Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Кабанова Артема Олександровича*

академічної групи *125м-19-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Метод реалізації системи виявлення порушень для розпізнання фактів комп'ютерного саботажу*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.т.н., доц. Сафаров О.О.			
розділів:				
спеціальний	ас. Ковальова Ю.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст.викл. Тимофєєв Д.С.			

Дніпро
2020

ЗАТВЕРДЖЕНО
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту *Кабанову Артему Олександровичу* **академічної групи** *125м-19-2*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації[1] _____

за освітньо-професійною програмою *Кібербезпека*

на тему *Метод реалізації системи виявлення порушень для розпізнання фактів комп'ютерного саботажу*

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Огляд джерел за темою та напрям досліджень	03.09.20-06.10.20
Розділ 2	Методи досліджень	07.10.20-31.10.20
	Результати досліджень	01.11.20-24.11.20
Розділ 3	Виконання економічного розділу	25.11.20-04.12.20
	Оформлення пояснювальної записки	05.12.20-10.12.20

Завдання видано _____ Сафаров О.О.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 02.09.2020 р.

Дата подання до екзаменаційної комісії: 11.12.2020 р.

Прийнято до виконання _____ Кабанов А.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 70 с., 9 рис., 14 табл., 4 додатків, 21 джерел.

Об'єкт досліджень: система виявлення порушень корпоративної ІТС.

Мета дипломної роботи: дослідження системи виявлення порушень корпоративної ІТС на можливість розпізнання фактів комп'ютерного саботажу.

Предметом досліджень є розпізнання комп'ютерного саботажу, інтегруючи систему виявлення порушень разом із системою відеоспостереження.

В першому розділі було обґрунтовано актуальність проблеми своєчасного виявлення порушень і визначено доцільність використання системи виявлення порушень. Охарактеризовано недоліки системи виявлення порушень в контексті розпізнання фактів комп'ютерного саботажу. Проаналізовано нормативні документи в сфері виявлення саботажу. Сформовано задачі, які необхідно вирішити в ході виконання роботи.

В другому розділі було доведено необхідність впровадження системи виявлення порушень для розпізнавання фактів комп'ютерного саботажу, обрано функціональний профіль захищеності та розроблено модель загроз. Проаналізовано і порівняно програмні рішення системи виявлення порушень, запропоновано метод реалізації такої системи з урахуванням висунутих інженерних і організаційних заходів. Запропонований метод реалізації системи виявлення порушення було реалізовано на практиці.

В третьому розділі проведено розрахунок витрат на розробку, впровадження та експлуатацію запропонованого методу, визначено термін окупності інвестицій.

Наукова новизна полягає в об'єднанні ознак саботажу в системі виявлення порушень та системі відеоспостереження всередині корпоративної ІТС.

СИСТЕМА ВИЯВЛЕННЯ ПОРУШЕНЬ, ПОРУШЕННЯ, МОДЕЛЬ ЗАГРОЗ, ПРОФІЛЬ ЗАХИЩЕНОСТІ, ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, КОМП'ЮТЕРНИЙ САБОТАЖ.

РЕФЕРАТ

Пояснительная записка: 70 с., 9 рис., 14 табл., 4 приложений, 21 источников.

Объект исследований: система обнаружения нарушений корпоративной ИТС.

Цель дипломной работы: исследование системы обнаружения нарушений корпоративной ИТС на возможность распознавания фактов компьютерного саботажа.

Предметом исследований является распознавание компьютерного саботажа, интегрируя систему обнаружения нарушений с системой видеонаблюдения.

В первом разделе обоснована актуальность проблемы своевременного обнаружения нарушений и определена целесообразность использования системы обнаружения нарушений. Охарактеризовано недостатки системы обнаружения нарушений в спектре распознавания фактов компьютерного саботажа. Проанализированы нормативные документы в сфере обнаружения саботажа. Сформированы задачи, которые необходимо решить в ходе выполнения работы.

Во втором разделе была доказана необходимость внедрения системы обнаружения нарушений для распознавания фактов компьютерного саботажа, выбран функциональный профиль защищенности и разработана модель угроз. Проанализированы и сравнены программные решения системы обнаружения нарушений, предложен метод реализации такой системы с учетом выдвинутых инженерных и организационных мероприятий. Предложенный метод реализации системы обнаружения нарушения был реализован на практике.

В третьем разделе проведен расчет затрат на разработку, внедрение и эксплуатацию предложенного метода, определен срок окупаемости инвестиций.

Научная новизна заключается в объединении признаков саботажа в системе обнаружения нарушений и системе видеонаблюдения внутри корпоративной ИТС.

СИСТЕМА ОБНАРУЖЕНИЯ НАРУШЕНИЙ, НАРУШЕНИЕ, МОДЕЛЬ УГРОЗ, ПРОФИЛЬ ЗАЩИЩЕННОСТИ, ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМА, КОМПЬЮТЕРНЫЙ САБОТАЖ.

ABSTRACT

Explanatory note: 70 p., 9 fig., 14 tab., 4 applications, 21 sources.

Object of research: breach detection system of the corporate information and telecommunications system.

Purpose of degree work: investigation of the breach detection system of the corporate information and telecommunications system for the possibility of recognizing the facts of computer sabotage.

The subject of research is the recognition of computer sabotage by integrating the breach detection system with the video surveillance system.

In the first section, the urgency of the problem of early detection of breaches was substantiated and the feasibility of using a breach detection system was determined. The disadvantages of breach detection system in the spectrum of recognition of facts of computer sabotage was characterized. The regulatory documents in the field of detection of sabotage was analyzed. The tasks that need to be solved in the course of the work are formed.

In the second section, the necessity of introducing a breach detection system to recognize the facts of computer sabotage was proved, a functional security profile was selected and a threat model was developed. The software solutions of the breach detection system are analyzed and compared, a method for implementing such a system is proposed, taking into account the proposed engineering and organizational measures. The proposed method for implementing of the breach detection system was implemented in practice.

In the third section, the costs of developing, implementing and operating the proposed method were calculated and ROSI has been determined.

The scientific novelty consists in the combination of signs of sabotage in the violation detection system and the video surveillance system within the corporate ITS.

BREACH DETECTION SYSTEM, BREACH, THREAT MODEL, SECURITY PROFILE, INFORMATION AND TELECOMMUNICATION SYSTEM, COMPUTER SABOTAGE.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

APT – advanced persistent threat;

BDS – breach detection system;

IDS – intrusion detection system;

IPS – intrusion prevention system;

NGFW – next-generation firewall;

SIEM – security information and event management;

SPAN – port mirroring;

TAP – test access point;

WAN – Wide Area Network;

АРМ – автоматизоване робоче місце;

ЕОМ – електронно-обчислювальна машина;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

ІТС – інформаційно-телекомунікаційна система;

ПЗ – програмне забезпечення;

СВП – система виявлення порушень;

СЗІ – служба захисту інформації;

ЗМІСТ

с.

ВСТУП 10

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ 12

1.1 Актуальність проблеми 12

1.2 Проблеми своєчасного виявлення порушень в корпоративній ІТС 13

1.3 Аналіз нормативно-правової бази в сфері виявлення фактів саботажу інформаційної та кібербезпеки 17

1.4 Система виявлення порушень: визначення і класифікація методів її розгортання 18

1.5 Архітектура методів розгортання систем виявлення порушень 19

1.6 Об'єкти виявлення BDS 21

1.6.1 Експлойт 22

1.6.2 Зловмисне ПЗ 23

1.6.3 Троян 23

1.6.4 Автономні інфекції 23

1.6.5 Вразливості нульового дня 24

1.7 Постановка задачі 24

1.8 Висновок 25

2 СПЕЦІАЛЬНА ЧАСТИНА 27

2.1 Вибір профілю захищеності і аналіз загроз 27

2.2 Огляд існуючих програмних рішень системи виявлення порушень 35

2.2.1 ESET Enterprise Inspector 36
2.2.2 Cisco Advanced Malware Protection (AMP) for Endpoints 36
2.2.3 Symantec Advanced Threat Protection 36
2.2.4 Microsoft Defender Advanced Threat Protection 37
2.2.5 FireEye Endpoint Security 37
2.2.6 Cyberbit EDR 37
2.3 Вимоги до системи виявлення порушень 38
2.4 Визначення шкали оцінювання програмних рішень системи виявлення порушень 39
2.5 Порівняльна характеристика функціоналу програмних рішень систем виявлення порушень 40
2.6 Розробка методу реалізації системи виявлення порушень для розпізнання фактів комп'ютерного саботажу 43
2.6.1 Впровадження засобів неперервного контролю за фізичним станом ЕОМ в корпоративній ІТС 44
2.6.1.1 Інтеграція системи виявлення порушень із детектором саботажу 47
2.6.2 Розробка організаційних заходів контролю цілісності інформації в корпоративній ІТС 50
2.6.2.1 Перелік правил адміністратора системи виявлення порушень для забезпечення контролю цілісності інформації в корпоративній ІТС 51
2.6.2.2 Перелік правил користувачів системи виявлення порушень для забезпечення цілісності інформації в корпоративній ІТС 52
2.7 Висновок 53
3 ЕКОНОМІЧНА ЧАСТИНА 55
3.1 Обґрунтування витрат на реалізацію запропонованого методу 55
3.2 Розрахунки витрат на реалізацію запропонованого методу 55

3.2.1 Розрахунок капітальних (фіксованих) витрат 55

3.2.2 Розрахунок річних поточних (експлуатаційних) витрат 56

3.3 Оцінка величини можливого збитку від атаки 58

3.4 Загальний ефект від впровадження методу 62

3.5 Визначення та аналіз показників економічної ефективності системи виявлення порушень 63

3.6 Висновок 64

ВИСНОВКИ 64

ПЕРЕЛІК ПОСИЛАНЬ 65

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ ДИПЛОМНОЇ РОБОТИ 68

ДОДАТОК Б. ПЕРЕЛІК МАТЕРІАЛІВ НА ОПТИЧНОМУ НОСІЇ 69

ДОДАТОК В. ВІДГУК КЕРІВНИКІВ РОЗДІЛІВ 70

ДОДАТОК Г. ВІДГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ 71

ВСТУП

Сучасні підприємства використовують останні тренди в розв'язуванні власних бізнес-задач задля досягання цілей. Ними вже стали інформаційні технології, автоматизація обробки інформації, електронна комерція, використання хмарних і мережевих технологій, та ін. Однак, з таким швидким зростанням попиту на програмно-апаратні продукти відбувається пропорційне зростання кількості загроз, що можуть нашкодити інформаційній системі установи або і взагалі призвести до її банкрутства. Зловмисники вдаються до різних маніпуляцій і цільових дій, починаючи від фальсифікації програмного забезпечення на робочій станції і завершуючи цілеспрямованими атаками на державні об'єкти критичної інфраструктури, які з легкістю долають системи виявлення/запобігання вторгнень, захищені веб-шлюзи, брандмауери нового покоління, системи керування подіями безпеки та ін. Новітнім захистом від таких загроз стала система виявлення порушень, яка зарекомендувала себе в західних країнах як засіб виявлення активності шкідливих програм всередині мережі після порушення.

Звіт Mandiant-Trends за 2016 рік показав, що для виявлення порушення компаніям в середньому необхідно 99 днів. В той час як для отримання адміністративного доступу і нанесення збитків зловмисникам необхідно лише 3 дні [1]. За цей час порушники можуть викрасти інформаційні активи підприємства, вивести з ладу елементи корпоративної мережі, тощо. Для того, щоб система функціонувала якісно, виявляла і відстежувала всі підозрілі мережеві активності, її необхідно правильно підготувати, налаштувати, управляти і підтримувати. Саме з цим виникають складності. Найбільш розповсюджена помилка налаштування системи виявлення порушень із такими важливими деталями, як: операційна система, список затверджених додатків та програм, яким дозволене підключення до мережі Інтернет. Спеціалісти СЗІ забувають своєчасно

переглядати список затверджених програм, через що певний перелік додатків не контролюється системою виявлення порушень корпоративної ІТС. Ще однією складністю при налаштуванні системи виявлення порушень є визначення можливої події шляхом аналізу вхідного трафіку, дослідження різних комбінацій еврістики, оцінки ризиків, аналізу звітності про порушення та ін. Однак, система виявлення порушень іноді може знаходити тільки порушення і джерело їх виникнення, а деколи виявляти порушення і побічні атаки, що раніше не були знайдені. В таких випадках важко спрогнозувати який варіант (подія або подія та побічна атака) відбудеться в поточний час.

Таким чином, система виявлення порушень має велику кількість переваг при правильному налаштуванні. В сукупності із брандмауерами нового покоління (NGFW), системам виявлення (IDS) та запобігання (IPS) вторгнень, антивірусним ПЗ, BDS стане уніфікованим рішенням для виявлення, моніторингу, контролю та запобіганням загрозам. Однак, незмінним лишається одне запитання: як система виявлення порушень протидіятиме виходу із ладу важливих елементів комп'ютерної системи, знищуючи або модифікуючи важливі інформаційні активи? Саме вирішення цього питання було поставлено як мета і доцільність дипломних досліджень.

Об'єктом досліджень в кваліфікаційній роботі виступає система виявлення порушень корпоративної ІТС. В свою чергу, предметом досліджень є розпізнання комп'ютерного саботажу, інтегруючи систему виявлення порушень разом із системою відеоспостереження. Поставлена мета винаходження методу протидії можливим фактам комп'ютерного саботажу з використанням системи виявлення порушень є важкою в часі і предметі оцінюванні в умовах обстежуваної корпоративної ІТС підприємства.

Важкість в часі полягає в тому, що з кожним днем з'являються нові шляхи обходу існуючих систем захисту інформації, використовуючи як прямий вивід з ладу елементів ІТС, так і зміну правил розмежування доступу з подальшим знищенням або викраденням інформації.

Важкість в предметі оцінюванні полягає в об'єктивності, адже кожна BDS є унікальною, адже має різні параметри налаштування і створити уніфіковане рішення захисту корпоративних ІТС від фактів комп'ютерного саботажу, яке задовільнить інформаційні системи різних установ, майже неможливо.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Актуальність проблеми

Зростання кількості кібератак, що панує в українському та світовому кіберпросторі, наштовхує організації більш ретельно захищати свої бізнес-активи [2]. Технології, які ще 2-3 роки тому були дієвим засобом захисту від тодішніх загроз, сьогодні стають нездатними протистояти новітнім атакам, які становлять небезпеку організаціям, що надходить з мережі Інтернет. Шахраї вдаються до складних алгоритмів, застосовуючи недоліки в програмному забезпеченні, тим самим обходячи системи виявлення вторгнень, брандмауери, антивірусне ПЗ, комплекс засобів захисту, тощо. Однак, швидке зростання кількості порушень, пов'язаних з втручанням в роботу комп'ютерних систем, заміною, приховуванням або стиранням програм та інформації робить корпоративну мережу комерційних установ вразливою і незахищеною. Як відслідкувати джерело виникнення проблем, якщо порушення сталося через людський фактор? Сучасні проблеми потребують сучасних рішень. Впровадження системи виявлення порушень в ІТС організації є доцільним рішенням для захисту активів установи від порушень, шляхом виявлення, запобігання та протидії можливому розповсюдженню зловмисної активності всередині корпоративної мережі. Однак його недостатньо для того, щоб встановити джерело порушення, якщо воно пов'язано із пошкодженням фізичного стану апаратного забезпечення, носіїв інформації, тощо.

Доцільність використання системи виявлення порушення в якості рішення захисту від потенційних атак ґрунтується декількома перевагами, серед яких:

– система виявлення порушень дозволяє вчасно виявити, дослідити діяльність порушення в мережі, знайти причину порушення і локалізувати;

– впровадження превентивних заходів, що унеможливлюють зловмисні дії, дозволяють зменшити ймовірність реалізації кіберзагрози, джерелом якої є виникнення порушення всередині корпоративної мережі;

– сучасні рішення систем виявлення порушень дозволяють знайти небезпечні вразливості, помилки та зловмисну активність мережевого трафіку, що може бути.

Однак, системі виявлення порушень не впоратись із цілеспрямованими діями, що виводять із ладу елементи комп'ютерної системи або взагалі знищують інформацію, що оброблюється. Наприклад, як системі виявлення порушень розпізнати сторонню людину в межах контрольованої зони, яка пройшла авторизацію через обліковий запис користувача системи, і планує наступними діями викрасти або знищити інформацію. Або інший приклад: як знайти людину, яка налаштувала на своєму робочому місці віддалений доступ і працює з дому, на маючи на це дозволу від керівництва і порушуючи при цьому політику безпеки. На вирішення цих, та інших задач спрямована кваліфікаційна робота.

1.2 Проблеми своєчасного виявлення порушень в корпоративній ІТС

Проблема своєчасного виявлення порушень сколихнула світ після масштабних кібератак у 2017 році. Так, влітку цього року на території України відбулася кібератака, яка використовувала вразливість в ПЗ «M.E.doc», в результаті чого сталася DDoS-атака. Наслідком цієї атаки була паралізована робота державних та приватних підприємств, таких як «Укрзалізниця», «Укрпошта», «Нова пошта» та ін. Після хвилі потужних втручань в роботу інформаційної системи великих підприємств, питання захисту інформаційних активів постало на перший план, поряд з такими показниками, як прибуток, ефективність та ін. Кібератаки, які вже сталися розслідувалися спеціалістами із захисту інформації вже після того, як сталася подія. Виявлення джерела порушення займало більше часу, аніж відновлення роботоспроможності системи. Саме тому на світовому ринку почали з'являтися різні засоби запобігання втручанням, такі як IPS, IDS, NGFW та інше. Спеціалісти IBM, вивчаючи питання

виявлення і запобігання порушень, в своєму щорічному звіті Cost of Data Breach Report за 2019 рік, дослідили середню кількість днів для виявлення порушення за галузями [3]. В цьому звіті аналізувалися різні галузі економіки, такі як охорона здоров'я, освіта, зв'язок, ЗМІ і визначалась кількість днів на виявлення та запобігання порушень. Значення в першому та другому графіку відрізняються, що ставить задачу виявлення і запобігання порушень більш гострою.

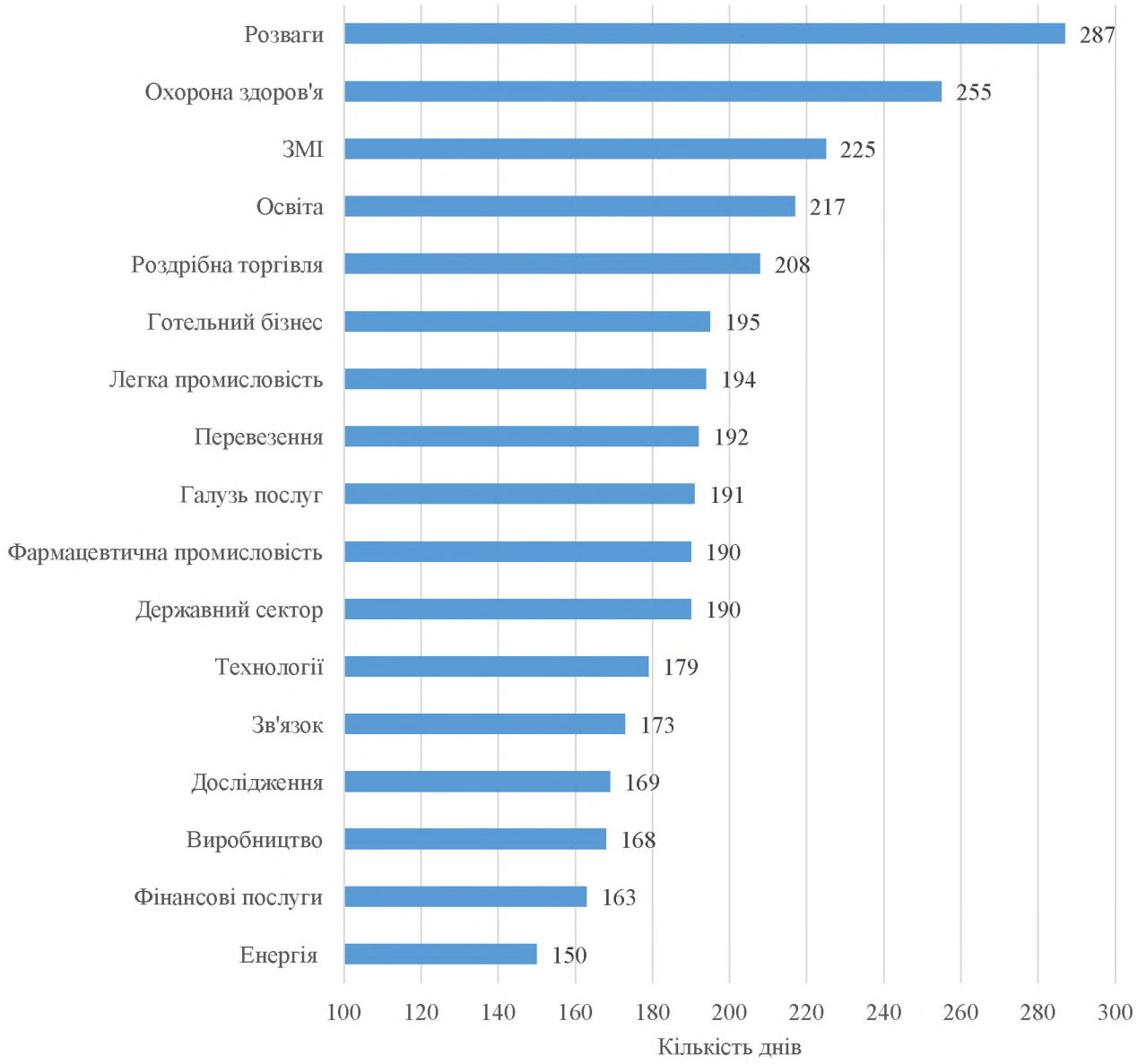

Рисунок 1.1 – Середня кількість днів для виявлення порушення за галузями

Найбільша кількість днів на виявлення порушення витрачається в індустрії розваг: середня значення перевищує 9 місяців. В той час як порушення в енергетичній сфері виявляється за 150 днів. Отримані дані свідчать про те, що своєчасне виявлення порушення допоможе уникнути установам фатальних збитків і зберегти цілісність інформаційних активів.

У другому графіку, фахівцями IBM було проаналізовано середню кількість днів для запобігання порушення за тими ж галузями [3]. Кількість днів значно змінилася, так само як і змінилась черговість галузей. Такі дані вказують на те, що виявлення порушення однієї сфери економіки може відбуватися швидше (або довше), аніж запобігання порушенню тої ж сфери. Що також свідчить на важливість своєчасного виявлення і запобігання порушень.

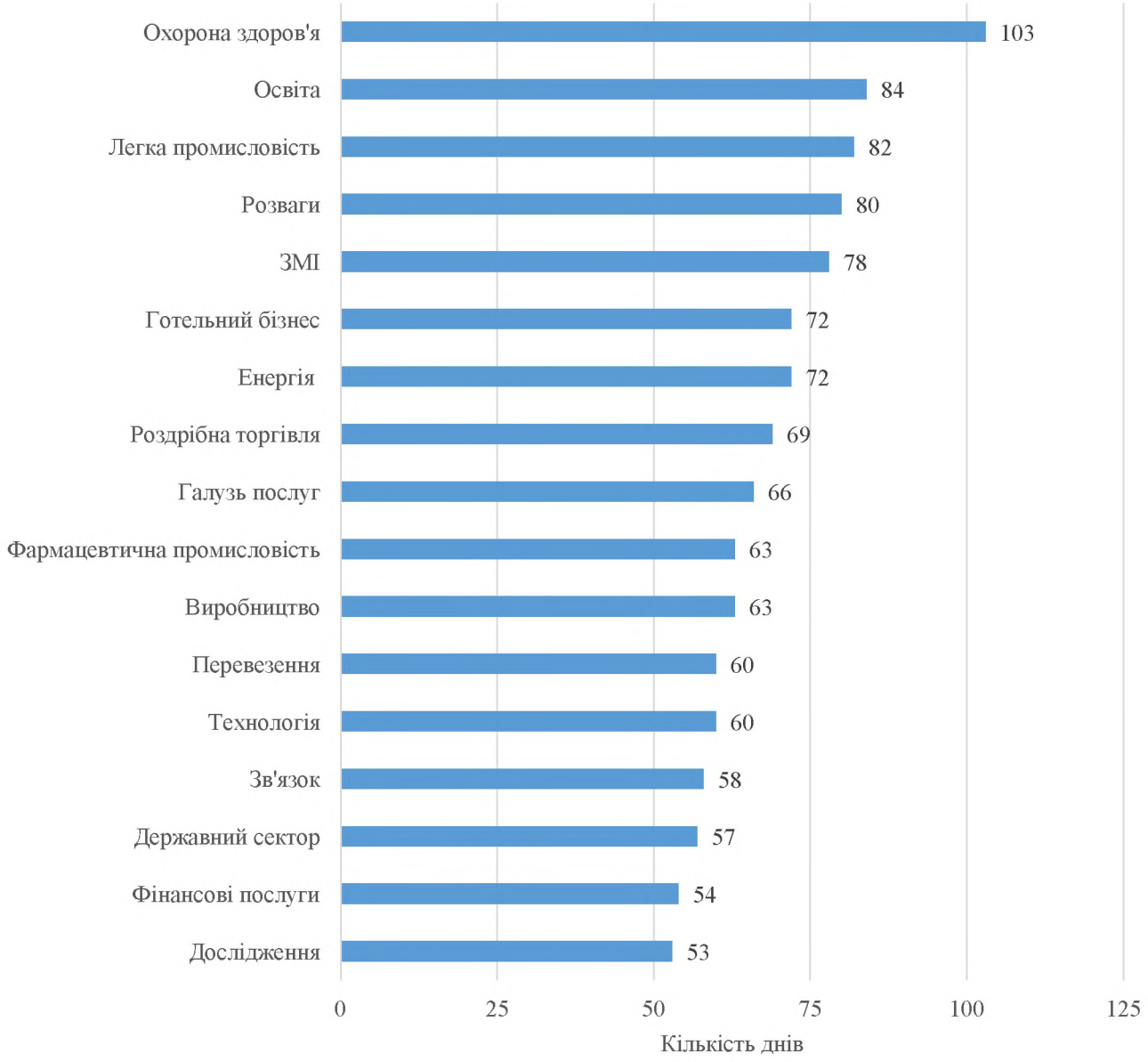

Рисунок 1.2 – Середня кількість днів для запобігання порушення за галузями

Таким чином, середній час запобігання порушення є значно меншим середнього часу виявлення порушення. Так, при запобіганні порушення, що виникає в сфері охорони здоров'я спеціалістами СЗІ витрачається в середньому 103 дні, а в науково-дослідницькій галузі цей час складатиме всього 53 дні.

Отримані статистичні дані свідчать про те, що процес виявлення порушення та його запобігання в сумарному значенні займає великий обсяг часу. Протягом усунення порушення ІТС підприємства функціонуватиме в модернізованому

вигляді, через що витрати на обробку та зберігання інформаційних активів в установі зростатимуть.

1.3 Аналіз нормативно-правової бази в сфері виявлення фактів саботажу інформаційної та кібербезпеки

Нормативно-правова база України в сфері виявлення фактів саботажу інформаційної та кібербезпеки нажаль лише продовжує свій повільний розвиток. Ба більше, в Україні немає уніфікованого визначення комп'ютерного саботажу. Лише стаття 361 Кримінального Кодексу України, яка трактує покарання за несанкціоновані дії, що впливають на роботу ЕОМ [4]. Однак ця стаття регламентує відповідальність, але не уточнює мотив, що є недоліком. В свою чергу Кримінальний Кодекс Естонії визначає комп'ютерний саботаж як «введення інформації або програм, їх модифікація, руйнування або блокування з метою створення перешкод в роботі комп'ютерної або телекомунікаційної системи» і визначає відповідальність саме за ці дії [5]. Враховуючи цей термін, поняття комп'ютерного саботажу в нормативно-правовій базі Естонії відділяється від поняття несанкціонованих дій в нормативно-правовій базі України. Саме тому в кваліфікаційній роботі за основу комп'ютерного саботажу буде взято визначення із Кримінального Кодексу Естонії.

В 1991 році за класифікатором Інтерполу комп'ютерний саботаж було віднесено до класифікатору інформаційних злочинів і визначено як вчинення протиправних дій, що призвели до видалення або привели до непридатного стану інформацію або складову комп'ютерної системи, що її оброблює [6].

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» визначено поняття «кіберінциденту», що може бути наслідком виникнення порушення інформаційної безпеки. Крім цього, цим Законом також розкрито основи забезпечення інтересів людини, суспільства та держави в цілому, національних інтересів України в кіберпросторі. Також цим Законом встановлено, що за порушення у сфері кібербезпеки особи несуть

відповідальність передбачену кримінальним, адміністративним та цивільним, законодавством [7].

Постановою Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» регламентовано, що держава повинна забезпечити мережевий захист компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури, серед яких захист від атак «нульового дня», фільтрації мережевого трафіка, виявлення та запобіганням атакам та вторгненням та ін. [8].

Законом України «Про інформацію» визначено поняття «захист інформації», а також статтею 9 затверджено, що захист інформації є одним із видів інформаційної діяльності [9].

Згідно до ДСТУ ISO 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки» термін «події інформаційної безпеки» [10] визначається як «будь-яка подія інформаційної безпеки, що може бути ідентифіковане появою певного стану системи, сервісу або мережі, яке вказує на можливе порушення політики ІБ або відмова заходів захисту, або виникнення невідомої раніше ситуації, яка може мати відношення до безпеки». Це визначення є суміжним поняттю «порушення інформаційної безпеки».

1.4 Система виявлення порушень: визначення і класифікація методів її розгортання

Виявлення порушень – це процес розкриття подій, що призвели до зміни початкового стану інформаційної безпеки.

Уніфікованого терміну «системи виявлення порушень» немає і кожен дослідник вкладає в це словосполучення свій зміст. Однак, спільним є те, що головним призначенням BDS є виявлення активності зловмисного ПЗ, заражених пристроїв або інших загроз в межах мережі після порушення, яке вже сталося. Тому, система виявлення порушень – це програмно-апаратний комплекс, призначений для виявлення активності зловмисних програм всередині мережі після порушення. BDS може бути як апаратним, так і програмним рішенням,

розробленим з метою виявлення ознак загрози та попередження організації про потенційно небезпечну діяльність [11].

Система виявлення порушень має 2 методи розгортання:

– позасмуговий моніторинг даних через TAP/SPAN (мережеве відведення/віддзеркалення портів);

– розгортання і встановлення кінцевих точок на АРМ користувачів системи.

Через складність проектування і велику вартість монтування впровадження системи виявлення порушень з-за допомогою першого методу відбувається дедалі рідше за інші.

Правильне розгортання BDS системи дозволяє:

– виявити активність зловмисних програм всередині мережі після акту порушення;

– синхронізувати свою роботу з системами безпеки першого рівня (система запобігання вторгнень, брандмауер та ін.);

– визначити порушення шляхом різних комбінацій евристики, оцінки ризику, аналізу трафіку, розуміння політику захисту даних, вивчення звітів про порушення та ін.;

– зосередитись на зловмисній діяльності в системі, яку вона захищає;

– знаходити APT та адаптивні загрози;

– виявляти кібератаки, які обійшли елементи управління мережевою безпекою;

– скоротити збитки від можливих успішних порушень.

1.5 Архітектура методів розгортання систем виявлення порушень

Архітектуру методу позасмугового моніторингу даних за допомогою віддзеркалення портів комутатора зображено на рисунку 1.3. Даний метод розгортання є більш фінансово затратним у встановленні та супроводі, аніж метод розгортання і встановлення кінцевих точок на АРМ користувачів системи. Однак перевагою цього методу є додатковий етап моніторингу вхідного трафіку, що в

разі настання події ІБ, завчасно інформує про факт порушення в тому або іншому елементі корпоративної мережі.

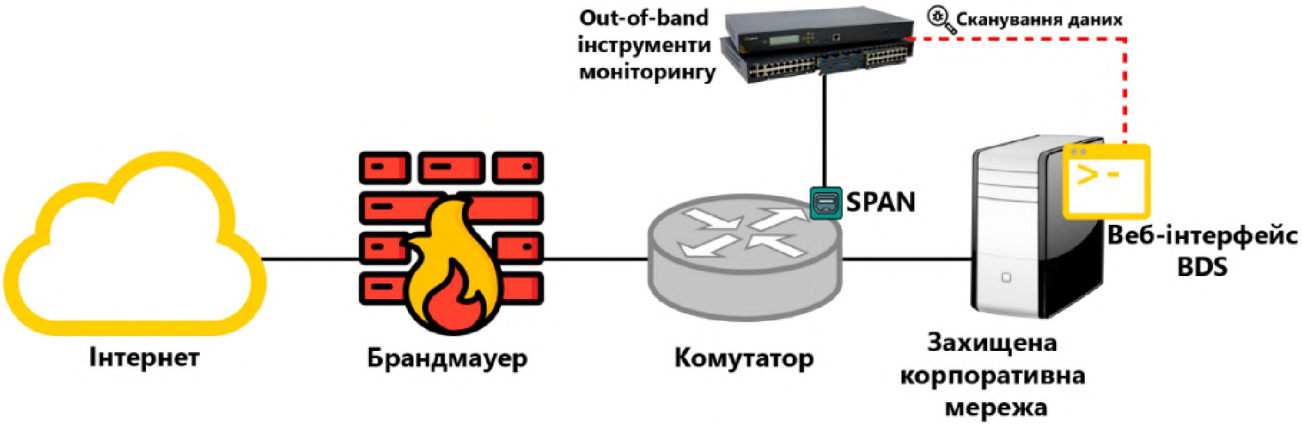

Рисунок 1.3 – Метод позасмугового моніторингу даних BDS

Комутатор зі SPAN портом віддзеркалює мережевий трафік і передає його зовнішнім (out-of-band) інструментам моніторингу. BDS сканує дані, що надходять від інструментів моніторингу і у разі виявлення підозрілої активності з одного або декількох портів комутатора, блокує роботу відповідного пристрою, що під'єднано до порту та ізолює його в системі. В ізоляції від основної корпоративної системи пристрій знаходиться до тих пір, поки адміністратор системи виявлення порушень не знайде джерело порушення і не усунить наслідки. Після чого, пристрою буде наданий доступ до корпоративної мережі установи.

Архітектуру розгортання і встановлення кінцевих точок на АРМ користувачів системи зображено на рисунку 1.4. Ця архітектура є уніфікованою в незалежності від обраного програмного рішення, оновлення та ін. Подальші дії із системою виявлення порушень будуть використовуватись за допомогою цього методу за рахунок його практичності.

Рішення щодо використання саме цієї архітектури розгортання було затверджено керівництвом досліджуваної установи в період проходження практики, оскільки воно не потребувало значних фінансових вливань в структуру існуючої корпоративної ІТС.

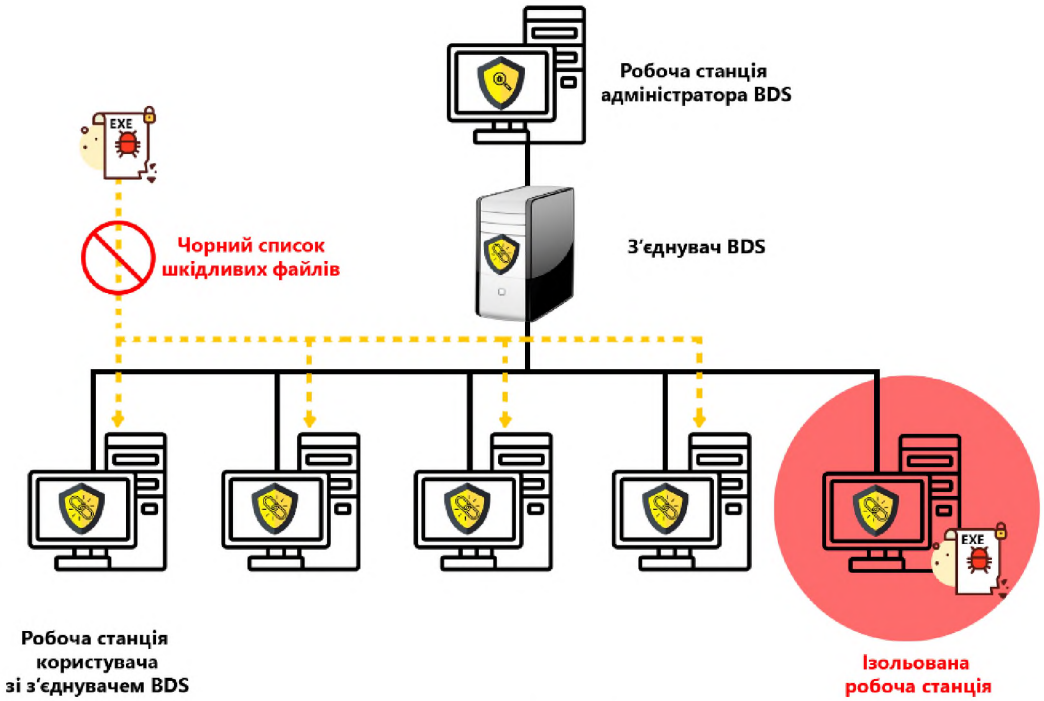

Рисунок 1.4 – Метод розгортання і встановлення кінцевих точок на АРМ користувачів системи

На робочій станції адміністратора системи виявлення порушення за допомогою веб-інтерфейсу BDS створюються облікові записи користувачів, вносяться налаштування в умови роботи системи, додаються політики інформаційної безпеки, що затверджені в установі та ін. Після того, як етап налаштування завершено, адміністратор BDS генерує і завантажує з'єднувач (або конектор) робочої станції користувача із загальною системою виявлення порушень. Останнім етапом є встановлення з'єднувача на робочі станції користувачів системи. Перевагою цього методу є те, що у разі виявлення порушення і ізоляції робочої станції, джерело порушення миттєво додається до чорного списку BDS, що унеможливлює поширення шкідливих файлів.

1.6 Об'єкти виявлення BDS

BDS направлена на виявлення порушень, що призводить, до таких типів атак та загроз, як:

- експлойт;
- зловмисне ПЗ;

– троян;

– автономні інфекції;

– вразливості нульового дня;

Це є основними атаками та загрозами, яким повинна протидіяти звичайна система виявлення порушень. Враховуючи зростання кібератак на мережу державних та приватних установ, програмні рішення системи виявлення порушень щодня вдосконалюються, адже у вивченні нових подій задіяно машинне навчання. Вони доповнюються з випуском оновлень захисних баз, випуском патчів безпеки та ін.

Крім того, система виявлення порушень підтримує корпоративну мережу підприємства під контролем, стежить за перебігом вхідного трафіку, що допомагає при проведенні розслідувань виникнення інцидентів.

1.6.1 Експлойт

Експлойт – це атака на комп'ютер, що використовує вразливість додатку для виконання неавторизованих задач.

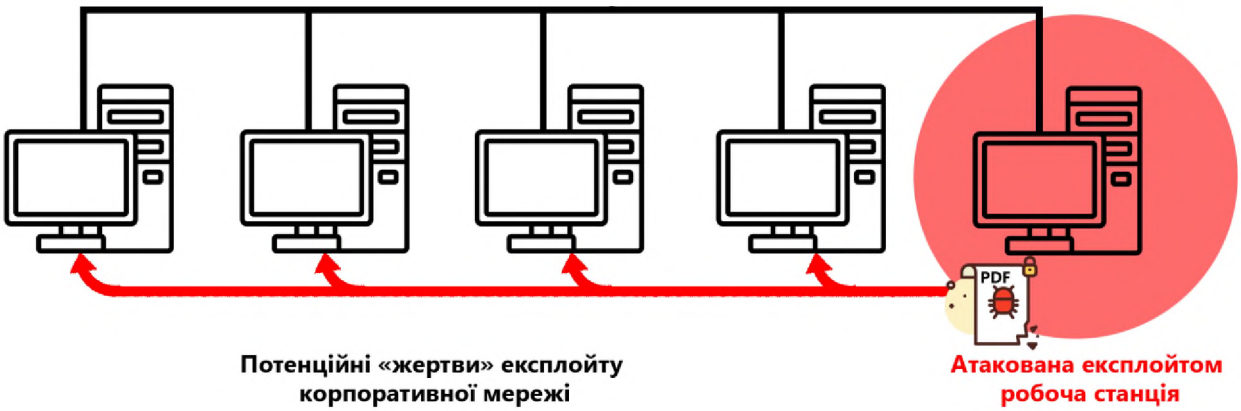

Рисунок 1.5 – Можливий сценарій розповсюдження експлойту в корпоративній мережі у разі несвоєчасного виявлення порушення

Мінімальним завданням системи виявлення порушень є ізолювати заражені пристрої інформаційно-телекомунікаційної системи та знайти активність від наступних типів експлойтів:

– drive-by експлойти, що направлені проти веб-браузерів, плагінів, розширень (наприклад Java, Flash);

– експлойти, які доставлені за допомогою соціальної інженерії:

– експлойти, які потребують взаємодії з користувачем;

– експлойти, які вбудовані в документи формату PDF, docx, HTML.

1.6.2 Зловмисне ПЗ

Зловмисне ПЗ – це настирливе програмне забезпечення, що призводить до таємного доступу до пристрою інформаційної системи без відома користувача цієї системи. Завантаження та встановлення зловмисного ПЗ потребує відповідних дій користувача системи. Система виявлення порушень повинна ізолювати в ІТС заражені пристрої, знаходячи такі дії, як:

– завантаження веб-браузера;

– завантаження вкладень електронної пошти;

– завантаження інформаційних активів, що зберігається на жорсткому диску пристрою та ін.;

– завантаження системного ПЗ, використання якого заборонено користувачам системи політикою ІБ установи і регламентовано в самій системі виявлення порушень.

1.6.3 Троян

Троян – це різновид зловмисного ПЗ, яке проникає в комп'ютер у вигляді ліцензованого ПЗ і розповсюджується за власним розсудом. Задачею системи виявлення порушень визначити підозрілу активність в переліку встановлених програм, запобігти її подальше розповсюдження, ізолюючи окремо від інформаційно-телекомунікаційної системи установи.

1.6.4 Автономні інфекції

Автономні інфекції – це інфікування інформаційної системи установи, шляхом використання заражених пристроїв (ноутбуків, планшетів та ін.) або

заражених носіїв інформації за межами корпоративної безпеки. До таких ситуацій можна віднести роботу в літаку, кафе з незахищеними мережами або при використанні заражених носіїв інформації (USB-накопичувач, зовнішній SSD-диск, тощо). Підключення до корпоративної мережі неідентифікованих пристроїв також може інфікувати внутрішню мережу установи. Завданням BDS є виявляти і повідомляти про такі інфекції та ізолювати її поширення шляхом зазначених дій.

1.6.5 Вразливості нульового дня

Вразливості нульового дня – це раніше невідома вразливість, яка функціонує в інформаційній системі і експлуатується зловмисниками в мережевих атаках. Завданням, що покладено на систему виявлення порушень, є визначення підозрілого трафіку, активності, процесів в інформаційній системі і їх своєчасне ізолювання від інших елементів ІТС установи. Крім того, адміністратору системи виявлення порушень рекомендується відстежувати оновлення баз захисту BDS і своєчасно встановлювати їх.

1.7 Постановка задачі

Враховуючи вищезазначене необхідно підкреслити, що корпоративна ІТС, на якій реалізована система виявлення порушень захищає від певного спектру порушень, що призводить до перелічених загроз у попередній главі, все ж є вразливою до виникнення фактів комп'ютерного саботажу. Таким чином, така інформаційно-телекомунікаційна система потребує вирішення наступних задач в дипломній роботі:

1) Дослідження ринку наявних систем виявлення порушень. Аналіз загроз і виявлення тих, що вказують на присутність фактів комп'ютерного саботажу.

2) Формування вимог до системи виявлення порушень, що мають стати чинником формування заходів для розпізнання фактів комп'ютерного саботажу.

3) Визначення найоптимальнішого програмного рішення, ураховуючи висунуті до нього вимоги.

4) Розробка методу реалізації системи виявлення порушень для розпізнання фактів комп'ютерного саботажу.

5) Визначення та аналіз економічної ефективності впровадження цього методу.

1.8 Висновок

Виявлення зловмисної активності в корпоративній мережі є складним завданням в організаціях, інформаційна система яких налічує десятки АРМ. Статистичні дані показали, що середній час виявлення порушення є набагато більшим, ніж час запобігання. В такому випадку державним та приватним установам необхідно контролювати події, що відбуваються всередині мережі, встановити засоби запобігання порушенням та максимально автоматизувати цей процес задля уникнення людського фактору. Система виявлення порушень є універсальним рішенням цієї проблеми, що з легкістю визначає, блокує порушення, а за необхідністю навіть впроваджує заходи протидії його подальшого розповсюдження. Сучасні програмні і апаратні рішення систем виявлення порушень вже зарекомендували як ефективний інструмент у виявленні порушень, що спонукають такі загрози, як: експлойти, APT-загрози, вразливості нульового дня та ін. Однак, невирішеним питанням є виявлення фактів комп'ютерного саботажу.

Система виявлення порушень є легкою у встановленні та подальшому управлінні цим комплексом. Організації, які хочуть захистити корпоративну мережу від потенційно небезпечних загроз, що призведуть до проблем у функціонуванні інформаційно-телекомунікаційної системи, а в деяких випадках до банкрутства, повинні обрати метод розгортання системи виявлення, який більше пасує до сформованого інформаційного, фізичного та обчислювального середовища. Найбільш розповсюдженим методом розгортання є встановлення кінцевих точок на АРМ користувачів, який дозволяє адміністратору системи виявлення порушень відстежувати стан корпоративної мережі установи через з'єднувач BDS, дистанційно встановлювати обмеження, правила блокування

зловмисних подій ІБ, правила ізоляції заражених пристроїв всередині корпоративної мережі та ін. Розгортання і управління системою виявлення порушень є економічно обґрунтованим, адже впровадження такої системи є значно дешевшим рішенням, аніж реалізація фактів комп'ютерного саботажу.

В розділі була наведена проблематика своєчасного виявлення порушень в цілому, а також спричинених комп'ютерним саботажем, визначені найдовше виявлювані і відновлювальні від порушень галузі економіки, визначено поняття системи виявлення порушень. Крім того, було проаналізовано нормативно-правову базу України в сфері виявлення порушень, сформовано визначення і висвітлено архітектуру методів розгортання системи виявлення порушень. В кваліфікаційній роботі були поставлені задачі, які необхідно вирішити в її межах.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Вибір профілю захищеності і аналіз загроз

Система виявлення порушень за своїм визначенням є захисним інструментом, що знаходить злоякісну активність всередині корпоративної мережі і сигналізує про можливе порушення. Однак, для того, щоб оцінити доцільність впровадження такої системи, необхідно обґрунтувати критичність типових корпоративних ІТС в питаннях виявлення комп'ютерного саботажу. Саме тому задачею дипломної роботи є розробка дієвого метод для розпізнання порушень, що можуть спонукати комп'ютерний саботаж.

Оскільки корпоративна ІТС обробляє інформацію з обмеженим доступом, до неї висувається ряд вимог, які повинні бути виконанні в умовах чинного законодавства України.

Відповідно до НД ТЗІ 2.5.005-99 в проаналізованій в період проходження практики ІТС було визначено функціональний профіль захищеності в КС, що входять до складу АС класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації [12].

3.КЦД.2 = { КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

Згідно з НД ТЗІ 2.5.004-99 [13]:

КД-2 – Базова довірча конфіденційність. Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

КА-2 – Базова адміністративна конфіденційність. Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості управління.

КО-1 – Повторне використання об'єктів. Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в

разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

КВ-2 – Базова конфіденційність при обміні. Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

ЦД-1 – Мінімальна довірча цілісність. Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

ЦА-2 – Базова адміністративна цілісність. Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

ЦО-1 – Обмежений відкат. Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат.

ЦВ-2 – Базова цілісність при обміні. Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

ДР-1 – Квоти. Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

ДВ-1 – Ручне відновлення. Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.

НР-2 – Захищений журнал. Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

НИ-2 – Одиночна ідентифікація і автентифікація. Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

НК-1 – Однонаправлений достовірний канал. Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ранжируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

НО-2 – Розподіл обов'язків адміністраторів. Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

НЦ-2 – КЗЗ з гарантованою цілісністю. Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

НТ-2 – Самотестування при старті. Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ранжируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

НВ-1 – Автентифікація вузла. Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

Висунуті вимоги до безпеки корпоративної ІТС стануть основою для захисту від вразливостей, що реалізують комп'ютерний саботаж.

При оцінці захищеності інформації всередині ІТС одну з найголовніших процедур складає розробка моделі загроз. Саме модель загроз є рушійною силою при прийнятті управлінського рішення щодо необхідності впроваджувати систему виявлення порушень в боротьбі з чинниками, що призводять до комп'ютерного саботажу.

Згідно з НД ТЗІ 1.1-003-99 під моделлю загроз розуміють абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз [14].

Оскільки модель загроз не має уніфікованого вигляду, розглянемо загрози, що можуть спричинити комп'ютерний саботаж в типових корпоративних ІТС. За основу взято методику побудови моделі загроз від НСД, що складається з:

– класифікації джерел загроз;

– класифікації вразливостей;

– аналізу взаємозв'язку загроз та вразливостей шляхом обчислення коефіцієнту небезпеки.

Джерела загроз можна поділити на антропогенні, техногенні та стихійні.

Коефіцієнт небезпеки обчислюється за формулою 2.1.

$$К_{неб} = \frac{К_1 \times К_2 \times К_3}{125} \quad (2.1)$$

де $К_1$, $К_2$, $К_3$ – показники критеріїв джерел загроз (оцінюється в діапазоні від 1 до 5);

125 – максимальне число добутків показників $К_{1\text{-}3}$.

Для антропогенних джерел загроз коефіцієнти визначаються як:

$К_1$ – ступінь доступності до об'єкту;

$К_2$ – ступінь кваліфікації і мотивації;

$К_3$ – рівень наслідків (фатальність).

Таблиця 2.1 – Антропогенні джерела загроз

Джерело загроз	$К_1$	$К_2$	$К_3$	$К_1 \cdot К_2 \cdot К_3$	$К_{неб}$
Основний персонал	5	4	5	100	0,800
Допоміжний персонал (прибиральниця, охоронець)	4	2	4	32	0,256
Технічний персонал (Інтернет провайдер, кур'єр, служба з доставки води та ін.)	3	2	2	12	0,096

Продовження таблиці 2.1

Джерело загроз	$К_1$	$К_2$	$К_3$	$К_1 \cdot К_2 \cdot К_3$	$К_{неб}$
Хакери	3	5	5	75	0,600
Конкуренти	3	4	4	48	0,384

Для техногенних джерел загроз коефіцієнти трактуються як:

$К_1$ – ступінь віддаленості від об'єкту захисту (можливість виникнення);

$К_2$ – наявність необхідних умов;

$К_3$ – рівень наслідків (фатальність).

Таблиця 2.2 – Техногенні джерела загроз

Джерело загроз	$К_1$	$К_2$	$К_3$	$К_1 \cdot К_2 \cdot К_3$	$К_{неб}$
Неліцензоване програмне забезпечення	3	5	5	75	0,600
Застаріле апаратне забезпечення	3	4	5	60	0,256
Мережа «Інтернет»	4	3	3	36	0,288
Лінії телефонного зв'язку	1	2	3	6	0,048
Система інженерних комунікацій	3	3	3	27	0,216

Для стихійних джерел загроз коефіцієнти визначаються як:

$К_1$ – особливості місцевості;

$К_2$ – наявність необхідних умов;

$К_3$ – рівень наслідків (фатальність).

Таблиця 2.3 – Стихійні джерела загроз

Джерело загроз	$К_1$	$К_2$	$К_3$	$К_1 \cdot К_2 \cdot К_3$	$К_{неб}$
Пожежа	3	3	4	36	0,288
Землетрус	2	1	3	6	0,048
Інші непізнані явища	2	1	2	4	0,032

Джерела загроз з коефіцієнтом нижче за 0,1 прийнято вважати тими, що не становлять суттєвої небезпеки.

Вразливості можна класифікувати на об'єктивні, суб'єктивні та випадкові.

Для класифікації вразливостей критерії визначаються наступним чином:

$К_1$ – ступінь впливу вразливості на неможливість ліквідувати наслідки (фатальність);

$К_2$ – можливість використання вразливості джерелом загроз

$К_3$ – кількість елементів об'єкту.

Формула вирахування коефіцієнту небезпеки вразливостей ідентична формулі вирахування коефіцієнту небезпеки джерела загроз (формула (2.1)).

Таблиця 2.4 – Об'єктивні вразливості

Вразливість	$К_1$	$К_2$	$К_3$	$К_1 \cdot К_2 \cdot К_3$	$К_{неб}$
Відсутність засобів захисту від комп'ютерного саботажу	5	5	3	75	0,600
Неналежне зберігання інформаційних активів	4	4	4	64	0,512
Неналежна захищеність мережі від атак зловмисників	3	4	3	36	0,288
Неправильне налаштування ПЗ	4	4	3	48	0,384
Місцезнаходження об'єкту	4	2	2	16	0,128

Таблиця 2.5 – Суб'єктивні вразливості

Вразливість	$К_1$	$К_2$	$К_3$	$К_1 \cdot К_2 \cdot К_3$	$К_{неб}$
Порушення режиму конфіденційності	3	3	3	27	0,216
Порушення режиму доступу на об'єкт	4	3	2	24	0,192
Помилки користувачів системи	2	4	4	32	0,256
Помилки системного адміністратора	4	4	4	64	0,512

Таблиця 2.6 – Випадкові вразливості

Вразливість	$К_1$	$К_2$	$К_3$	$К_1 \cdot К_2 \cdot К_3$	$К_{неб}$
Збої в роботі програмного забезпечення	4	3	4	48	0,384
Відмова в роботі технічних засобів	3	5	2	30	0,240
Пошкодження огороджувальних конструкцій	2	2	3	18	0,144
Пошкодження систем електроживлення	3	4	3	36	0,288

Визначимо взаємозв'язок перерахованих вище джерел загроз та вразливостей. Розрахунок і подальше визначення актуальних загроз, що можуть призвести до комп'ютерного саботажу, відбуватиметься за допомогою формули:

$$К_{неб} = К_{неб\ (д.з.)} \times К_{неб\ (вр.)} \quad (2.2)$$

де:

$К_{неб\ (д.з.)}$ – коефіцієнт небезпеки джерел загроз, який розраховано в таблицях 2.1-2.3;

$К_{неб\ (вр.)}$ – коефіцієнт небезпеки вразливостей, який розраховано в таблицях 2.4-2.6.

Таблиця 2.7 – Взаємозв'язок джерел загроз і об'єктивних вразливостей

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливість	$К_{неб\ (вр.)}$	$К_{неб}$
Антропогенні джерела загроз				
Основний персонал	0,800	Відсутність засобів захисту від комп'ютерного саботажу	0,600	0,480
		Неналежне зберігання інформаційних активів	0,512	0,410
		Неналежна захищеність мережі від атак зловмисників	0,288	0,230
		Неправильне налаштування ПЗ	0,384	0,307
Допоміжний персонал (прибиральниця, охоронець)	0,256	Відсутність засобів захисту від комп'ютерного саботажу	0,600	0,154
Хакери	0,600	Відсутність засобів захисту від комп'ютерного саботажу	0,600	0,360
		Неналежна захищеність мережі від атак зловмисників	0,288	0,173
		Неправильне налаштування ПЗ	0,384	0,230
Конкуренти	0,384	Відсутність засобів захисту від комп'ютерного саботажу	0,600	0,230
		Неналежна захищеність мережі від атак зловмисників	0,288	0,111
		Неправильне налаштування ПЗ	0,384	0,147
Техногенні джерела загроз				
Неліцензоване програмне забезпечення	0,600	Неправильне налаштування ПЗ	0,384	0,230
Застаріле апаратне забезпечення	0,256	Відсутність засобів захисту від комп'ютерного саботажу	0,600	0,154

		Неправильне налаштування ПЗ	0,384	0,098
Мережа «Інтернет»	0,288	Відсутність засобів захисту від комп'ютерного саботажу	0,600	0,173

Продовження таблиці 2.7

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливість	$К_{неб\ (вр.)}$	$К_{неб}$
Техногенні джерела загроз				
Мережа «Інтернет»	0,288	Неналежне зберігання інформаційних активів	0,512	0,147
		Неналежна захищеність мережі від атак зловмисників	0,288	0,083
		Неправильне налаштування ПЗ	0,384	0,111
Система інженерних комунікацій	0,216	Відсутність засобів захисту від комп'ютерного саботажу	0,600	0,130
		Неналежне зберігання інформаційних активів	0,512	0,111
Стихійні джерела загроз				
Пожежа	0,288	Місцезнаходження об'єкту	0,128	0,037

Таблиця 2.8 – Взаємозв'язок джерел загроз і суб'єктивних вразливостей

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливість	$К_{неб\ (вр.)}$	$К_{неб}$
Антропогенні джерела загроз				
Основний персонал	0,800	Порушення режиму конфіденційності	0,216	0,173
		Порушення режиму доступу на об'єкт	0,192	0,154
		Помилки користувачів системи	0,256	0,205
		Помилки системного адміністратора	0,512	0,410
Допоміжний персонал (прибиральниця, охоронець)	0,256	Порушення режиму доступу на об'єкт	0,192	0,049
Хакери	0,600	Порушення режиму доступу на об'єкт	0,192	0,115
Конкуренти	0,384	Порушення режиму доступу на об'єкт	0,192	0,074

Таблиця 2.9 – Взаємозв'язок джерел загроз і випадкових вразливостей

Джерело загроз	$К_{неб\ (д.з.)}$	Вразливість	$К_{неб\ (вр.)}$	$К_{неб}$
Техногенні джерела загроз				
Неліцензоване програмне забезпечення	0,600	Збої в роботі програмного забезпечення	0,384	0,230

		Відмова в роботі технічних засобів	0,240	0,144

Продовження таблиці 2.9

Джерело загроз	$К_{неб (д.з.)}$	Вразливість	$К_{неб (вр.)}$	$К_{неб}$
Техногенні джерела загроз				
Застаріле апаратне забезпечення	0,256	Відмова в роботі технічних засобів	0,240	0,062
Мережа «Інтернет»	0,288	Збої в роботі програмного забезпечення	0,384	0,111
		Відмова в роботі технічних засобів	0,240	0,069
Система інженерних комунікацій	0,216	Збої в роботі програмного забезпечення	0,384	0,083
		Відмова в роботі технічних засобів	0,240	0,052
Стихійні джерела загроз				
Пожежа	0,288	Пошкодження огороджувальних конструкцій	0,144	0,041
		Пошкодження систем електроживлення	0,288	0,083

Показники, які більше 0,1, несуть загрозу виникнення комп'ютерного саботажу всередині корпоративної ІТС.

2.2 Огляд існуючих програмних рішень системи виявлення порушень

Ринок представлених рішень систем виявлення порушень різноманітний і залежить від таких факторів, як: розмір підприємства, кількість АРМ, функціонал ПЗ та ін. Найбільші корпорації ІТ-індустрії, такі як ESET, Cisco, Symantec, Microsoft, FireEye, Cyberbit мають власні BDS-рішення, якими користуються різні компанії світу. Однак, встановлення та обслуговування програмного забезпечення від цих виробників для власників компаній можуть обійтися чималими коштами, що значно перевищуватиме самі збитки від реалізації загроз. Саме тому, при огляді представлених на ринку систем виявлення порушень важливим фактором буде вартість встановлення та утримання такої системи.

2.2.1 ESET Enterprise Inspector

ESET Enterprise Inspector (EEI) – це комплексна система виявлення порушень і реагування кінцевих точок, яка включає в себе такі функції, як виявлення інцидентів, управління інцидентами і реагуванням, збір даних, індикатори виявлення компромісів, виявлення аномалій, виявлення поведінки, порушення політики.

Основні переваги EEI: виявлення APT-загроз, розслідування порушень та їх виправлення, виявлення підозрілої поведінки, виявлення порушення політики ІБ компанії, миттєва ізоляція скомпрометованих пристроїв, оцінка критичності загроз, тегування важливих пристроїв/задач/файлів/процесів [15].

2.2.2 Cisco Advanced Malware Protection (AMP) for Endpoints

Cisco Advanced Malware Protection (AMP) for Endpoints – це єдина система вдосконаленого захисту від шкідливого ПЗ, що охоплює весь період атаки: до її початку, під час її проведення і після завершення. Система забезпечує безперервний аналіз і розширену аналітику, що підтримують можливості ретроспективної безпеки Cisco.

Основні переваги Cisco AMP for Endpoints: точковий захист АРМ, контроль епідемій, відстеження репутації файлу, ізольоване середовище, контроль ланцюга атаки, розширений аналіз загроз, виявлення підозрілої активності, спрощене утримання загроз, сигналізування при виявленні змін в роботі корпоративної мережі, контроль траєкторії файлу та скомпрометованих пристроїв [16].

2.2.3 Symantec Advanced Threat Protection

Symantec Advanced Threat Protection (ATP: Endpoint) – рішення щодо захисту від складних і цілеспрямованих загроз на рівні кінцевих точок, що забезпечує повний цикл безпеки від запобігання простих загроз до виявлення і реагування на більш складні: блокування загроз на різних етапах атаки з мінімальним числом помилкових спрацьовувань; виявлення аномалій і

розслідування підозрілих подій; оперативне відображення комплексних атак і наслідків від них на всіх кінцевих точках.

Основними перевагами Symantec ATP є: аналітика загроз, розслідування підозрілих подій, ізоляція заражених пристроїв та інше [17].

2.2.4 Microsoft Defender Advanced Threat Protection

Microsoft Defender Advanced Threat Protection забезпечує профілактичний захист від загроз, дозволяє виявляти порушення і виявляти загрози, в тому числі вразливості нульового дня, використовуючи сучасні можливості аналізу поведінки і машинного навчання. А також надає функціональність з розслідування і реагування на порушення.

Основні переваги Microsoft Defender Advanced Threat Protection: виявлення розширених атак, сигналізування при виявленні змін в корпоративній мережі, розслідування і усунення наслідків, взаємодія з Microsoft Defender, вбудована база даних аналітики загроз [18].

2.2.5 FireEye Endpoint Security

FireEye Endpoint Security – захист робочих станцій від сучасних кіберзагроз. Забезпечує співробітників інформаційної безпеки надійним інструментом для виявлення, аналізу та розслідування інцидентів в найкоротші терміни в порівнянні з традиційними підходами. Рішення дозволяє швидко і точно вживати заходів щодо подій на кінцевих станціях, а також дозволяє об'єднати активності, які виробляються на рівні мережі і на рівні робочих місць, що дозволяє скоротити часові витрати на відновлення в зв'язку з інцидентом інформаційної безпеки.

Основні переваги FireEye Endpoint Security: моніторинг і підтвердження порушень, блокування порушень, інтеграція з іншими платформами FireEye [19].

2.2.6 Cyberbit EDR

Cyberbit EDR – система виявлення порушень і реагування на них для кінцевих пристроїв, яка виявляє і запобігає появі невідомих загроз, в тому числі

програм-вимагачів, а також надає розширені можливості для проведення експертизи та виявлення різних загроз. Завдяки машинного навчання, аналізу шкідливих програм, поведінкової аналітиці та великих масивів даних щодо подій на IT-мережі Cyberbit EDR може швидко знаходити загрози, з якими не справляються традиційні системи ІБ, і автоматизувати процес виявлення загроз, економлячи при цьому робочий час аналітиків.

Основні переваги: виявлення невідомих APT-загроз в режимі реального часу, прискорення реагування на порушення, активний пошук загроз, визначення пріоритетності загроз [20].

2.3 Вимоги до системи виявлення порушень

Перелічені рішення систем виявлення порушень в розділі 2.1 мають спектр переваг, які зазначені виробником. Однак, для визначення найкращої системи виявлення порушень, що має розпізнавати факти комп'ютерного саботажу, порівняємо програмні рішення за наступними параметрами:

1) Ізоляція скомпрометованого пристрою та відновлення.
2) Наявність детального журналу історії подій.
3) Наявність детального списку задач з виправленнями.
4) Можливість зміни кінцевих точок.
5) Можливість припинення зловмисної діяльності.
6) Можливість відновити реєстру.
7) Можливість вимкнення облікового запису користувача BDS системи.
8) Можливість вимкнення мережевої плати.
9) Можливість відкату системи.
10) Розширене виявлення зловмисних програм.
11) Виявлення порушення політики ІБ.
12) Виявлення експлойтів.
13) Поведінкова аналітика.
14) Аналіз репутації файлів.
15) Наявність хмарних пісочниць.

16) Інфраструктура (на базі Windows, Windows Server, Linux, Mac, Android, Virtual).

17) Автоматизована кореляція інцидентів.

18) Візуалізація інцидентів.

19) Наявність робочого процесу управління сповіщеннями.

20) Перегляд порушень з урахуванням пріоритетності ризиків.

21) Наявність автоматизованої вибірки файлів інциденту.

22) Комплексний аналіз підозрілих файлів або процесів.

23) Формування електронних звітів стану системи.

24) Можливість роботи із інтеграційними протоколами Third Party Protocol, SDK та CGI.

Перелічені параметри стануть у нагоді для розгортання системи виявлення порушень з метою розпізнання фактів комп'ютерного саботажу.

2.4 Визначення шкали оцінювання програмних рішень системи виявлення порушень

Визначимо шкалу оцінювання BDS рішень, перелічених в розділі 2.2.

Таблиця 2.10 – Шкала оцінювання BDS рішень

Оцінка	Характеристика
0	Функціонал програмного рішення системи виявлення порушень взагалі не реалізовує поточний параметр.
1	Функціонал програмного рішення системи виявлення порушень частково реалізовує поточний параметр, ураховуючи певні обставини.
2	Функціонал програмного рішення системи виявлення порушень повністю реалізовує поточний параметр.

Перелічені вимоги є базисом для розгортання системи в типових корпоративних ІТС. Програмне рішення, яке отримає найбільший загальний бал, стане основою для формування методу розпізнавання фактів комп'ютерного саботажу.

2.5 Порівняльна характеристика функціоналу програмних рішень систем виявлення порушень

Таблиця 2.11 – Порівняння систем виявлення порушень

Параметр	ESET Enterprise Inspector	Cisco AMP for Endpoints	Symantec ATP	Microsoft Defender ATP	FireEye Endpoint Security	Cyberbit EDR	Примітка
Ізоляція скомпрометованого пристрою та відновлення	2	2	2	1	1	2	Програмні рішення від Microsoft та FireEye лише ізолюють скомпрометований пристрій
Наявність детального журналу історії подій	2	2	2	1	2	2	Microsoft Defender ATP має обмежений журнал подій, що складається з події, часу виникнення, місця виникнення
Наявність детального списку задач з виправленнями	1	2	1	1	1	1	Cisco AMP занотовує та зберігає всі виправлення BDS
Можливість зміни кінцевих точок	0	0	0	0	0	1	
Можливість припинення зловмисної діяльності	2	2	2	2	2	2	
Можливість відновлення реєстру	2	2	2	0	0	0	
Можливість вимкнення облікового запису користувача BDS	2	2	0	0	0	2	
Можливість вимкнення мережевої плати	2	2	0	0	0	0	

Можливість відкату системи	2	2	0	0	0	2	

Продовження таблиці 2.11

Параметр	ESET Enterprise Inspector	Cisco AMP for Endpoints	Symantec ATP	Microsoft Defender ATP	FireEye Endpoint Security	Cyberbit EDR	Примітка
Розширене виявлення зловмисних програм	0	1	2	2	0	2	Cisco AMP виявляє зловмисні програми, використовуючи лише власні бази даних
Виявлення порушення політики ІБ	2	2	0	0	0	0	
Виявлення експлойтів	2	2	2	0	0	0	
Поведінкова аналітика	1	2	2	1	1	2	
Аналіз репутації файлів	0	0	2	0	0	0	
Наявність хмарних пісочниць	0	2	2	0	2	0	
Інфраструктура (на базі Windows, Windows Server, Linux, Mac, Android, Virtual)	2	1	1	1	1	0	ESET Enterprise Inspector має повністю розвинену інфраструктуру
Автоматизована кореляція інцидентів	2	2	0	0	2	0	
Візуалізація інцидентів	0	2	0	0	0	0	Cisco AMP формує статистичні звіти за інцидентами, що відбулися всередині корпоративної мережі.
Наявність процесу управління сповіщеннями	2	2	0	2	0	0	

Продовження таблиці 2.11

Параметр	ESET Enterprise Inspector	Cisco AMP for Endpoints	Symantec ATP	Microsoft Defender ATP	FireEye Endpoint Security	Cyberbit EDR	Примітка
Перегляд порушень з урахуванням пріоритетності ризиків	2	2	2	2	2	2	
Наявність автоматизованої вибірки файлів інциденту	1	1	1	1	1	1	Вибірка файлів інциденту відбувається за допомогою людського фактору
Комплексний аналіз підозрілих файлів або процесів	2	2	2	0	2	0	
Формування електронних звітів стану системи	2	2	2	2	2	2	
Можливість роботи із інтеграційними протоколами Third Party Protocol, SDK та CGI	1	1	0	0	0	0	
Загалом	34	40	27	16	19	21	

Оцінка програмних рішень системи виявлення порушень показала, що найбільш ефективним і наповненим більшою кількістю необхідних функцій для розпізнання фактів комп'ютерного саботажу є Cisco Advanced Malware Protection (AMP) for Endpoints. Подальша розробка методу відбуватиметься саме з урахуванням можливостей цього ПЗ.

Система виявлення порушень здатна сигналізувати про можливий акт порушення в тій або іншій ланці корпоративної мережі. Однак, цій системі при класичному методі розгортанні не вистачає можливості дослідження ознак, що інформують про зміну фізичного стану елементу комп'ютерної системи. До таких ознак можна віднести:

– признак розпізнання обличчя (виявлення обличь, яким дозволений вхід в спостережувану зону і виявлення несанкціонованих обличь в цій зоні);

– признак несанкціонованого перетинання кордону контрольованої зони;

– признак зміни стану приміщення (виявлення нез'ясованих явищ в спостережуваному приміщенні, таких як засвіти камери, вогонь, дим та ін.).

В основі розробки методу реалізації системи виявлення порушень лежатиме створення такої системи, що зможе сигналізувати про наявність цих вищеперерахованих фактів, які можуть призвести до комп'ютерного саботажу.

2.6 Розробка методу реалізації системи виявлення порушень для розпізнання фактів комп'ютерного саботажу

Обране програмне рішення від Cisco має перелік переваг, однак їх недостатньо для того, щоб забезпечити захист від можливого втручання в роботу корпоративної ІТС з подальшим видаленням інформації або виходу із ладу елементів комп'ютерної системи.

Цим недоліком є невиконана вимога аналізу репутації файлів і можливість зміни кінцевих точок. Автоматична оцінка безпечності файлів і процесів, що виконуються на АРМ працівника є додатковим рівнем захищеності від можливих порушень. Зміна кінцевих точок сприяє легшій модифікації корпоративної ІТС у разі виходу із ладу елементу ІТС, на якому оброблюється ІзОД. Однак

невиконаною задачею системи виявлення порушень стала можливість розпізнання виходу із ладу такого елементу і своєчасне сигналізування про це адміністратору системи. Ще одним рівносильним недоліком стала неможливість сигналізування про руйнування або модифікацію інформації, що оброблюється в корпоративній ІТС.

Таким чином, в умовах типових корпоративних ІТС оптимальним рішенням для розпізнавання фактів комп'ютерного саботажу з використанням Cisco AMP for Endpoints стане:

1 Впровадження засобів неперервного контролю за фізичним станом ЕОМ в корпоративній ІТС.

2 Розробка організаційних заходів контролю цілісності інформації в корпоративній ІТС.

2.6.1 Впровадження засобів неперервного контролю за фізичним станом ЕОМ в корпоративній ІТС

Як було доведено в попередньому розділі, система виявлення порушень за своїм визначенням є програмно-апаратним комплексом, яка може контролювати стан корпоративної мережі, але не в змозі контролювати фізичний стан елементів цієї мережі. Тому, одним із запропонованих рішень реалізації BDS для розпізнання факту комп'ютерного саботажу, що призводить до виходу із ладу ЕОМ є встановлення детектору саботажу систем відеоспостереження із подальшою інтеграцією із системою виявлення порушень.

Детектор саботажу – це засіб моніторингу і фіксації порушень з камер відеоспостереження з подальшим виявленням тривожних ситуацій, таких як втрата відеосигналу, розфокусування зображення, перекриття камери стороннім предметом, відвертанням камери та ін.

Звичайна система відеоспостереження лише фіксує події, які відбуваються в контрольованій зоні організації, і дозволяє встановити джерело порушень, що вже сталося. В той час як система відеоспостереження із встановленим детектором саботажу інформує адміністратора BDS в панелі керування системою виявлення

порушень про розпізнання можливих фактів саботажу. В свою чергу, адміністратор системи приймає завчасне рішення про ліквідацію саботажу шляхом впровадження контрзаходів.

Головна відмінність звичайної системи відеоспостереження і системи відеоспостереження із детектором саботажу полягає у відеоаналітиці. Звичайна система відеоспостереження залежить від людського фактору, а саме від моніторингу і контролю, в той час як використовуючи детектор саботажу, штучний інтелект самостійно аналізує все, що відбувається в режимі реального часу і сигналізує про порушення тільки у випадку, коли на те є необхідні признаки.

Рисунок 2.1 – Відмінність звичайної системи відеоспостереження від системи відеоспостереження із використанням детектору саботажу

Саме тому було обрано систему відеоспостереження з використанням детектору саботажу.

Детектори саботажу мають змогу працювати з протоколами, які дозволяють інтегрувати власну роботу із роботою різних засобів захисту ІТС. Цими інтеграційними протоколами є Third Party Protocol, SDK та CGI.

Таблиця 2.12 – Тлумачення інтеграційних протоколів

Назва протоколу	Опис
TPP (Third Party Protocol)	Клієнт-серверний протокол з трьома типами відношень: запит (використовується клієнтом), повідомлення (використовується сервером для надсилання інформації про стан клієнту), відповідь (надіслані як відповідь на запит). TPCP використовується для ініціювання, контролю та спостереження за сеансами між віддаленими сторонами.
SDK (Software Development Kit)	Набір засобів розробки, що дозволяє фахівцям з програмного забезпечення створювати додатки для певного пакету програм, програмного забезпечення базових засобів розробки, апаратної платформи, комп'ютерної системи, ігрових консолей, операційних систем і інших платформ.
CGI (Common Gateway Interface)	Стандарт інтерфейсу, використовуваного для зв'язку зовнішньої програми з веб-сервером. Програму, яка працює за таким інтерфейсу спільно з веб-сервером, прийнято називати шлюзом, хоча багато хто воліє назви «скрипт» (сценарій) або «CGI-програма». По суті дозволяє використовувати консоль введення і виведення для взаємодії з клієнтом.

Ці інтеграційні протоколи полягають за основу комутації системи виявлення порушень із детектором саботажу. Впровадження детектору саботажу реалізує недолік системи виявлення порушень в питанні виходу із ладу елементів комп’ютерної системи, своєчасно повідомляючи про можливе порушення, що відбувається в тій або іншій області контрольованої зони організації.

На ринку детекторів саботажу в Україні найбільш розповсюджено представлені програмні рішення від TRASSIR, Macroscop.

Порівняємо обидва рішення за наступними критеріями:

1) Підрахунок відвідувачів.

2) Виявлення обличь.

3) Відстеження переміщення осіб між камерами в режимі реального часу.

4) Розпізнання обличь.

5) Розпізнання автомобільних номерів.

6) Підрахунок кількості людей.

7) Можливість встановлення ПЗ на робоче місце працівника (мережевий клієнт).

8) Синхронізація із системами виявлення порушень.

Порівняємо програмні рішення за переліченими параметрами з використанням шкали від 0 до 1, де:

0 – поточний параметр не реалізовано;

1 – поточний параметр реалізовано.

Таблиця 2.13 – Порівняння детекторів саботажу

Параметр	TRASSIR	Macroscop
Підрахунок відвідувачів	0	1
Виявлення обличь	1	1
Відстеження переміщення осіб між камерами в режимі реального часу	1	1
Розпізнання обличь	1	0
Розпізнання автомобільних номерів	1	1
Підрахунок кількості людей	0	1
Можливість встановлення ПЗ на робоче місце працівника (мережевий клієнт)	1	0
Синхронізація із системами виявлення порушень	1	1
Невелика вартість встановлення	1	0
Загалом	6	5

Отримані показники свідчать про те, що найкращим детектором саботажу у співвідношенні «ціна-якість» є TRASSIR.

2.6.1.1 Інтеграція системи виявлення порушень із детектором саботажу

Проведемо практичне налаштування системи виявлення порушень із детектором саботажу і відтворимо признак розпізнання обличчя.

Для того, щоб правильно інтегрувати досліджуваний Cisco AMP for Endpoints із обраним детектором саботажу TRASSIR, в налаштуваннях системи виявлення порушень необхідно дозволити використання протоколу TTP і додати систему відеоспостереження у перелік інтеграції. Ці дії дозволять системі виявлення порушень використовувати інтеграційні протоколи для роботи із програмно-апаратним забезпеченням, яке також використовує для комутації ці

протоколи, і з'єднають систему відеоспостереження разом із системою виявлення порушень.

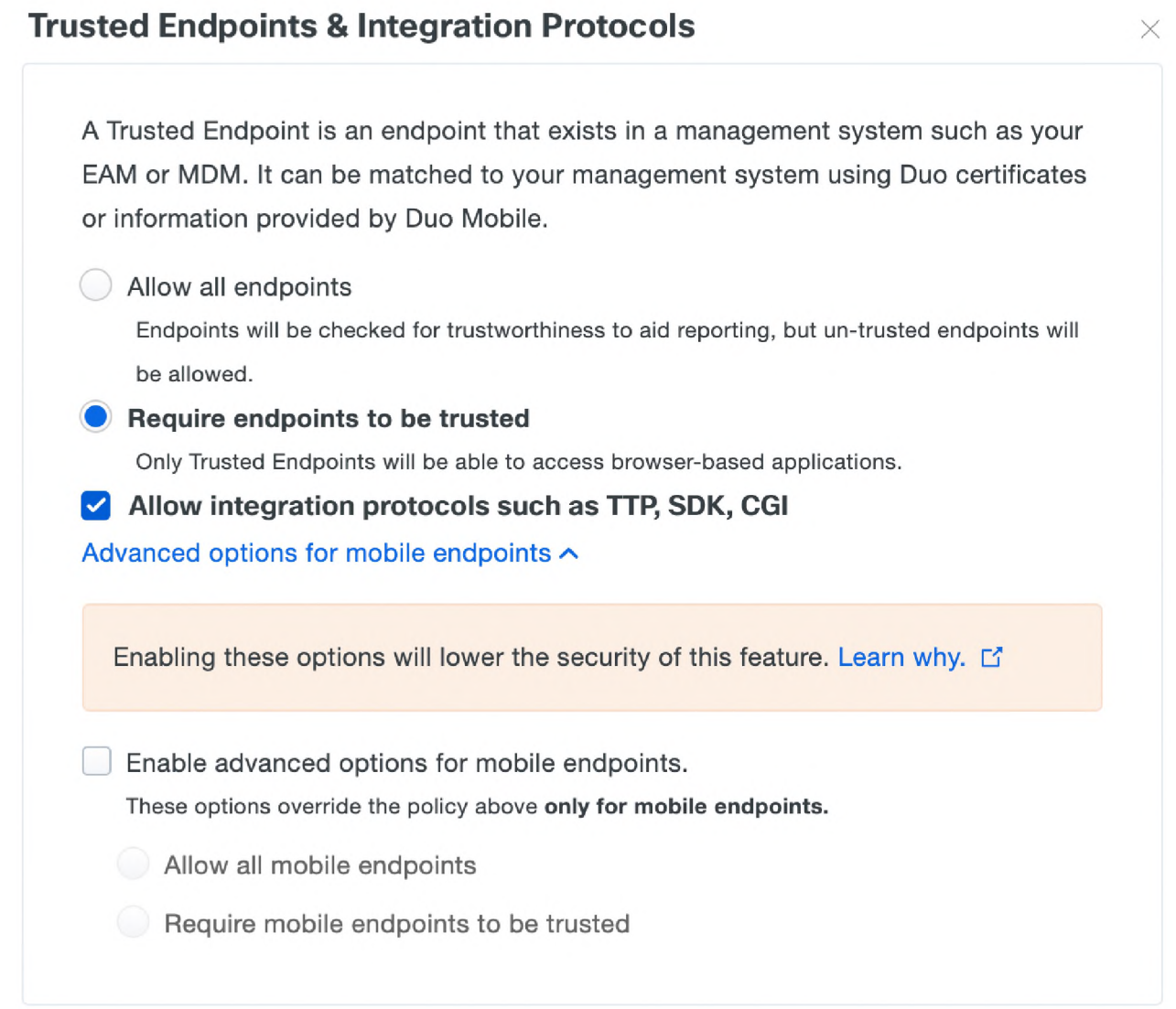

Рисунок 2.2 – Вікно налаштування інтеграції в Cisco AMP for Endpoints

Скріншот з додаванням в перелік інтеграції системи відеоспостереження з вимог конфіденційності підприємства додано не буде.

Схожі налаштування також відбуваються в програмному забезпеченні детектору саботажу TRASSIR.

Змоделюємо ситуацію. Нехай на контрольовану зону підприємства увійде людина, яка несанкціоновано перейде пропускний пункт без ідентифікації і буде рухатися уздовж контрольованої зони. Детектор саботажу, в разі правильного

налаштування, за своїм звичним призначенням повинен виявити перетинання кордону контрольованої зони неопізнаної людини і оголосити тривогу, додатково повідомивши про це адміністратора системи відеоспостереження.

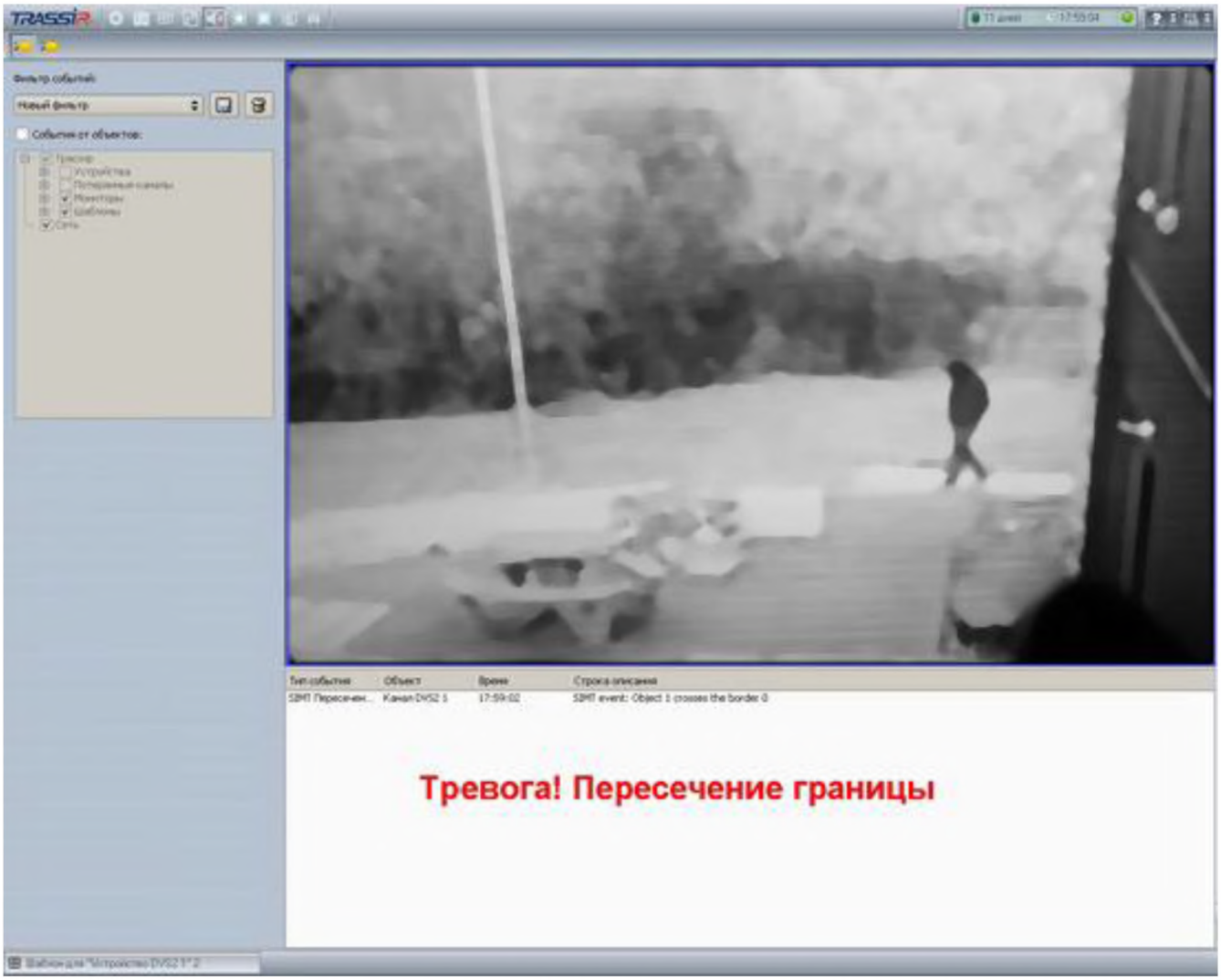

Рисунок 2.3 – Виявлення неопізнаної людини в програмному вікні TRASSIR

Факт можливого саботажу було виявлено в детекторі саботажу. Однак, сигнал (окрім детектору саботажу) повинен бути відображений в самій системі виявлення порушень, про що невідкладно повідомлено адміністратора системи. Саме цей показник може зафіксувати правильність налаштування та працездатність запропонованого методу. Випадки помилкових спрацювань можливі, але вони потребують детального вивчення цього питання, що не входить в межі кваліфікаційної роботи. Працездатність запропонованого методу в

подальшому може залежати від функціоналу програмного забезпечення обраної системи виявлення порушень та детектору саботажу.

Рисунок 2.4 – Повідомлення про факт виявлення порушення в Cisco AMP for Endpoints

Таким чином, отримане повідомлення у вікні системи виявлення порушень свідчить про те, що запропоноване рішення є ефективним у розпізнанні фактів комп'ютерного саботажу.

2.6.2 Розробка організаційних заходів контролю цілісності інформації в корпоративній ІТС

Оскільки до комп'ютерного саботажу відноситься не тільки вихід із ладу елементів комп'ютерної системи, але й знищення або модифікація інформації, тому для недопущення виникнення такого порушення, адміністратору системи виявлення порушень та її користувачам необхідно дотримуватися певного

переліку правил, що в подальшому унеможливить цю подію. Запропонований перелік правил можна включити в Посадову інструкцію користувачів системи.

2.6.2.1 Перелік правил адміністратора системи виявлення порушень для забезпечення контролю цілісності інформації в корпоративній ІТС

1 Опис. Цей перелік визначає основні правила контролю цілісності інформації, що оброблюється для адміністратора системи виявлення порушень (далі – Адміністратор СВП).

2 Призначення. Цей перелік призначений для уникнення фактів комп'ютерного саботажу шляхом модифікації або знищення інформації та формує перелік дій Адміністратора СВП для контролю за цілісністю інформації, що оброблюється.

3 Область застосування. Вимоги цього переліку стосуються Адміністратора СВП.

4 Правила.

4.1 Адміністратор СВП повинен переглядати надані права доступу користувачів СВП до інформації в корпоративній ІТС установи не рідше 1 разу на місяць.

4.2 Адміністратор СВП повинен видаляти права доступу до інформації облікових записів користувачів СВП, які були звільнені. Адміністратор СВП також повинен переглядати наявність таких облікових записів 1 раз на місяць.

4.3 Адміністратор СВП повинен приховати можливість видалення записів в журналі подій для користувачів СВП.

4.4 Адміністратор СВП повинен робити резервне копіювання даних не рідше 1 разу на 3 місяці.

4.5 Адміністратор СВП повинен приховати можливість надання прав зміни налаштування в системі виявлення порушень для користувачів СВП.

4.6 Адміністратор СВП повинен 1 раз в 3 місяці проводити «тест на проникнення», узгоджуючи час проведення і область проникнення з Керівництвом установи.

4.7 Адміністратор СВП повинен проводити «тести на проникнення» за допомогою власних можливостей, що не суперечить вимогам чинного законодавства України, або залучаючи до цього фахівців цієї сфери. Обране рішення повинно бути узгоджене з Керівництвом установи і письмово задекларованe розпорядженням з підписом Керівника установи.

4.8 Адміністратор СВП, виявивши зміну стану інформації, що оброблюється в корпоративній ІТС, повинен негайно повідомити про це Керівництво установи та діяти за їх розпорядженням.

2.6.2.2 Перелік правил користувачів системи виявлення порушень для забезпечення цілісності інформації в корпоративній ІТС

1 Опис. Цей перелік визначає основні правила для забезпечення цілісності інформації, що оброблюється для користувачів системи виявлення порушень (далі – Користувач СВП).

2 Призначення. Цей перелік призначений для уникнення фактів комп'ютерного саботажу шляхом модифікації або знищення інформації та формує перелік дій Користувача СВП для забезпечення цілісності інформації, що оброблюється в корпоративній ІТС.

3 Область застосування. Вимоги цього переліку стосуються всіх Користувачів СВП.

4 Правила.

4.1 У разі виявлення фактів зміни стану або видалення критично важливої інформації Користувач СВП повинен негайно повідомити про це Адміністратора СВП.

4.2 Користувачу СВП заборонено вносити зміни в налаштування системи виявлення порушень, намагатися видалити інформацію без наявних для цього прав доступу.

4.3 Користувач СВП при роботі з інформацією повинен використовувати тільки службові носії інформації (USB накопичувачі, зовнішні диски, тощо).

4.4 Користувачу СВП заборонено змінювати налаштування системи, видаляти системний журнал подій, тощо.

4.5 Користувач СВП у разі виявлення порушення на робочій станції повинен перервати свою роботу та викликати Адміністратора СВП на своє робоче місце.

4.6 Користувачу СВП заборонено самостійно усувати порушення та приховувати факт виявлення порушення.

4.7 У разі виходу із ладу робочої станції Користувач СВП повинен викликати Адміністратора СВП на своє робоче місце.

Запропонована методика реалізації системи виявлення порушень полягає у встановленні детектора саботажу, формування переліку правил для персоналу установи допоможе вчасно виявити і протидіяти можливим фактам комп'ютерного саботажу.

2.7 Висновок

Спеціальна частина складається з обґрунтування доцільності впровадження системи виявлення порушень в питанні розпізнавання комп'ютерного саботажу шляхом визначення функціонального профілю захищеності АС та побудови моделі загроз.

Отримані результати, що доводять наявність фактів комп'ютерного саботажу в корпоративній ІТС, стали одним із головних чинників в підборі наявних програмних рішень системи виявлення порушень. Була проведена порівняльна характеристика всіх існуючих програмних продуктів за критеріями, що повинні задовольняти кожну СВП, і обрано найоптимальніше рішення, що полягло за основу розробки методу розпізнання комп'ютерного саботажу шляхом використання такої системи.

Обрана система виявлення порушень з урахуванням інженерних та організаційних заходів, таких як встановлення детекторів саботажу та впровадження переліку правил користувачів та адміністраторів СВП полягли в основу методу реалізації системи виявлення порушень для розпізнання фактів

комп'ютерного саботажу. Також, питання підбору детектору саботажу розглядалося з урахуванням критеріїв, що можуть сигналізувати факт виходу із ладу елементів корпоративної ІТС. Крім того, задля закріплення теоретичних засад запропонованого методу було практично реалізовано і перевірено ефективність інтегрування системи відеоспостереження із використанням детектору саботажу із системою виявлення порушень.

Запропонований метод було впроваджено в корпоративну ІТС місця проходження практики. Загальний висновок ефективності і доцільності методу було висвітлено керівництвом організації окремим відгуком.

3 ЕКОНОМІЧНА ЧАСТИНА

3.1 Обґрунтування витрат на реалізацію запропонованого методу

Метою обґрунтування витрат на впровадження методу реалізації системи виявлення порушень для розпізнання фактів комп'ютерного саботажу є доведення доцільності запропонованих рішень шляхом розрахунку капітальних та експлуатаційних витрат, оцінка величини можливого збитку від атаки, визначення та аналіз показників економічної ефективності.

3.2 Розрахунки витрат на реалізацію запропонованого методу

При розробці та впровадженні запропонованого методу необхідно розрахувати витрати обстежуваної установи. З урахуванням вимоги керівництва назву установи в дипломній роботі змінено на ТОВ «АвтоПлюс».

3.2.1 Розрахунок капітальних (фіксованих) витрат

Капітальні (фіксовані) витрати на розробку та впровадження запропонованого методу складають [21]:

$$К = К_{пр} + К_{аз} + К_{зпз} + К_{навч} + К_{н} \quad (3.1)$$

де $К_{пр}$ – вартість розробки системи виявлення порушень та залучення для цього зовнішніх консультантів, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{навч}$ – витрати на навчання технічних спеціалістів і обслуговуючого персоналу, тис. грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

Вихідні дані становлять:

$К_{пр}$ = 13500 грн (вартість розробки системи виявлення порушень та залучення до цього зовнішніх консультантів);

$К_{аз}$ = 16345 грн (вартість додаткових камер відеоспостереження);

$$К_{зпз} = 64760 \text{ грн} \begin{cases} 54960 \text{ грн за СВП } Cisco\ AMP\ for\ Endpoints \\ 9800 \text{ грн за детектор саботажу } TRASSIR \end{cases}$$

Вартість закупівлі ліцензійного програмного забезпечення системи виявлення порушень Cisco AMP for Endpoints становить 54960 грн, враховуючи кількість робочих станцій на проаналізованому підприємстві.

Вартість закупівлі ліцензійного програмного забезпечення детектору саботажу TRASSIR до існуючих камер відеоспостереження (враховуючи їхню кількість) становить 9800 грн.

$К_{навч}$ = 13450 грн (витрати на навчання адміністратора системи виявлення порушень);

$К_{н}$ = 2750 грн (витрати на встановлення обладнання та налагодження системи виявлення порушень).

Визначимо капітальні витрати:

$$К = 13500 + 16345 + 64760 + 13450 + 2750 = 110805 \text{ грн}$$

3.2.2 Розрахунок річних поточних (експлуатаційних) витрат

Річні поточні витрати складаються з:

$$С = С_а + С_{ел} + С_о + С_{тос} \quad (3.2)$$

де $С_а$ – річний фонд амортизаційних відрахувань;

$С_{ел}$ – вартість електроенергії, що споживається апаратурою системи виявлення порушень протягом року:

$$С_{ел} = Р \times F_р \times Ц_е \quad (3.3)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи виявлення порушень;

$Ц_е$ – тариф на електроенергію, грн/кВт·годин;

$С_о$ – витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу;

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс системи виявлення порушень.

Річний фонд амортизаційних відрахувань ($С_а$) складає 25% від капітальних витрат:

$$С_а = 110805 \times 0{,}25 = 27701{,}25 \text{ грн}$$

Потужність (Р) комп'ютерів та ноутбуків становить 1,12 кВт.

За 40-годинного робочого тижня річний фонд робочого часу системи інформаційної безпеки ($F_р$) становить 1920.

Тариф на електроенергію ($Ц_е$) складає 1,96 грн/кВт·годин.

Вартість електроенергії, що споживається апаратурою системи виявлення порушень протягом року ($С_{ел}$) становить:

$$С_{ел} = 1{,}12 \times 1920 \times 1{,}96 = 4214{,}78 \text{ грн}$$

Витрати на технічне й організаційне адміністрування та сервіс системи виявлення порушень ($С_о$) складають 11500 грн.

$$С_о = 11500 \text{ грн}$$

Витрати на технічне й організаційне адміністрування та сервіс системи виявлення порушень ($С_{тос}$) визначаються ТОВ «АвтоПлюс» і складають 2% від вартості капітальних витрат.

$$С_{тос} = 110805 \times 0,02 = 2216,10 \text{ грн}$$

Визначимо річні поточні витрати:

$$С = 27701,25 + 4214,78 + 11500 + 2216,10 = 45632,13 \text{ грн}$$

3.3 Оцінка величини можливого збитку від атаки

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V \quad (3.4)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = \frac{\sum З_с \times Ч_с}{F} \times t_п \quad (3.5)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 год)

$З_с$ – місячна заробітна плата співробітника атакованого вузла або сегмента корпоративної мережі з нарахуванням єдиного соціального внеску, грн на місяць;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.;

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин.

Розрахунок витрат на заробітну плату співробітників за місяць з нарахуванням ЄСВ приведено в таблиці 3.1.

Таблиця 3.1 – Витрати на заробітну плату співробітників за місяць з нарахуванням ЄСВ

Посада	Кількість співробітників, осіб	Місячна заробітна плата, грн	Витрати на заробітну плату, грн	Єдиний соціальний внесок, грн	Витрати на заробітну плату з урахуванням ЄСВ, грн
Регіональний директор	1	25000	25000	5500	30500
Фінансовий директор	1	18700	18700	4114	22814
Керівник відділу продажу авто	1	15000	15000	3300	18300
Керівник відділу прокату авто	1	15500	15500	3410	18910
Менеджер з продажу авто	3	12000	36000	7920	43920
Менеджер з прокату авто	2	12000	24000	5280	29280
Менеджер з відновлення авто	1	10500	10500	2310	12810
Системний адміністратор	1	11800	11800	2596	14396
Всього					190930

Визначимо оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі:

$$П_п = (190930 / 176) \times 4 = 4339{,}32 \text{ грн}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч} \quad (3.6)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с \times Ч_с}{F} \times t_{ви} \quad (3.7)$$

де $t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин.

$$П_{ви} = (190930 / 176) \times 5 = 5424{,}15 \text{ грн}$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати системного адміністратора:

$$П_{пв} = \frac{\sum З_о \times Ч_о}{F} \times t_в \quad (3.8)$$

де $З_о$ – місячна заробітна плата системного адміністратора з нарахуванням єдиного соціального внеску, грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу, осіб;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$$З_о = 11800 + 11800 \times 0,22 = 14396 \text{ грн}$$

$$П_{пв} = (14396 / 176) \times 3 = 245,39 \text{ грн}$$

Визначимо вартість відновлення працездатності вузла або сегмента корпоративної мережі:

$$П_в = 5424,15 + 245,39 + 0 = 5669,54 \text{ грн}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{F_г} \times (t_п + t_в + t_{ви}) \quad (3.9)$$

де О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік;

$F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$V = 12792000 / 2080 \times (4 + 3 + 5) = 73800 \text{ грн}$$

Визначимо упущену вигоду від простою атакованого вузла або сегмента корпоративної мережі:

$$U = 4339,32 + 5669,54 + 73800 = 83808,86 \text{ грн}$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$B = \sum\sum U \times N \times I \quad (3.10)$$

де N – середнє число можливих атак на рік;

I – число атакованих вузлів або сегментів корпоративної мережі.

$$B = 83808,86 \times 4 \times 11 = 3687589,80 \text{ грн}$$

3.4 Загальний ефект від впровадження методу

Загальний ефект від впровадження запропонованого методу визначається з урахуванням ризиків виникнення фактів комп'ютерного саботажу і становить:

$$E = B \times R - C \quad (3.11)$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі організації;

R – очікувана ймовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи виявлення порушень, тис. грн.

За величину R береться середнє значення коефіцієнту небезпеки із моделі загроз, що розташовано в таблиці 2.9 і дорівнює 0,203.

$$E = 3687589,80 \times 0,203 - 45632,13 = 702948,60 \text{ грн}$$

3.5 Визначення та аналіз показників економічної ефективності системи виявлення порушень

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломної роботи, здійснюється на основі визначення та аналізу наступних показників:

а) коефіцієнт повернення інвестицій (ROI).

б) термін окупності капітальних інвестицій T_o.

Коефіцієнт повернення інвестицій показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки. Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = \frac{E}{K} \tag{3.12}$$

де ROSI – коефіцієнт повернення інвестицій;

Е – загальний ефект від впровадження системи інформаційної безпеки, тис. грн;

К – капітальні інвестиції, що забезпечили цей ефект, тис. грн.

$$\text{ROSI} = 702948{,}60 / 110805 = 6{,}34$$

Термін окупності капітальних інвестицій показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_o = \frac{K}{E} = \frac{1}{ROSI} \tag{3.13}$$

де T_o – термін окупності капітальних інвестицій.

T_o = 110805 / 702948,60 = 0,16, що становить 59 днів.

3.6 Висновок

В економічному розділі було обґрунтовано економічну доцільність впровадження запропонованого методу реалізації системи виявлення порушень для розпізнання фактів комп'ютерного саботажу.

Розраховано капітальні і експлуатаційні витрати, які показали, що на розробку і впровадження запропонованого методу керівництво організації витратить 110805 грн, а щорічні витрати на експлуатацію системи виявлення порушень з можливістю виявляти факти комп'ютерного саботажу становитимуть 45632,13 грн.

Визначено величину можливого збитку від реалізованої атаки через упущену вигоду, що складає 702948,60 грн.

Крім того, було оцінено термін окупності капітальних інвестицій, що складає 0,16 частку року, що приблизно становить 59 днів.

Отримані результати свідчать про те, що запропонований метод реалізації системи виявлення порушень можна вважати економічно ефективним рішенням в питаннях виявлення фактів комп'ютерного саботажу, що захистить корпоративну ІТС від можливого виходу із ладу певного елементу системи або від знищення чи несанкціонованої модифікації важливих інформаційних активів установи шляхом своєчасного оповіщення про це адміністратора СВП.

ВИСНОВКИ

В першій частині кваліфікаційної роботи було обґрунтовано актуальність проблеми своєчасного виявлення і запобігання порушень в різних галузях економіки, висвітлено існуючі шляхи вирішення цієї проблеми шляхом впровадження системи виявлення порушень, перелічено доцільність її використання, а також визначено недоліки в питанні розпізнання фактів, що можуть призвести до комп'ютерного саботажу. Окрім того, було проаналізовано нормативно-правову базу в сфері виявлення порушень кібербезпеки, сформовано поняття системи виявлення порушень і класифіковано методи розгортання, а також побудовано архітектуру розгортання. Визначено об'єкти виявлення такої системи. Поставлено задачі, що необхідно вирішити в ході виконання цієї роботи.

В другій частині кваліфікаційної роботи було обґрунтовано необхідність впровадження системи виявлення порушень в питанні розпізнавання фактів комп'ютерного саботажу шляхом обрання функціонального профілю захищеності АС і побудови моделі загроз. Також було проаналізовано існуючі програмні рішення системи виявлення порушень, сформовано вимоги до системи виявлення порушень, а також виконано порівняльну характеристику наявних рішень і обрано найоптимальнішу. Крім того, було запропоновано впровадити в корпоративну ІТС установи детектори саботажу та сформувати перелік правил для користувачів і адміністраторів системи виявлення порушень задля для ефективного розпізнання комп'ютерного саботажу. А також було практично реалізовано запропонований метод інтеграції системи виявлення порушень із системою відеоспостереження з використанням детектору саботажу.

В третій частині кваліфікаційної роботи було обґрунтовано витрати на розробку, впровадження і експлуатації запропонованого методу. Отримані результати капітальних та експлуатаційних витрат, величини можливого збитку від реалізованої атаки через упущену вигоду та терміну окупності капітальних інвестицій показали, що витрати є економічно доцільними та ефективними.

ПЕРЕЛІК ПОСИЛАНЬ

1. M-Trends 2016 by Travis Reese [Електронний ресурс]. – Режим доступу: https://www.fireeye.com/blog/executive-perspective/2016/02/m-trends_2016.html

2. Підсумки 2018 року [Електронний ресурс]. – Режим доступу: https://cyberpolice.gov.ua/results/2018/

3. 2019: Cost of Data Breach Report [Електронний ресурс]. – Режим доступу: https://bit.ly/2DCughQ

4. Кримінальний Кодекс України від 14.11.2020 [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/2341-14#Text

5. Кримінальний Кодекс Естонії [Електронний ресурс]. – Режим доступу: https://www.legislationline.org/download/id/6462/file/Estonia_CC_as_of_2002_ru.pdf

6. Міжнародні проблеми класифікації кіберзлочинів [Електронний ресурс]. – Режим доступу: http://www.jurnaluljuridic.in.ua/archive/2017/4/43.pdf

7. Закон України «Про основні засади забезпечення кібербезпеки України» від 21.06.2018 № 2163-VIII // Відомості Верховної Ради України. – 2017. – № 45. [Електронний ресурс]. – Режим доступу http://zakon5.rada.gov.ua/laws/show/2163-19

8. Постанова Кабінету Міністрів України від 19.06.2019 №518. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

9. Закон України «Про інформацію» від 02.10.1992 №2657-XII // Відомості Верховної Ради України. – 1992. – № 48. [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/laws/show/2657-12

10. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT)

11. Breach Detection System (BDS) – Overview [Електронний ресурс]. – Режим доступу: https://www.nsslabs.com/tested-technologies/breach-detection-system/

12. НД ТЗІ 2.5.005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від

несанкціонованого доступу. – [Чинний від 1999.04.28]. – К. : ДСТСЗІ СБУ, 1999. – № 22. – (Нормативний документ системи технічного захисту інформації).

13. НД ТЗІ 2.5.004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – [Чинний від 1999.04.28]. – К. : ДСТСЗІ СБУ, 1999. – № 22. – (Нормативний документ системи технічного захисту інформації).

14. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – [Чинний від 1999.04.28]. – К. : ДСТСЗІ СБУ, 1999. – № 22. – (Нормативний документ системи технічного захисту інформації).

15. ESET Enterprise Inspector [Електронний ресурс]. – Режим доступу: https://help.eset.com/esmc_admin/70/ru-RU/enterprise_inspector.html

16. Cisco AMP for Endpoints [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/dam/assets/global/RU/pdfs/brochures/C45-731874-00-AMP-endpoint-AAG-v1a.pdf

17. About Symantec ATP [Електронний ресурс]. – Режим доступу: https://help.symantec.com/cs/ATP_3.0.5/ATP/v96380626_v125316101/About-Symantec-Advanced-Threat-Protection-(ATP)?locale=EN_US

18. Microsoft Defender ATP [Електронний ресурс]. – Режим доступу: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-advanced-threat-protection

19. Endpoint Security [Електронний ресурс]. – Режим доступу: https://www.fireeye.com/products/endpoint-security.html

20. Cyberbit EDR [Електронний ресурс]. – Режим доступу: https://ru.cyberbit.com/solutions/endpoint-detection-response/

21. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн. І.В. Шереметьєва, Д.П. Пілова, Н.М. Романюк - Дніпро: Національний технічний університет "Дніпровська політехніка", 2017. - 17 с.

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ ДИПЛОМНОЇ РОБОТИ

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	3	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	13	
6	А4	Спеціальна частина	29	
7	А4	Економічна частина	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. ПЕРЕЛІК МАТЕРІАЛІВ НА ОПТИЧНОМУ НОСІЇ

Кабанов А.О. 125м-19-2.docx

Кабанов А.О. 125м-19-2.pptx

ДОДАТОК В. ВІДГУК КЕРІВНИКІВ РОЗДІЛІВ

Відгук керівника економічного розділу:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

ВІДГУК

на кваліфікаційну роботу студента групи 125м-19-2 Кабанова А.О.

на тему: «Метод реалізації системи виявлення порушень для розпізнання фактів комп'ютерного саботажу»

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 70 сторінках та містить 9 рисунків, 14 таблиць, 21 джерела та 4 додатки.

Актуальність теми полягає в необхідності розробки методу своєчасного виявлення порушень, які можуть призвести до комп'ютерного саботажу в корпоративній ІТС.

Зміст та структура кваліфікаційної роботи дозволяють розкрити поставлену тему в повному обсязі.

Студент показав достатній рівень обізнаності в цьому питанні, проаналізувавши проблематику, вивчивши нормативно-правову базу, дослідивши існуючі програмні рішення і винайшовши новий метод розпізнання комп'ютерного саботажу, використовуючи систему виявлення порушень та систему відеоспостереження. Крім того, студент показав власну точку зору щодо поставлених питань в роботі, обґрунтовано надаючи відповіді та низку питань.

Практична значущість полягає в можливому використанні запропонованого методу реалізації системи виявлення порушень для розпізнання фактів комп'ютерного саботажу в існуючій корпоративній ІТС.

В якості недоліків слід відзначити наступне: нечіткість окремих висновків, окремі невідповідності вимогам при оформленні.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату».

Кваліфікаційна робота відповідає усім вимогам щодо підготовки робіт магістрів та заслуговує оцінки «відмінно», а її автор Кабанов А.О. – присвоєння кваліфікації магістра за спеціальністю 125 Кібербезпека.

Керівник кваліфікаційної роботи,
кандидат технічних наук, доцент О.О. Сафаров

Керівник спеціальної частини,
асистент Ю.В. Ковальова