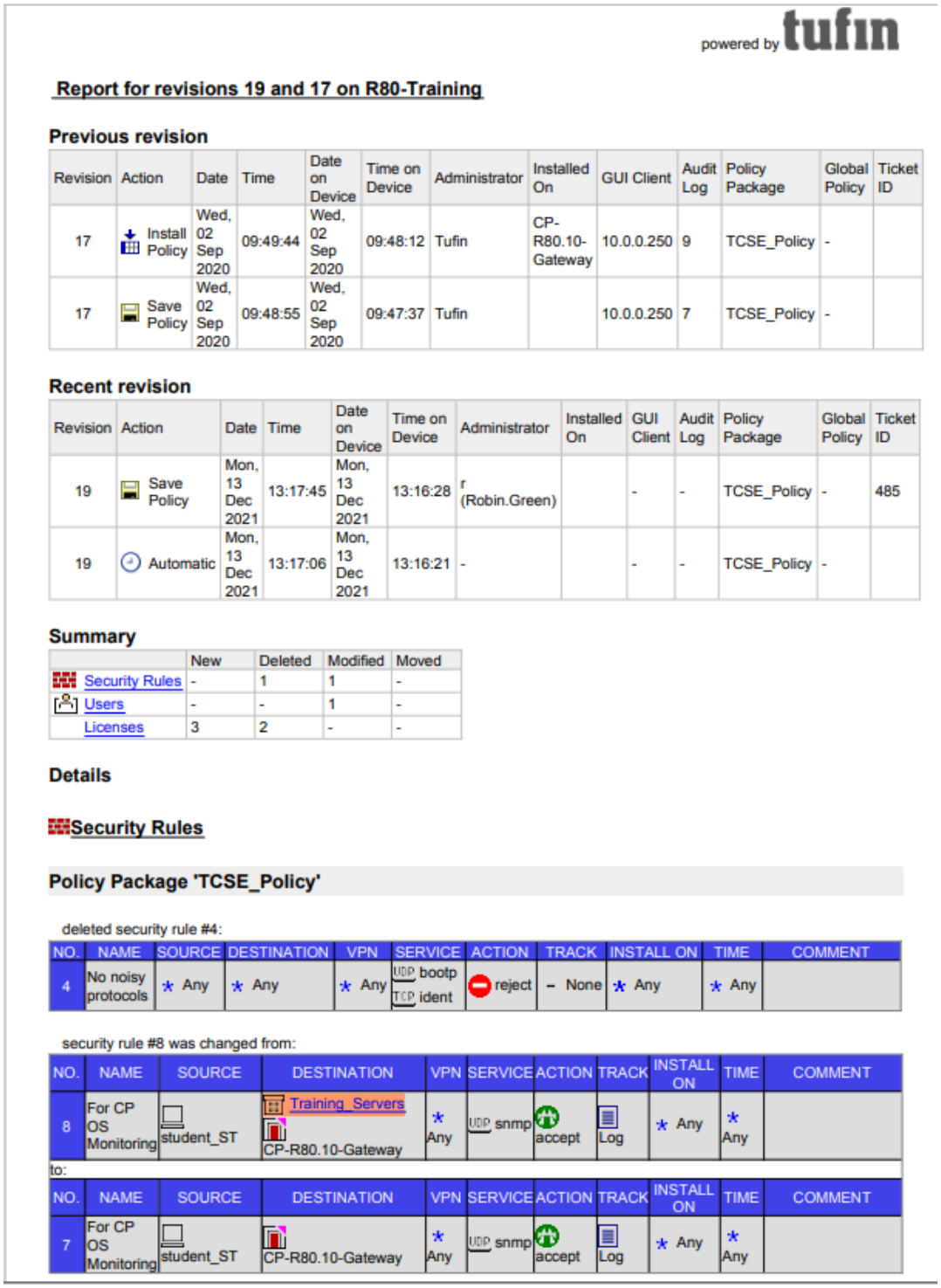
Rule
6.1194,"192.168.54.30/32","10.23.237.24/32","5444","TCP","3","1"

Rule 6.1709,"172.16.11.33/32","170.224.0.0/16","161","UDP","3","21"

Rule
6.1244,"192.168.54.107/32","10.30.38.16/32","443","TCP","3","1"
Rule 6.1637,"10.33.35.36/32","170.224.0.0/16","443","TCP","3","21"
Rule 6.1329,"192.168.55.144/32","10.33.0.0/16","8","ICMP","3","21"
Rule 6.1622,"10.0.0.0/8","192.168.54.85/32","1579","TCP","3","31"
Rule 6.1617,"10.0.0.0/8","192.168.54.19/32","162","UDP","3","31"
Rule 6.1643,"10.33.35.36/32","63.83.37.0/24","80","TCP","2","11"
Rule 6.1152,"192.168.54.30/32","10.15.86.132/32","","Any","2","22"
Rule
6.1191,"192.168.54.30/32","10.11.77.0/24","2463","TCP","2","11"
Rule 6.1232,"192.168.54.112/32","10.22.76.0/24","81","TCP","2","11"
Rule
6.1238,"192.168.54.77/32","10.24.76.0/24","5050","TCP","2","11"
Rule 6.1539,"10.33.35.36/32","10.33.208.0/24","80","TCP","2","11"
Rule 6.1542,"10.33.35.36/32","10.41.199.15/32","443","TCP","2","1"
Rule 6.1646,"10.33.35.36/32","170.224.100.0/24","80","TCP","2","11"
Rule 6.1683,"192.168.54.18/32","172.16.2.0/24","8","ICMP","2","11"
Rule 6.1691,"192.168.54.19/32","172.16.2.0/24","161","UDP","2","11"
Rule 6.1245,"192.168.54.19/32","10.34.16.8/32","162","UDP","1","1"
Rule 6.1243,"192.168.54.18/32","10.30.16.8/32","162","UDP","1","1"
Rule
6.1169,"192.168.54.30/32","10.30.80.66/32","6112","TCP","1","1"
Rule 6.1241,"192.168.54.18/32","10.24.16.11/32","162","UDP","1","1"
Rule 6.1712,"172.16.11.33/32","32.83.13.126/32","8","ICMP","1","1"
Rule
6.1686,"192.168.54.18/32","192.168.128.68/32","8","ICMP","1","1"
Rule 6.1688,"192.168.54.19/32","32.83.13.147/32","8","ICMP","1","1"

Rule 6.1689,"192.168.54.19/32","172.16.2.103/32","8","ICMP","1","1"
Rule
6.1155,"192.168.54.30/32","10.15.80.155/32","2463","TCP","1","1"
Rule 6.1694,"192.168.54.18/32","172.31.1.35/32","161","UDP","1","1"
Rule 6.1236,"192.168.54.112/32","10.65.76.12/32","80","TCP","1","1"
Rule
6.1699,"192.168.55.141/32","172.16.2.106/32","8","ICMP","1","1"
Rule
6.1701,"192.168.157.51/32","192.168.55.60/32","8530","TCP","1","1"
Rule
6.1702,"192.168.157.85/32","192.168.54.48/32","5529","TCP","1","1"
Rule
6.1235,"192.168.54.112/32","10.11.104.149/32","2525","TCP","1","1"
Rule
6.1627,"10.15.145.175/32","192.168.54.21/32","6083","TCP","1","1"
Rule 6.1629,"10.57.12.4/32","192.168.54.15/32","2052","TCP","1","1"
Rule
6.1626,"10.28.16.20/32","192.168.54.86/32","1579","TCP","1","1"

# ДОДАТОК Д
# ЗГЕНЕРОВАНИЙ ЗВІТ РЕВІЗІЙ ВИКОНАНОЇ РОБОТИ В TOS



powered by tufin

**Report for revisions 19 and 17 on R80-Training**

**Previous revision**

| Revision | Action | Date | Time | Date on Device | Time on Device | Administrator | Installed On | GUI Client | Audit Log | Policy Package | Global Policy | Ticket ID |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 17 | Install Policy | Wed, 02 Sep 2020 | 09:49:44 | Wed, 02 Sep 2020 | 09:48:12 | Tufin | CP-R80.10-Gateway | 10.0.0.250 | 9 | TCSE_Policy | - | |
| 17 | Save Policy | Wed, 02 Sep 2020 | 09:48:55 | Wed, 02 Sep 2020 | 09:47:37 | Tufin | | 10.0.0.250 | 7 | TCSE_Policy | - | |

**Recent revision**

| Revision | Action | Date | Time | Date on Device | Time on Device | Administrator | Installed On | GUI Client | Audit Log | Policy Package | Global Policy | Ticket ID |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 19 | Save Policy | Mon, 13 Dec 2021 | 13:17:45 | Mon, 13 Dec 2021 | 13:16:28 | r (Robin.Green) | | - | - | TCSE_Policy | - | 485 |
| 19 | Automatic | Mon, 13 Dec 2021 | 13:17:06 | Mon, 13 Dec 2021 | 13:16:21 | - | | - | - | TCSE_Policy | - | |

**Summary**

| | New | Deleted | Modified | Moved |
|---|---|---|---|---|
| Security Rules | - | 1 | 1 | - |
| Users | - | - | 1 | - |
| Licenses | 3 | 2 | - | - |

**Details**

**Security Rules**

**Policy Package 'TCSE_Policy'**

deleted security rule #4:

| NO. | NAME | SOURCE | DESTINATION | VPN | SERVICE | ACTION | TRACK | INSTALL ON | TIME | COMMENT |
|---|---|---|---|---|---|---|---|---|---|---|
| 4 | No noisy protocols | Any | Any | Any | UDP bootp<br>TCP ident | reject | None | Any | Any | |

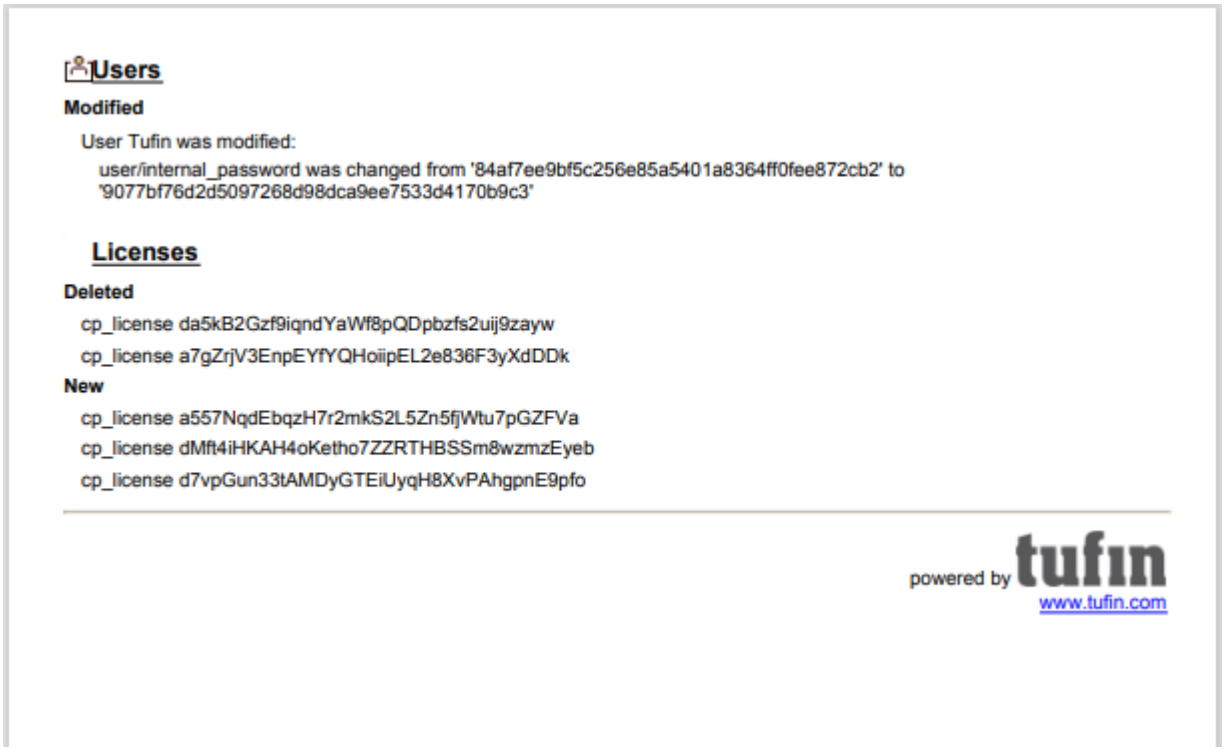
security rule #8 was changed from:

| NO. | NAME | SOURCE | DESTINATION | VPN | SERVICE | ACTION | TRACK | INSTALL ON | TIME | COMMENT |
|---|---|---|---|---|---|---|---|---|---|---|
| 8 | For CP OS Monitoring | student_ST | Training_Servers<br>CP-R80.10-Gateway | Any | UDP snmp | accept | Log | Any | Any | |

to:

| NO. | NAME | SOURCE | DESTINATION | VPN | SERVICE | ACTION | TRACK | INSTALL ON | TIME | COMMENT |
|---|---|---|---|---|---|---|---|---|---|---|
| 7 | For CP OS Monitoring | student_ST | CP-R80.10-Gateway | Any | UDP snmp | accept | Log | Any | Any | |

Рисунок Д.1 – Перша сторінка звіту



## Users

**Modified**

User Tufin was modified:

user/internal_password was changed from '84af7ee9bf5c256e85a5401a8364ff0fee872cb2' to '9077bf76d2d5097268d98dca9ee7533d4170b9c3'

## Licenses

**Deleted**

cp_license da5kB2Gzf9iqndYaWf8pQDpbzfs2uij9zayw

cp_license a7gZrjV3EnpEYfYQHoiipEL2e836F3yXdDDk

**New**

cp_license a557NqdEbqzH7r2mkS2L5Zn5fjWtu7pGZFVa

cp_license dMft4iHKAH4oKetho7ZZRTHBSSm8wzmzEyeb

cp_license d7vpGun33tAMDyGTEiUyqH8XvPAhgpnE9pfo

powered by tufin
www.tufin.com

Рисунок Д.2 – Друга сторінка звіту